Cisco

Exam Questions 300-440

Designing and Implementing Cloud Connectivity (ENCC)

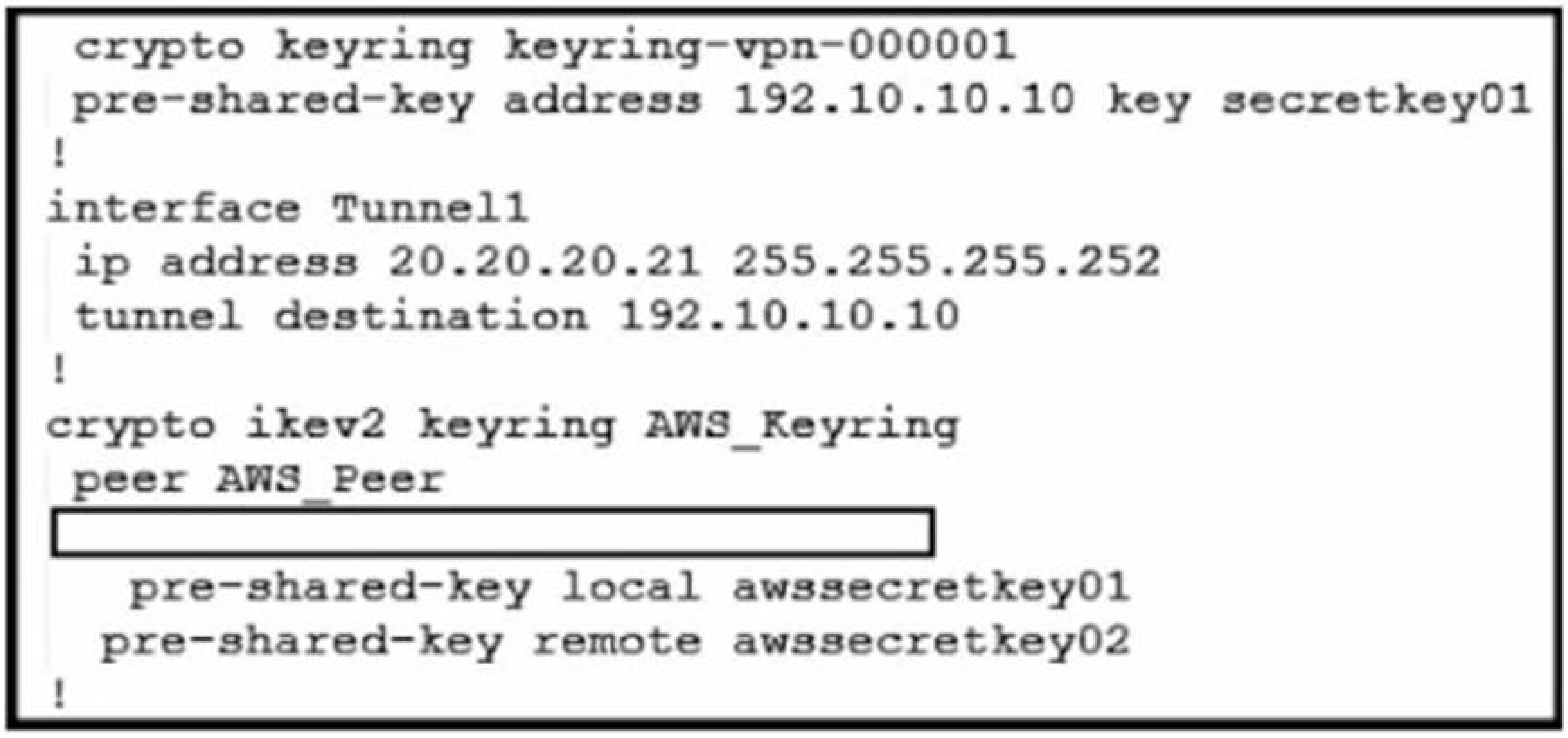
NEW QUESTION 1
A company with multiple branch offices wants a connectivity model to meet its network architecture requirements. The company focuses on ensuring low latency and efficient routing for its critical business applications. Which connectivity model meets these requirements?

