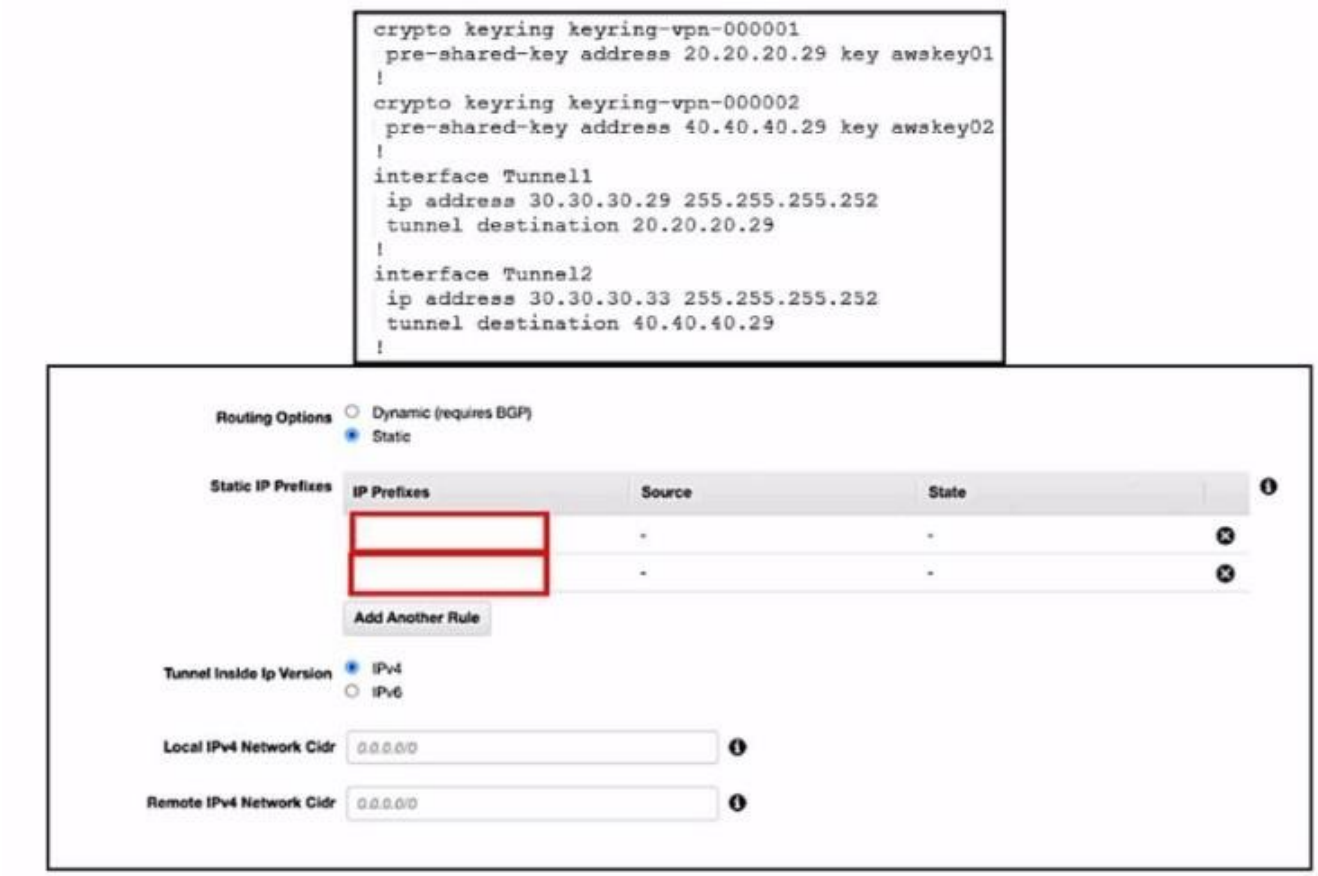
Question 1:
Refer to the exhibits.



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 2:
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)

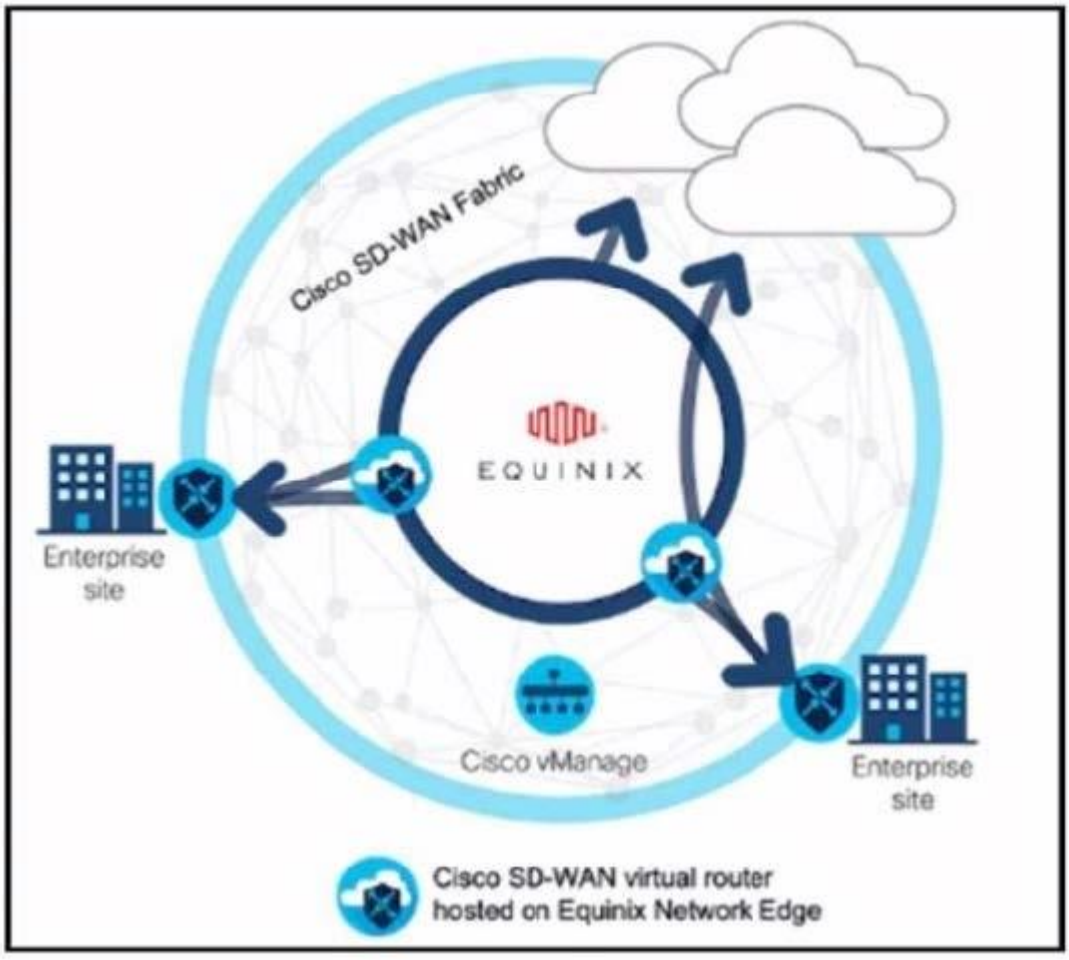
2: Cisco ASA Site-to-Site VPN

3: What Is Elastic Load Balancing?

