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

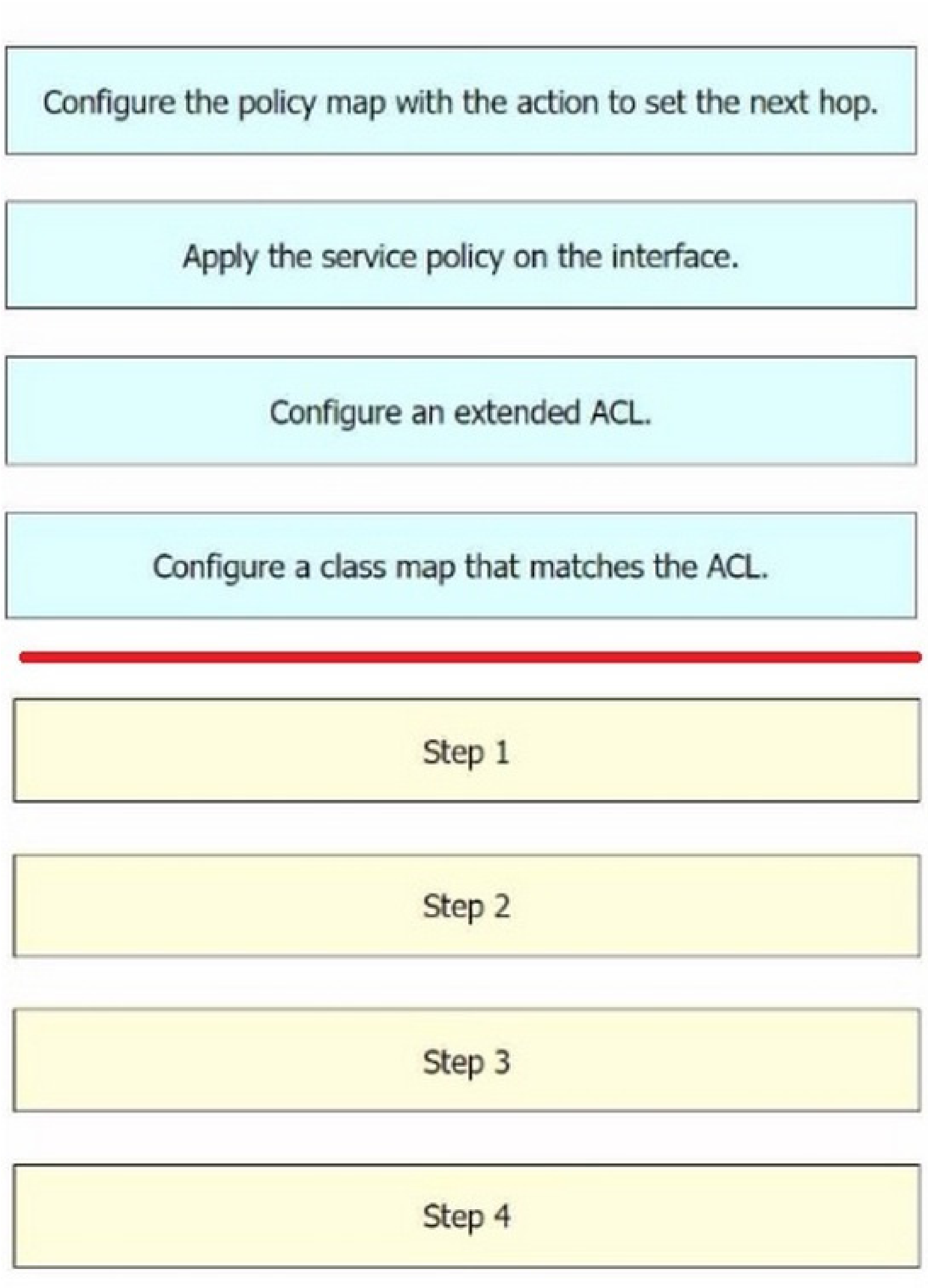
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