A. hub-and-spoke topology with SD-WAN technology, using dynamic routing and OSPF as the routing protocol
B. fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol
C. point-to-point topology using dedicated leased lines and static routing
D. star topology with internet-based VPN connections and static routing

Answer: B

Explanation:
A fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol, meets the requirements of the company because it provides the following benefits:
? It allows direct and secure connectivity between any two branch offices, without the need for a central hub or intermediary devices12. This reduces the latency and improves the performance of the critical business applications.
? It leverages SD-WAN technology to optimize the traffic flow and application quality of service (QoS) across the WAN13. SD-WAN can dynamically select the best path for each application based on the network conditions and policies13. SD- WAN can also provide redundancy, security, and visibility for the WAN13.
? It uses dynamic routing and BGP as the routing protocol to exchange routing information and establish connectivity between the branch offices14. BGP is a scalable and flexible protocol that can support multiple address families, such as IPv4 and IPv6, and multiple routing policies, such as local preference and route filtering14. BGP can also enable seamless integration with the cloud service providers (CSPs) and internet service providers (ISPs)14.
References :=
? 1: Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5) (Cisco U. login required)
? 2: Cisco SD-WAN Design Guide

NEW QUESTION 2
Refer to the exhibit.



```
 crypto keyring keyring-vpn-000001
 pre-shared-key address 192.10.10.10 key secretkey01
!
interface Tunnel1
 ip address 20.20.20.21 255.255.255.252
 tunnel destination 192.10.10.10
!
crypto ikev2 keyring AWS_Keyring
 peer AWS_Peer

   pre-shared-key local awssecretkey01
  pre-shared-key remote awssecretkey02
!
```

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 configuration command must be placed in the blank in the code to complete the tunnel configuration?

A. address 20.20.20.21
B. address 192.10.10.10
C. tunnel source 20.20.20.21
D. tunnel source 192.10.10.10

Answer: C

Explanation:
In the given scenario, an engineer is configuring a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router and AWS. The correct command to complete the tunnel configuration is ??tunnel source 20.20.20.21??. This command specifies the source IP address for the tunnel, which is essential for establishing a secure connection between two endpoints over the internet or another network1. References:
? Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco
Community
? [Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S - Config

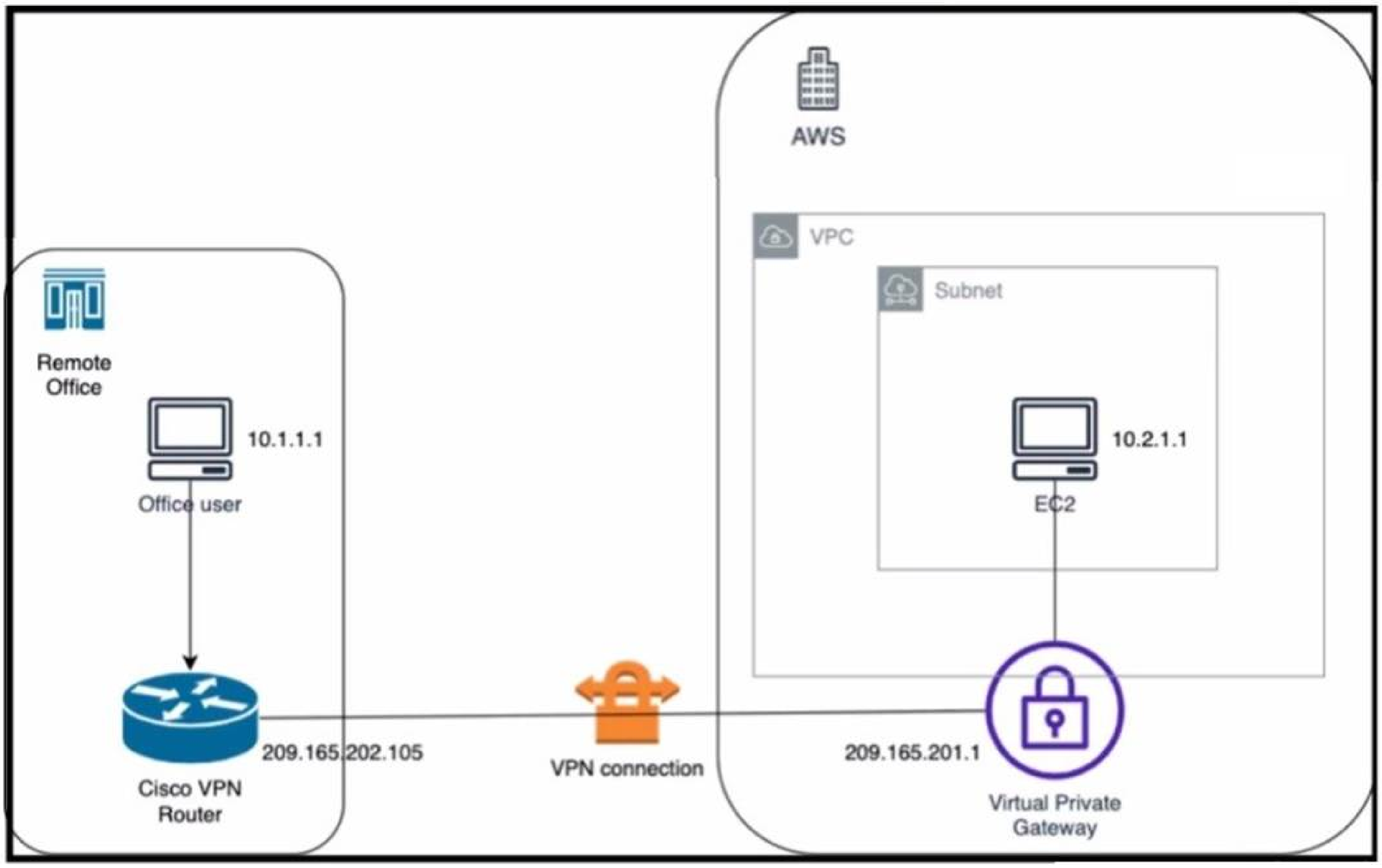
NEW QUESTION 3
Which Microsoft Azure service enables a dedicated and secure connection between an on- premises infrastructure and Azure data centers through a colocation provider?