4: What is AWS Direct Connect?

Question 3:
DRAG DROP

Refer to the exhibit.



These configurations are complete:

1.

Create an account in the Equinix portal.

2.

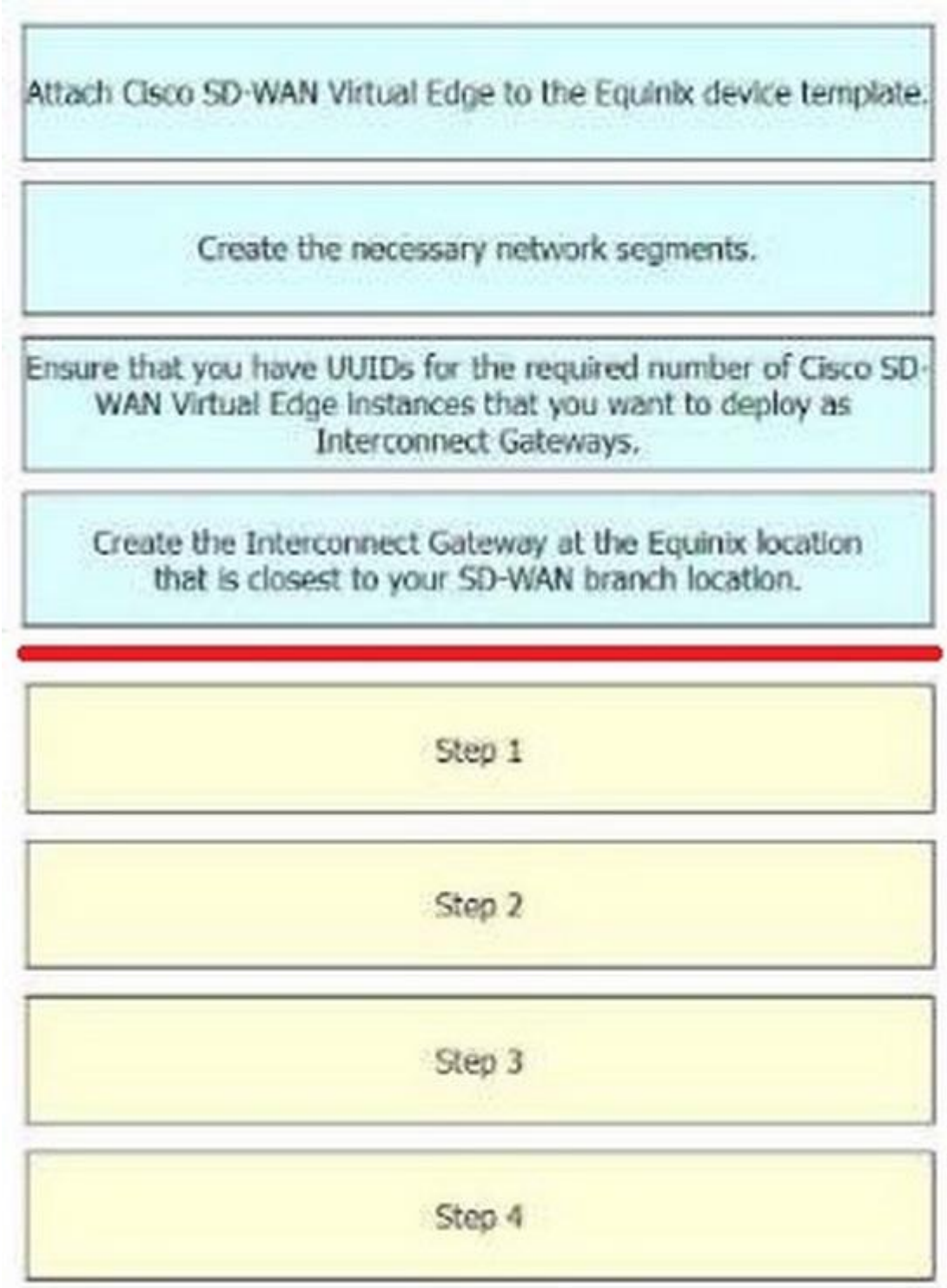
Associate the Equinix account with Cisco vManage.

3.

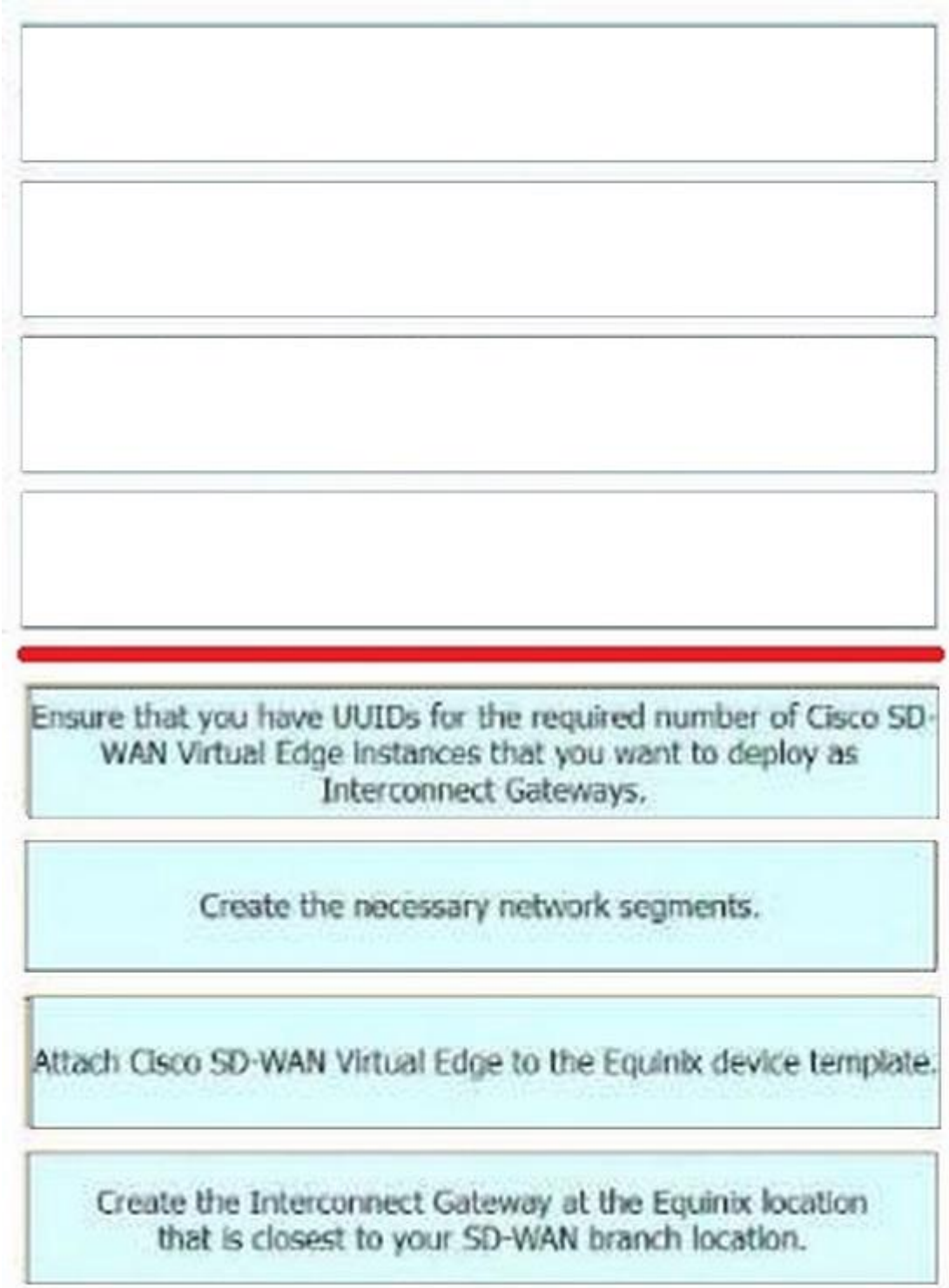
Configure the global settings for Interconnect Gateways.

