Free Questions for 300-440

Shared by Lawson on 16-04-2026

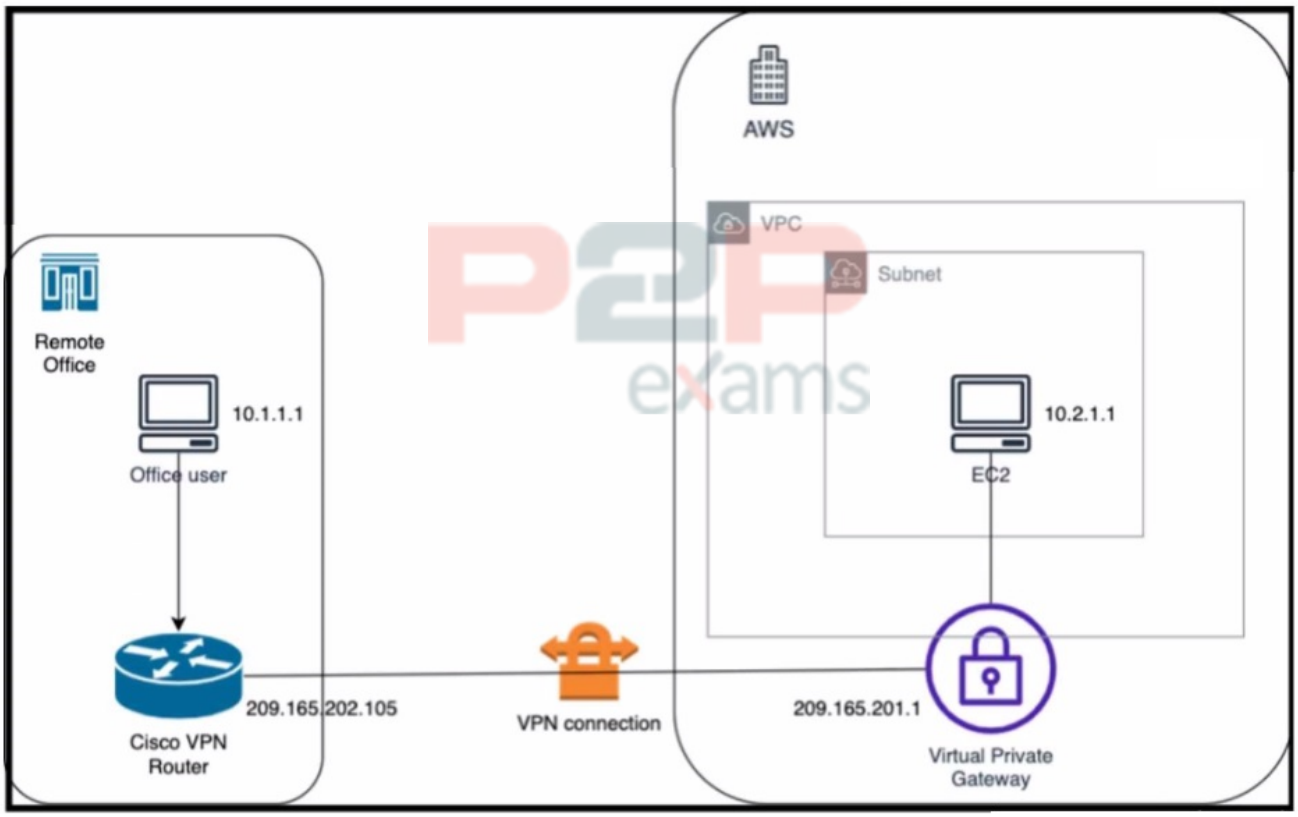
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.



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.)

Options:

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:

B, C

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.Reference:=

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

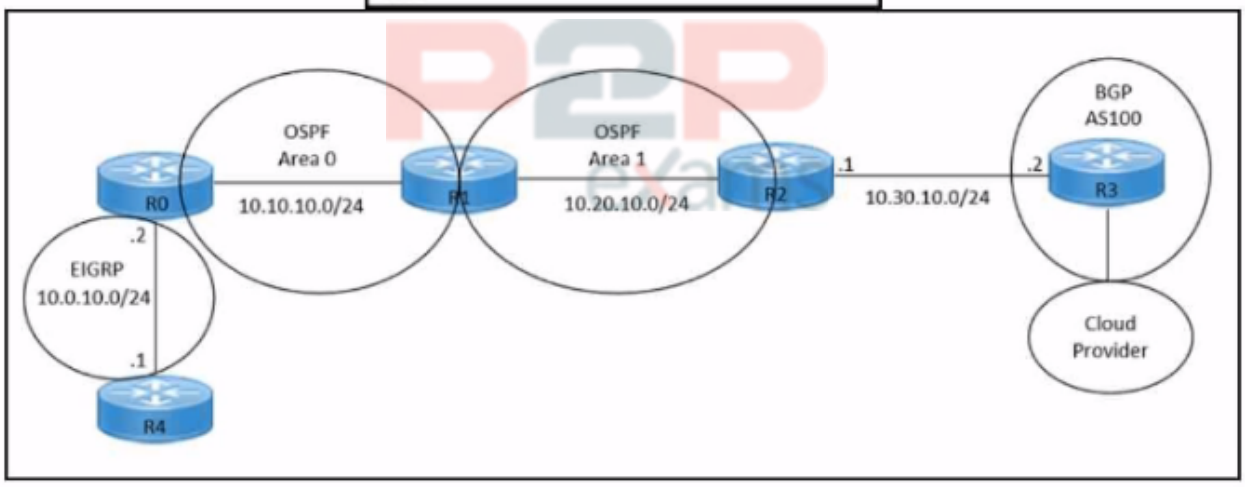
AWS Documentation, User Guide for AWS VPN, Section: Security Groups for Your VPC

Question 2

Question Type: MultipleChoice

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
!
neighbor 10.30.10.2 remote-as 100
!
end
```



Refer to the exhibits. An engineer must redistribute OSPF internal routes into BGP to connect an on-premises network to a cloud provider without introducing extra routes. Which two commands must be configured on router R2? (Select two.)

Options:

A- router ospf 1
B- router bgp 100
C- redistribute ospf 1
D- redistribute bgp 100
E- redistribute ospf 1 match internal external

Answer:

B, E

Explanation:

To redistribute OSPF internal routes into BGP, the engineer needs to configure two commands on router R2. The first command isrouter bgp 100, which enables BGP routing process and specifies

the autonomous system number of 100. The second command isredistribute ospf 1 match internal external, which redistributes the routes from OSPF process 1 into BGP, and matches both internal and external OSPF routes. This way, the engineer can avoid introducing extra routes that are not part of OSPF process 1, such as the default route or the connected routes.Reference: =Designing and Implementing Cloud Connectivity (ENCC) v1.0, [ENCC: Configuring IPsec VPN from Cisco IOS XE to AWS], [Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs]

Question 3

Question Type: MultipleChoice

Which method is used to create authorization boundary diagrams (ABDs)?

Options:

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 customer1.The other options are incorrect because they do not capture the full scope and details of the authorization boundary as required by FedRAMP.Reference:= FedRAMP Authorization Boundary Guidance document1