A. Azure Private Link
B. Azure ExpressRoute
C. Azure Virtual Network
D. Azure Site-to-Site VPN

Answer: B

Explanation:
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

NEW QUESTION 4
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.

Answer: BC

Explanation:
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

NEW QUESTION 5
Which architecture model establishes internet-based connectivity between on-premises networks and AWS cloud resources?

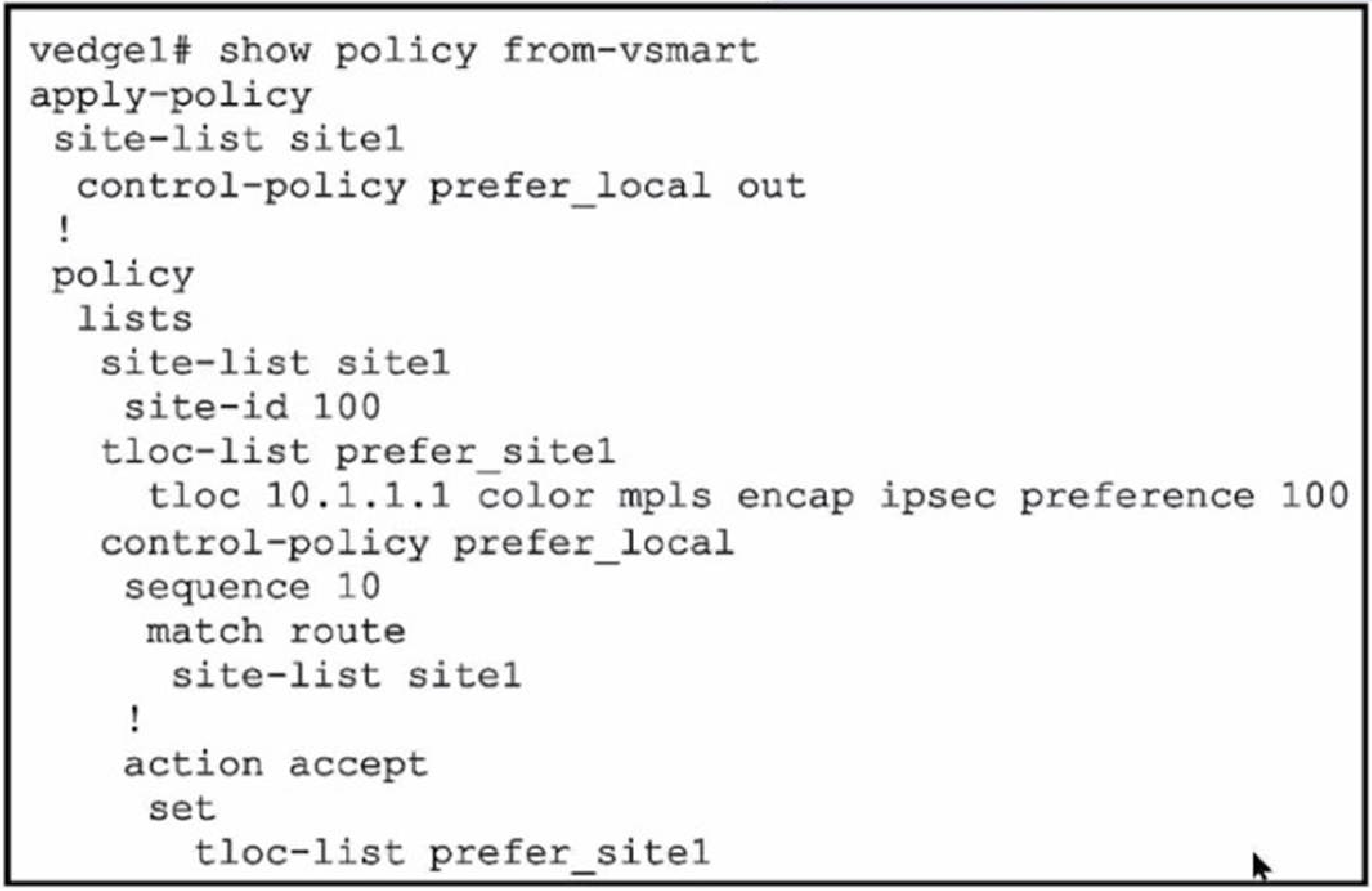
A. That establishes an iPsec VPN tunnel with Internet Key Exchange (IKE) for secure key negotiation and encrypted data transmission