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:

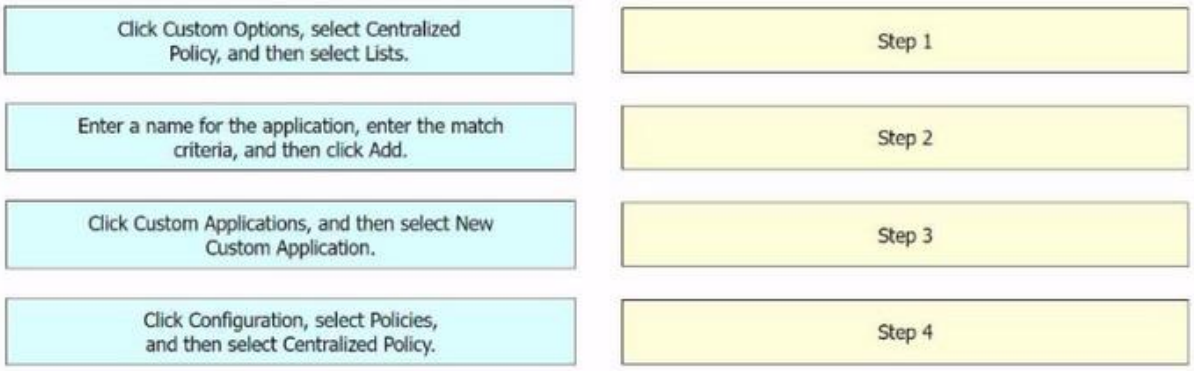
[Cisco SD-WAN Cloud Interconnect with Equinix]

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

Question 4:
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 5:
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.

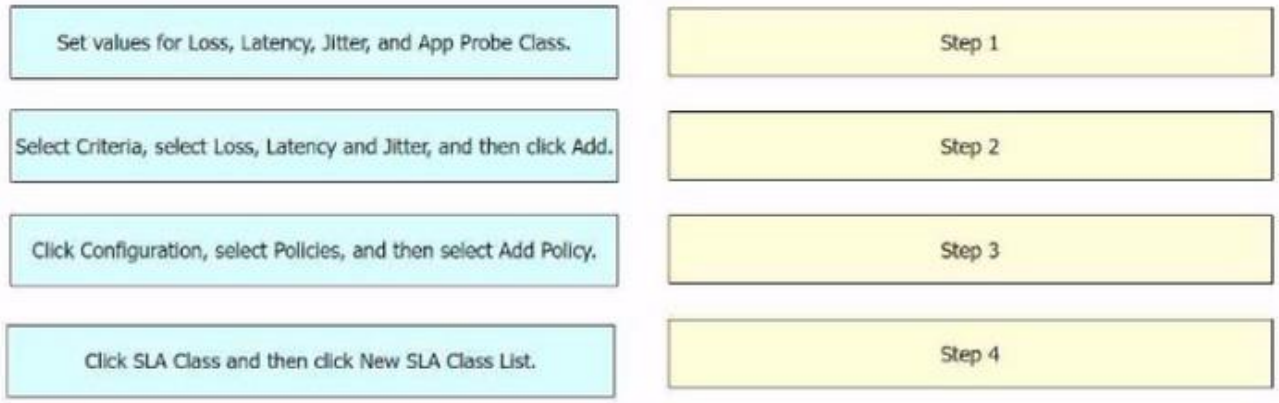
References:

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 6:
DRAG DROP

An engineer must use Cisco vManage to configure an SLA class to specify the maximum packet loss, packet latency, and jitter allowed on a connection. 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 an SLA class to specify the maximum packet loss, packet latency, and jitter allowed on a connection using Cisco vManage involves several steps. Click Configuration, select Policies, and then select Add Policy:

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

Click SLA Class and then click New SLA Class List: In this step, you create a new SLA Class List.

Select Criteria, select Loss, Latency and Jitter, and then click Add: After setting up the SLA Class List, you select the criteria for the SLA class. In this case, the criteria are Loss, Latency, and Jitter.

Set values for Loss, Latency, Jitter, and App Probe Class: Finally, you set the values for Loss, Latency, Jitter, and App Probe Class.

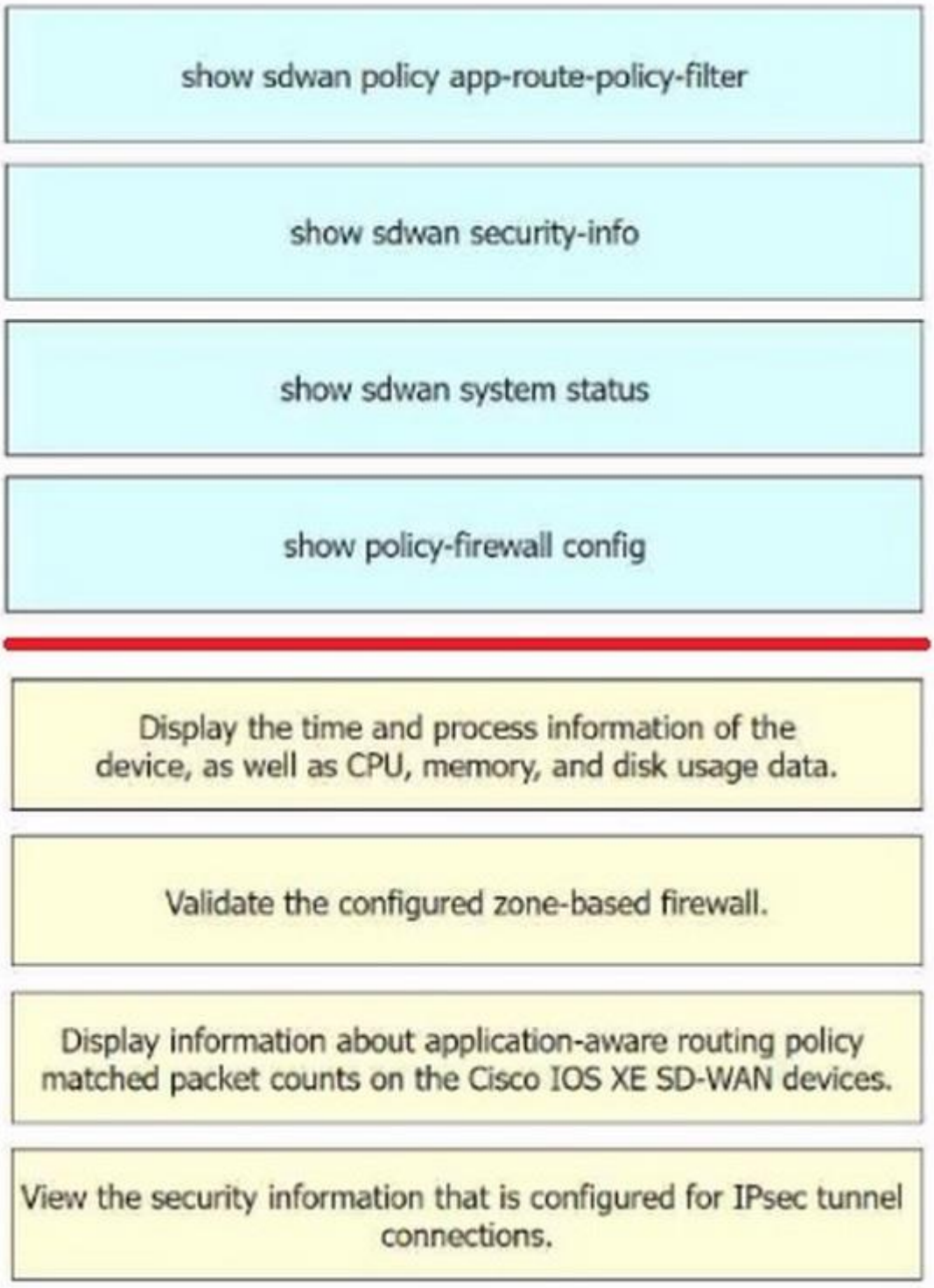
References:

Information About Application-Aware Routing - Cisco Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Release

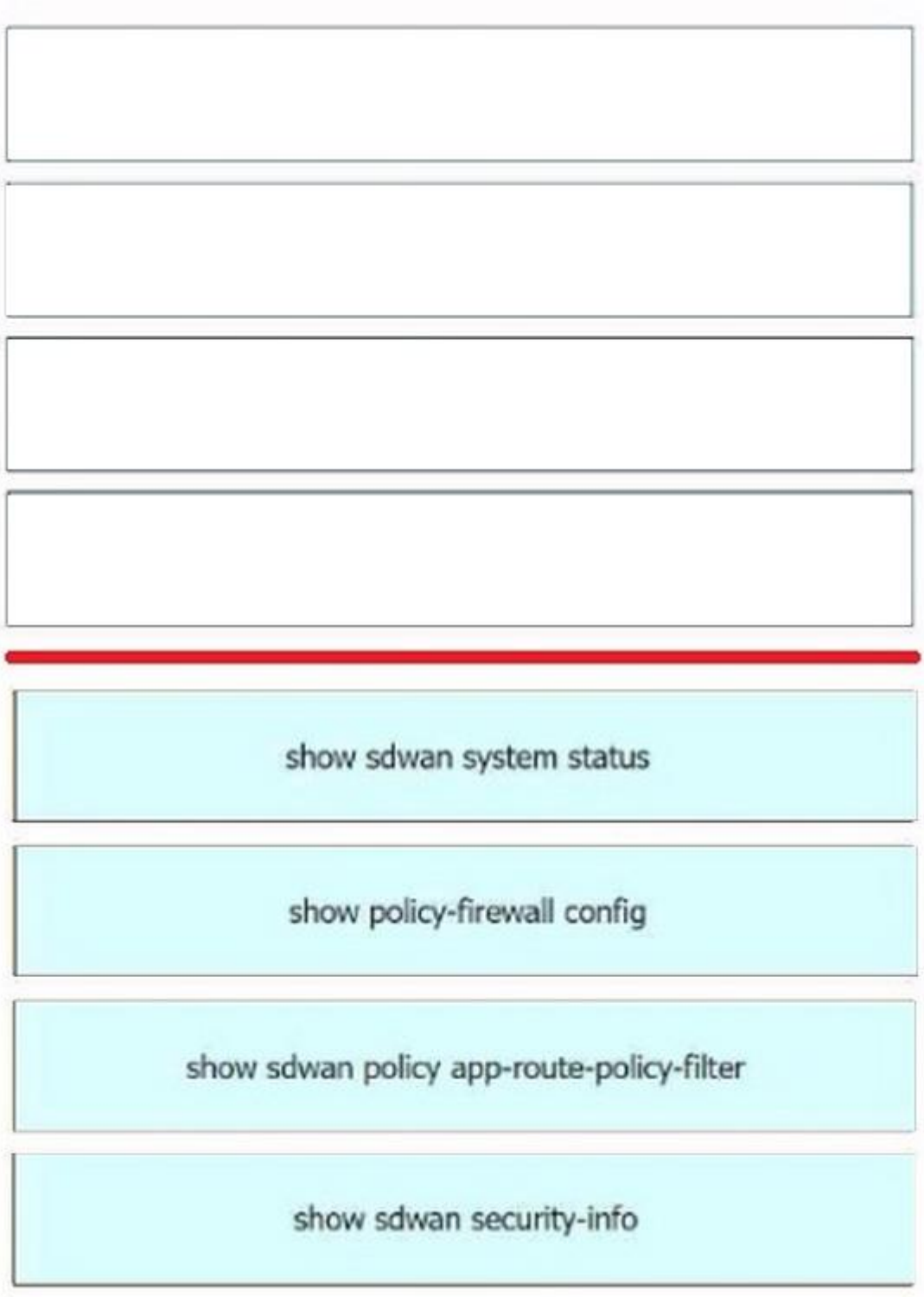
Question 7:
DRAG DROP

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:



Correct Answer:



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 8:
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

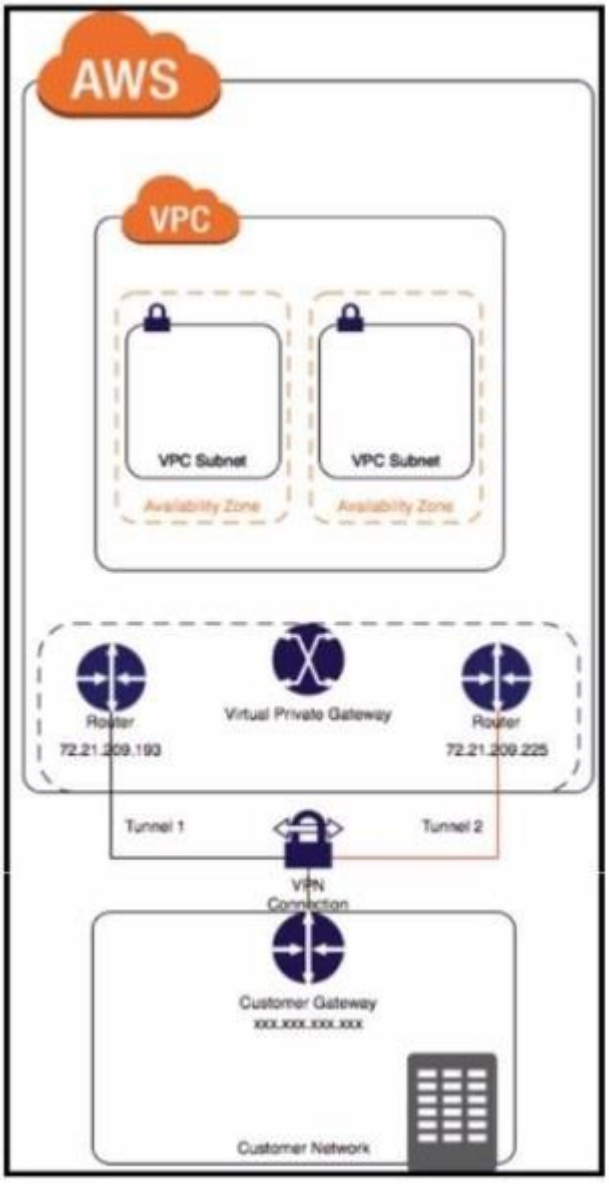
Security groups are a feature in AWS that allow you to control the inbound and outbound traffic to your instances. They act as a virtual firewall that can filter the traffic based on the source, destination, protocol, and port. You can assign one or more security groups to your instances, and each security 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