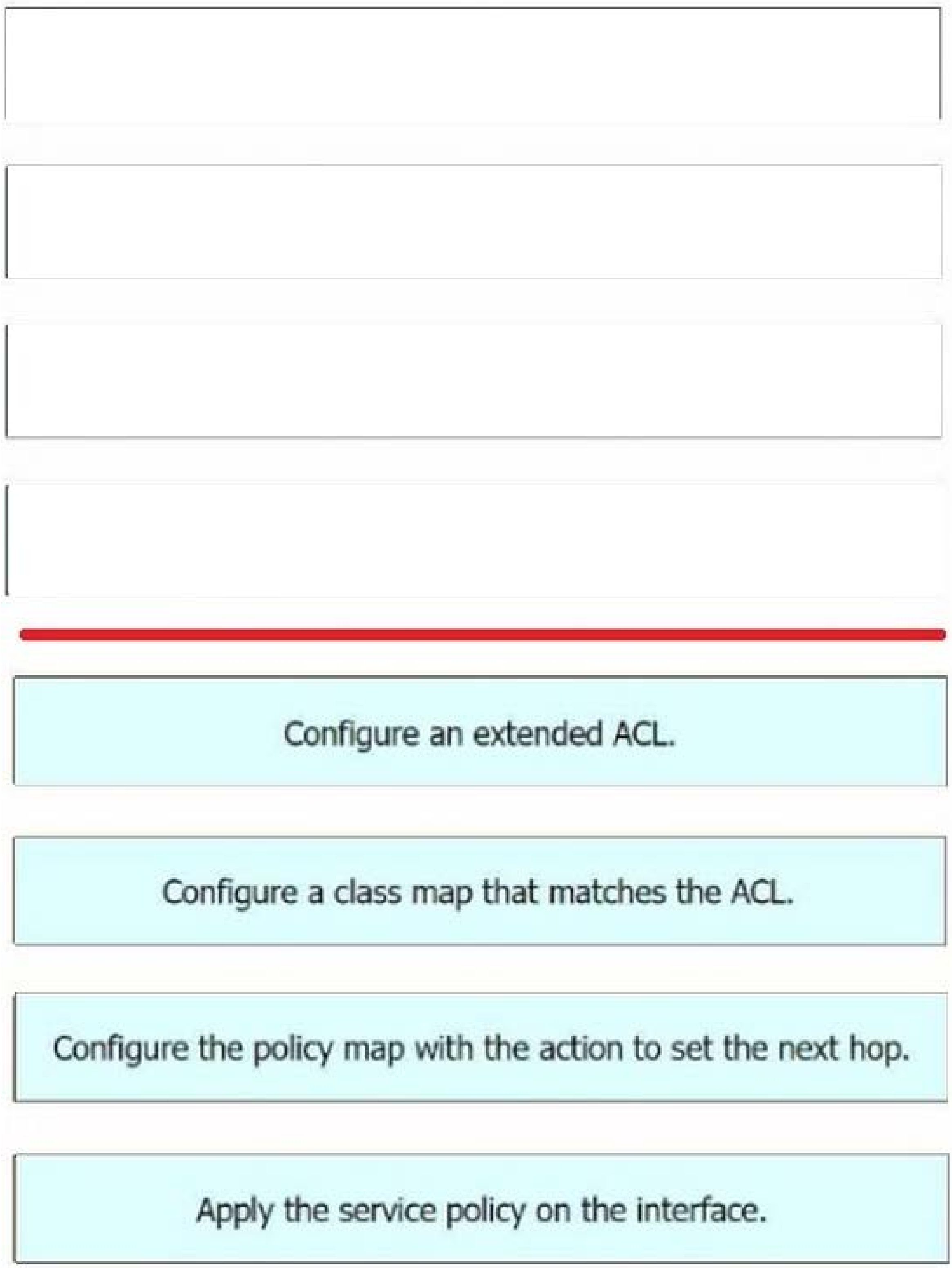
DRAG DROP

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

An engineer must enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device. What should be configured after the global address-family ipv4 is configured?

A. Set the VRF-specific route advertisements.

B. Enable bgp advertisement.

C. Enter sdwan mode.

D. Disable bgp advertisement.

Correct Answer: B

To enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device, the engineer must first configure the global address-family ipv4 and then enable bgp advertisement under the vrf definition.

This will allow the device to advertise the BGP routes learned from the cloud provider to the OMP control plane, which will then distribute them to the other SD-WAN devices in the overlay network.

References:

Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:Implementing Cloud Connectivity, Lesson 3: Configuring IPsec VPN from Cisco IOS XE to AWS, Topic: Configuring BGP on the Cisco IOS XE Device, Page 3-24.