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.

Answer: A

Explanation:
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 model12. It allows multiple remote sites to connect to the same virtual private gateway in AWS, creating a hub-and-spoke topology1. The VPN CloudHub model provides the following benefits12:
? 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 networks3. 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 internet4. 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 networks5.
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?

NEW QUESTION 6
Refer to the exhibit.



```
vedge1# show policy from-vsmart
apply-policy
 site-list site1
  control-policy prefer_local out
 !
 policy
  lists
   site-list site1
    site-id 100
   tloc-list prefer_site1
     tloc 10.1.1.1 color mpls encap ipsec preference 100
   control-policy prefer_local
    sequence 10
     match route
      site-list site1
    !
    action accept
     set
       tloc-list prefer_site1
```

A network engineer discovers that the policy that is configured on an on-premises Cisco WAN edge router affects only the route tables of the specific devices that are listed in the site list. What is the problem?

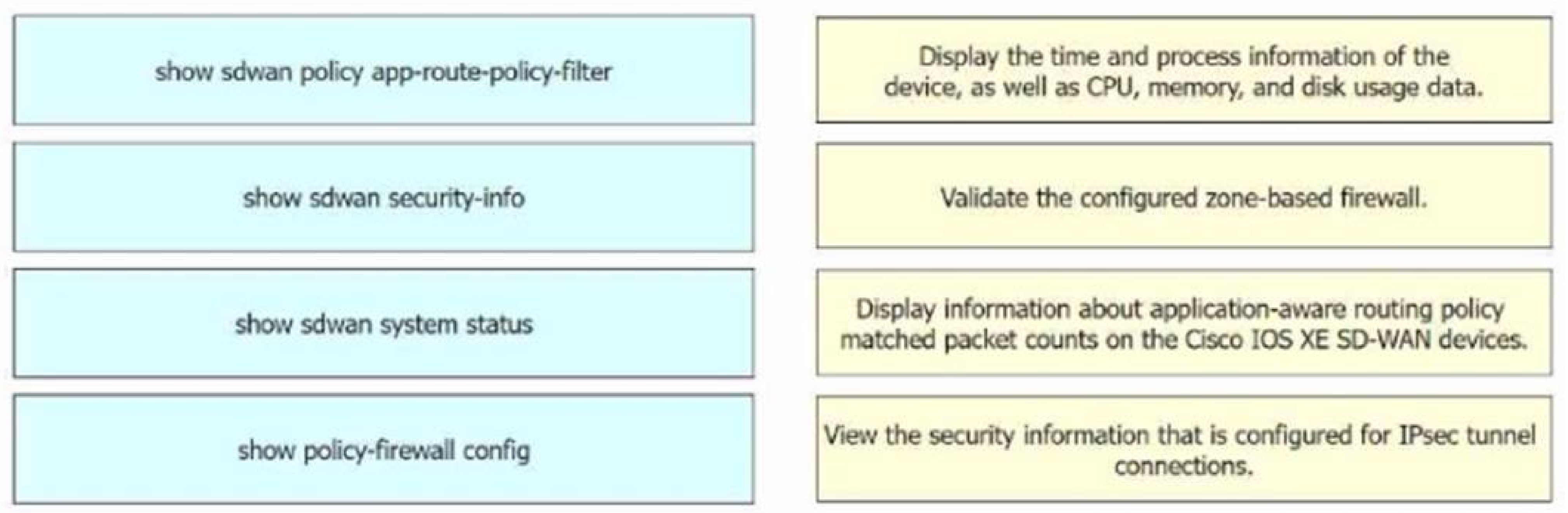
A. An inbound policy must be applied.
B. The action must be set to deny
C. A localized data policy must be configured.
D. A centralized data policy must be configured

Answer: D

Explanation:
A centralized data policy is a policy that is applied to all devices in the overlay network, regardless of the site list. A localized data policy is a policy that is applied only to the devices that are listed in the site list. In this case, the network engineer wants to apply the policy to all devices in the overlay network, not just the

specific devices in the site list. Therefore, a centralized data policy must be configured on the on-premises Cisco WAN edge router. References :=
? Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:
Implementing Cloud Connectivity, Lesson 3: Implementing Cisco SD-WAN Cloud OnRamp for Colocation, Topic: Centralized Data Policy
? [Cisco SD-WAN Cloud OnRamp for Colocation Deployment Guide], Chapter:
Configuring Centralized Data Policy

NEW 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.



show sdwan policy app-route-policy-filter

show sdwan security-info

show sdwan system status

show policy-firewall config

Display the time and process information of the device, as well as CPU, memory, and disk usage data.