---

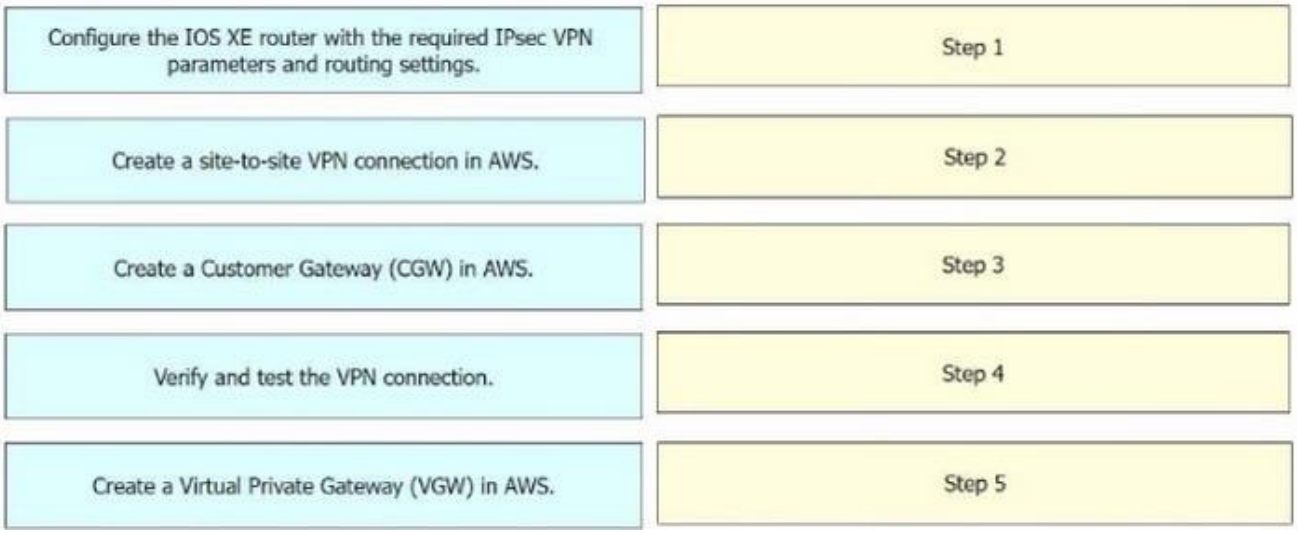
Question 9:
DRAG DROP

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

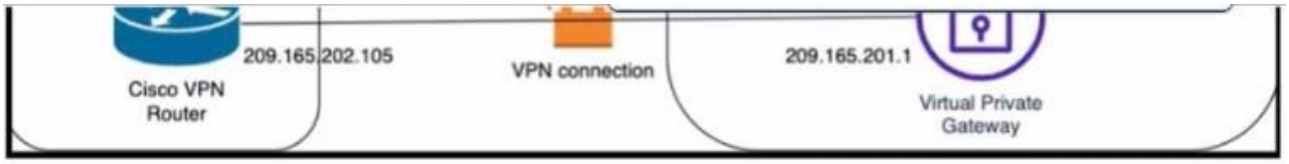
and test the VPN connection: Finally, you verify and test the VPN connection to ensure that it is working correctly.

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 10:
Refer to the exhibit.



Which Cisco lKEv2 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:

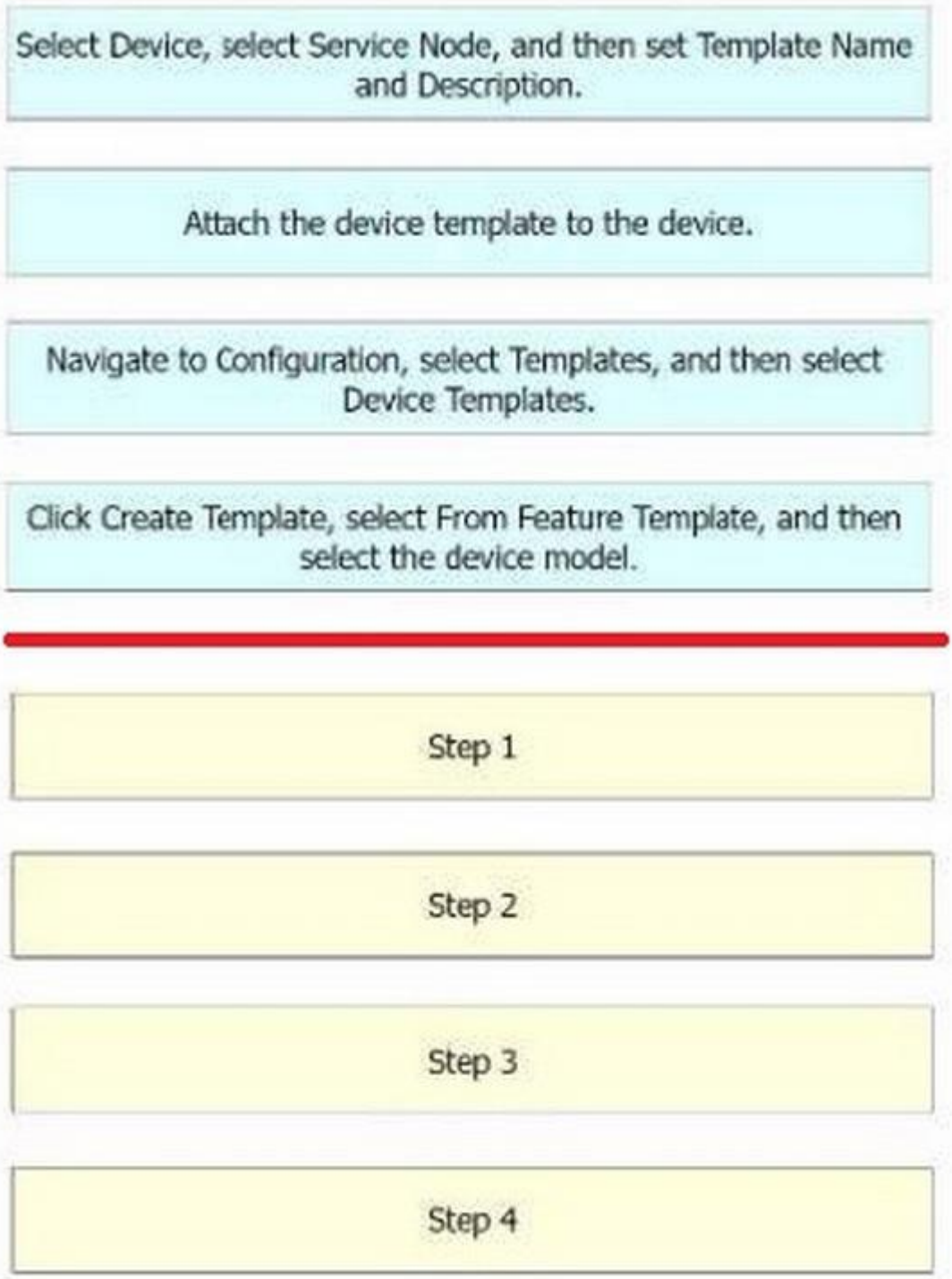
1: AWS VPN Configuration Guide for Cisco IOS-XE

