



300-440^{Q&As}

Designing and Implementing Cloud Connectivity (ENCC)

Pass Cisco 300-440 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/300-440.html>

100% Passing Guarantee
100% Money Back Assurance

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

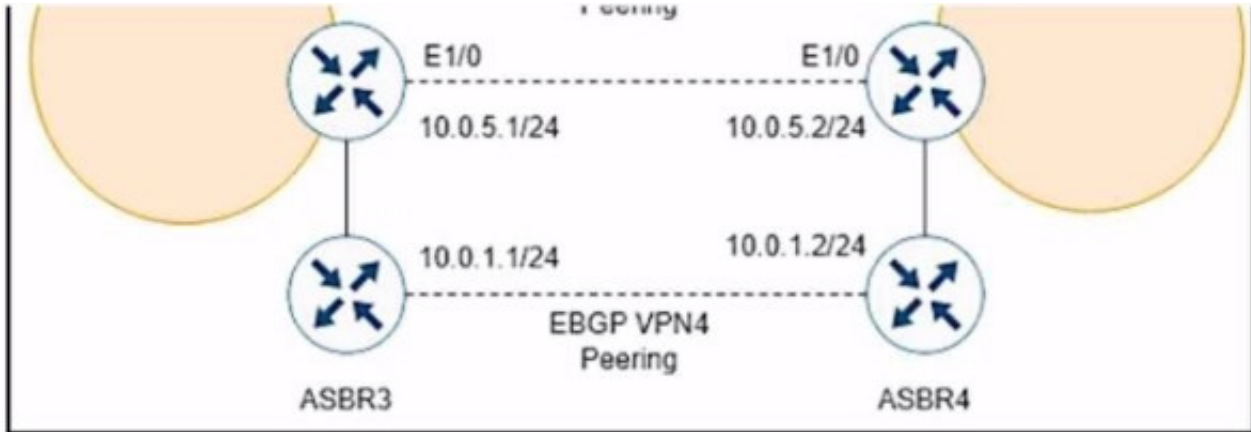
-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Refer to the exhibits.



While troubleshooting, a network engineer discovers that the backup path fails between ASBR3 and ASBR4 for traffic between BGP AS6000 and BGP AS6500 when the connection between ASBR1 and ASBR2 goes down. The following configurations were performed on ASBR1:

```
ASBR1(config)# router bgp 6000
ASBR1 (config-router)# address-family vpn4
ASBR1 (config-router-af)# neighbor 10.0.5.2 remote-as 6500
ASBR1 (config-router-af)# neighbor 10.0.5.2 activate
ASBR1 (config-router-af)# neighbor 10.0.5.2 fall-over bfd
ASBR1 (config-router-af)# end
```

Which command is missing?

- A. bgp additional-paths install
- B. bgp additional-paths select
- C. redistribute static
- D. bgp advertise-best-external

Correct Answer: D

The `bgp advertise-best-external` command is used to enable the advertisement of the best external path to internal BGP peers. This command is useful when there are multiple exit points from the local AS to other ASes, and the local AS wants to use the closest exit point for each destination. By default, BGP only advertises the best path to its peers, and the best path is usually the one with the lowest IGP metric to the next hop. However, this may not be the optimal path for traffic leaving the local AS, as it may result in suboptimal hot-potato routing or MED oscillations. The `bgp advertise-best-external` command allows BGP to advertise the best external path, which is the path with the lowest MED among the paths from different neighboring ASes, in addition to the best path. This way, the internal BGP peers can choose the best exit point based on the MED value, rather than the IGP metric. In this scenario, ASBR1 is configured 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 2