Validate the configured zone-based firewall.

Display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices.

View the security information that is configured for IPsec tunnel connections.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Display the time and process information of the device, as well as CPU, memory, and disk usage data. = show sdwan system status1
? 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-filter1
? 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 follows1:
? 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 data1.
? show policy-firewall config: This command is used to validate the configured zone- based firewall1.
? 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 devices1.
? show sdwan security-info: This command is used to view the security information that is configured for IPsec tunnel connections1.
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

NEW QUESTION 8
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

Answer: A

Explanation:
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

NEW QUESTION 9
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?

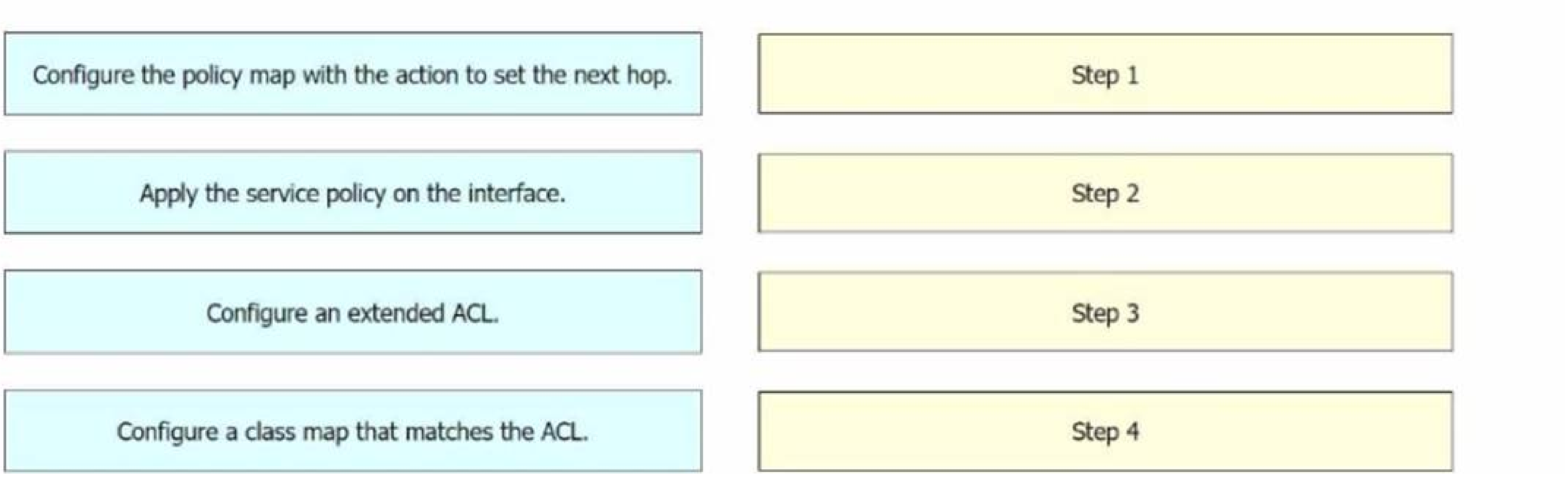
A. ExpressRoute with private peering using SDCI
B. hybrid connectivity with SD-WAN
C. AWS Direct Connect with dedicated connections

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

Answer: A

Explanation:
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 network1.
? 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 databases2.
? 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

NEW QUESTION 10
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.



Configure the policy map with the action to set the next hop.

Apply the service policy on the interface.

Configure an extended ACL.

Configure a class map that matches the ACL.