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

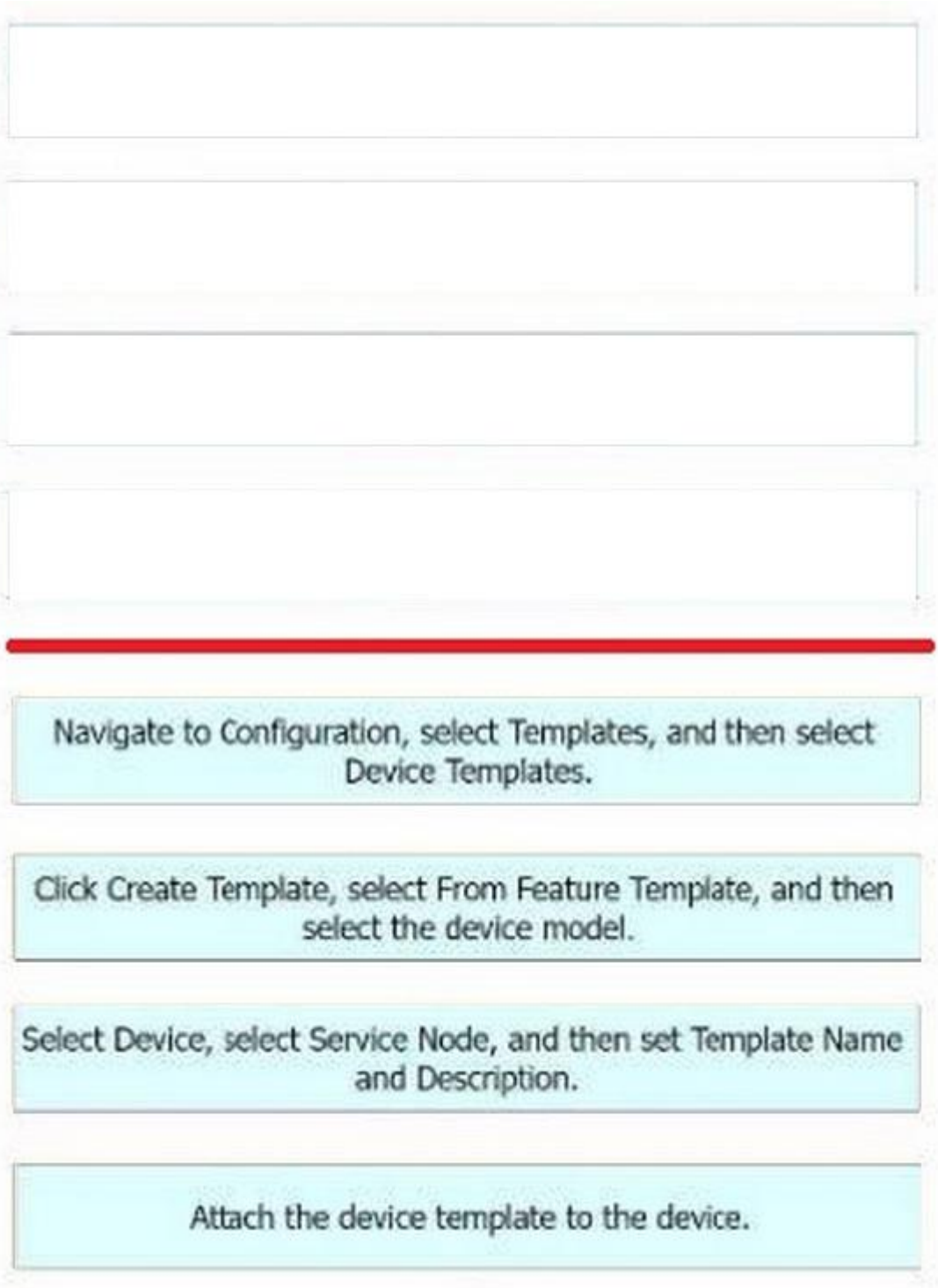
Question 11:
DRAG DROP

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:



Correct Answer:



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 12:
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 13:
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,

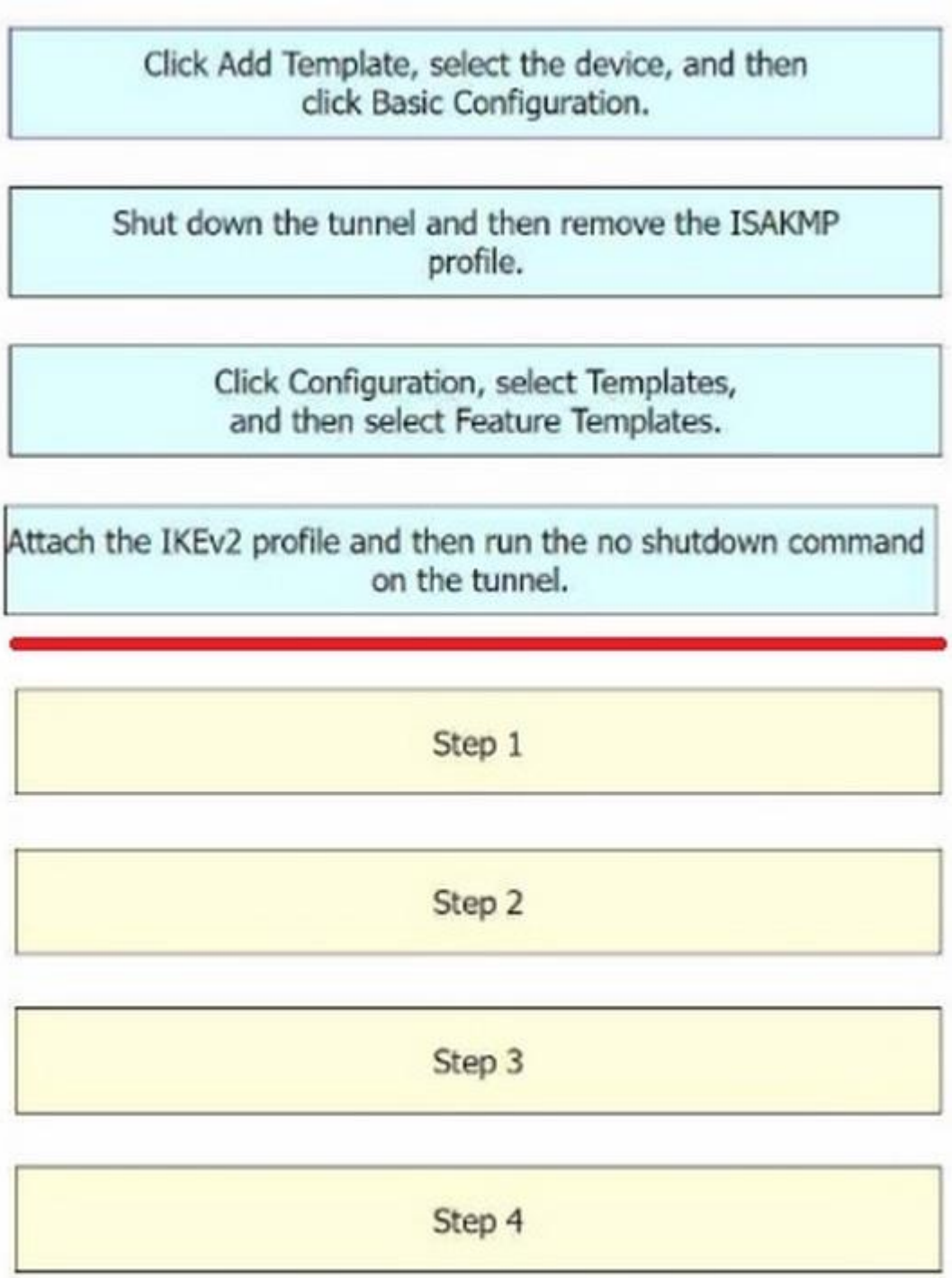
while the premium model offers connectivity to all Azure regions globally, as well as additional features such as increased route limits, global reach, and Microsoft peering.

