PassQueen
a.k.a dumpsqueen.com

# Designing and Implementing Cloud Connectivity (ENCC)

## Cisco 300-440

**Version Demo**

**Total Demo Questions: 4**

**Total Premium Questions: 44**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Architecture | 15 |
| Topic 2, Network | 14 |
| Topic 3, Security | 10 |
| Topic 4, Troubleshooting | 5 |
| Total | 44 |

QUESTION NO: 1 - (DRAG DROP)

An engineer must configure cloud connectivity with Cisco Umbrella Secure Internet Gateway (SIG) in active/backup mode. The engineer already configured the SIG Credentials and SIG Feature Templates. Drag and drop the steps from the left onto the order on the right to complete the configuration.




**ANSWER:**

**Explanation:**

After the Cisco Umbrella SIG credentials and SIG feature templates are available, the configuration begins by selecting the SIG provider for the primary tunnel. This establishes the main Umbrella SIG tunnel definition and associates it with the configured cloud-security provider information. The primary tunnel is the preferred forwarding path for protected internet-bound traffic in an active/backup design.

The next action is to add the secondary tunnel. This provides an alternate SIG tunnel endpoint that can take over when the preferred tunnel is unavailable. With both tunnel definitions present, they can be joined by creating one high-availability pair using the primary and secondary tunnels. The HA-pair object defines their active/backup relationship so that tunnel health and failover behavior are handled as one resilient SIG connection rather than as unrelated tunnels.

After the tunnel pair has been created, the service-side VPN template is edited to inject a service route. The service route supplies the routing integration needed to steer applicable traffic into the service insertion path and toward the Umbrella SIG tunnel pair. Configuring it after the HA pair exists ensures the route points to a completed, resilient service construct. This order follows Cisco's documented active/backup SIG workflow: define the primary SIG tunnel, add its backup, form the HA pair, and configure the service VPN routing needed for traffic redirection. Cisco documents this tunnel and HA-pair process in Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios. Additional deployment context is available in Cisco's Cisco SD-WAN Security Configuration Guide.

## QUESTION NO: 2

A company deploys a security virtual appliance in an Azure hub virtual network. All internet-bound traffic from a spoke virtual network must traverse the appliance before leaving Azure. The appliance has a private IP address of 10.10.0.4. Which configuration enforces this requirement for workloads in the spoke subnet?

**A.** Associate a network security group with the spoke subnet and allow outbound HTTPS traffic.

**B.** Create a user-defined route for 0.0.0.0/0 with a virtual appliance next hop of 10.10.0.4 and associate it with the spoke subnet.