QUESTION 3

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

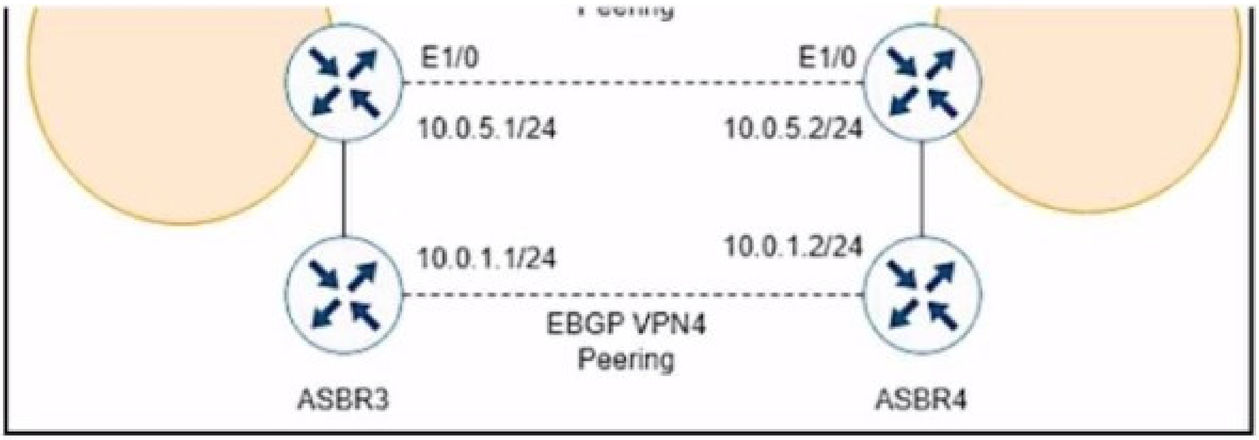
to establish private connectivity to Google Cloud Virtual Private Cloud (VPC) networks.

References:

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

QUESTION 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

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

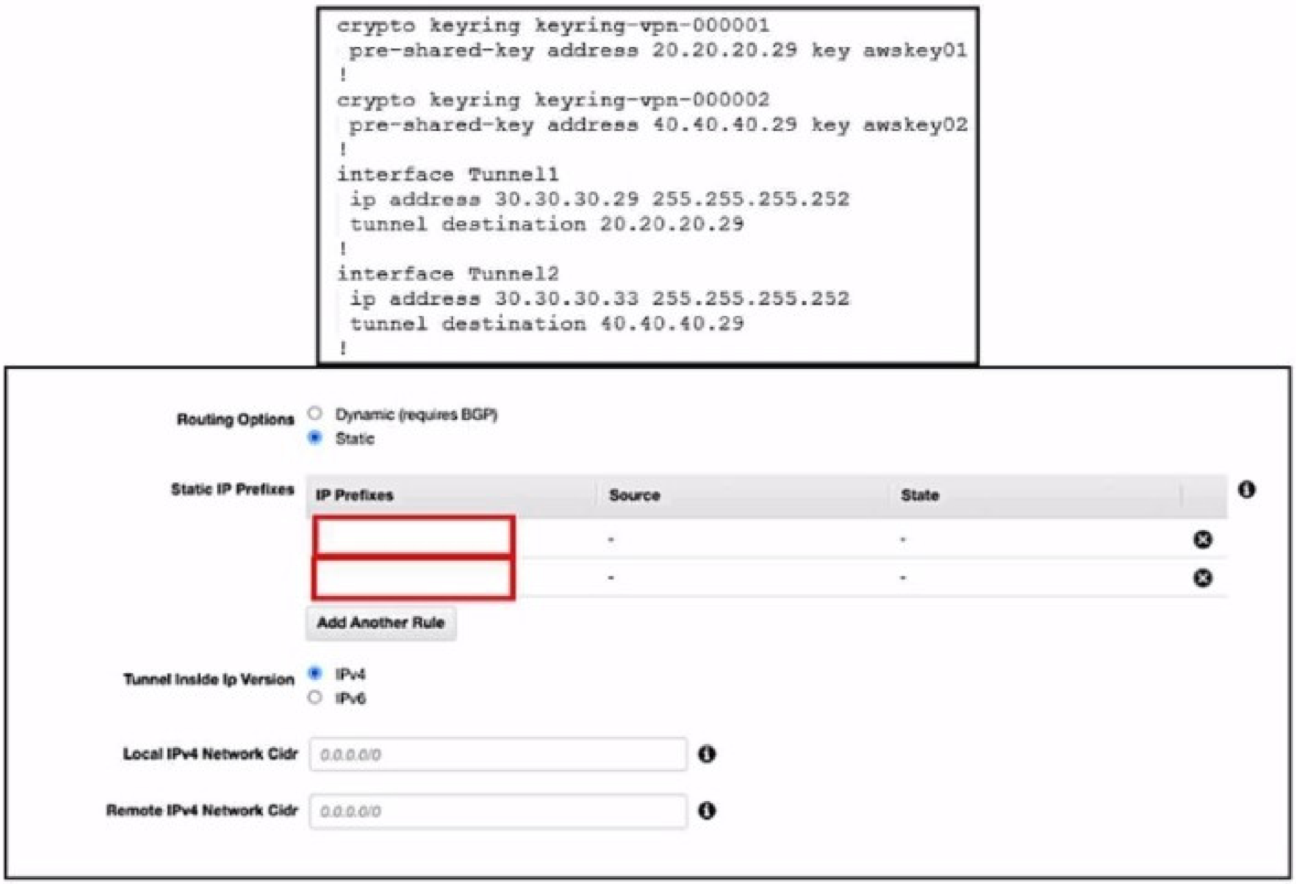
Correct Answer: C

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

Refer to the exhibits.



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

A. 30.30.30.0/30

B. 20.20.20.0/24

C. 30.30.30.0/24

D. 50.50.50.0/30

E. 40.40.40.0/24

Correct Answer: AE

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

QUESTION 7

Which architecture model establishes internet-based connectivity between on-premises networks and AWS cloud resources?

A. That establishes an iPsec VPN tunnel with Internet Key Exchange (IKE) for secure key negotiation and encrypted data transmission

B. That relies on AWS Elastic Load Balancing (ELB) for traffic distribution and uses SSL/TLS encryption for secure data transmission.

C. That employs AWS Direct Connect for a dedicated network connection and uses private IP addresses tor secure communication.

D. That uses Amazon CloudFrontfor caching and distributing content globally and uses HTTPS for secure data transfer.

Correct Answer: A

The architecture model that establishes internet-based connectivity between on-premises networks and AWS cloud resources is the one that establishes an iPsec VPN tunnel with Internet Key Exchange (IKE) for secure key negotiation and encrypted data transmission. This model is also known as the VPN CloudHub model. It allows multiple remote sites to connect to the same virtual private gateway in AWS, creating a hub-and- spoke topology. The VPN CloudHub model provides the following benefits: It enables secure communication between remote sites and AWS over the public internet, using encryption and authentication protocols such as IPsec and IKE. It supports dynamic routing protocols such as BGP, which can automatically adjust the routing tables based on the availability and performance of the VPN tunnels. It allows for redundancy and load balancing across multiple VPN tunnels, increasing the reliability and throughput of the connectivity. It simplifies the management and configuration of the VPN connections, as each remote site only needs to establish one VPN tunnel to the virtual private gateway in AWS, rather than multiple tunnels to different VPCs or regions. The other options are not correct because they do not establish internet-based connectivity between on-premises networks and AWS cloud resources. Option B relies on AWS Elastic Load Balancing (ELB) for traffic distribution and uses SSL/TLS encryption for secure data transmission. However, ELB is a service that distributes incoming traffic across multiple targets within a VPC, not across different networks. Option C employs AWS Direct Connect for a dedicated network connection and uses private IP addresses for secure communication. However, AWS Direct Connect is a service that establishes a private connection between on-premises networks and AWS, bypassing the public internet. Option D uses Amazon CloudFront for caching and distributing content globally and uses HTTPS for secure data transfer. However, Amazon CloudFront is a service that delivers static and dynamic web content to end users, not to on-premises networks.

References:

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

2: Cisco ASA Site-to-Site VPN

3: What Is Elastic Load Balancing?

4: What is AWS Direct Connect?

QUESTION 8

Which Microsoft Azure service enables a dedicated and secure connection between an on- premises infrastructure and Azure data centers through a colocation provider?