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

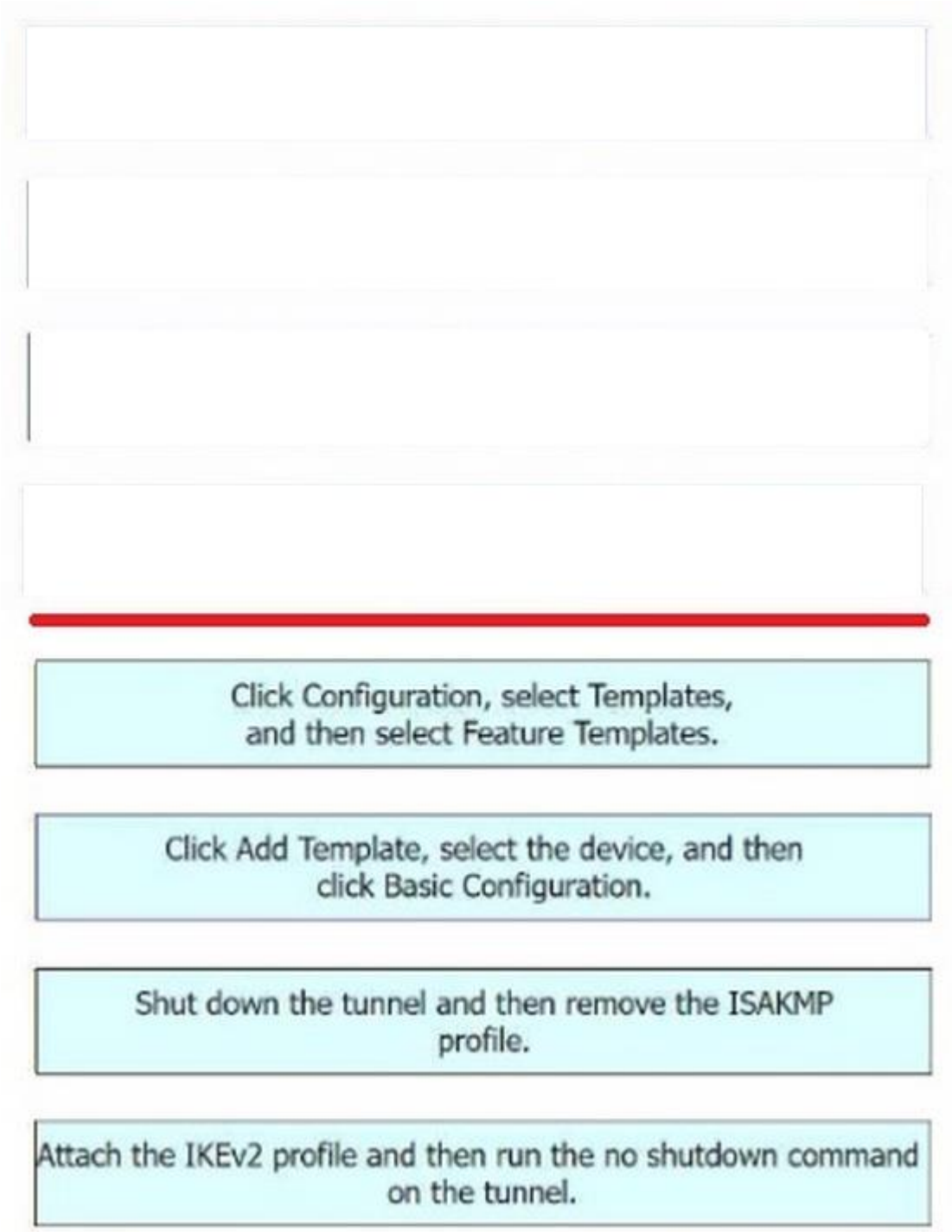
Question 14:
DRAG DROP

An engineer must configure a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router In Controller mode and AWS. The IKE version must be changed from IKEv1to IKEv2 in Cisco vManage. Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:



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

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

Step 3 = Shut down the tunnel and then remove the ISAKMP profile.

Step 4 = Attach the IKEv2 profile and then run the no shutdown command on the tunnel.

The process of configuring a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router in Controller mode and AWS, and changing the IKE version from IKEv1 to IKEv2 in Cisco vManage involves several steps123. 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 vManage1.

Click Add Template, select the device, and then click Basic Configuration: In this step, you add a new template for the device and proceed with the basic configuration.

Shut down the tunnel and then remove the ISAKMP profile: Before changing the IKE version, you need to shut down the existing tunnel and remove the ISAKMP profile that is configured for IKEv12.

Attach the IKEv2 profile and then run the no shutdown command on the tunnel:

Finally, you attach the newly created IKEv2 profile to the tunnel and bring the tunnel back up.

References:

Configuring Internet Key Exchange Version 2 (IKEv2) - Cisco Switch from IKEv1 to IKEv2 on Cisco Routers - Cisco Community Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

---

Question 15:
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.

