QUESTION 1
An engineer is implementing a highly secure multitier application 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 resources. The private links can also prevent the exposure of the data and the application logic to the public internet.
- Bucket policies are needed to control the access to the S3 buckets that store the application data. 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. Bucket policies can also enforce encryption in transit and at rest for the data in S3.

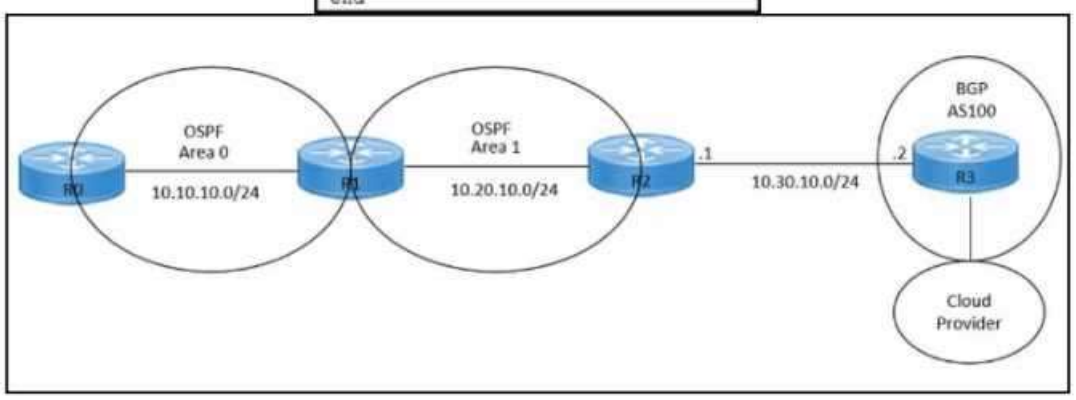
QUESTION 2
What is the role of service providers to establish private connectivity between on-premises networks and Google Cloud resources?

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.

QUESTION 3
Refer to the exhibits. 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?

```
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
```



A. redistribute ospf 1
B. redistribute bgp 100 ospf 1
C. redistribute bgp 100 subnets
D. bgp redistrlbute-lnternal

Answer: B
Explanation:
This command redistributes the routes learned from BGP AS100 into OSPF Area 1, which allows router R2 to advertise those routes to router R1 and connect the on-premises network to the cloud provider. The other options are incorrect because they either redistribute the wrong routes or use the wrong syntax .

QUESTION 4
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.

Answer: AE
Explanation:
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.

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 CloudFront for 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 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.

QUESTION 6
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

Answer: B
Explanation:
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. You can also use security groups to isolate your nodes from other instances in the same VPC or subnet, or to allow communication between nodes in different clusters or regions.

QUESTION 7
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.

QUESTION 8
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.

Answer: B
Explanation:
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 hub. 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 center. 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 infrastructure. Therefore, the correct answer is option B, which describes the basic function of a centralized internet gateway.

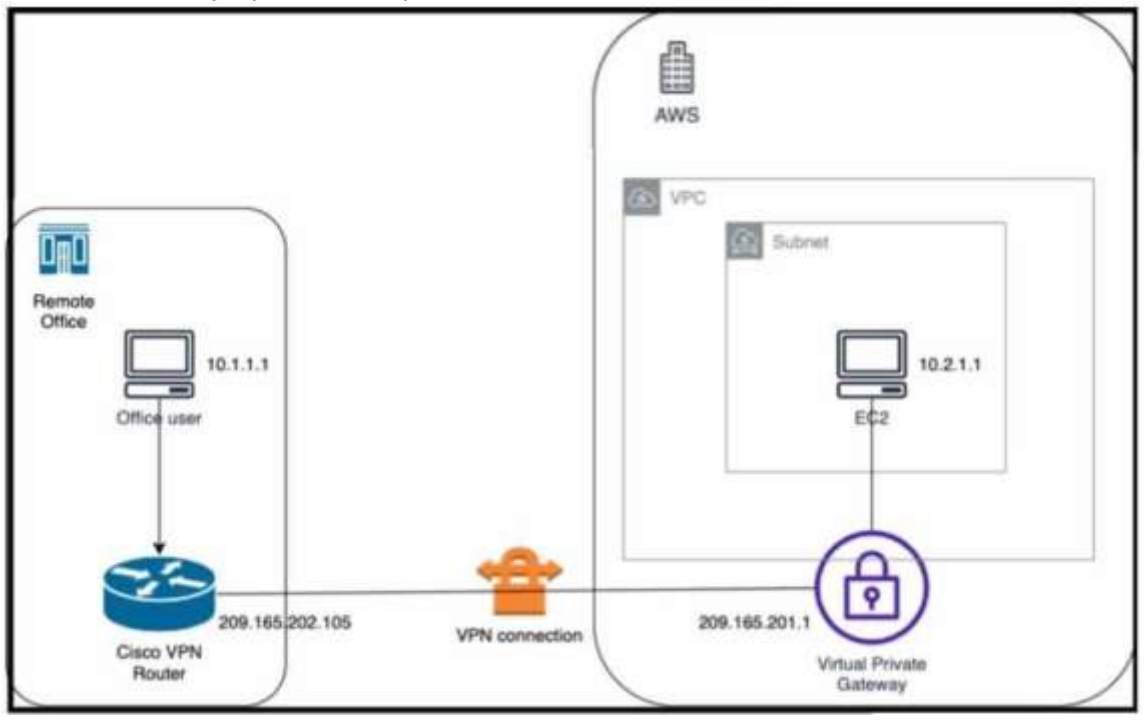
QUESTION 9
Refer to the exhibit. An engineer needs to configure a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS). Which configuration command must be placed in the blank in the code to complete the tunnel configuration?

```
 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
!
```