Step 1

Step 2

Step 3

Step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
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

NEW QUESTION 10
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

Answer: A

Explanation:
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]

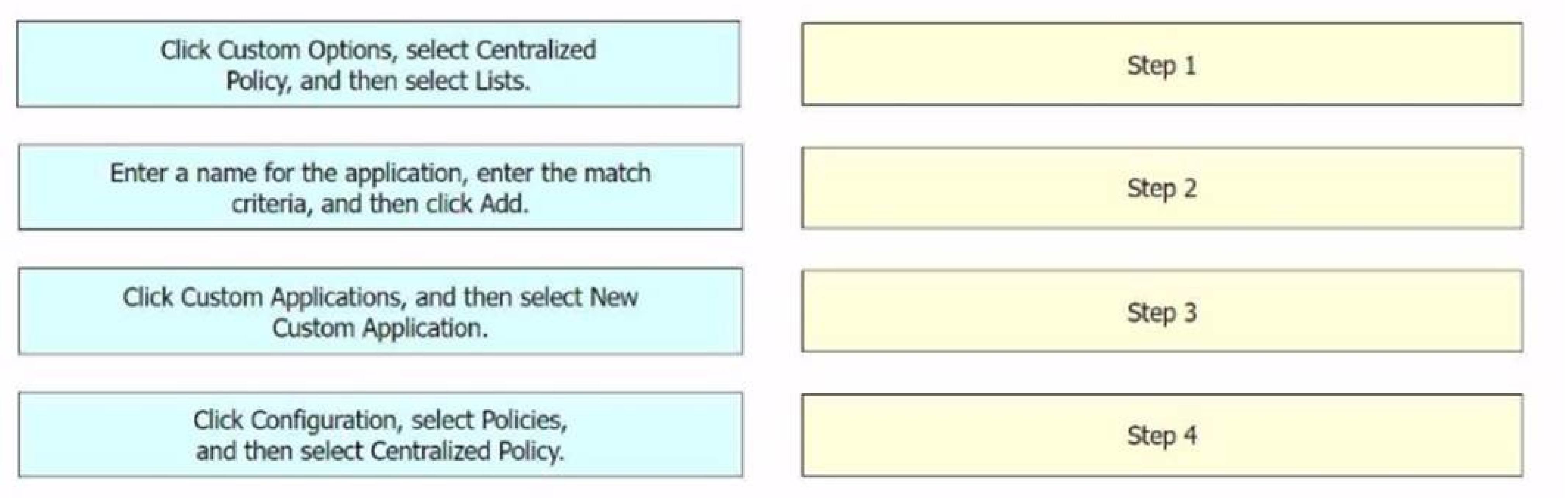
NEW QUESTION 11
An engineer is implementing a highly securemultitierapplication in AWS that includes S3. RDS, and some additional private links. What is critical to keep the traffic safe?

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

Answer: B

Explanation:
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

NEW QUESTION 14
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.



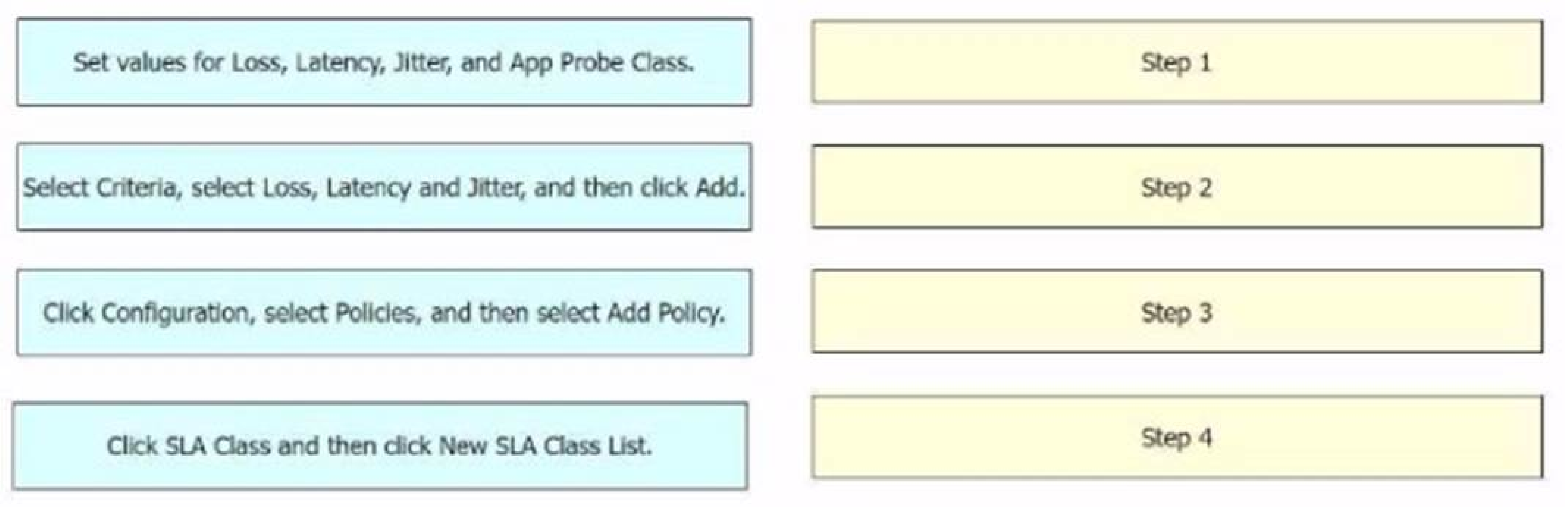
Click Custom Options, select Centralized Policy, and then select Lists.	Step 1
Enter a name for the application, enter the match criteria, and then click Add.	Step 2
Click Custom Applications, and then select New Custom Application.	Step 3
Click Configuration, select Policies, and then select Centralized Policy.	Step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? To configure a custom application with Cisco SD-WAN centralized policy, you need to follow these steps25:
The process of configuring a custom application with a Cisco SD-WAN centralized policy using Cisco vManage involves several steps1.
? 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 vManage1.
? 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 Lists1.
? Click Custom Applications, and then select New Custom Application: After setting up the Lists, you click on Custom Applications and then select New Custom Application1.
? 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 configuration1.
References :=
? Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE