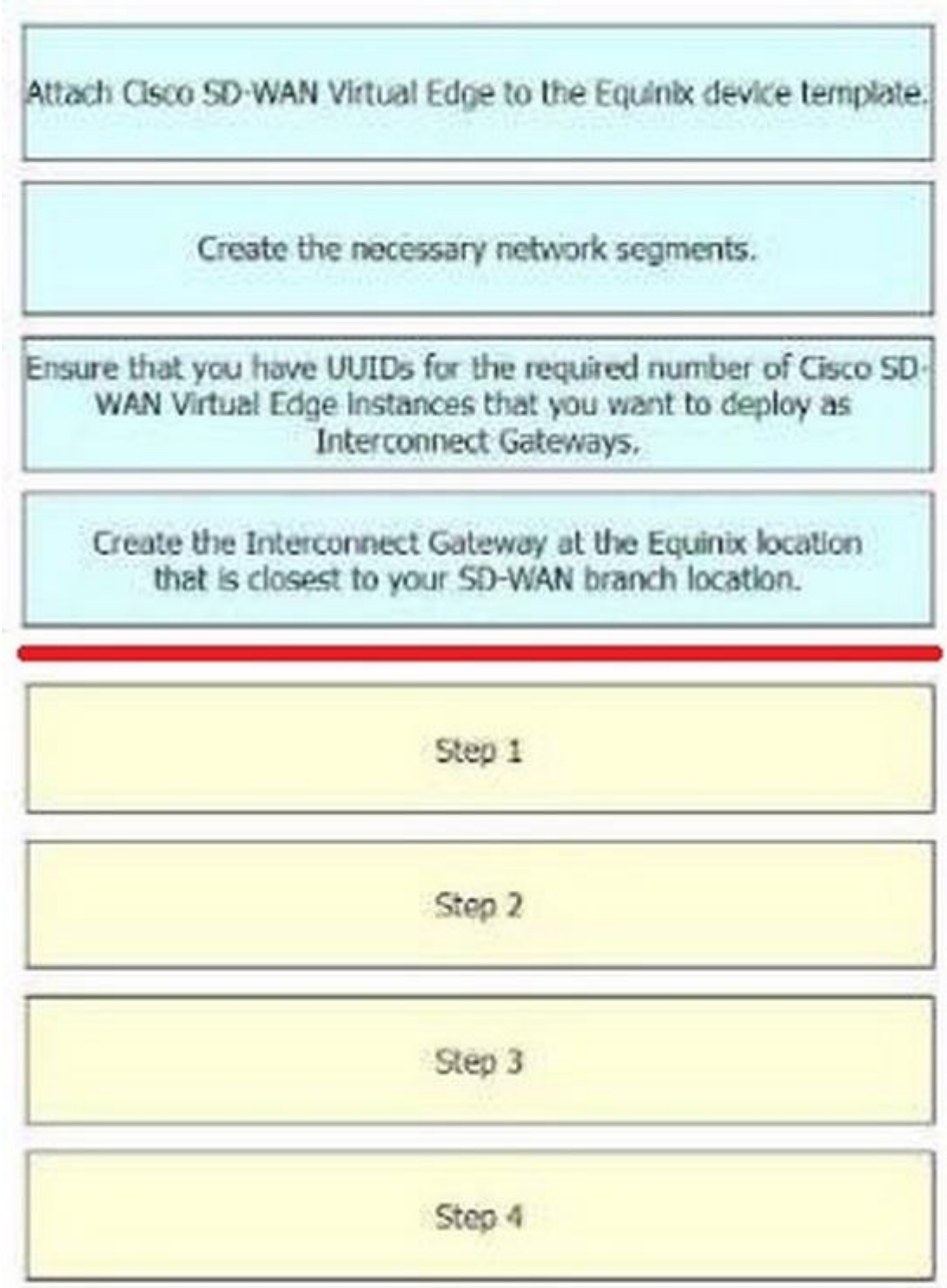
C. VPN connections are used to provide secure access to SaaS applications from the on-premises infrastructure.

D. A dedicated, private connection is established between the on-premises infrastructure and the SaaS provider data center using colocation services.

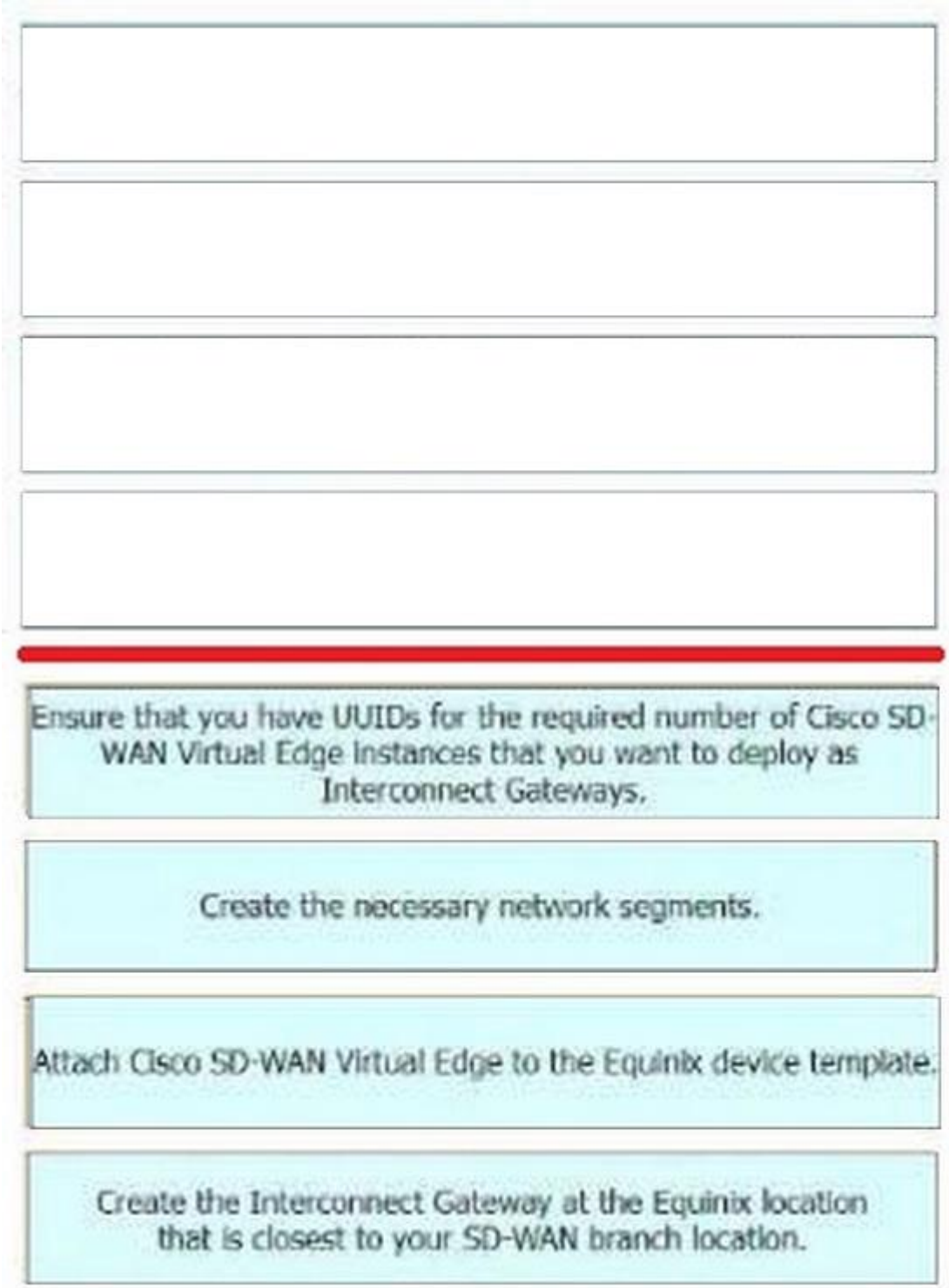
Correct Answer: B

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.



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]