A. Azure Private Link

B. Azure ExpressRoute

C. Azure Virtual Network

D. Azure Site-to-Site VPN

Correct Answer: B

Azure ExpressRoute is a service that enables a dedicated and secure connection between an on-premises infrastructure and Azure data centers through a colocation provider. A colocation provider is a third-party data center that offers network connectivity services to multiple customers. Azure ExpressRoute allows customers to bypass the public internet and connect directly to Azure services, such as virtual machines, storage, databases, and more. This provides benefits such as lower latency, higher bandwidth, more reliability, and enhanced security. Azure ExpressRoute also supports hybrid scenarios, such as connecting to Office 365, Dynamics 365, and other SaaS applications hosted on Azure. Azure ExpressRoute requires a physical connection between the customer\\'s network and the colocation provider\\'s network, as well as a logical connection between the customer\\'s network and the Azure virtual network. The logical connection is established using a Border Gateway Protocol (BGP) session, which exchanges routing information between the two networks. Azure ExpressRoute supports two models: standard and premium. The standard model offers connectivity to all Azure regionswithin the same geopolitical region, while the premium model offers connectivity to all Azure regions globally, as well as additional features such as increased route limits, global reach, and Microsoft peering.

References: Designing and Implementing Cloud Connectivity (ENCC) v1.0, Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300-440) Exam Prep, ENCC | Designing and Implementing Cloud Connectivity | Netec

---

QUESTION 9

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 10

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 11

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 12

A company has multiple branch offices across different geographic locations and a centralized data center. The company plans to migrate Its critical business applications to the public cloud infrastructure that is hosted in Microsoft Azure. The company requires high availability, redundancy, and low latency for its business applications. Which connectivity model meets these requirements?

A. ExpressRoute with private peering using SDCI

B. hybrid connectivity with SD-WAN

C. AWS Direct Connect with dedicated connections

D. site-to-site VPN with Azure VPN gateway

Correct Answer: A

The connectivity model that meets the requirements of high availability, redundancy, and low latency for the company\\'s business applications is ExpressRoute with private peering using SDCI.

ExpressRoute is a service that provides a dedicated, private, and high-bandwidth connection between the customer\\'s on-premises network and Microsoft Azure cloud network.

Private peering is a type of ExpressRoute circuit that allows the customer to access Azure services that are hosted in a virtual network, such as virtual machines, storage, and databases.

SDCI (Secure Data Center Interconnect) is a Cisco solution that enables secure and scalable connectivity between multiple data centers and cloud providers, using technologies such as MPLS, IPsec, and SD-WAN3.

By using ExpressRoute with private peering and SDCI, the company can achieve the following benefits:

References:

What is Azure ExpressRoute?

Azure ExpressRoute peering

Cisco Secure Data Center Interconnect

ExpressRoute circuit and routing domain

QUESTION 13

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

A. VPC peering and bucket policies

B. specific routing and bucket policies

C. EC2 super policies and specific routing policies

D. gateway load balancers and specific routing policies

Correct Answer: B

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

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

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

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

References:

1: AWS PrivateLink

2: AWS PrivateLink FAQs

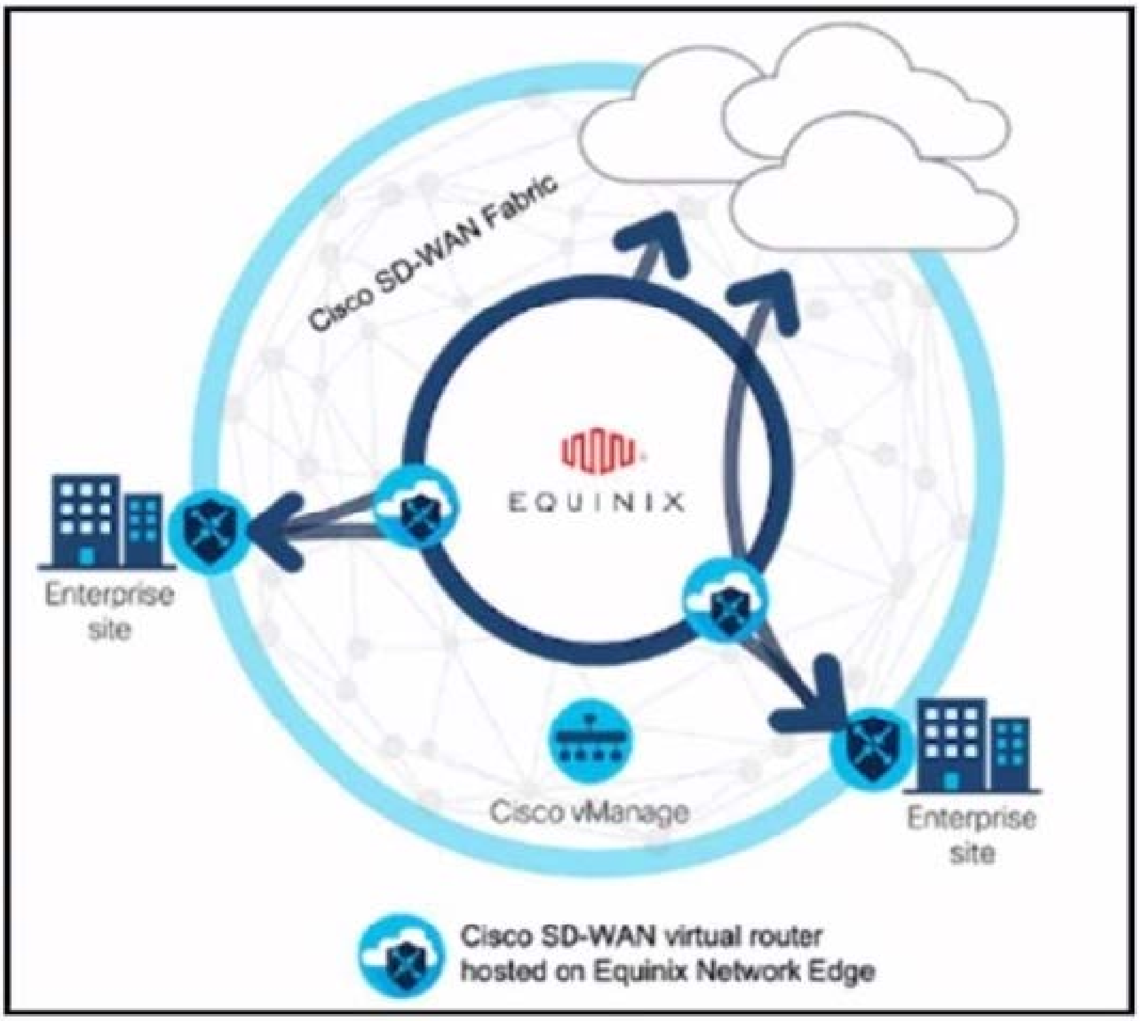
3: Using Bucket Policies and User Policies

4: Bucket Policy Examples

QUESTION 14

DRAG DROP

Refer to the exhibit.



These configurations are complete:

1.

Create an account in the Equinix portal.

2.