NEW QUESTION 15
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.



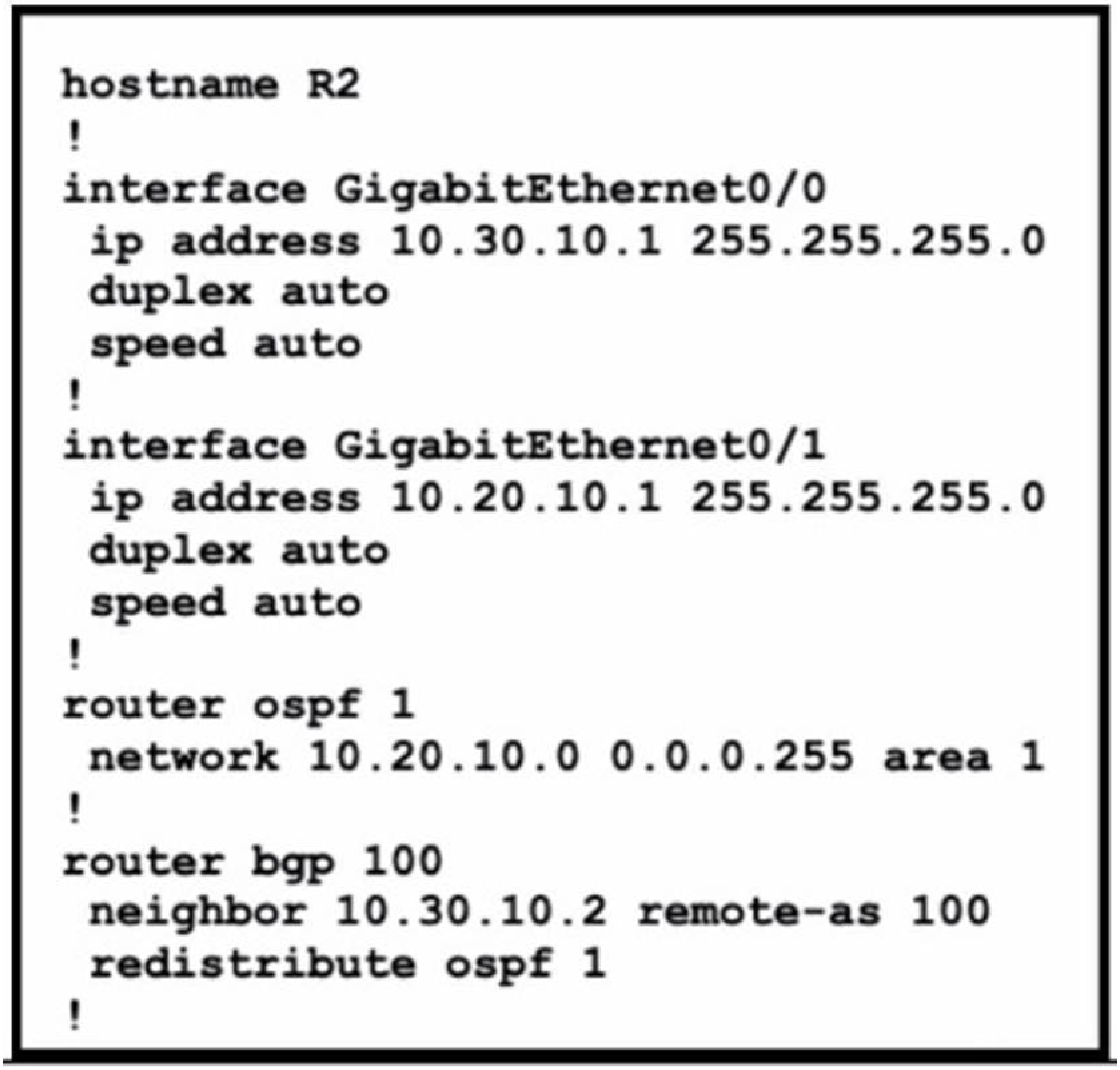
Set values for Loss, Latency, Jitter, and App Probe Class.	Step 1
Select Criteria, select Loss, Latency and Jitter, and then click Add.	Step 2
Click Configuration, select Policies, and then select Add Policy.	Step 3
Click SLA Class and then click New SLA Class List.	Step 4