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 3

Refer to the exhibit.



```
crypto keyring keyring-vpn-000001
pre-shared-key address 192.10.10.10 key secretkey01
!
interface Tunnell
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

Correct Answer: C

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.

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

QUESTION 4

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

- A. facilitate direct, dedicated network connections through Google Cloud Interconnect
- B. enable intelligent routing and dynamic path selection using software-defined networking
- C. provide end-to-end encryption for data transmission using native IPsec
- D. accelerate content delivery through integration with Google Cloud CDN

Correct Answer: A



The role of service providers to establish private connectivity between on-premises networks and Google Cloud resources is to facilitate direct, dedicated network connections through Google Cloud Interconnect. Google Cloud Interconnect is

a service that allows customers to connect their on-premises networks to Google Cloud through a service provider partner. This provides low latency, high bandwidth, and secure connectivity to Google Cloud services, such as Google

Compute Engine, Google Cloud Storage, and Google BigQuery. Google Cloud Interconnect also supports hybrid cloud scenarios, such as extending on-premises networks to Google Cloud regions, or connecting multiple Google Cloud

regions together. Google Cloud Interconnect offers two types of connections: Dedicated Interconnect and Partner Interconnect. Dedicated Interconnect provides physical connections between the customer's network and Google's network at

a Google Cloud Interconnect location. Partner Interconnect provides virtual connections between the customer's network and Google's network through a supported service provider partner. Both types of connections use VLAN attachments

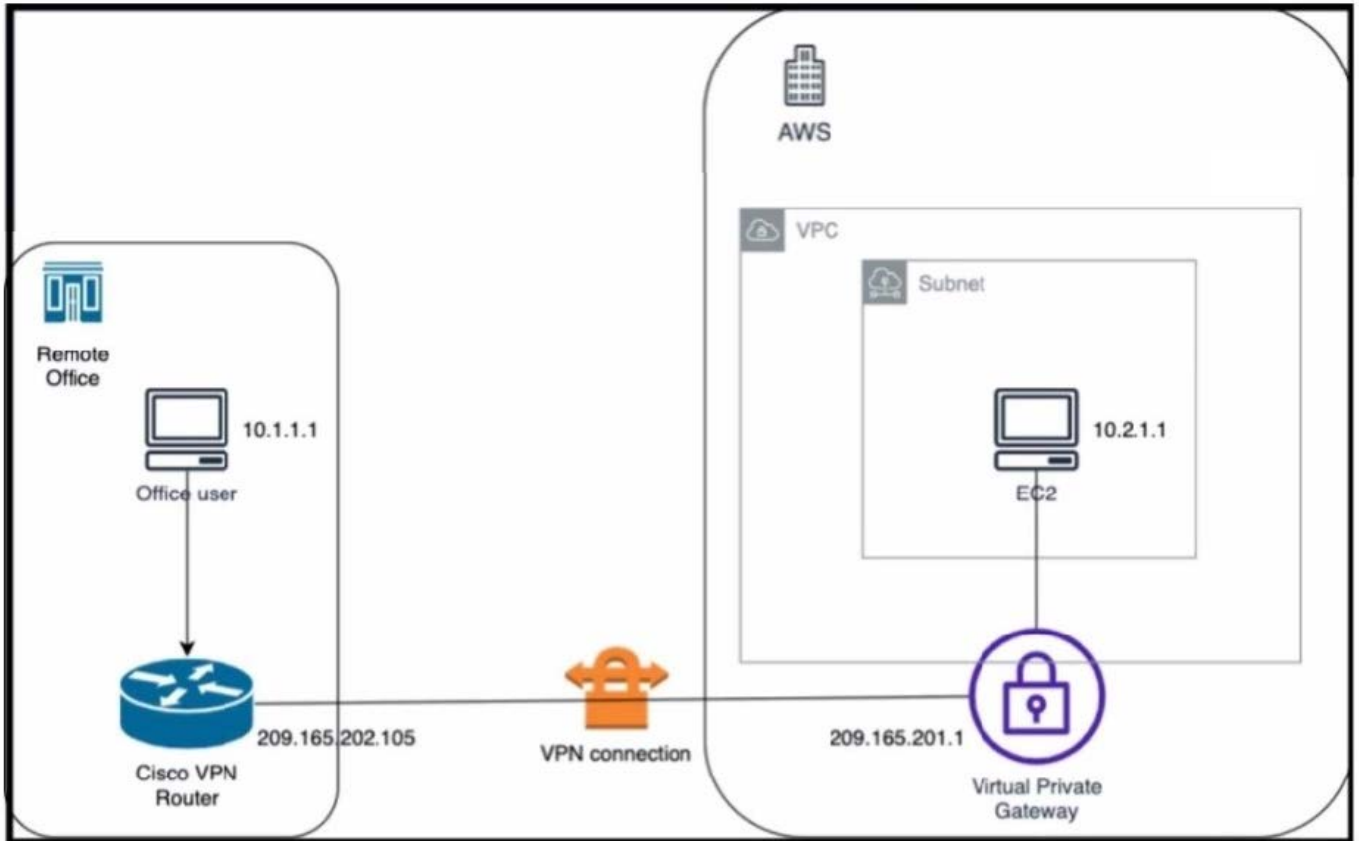
to establish private connectivity to Google Cloud Virtual Private Cloud (VPC) networks.

References:

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

QUESTION 5

Refer to the exhibit.



An engineer successfully brings up the site-to-site VPN tunnel between the remote office and the AWS virtual private gateway, and the site-to-site routing works correctly. However, the end-to-end ping between the office user PC and the AWS EC2 instance is not working.

Which two actions diagnose the loss of connectivity? (Choose two.)

- A. Check the network security group rules on the host VNET.
- B. Check the security group rules for the host VPC.
- C. Check the IPsec SA counters.
- D. On the Cisco VPN router, configure the IPsec SA to allow ping packets.
- E. On the AWS private virtual gateway, configure the IPsec SA to allow ping packets.

Correct Answer: BC

The end-to-end ping between the office user PC and the AWS EC2 instance is not working because either the security group rules for the host VPC are blocking the ICMP traffic or the IPsec SA counters are showing errors or drops. To

diagnose the loss of connectivity, the engineer should check both the security group rules and the IPsec SA counters. The network security group rules on the host VNET are not relevant because they apply to Azure, not AWS. The IPsec SA

configuration on the Cisco VPN router and the AWS private virtual gateway are not likely to be the cause of the problem because the site- to-site VPN tunnel is already up and the site-to-site routing works correctly.

References:



Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5), Module 3:

Configuring IPsec VPN from Cisco IOS XE to AWS, Lesson 3: Verify IPsec VPN Connectivity

Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter: IPsec VPN Overview, Section: IPsec Security Association AWS Documentation, User Guide for AWS VPN, Section: Security Groups for Your VPC

[Latest 300-440 Dumps](#)

[300-440 Study Guide](#)

[300-440 Braindumps](#)