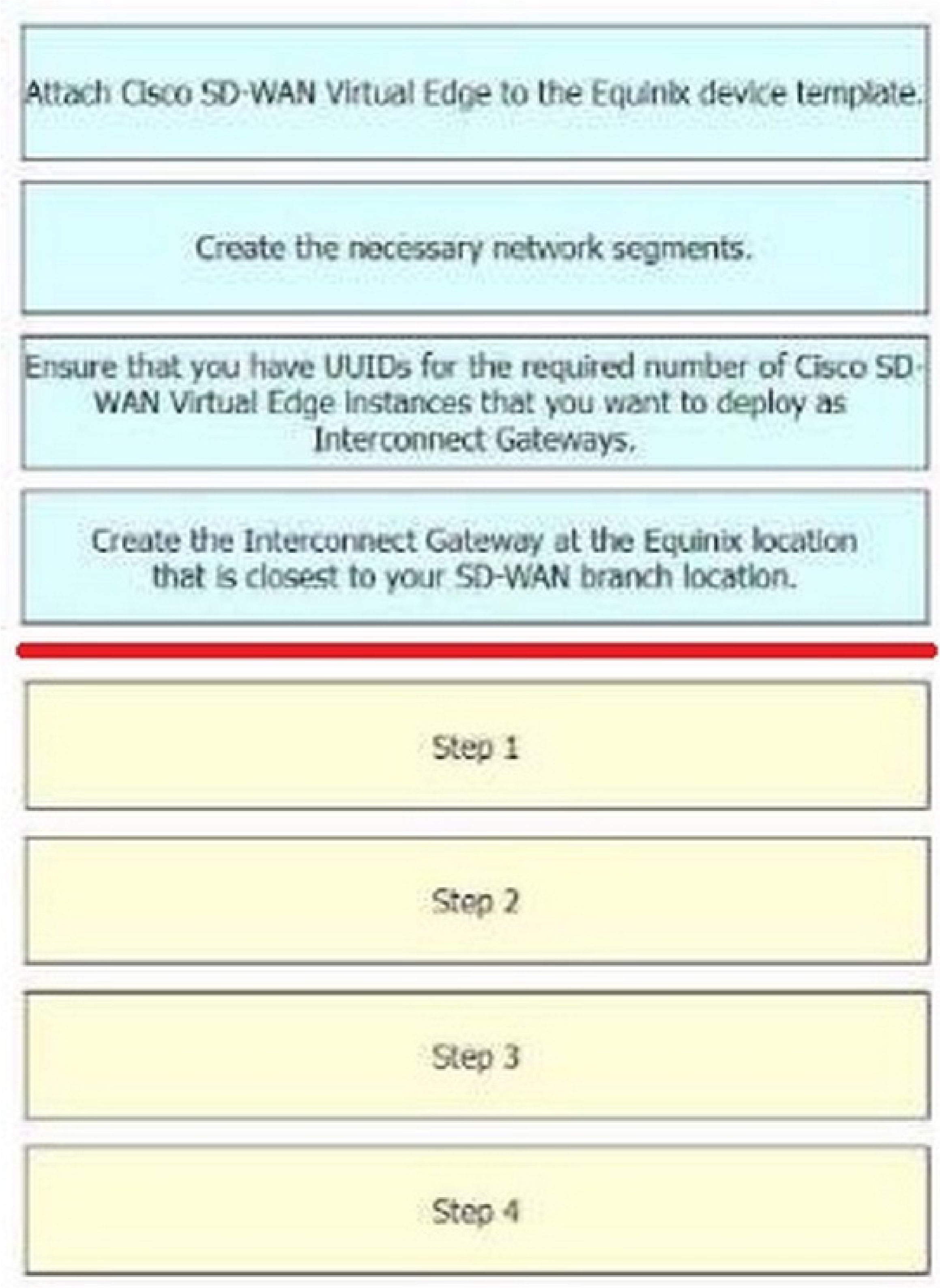
Associate the Equinix account with Cisco vManage.

3.