A. Mastered
B. Not Mastered

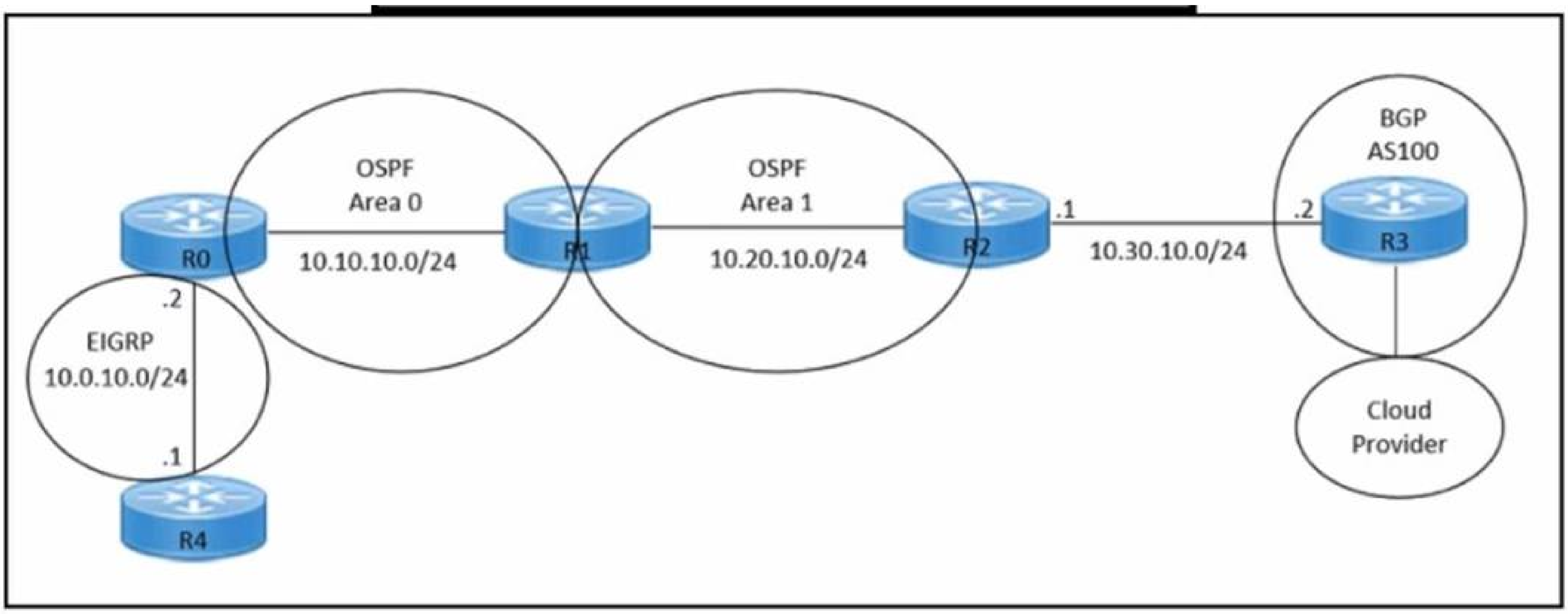
Answer: A

Explanation:
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 steps12.
? 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 vManage1.
? Click SLA Class and then click New SLA Class List: In this step, you create a new SLA Class List1.
? 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 Jitter1.
? Set values for Loss, Latency, Jitter, and App Probe Class: Finally, you set the values for Loss, Latency, Jitter, and App Probe Class1.
References :=
? Information About Application-Aware Routing - Cisco
? Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20

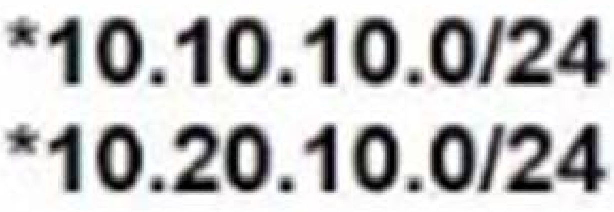
NEW QUESTION 16
Refer to the exhibits.



```
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

Answer: C

Explanation:
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

NEW QUESTION 20
......