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 network.

QUESTION 10
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.

QUESTION 11
Refer to the exhibit. A company uses Cisco SD-WAN in the data center. All devices have the default configuration. An engineer attempts to add a new centralized control policy in Cisco vManage but receives an error message. What is the problem?

```
1-Aug-2021 20:12:11 EDT] Failed to apply policy - Failed to
process device request -
Error type : application
Error tag : operation-failed
Error Message : /apply-policy/site-list[name='All-Site']:
Overlapping apply-policy site-list Hub site id 200-299 with
site-list All-Site
Error info : <error-info>
<bad-element>site-list</bad-element>
</error-info>
```

A. A centralized control policy is already applied to the specific site ID and direction
B. The policy for "Hub" should be applied in the outbound direction, and the policy for "All-Site" should be applied inbound.
C. Apply an additional outbound control policy to override the site ID overlaps.
D. Site-list "All-Site" should be configured with a new match sequence that is lower than the sequence for site-list "Hub*.

Answer: D
Explanation:
The problem is that the site-list "All-Site" has a higher match sequence than the site-list "Hub", which means that the policy for "All-Site" will take precedence over the policy for "Hub" for any site that belongs to both lists. This creates a conflict and prevents the engineer from adding a new centralized control policy in Cisco vManage. To resolve this issue, the site-list "All-Site" should be configured with a new match sequence that is lower than the sequence for site-list "Hub", so that the policy for "Hub" will be applied first and then the policy for "All-Site" will be applied only to the remaining sites that are not in the "Hub" list.

QUESTION 12
A company with multiple branch offices wants a suitable connectivity model to meet these network architecture requirements:
- high availability
- quality of service (QoS)
- multihoming
- specific routing needs

Which connectivity model meets these requirements?

A. hub-and-spoke topology using MPLS with static routing and dedicated bandwidth for QoS
B. star topology with internet-based VPN connections and BGP for routing
C. hybrid topology that combines MPLS and SD-WAN
D. fully meshed topology with SD-WAN technology using dynamic routing and prioritized traffic for QoS

Answer: D
Explanation:
A fully meshed topology with SD-WAN technology using dynamic routing and prioritized traffic for QoS meets the network architecture requirements of the company. A fully meshed topology provides high availability by eliminating single points of failure and allowing multiple paths between branch offices. SD-WAN technology enables multihoming by supporting multiple transport options, such as MPLS, internet, LTE, etc. SD-WAN also provides QoS by applying policies to prioritize traffic based on application, user, or network conditions. Dynamic routing allows the SD-WAN solution to adapt to changing network conditions and optimize the path selection for each traffic type. A fully meshed topology with SD-WAN technology can also support specific routing needs, such as segment routing, policy-based routing, or application-aware routing.

QUESTION 13
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 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-WAN.

By using ExpressRoute with private peering and SDCI, the company can achieve the following benefits:
- High availability: ExpressRoute circuits are redundant and resilient, and can be configured with multiple service providers and locations for failover and load balancing. SDCI also provides high availability by using dynamic routing protocols and encryption mechanisms to ensure optimal and secure path selection.
- Redundancy: ExpressRoute circuits can be paired together to form a redundant connection between the customer's network and Azure. SDCI also supports redundancy by allowing multiple connections between data centers and cloud providers, using different transport technologies and service levels.
- Low latency: ExpressRoute circuits offer lower latency than public internet connections, as they bypass the congestion and variability of the internet. SDCI also reduces latency by using MPLS and SD-WAN to optimize the performance and quality of service for the traffic between data centers and cloud providers.

QUESTION 14
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

Answer: C
Explanation:
According to the FedRAMP Authorization Boundary Guidance document1, the method used to create authorization boundary diagrams (ABDs) is to identify all tools as either external or internal 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.