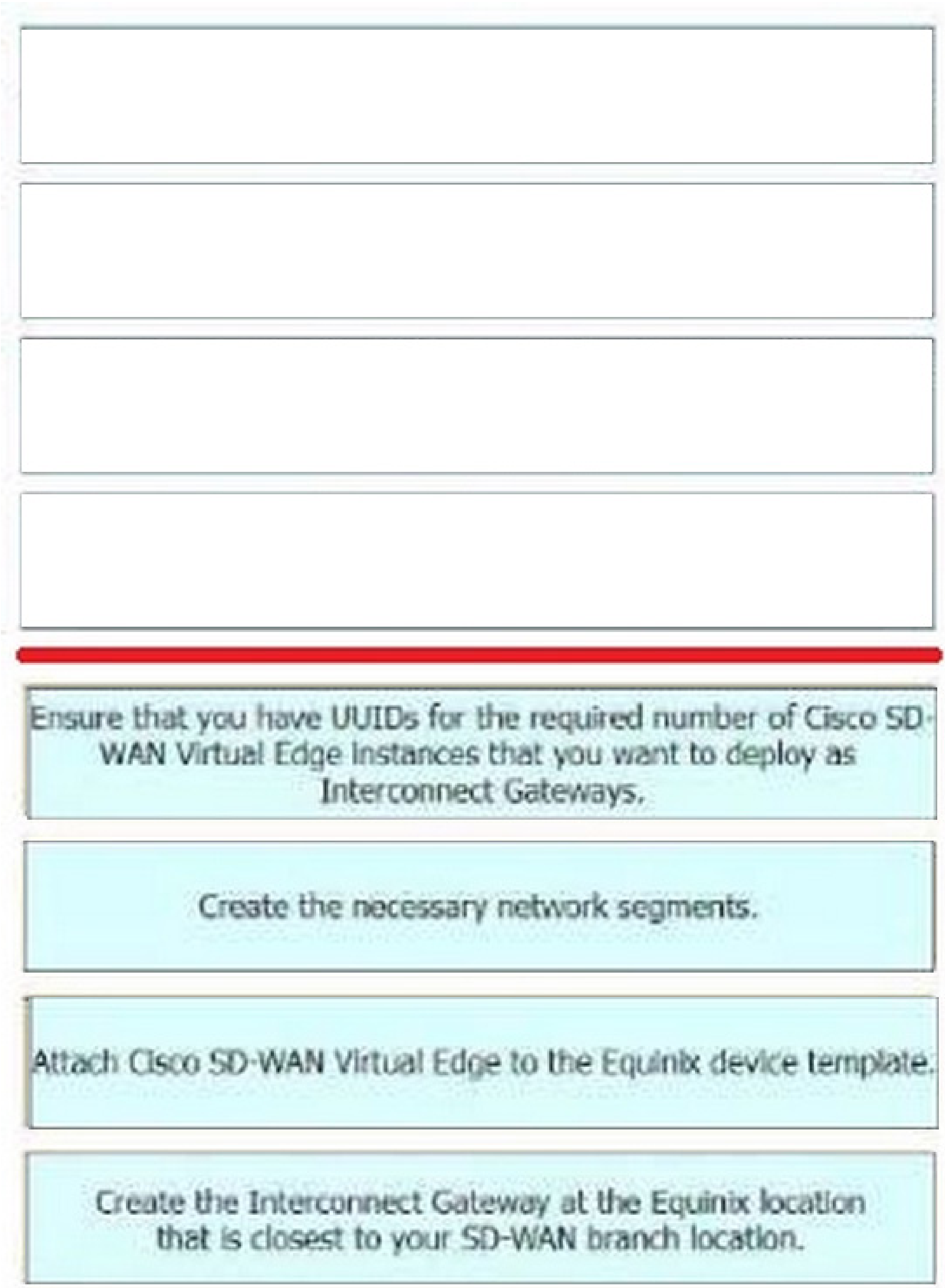
Configure the global settings for Interconnect Gateways.

Drag the prerequisite steps from the left onto the order on the right to configure a Cisco SD-WAN Cloud Interconnect with Equinix

Select and Place:



Correct Answer:



The process of configuring a Cisco SD-WAN Cloud Interconnect with Equinix involves several steps.

Ensure that you have UUIDs for the required number of Cisco SD WAN Virtual Edge instances that you want to deploy as Interconnect Gateways: This is the first step where you ensure that you have the necessary UUIDs for the Cisco SDWAN Virtual Edge instances that you want to deploy.

Create the necessary network segments: After ensuring the availability of UUIDs, you create the necessary network segments.

Attach Cisco SD-WAN Virtual Edge to the Equinix device template: After setting up the network segments, you attach the Cisco SD-WAN Virtual Edge to the Equinix device template.

Create the Interconnect Gateway at the Equinix location that is closest to your SD- WAN branch location: Finally, you create the Interconnect Gateway at the Equinix location that is closest to your SD-WAN branch location.

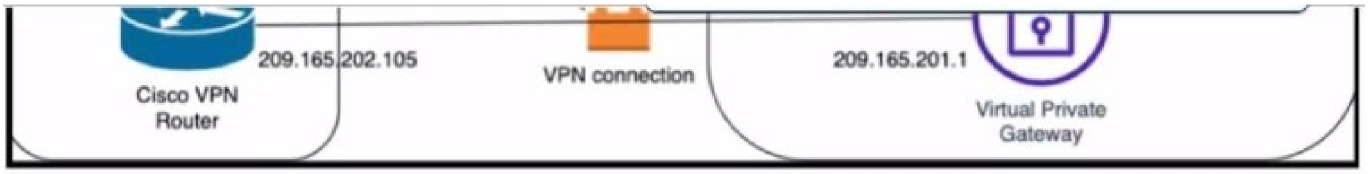
References:

[Cisco SD-WAN Cloud Interconnect with Equinix]

[Cisco SD-WAN Cloud OnRamp for CoLocation Deployment Guide]

QUESTION 15

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 PROFILE-PoC
  match address local 209.165.201.1
  match identity remote address 209.165.202.105 255.255.255.255
  authentication remote 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