**C.** Enable a service endpoint for Azure Storage on the spoke subnet.

**D.** Create a user-defined route for 0.0.0.0/0 with an Internet next hop and associate it with the spoke subnet.

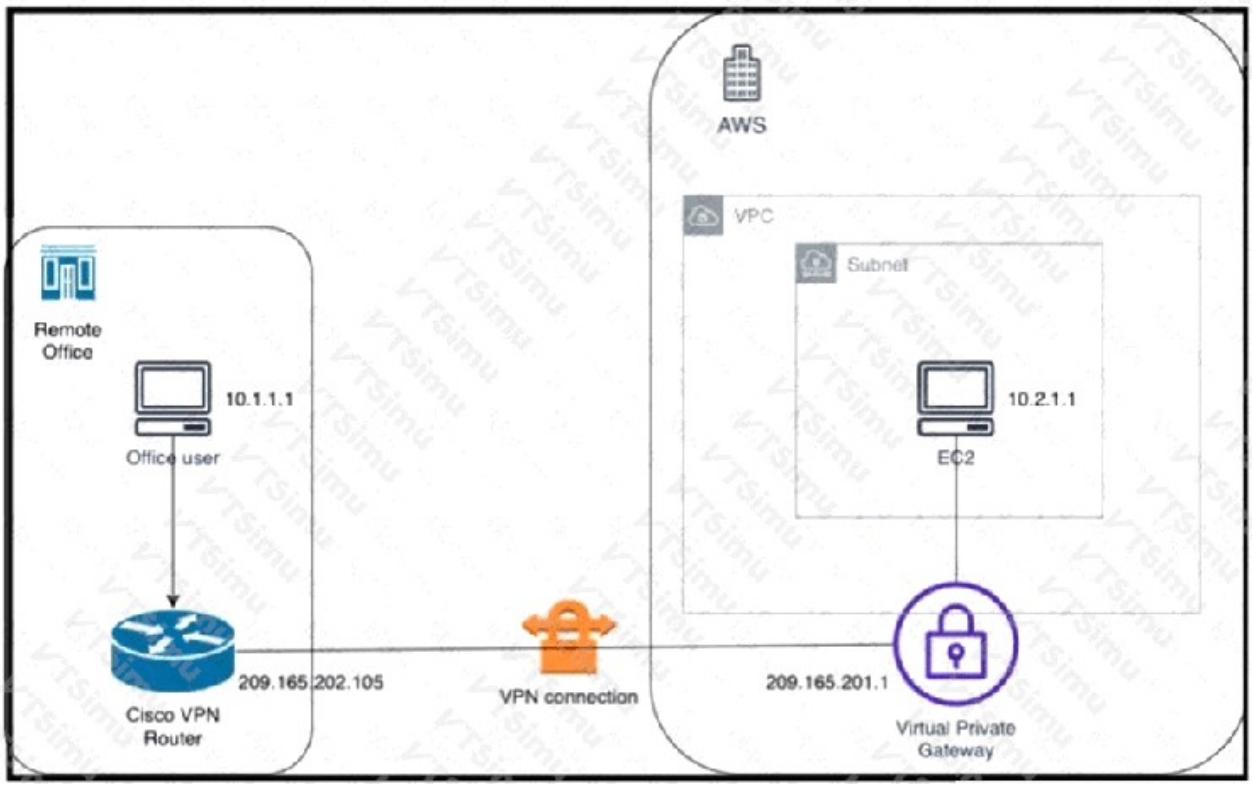
**ANSWER: B**

**Explanation:**

A user-defined route associated with the spoke subnet, with the 0.0.0.0/0 prefix and a virtual appliance next hop of 10.10.0.4, is correct. The route directs traffic that does not match a more-specific route to the security appliance for inspection and forwarding.

A network security group can allow or deny traffic but does not select a next-hop appliance. A service endpoint provides optimized access to supported Azure services and does not steer general internet traffic. A route with an Internet next hop bypasses the appliance rather than enforcing inspection.

## QUESTION NO: 3 - (SIMULATION)




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.)

**ANSWER: See the explanation for the answer**

**Explanation:**

**Choose these two actions:**

The tunnel and routing being up only prove that the VPN control plane is established and routes exist; they do not prove that data traffic passes end to end. The IPsec SA counters identify whether traffic is entering and returning through the encrypted tunnel. AWS security groups are stateful firewalls and can still block ICMP to or from the EC2 instance even when VPN routing is correct.

## QUESTION NO: 4

A Cisco SD-WAN edge router is deployed at a small branch behind a NAT device. The router must discover the SD-WAN controllers and establish control-plane connectivity without requiring the branch firewall to accept unsolicited inbound sessions. Which Cisco SD-WAN component performs the initial orchestration function for this deployment?

**A.** vManage

**B.** vSmart controller

**C.** vBond orchestrator

**D.** SD-WAN tunnel interface

**ANSWER: C**

**Explanation:**

vBond orchestrator is correct because it assists WAN edge devices with controller discovery and orchestrates control connections, particularly when devices are behind NAT. The WAN edge initiates its outbound connection, and vBond provides information that enables the appropriate controller connections to be formed.

vManage provides centralized management and configuration, while vSmart distributes centralized control-plane policy and routing information. A Cisco SD-WAN tunnel interface carries overlay data-plane traffic but does not perform the initial controller-orchestration role.