QUESTION 15
Refer to the exhibit. 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?

```
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
```

A. wrong ISAKMP policy
B. identity mismatch
C. wrong encryption
D. IKE version mismatch

Answer: B
Explanation:
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.

QUESTION 16
Refer to the exhibit. 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?

```
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. 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.

QUESTION 17

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 devices. 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 WAN. SD-WAN can dynamically select the best path for each application based on the network conditions and policies. SD-WAN can also provide redundancy, security, and visibility for the WAN.
- It uses dynamic routing and BGP as the routing protocol to exchange routing information and establish connectivity between the branch offices. 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 filtering. BGP can also enable seamless integration with the cloud service providers (CSPs) and internet service providers (ISPs).

QUESTION 18
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 regions within 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.

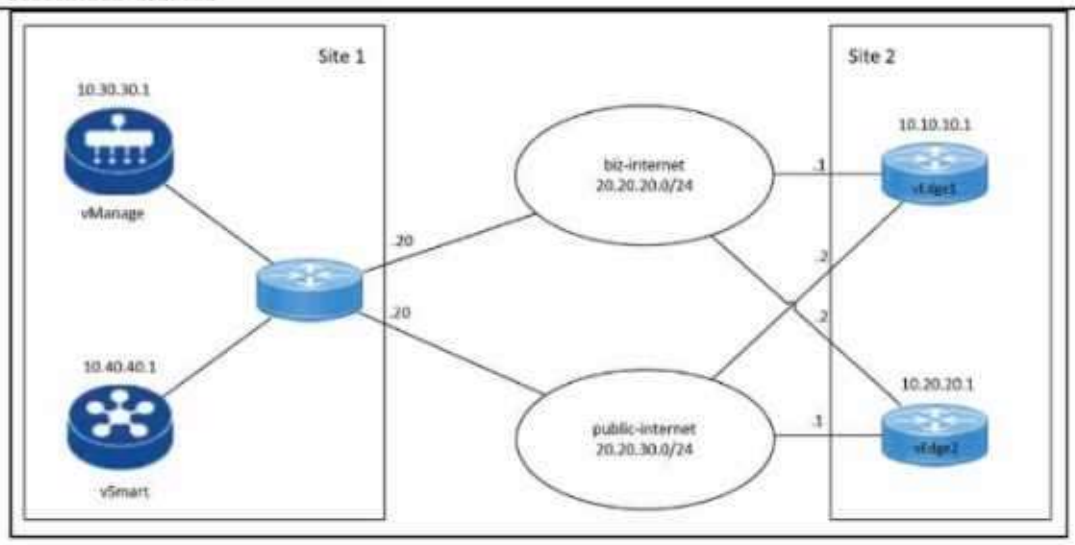
QUESTION 19
An engineer must enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device. What should be configured after the global address-family ipv4 is configured?

A. Set the VRF-specific route advertisements.
B. Enable bgp advertisement.
C. Enter sdwan mode.
D. Disable bgp advertisement.

Answer: B
Explanation:
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.

QUESTION 20
Refer to the exhibits. An engineer troubleshoots a Cisco SD-WAN connectivity issue between an on-premises data center WAN Edge and a public cloud provider WAN Edge. The engineer discovers that BFD is Dapping on vEdge1. What is the problem?

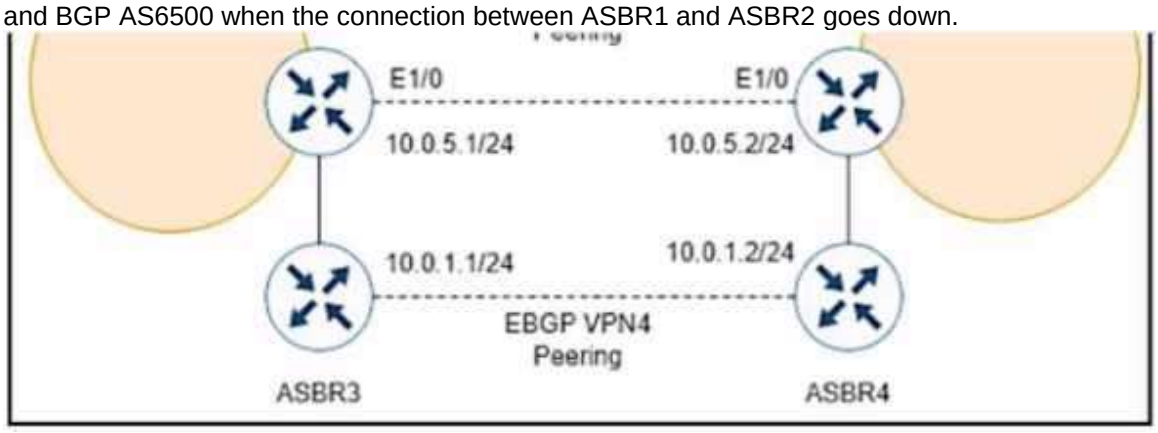
```
local7.debug: Mar 11 11:31:11 VEDGE-1 VDAEMON[1136]: vdaemon_disable_my_tloc[1308]:
%VDAEMON_DBG_EVENTS-1: Disabling tloc ge0_1.
local7.info: Mar 11 11:31:11 VEDGE-1 VDAEMON[1136]: %Viptela-VEDGE-1-vdaemon-6-INFO-1400002:
Notification:
 3/11/2023 11:31:11 control-connection-state-change severity-level:major host-name:"VEDGE-1"
 system-ip:10.10.10.1
 personality:vEdge peer-type:vmanage peer-system-ip:10.30.30.1 peer-vmanage-system-ip:0.0.0.0
 public-ip:20.20.20.20
 public-port:12947 src-color:biz-internet remote-color:public-internet uptime:"0:01:36:34" new-
 state:down
local7.info: Mar 11 11:31:11 VEDGE-1 FTMD[1126]: %Viptela-VEDGE-1-ftmd-6-INFO-1400002:
Notification:
 3/11/2023 11:31:11 bfd-state-change severity-level:major host-name:"VEDGE-1" system-
 ip:10.10.10.1 src-ip:20.20.30.2
dst-ip:20.20.30.20   proto:ipsec src-port:12406 dst-port:12347 local-system-ip:10.10.10.1 local-
color:"biz-internet"
  emote-system-ip:10.10.10.4 remote-color:"public-internet" new-state:down deleted:false flap-
  reason:bfd-deleted
```



A. The remote Edge device BFD is down.
B. The remote Edge device failed to respond BFD keepalives.
C. The remote Edge device has a duplicate IP address.
D. The control plane deleted the BFD session.

Answer: B
Explanation:
BFD (Bidirectional Forwarding Detection) is a protocol that detects failures in the overlay tunnel between Cisco SD-WAN devices. BFD packets are sent and received periodically by each device to check the liveliness and quality of the connection. If a device does not receive a BFD packet from its peer within a specified timeout interval, it considers the peer to be unreachable and reports a BFD down event. This event triggers a control connection state change and a possible route change in the SD-WAN fabric.
In this scenario, the engineer discovers that BFD is flapping on vEdge1, which means that the BFD session between vEdge1 and the remote Edge device is going up and down repeatedly. This indicates a connectivity issue between the two devices, such as network congestion, packet loss, or misconfiguration. The most likely cause of the problem is that the remote Edge device failed to respond BFD keepalives within the timeout interval, which resulted in a BFD timeout event on vEdge1. This event caused vEdge1 to mark the remote Edge device as down and notify the control plane. The control plane then tried to establish a new BFD session with the remote Edge device, which may have succeeded or failed depending on the network condition. This cycle of BFD session creation and deletion caused the BFD flapping on vEdge1.

QUESTION 21
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

Answer: D
Explanation:
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 receives two 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.

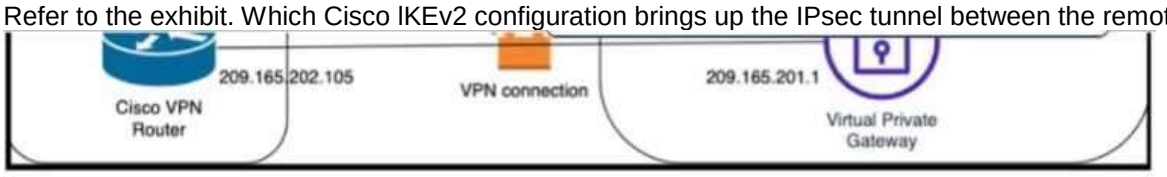
QUESTION 22
Refer to the exhibits. An engineer needs to configure a site-to-site IPsec VPN connection between an on premises Cisco IOS XE router and Amazon Web Services (AWS). Which two IP prefixes should be used to configure the AWS routing options? (Choose two.)

```
crypto keyring keyring-vpn-000001
 pre-shared-key address 20.20.20.29 key awskey01
!
crypto keyring keyring-vpn-000002
 pre-shared-key address 40.40.40.29 key awskey02
!
interface Tunnel1
 ip address 30.30.30.29 255.255.255.252
 tunnel destination 20.20.20.29
!
interface Tunnel2
 ip address 30.30.30.33 255.255.255.252
 tunnel destination 40.40.40.29
!
```

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

Answer: AE
Explanation:
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.

QUESTION 23
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
!
```

Answer: C
Explanation:
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 IPsec profile 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 pre-share 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 AWS1 and Cisco2 for setting up an IKEv2 IPsec site-to-site VPN between a Cisco IOS-XE router and an AWS virtual private gateway.