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.leads4pass.com/300-440.html

100% Passing Guarantee
100% Money Back Assurance

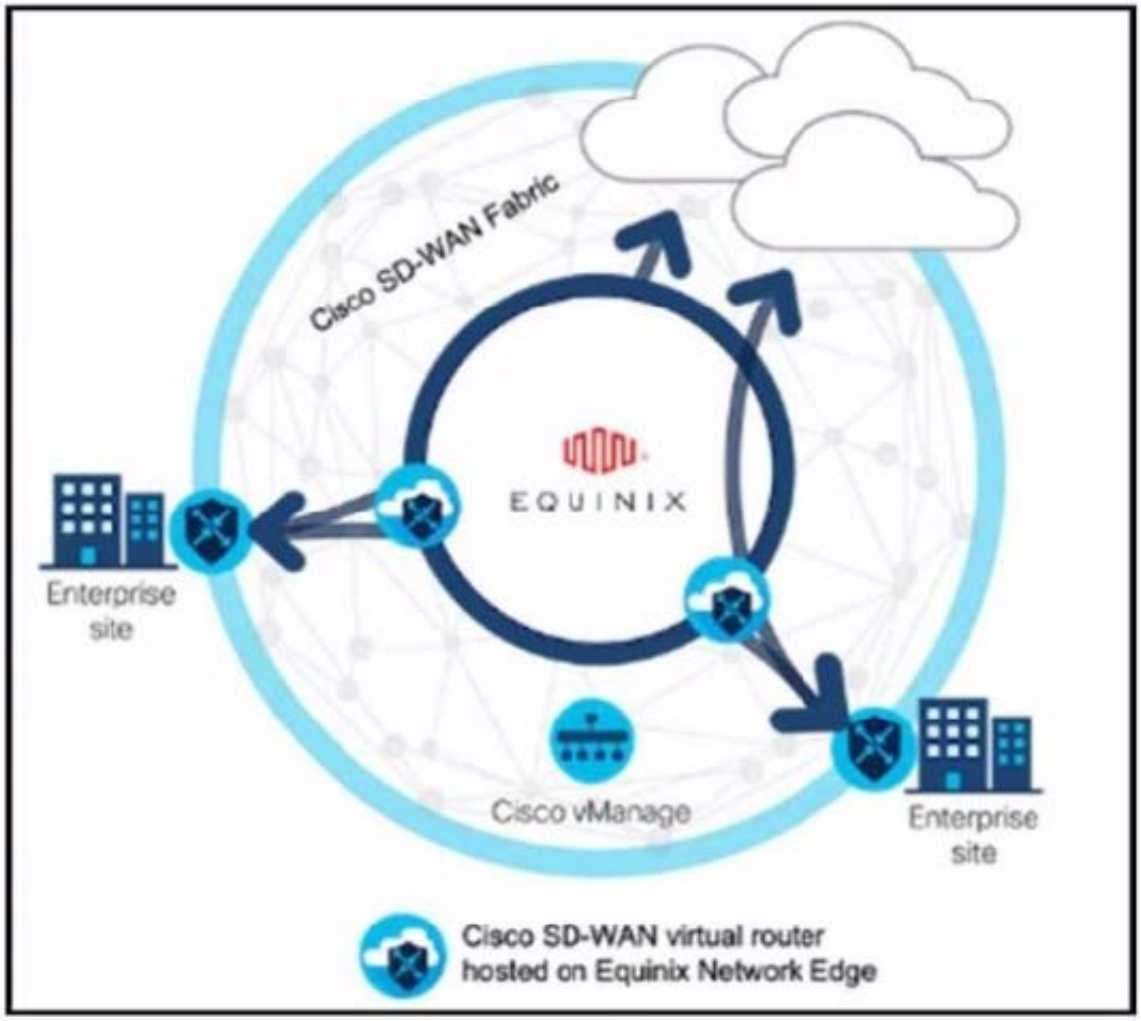
Following Questions and Answers are all new published by Cisco Official Exam Center

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

QUESTION 1

DRAG DROP

Refer to the exhibit.



These configurations are complete:

1.

Create an account in the Equinix portal.

2.

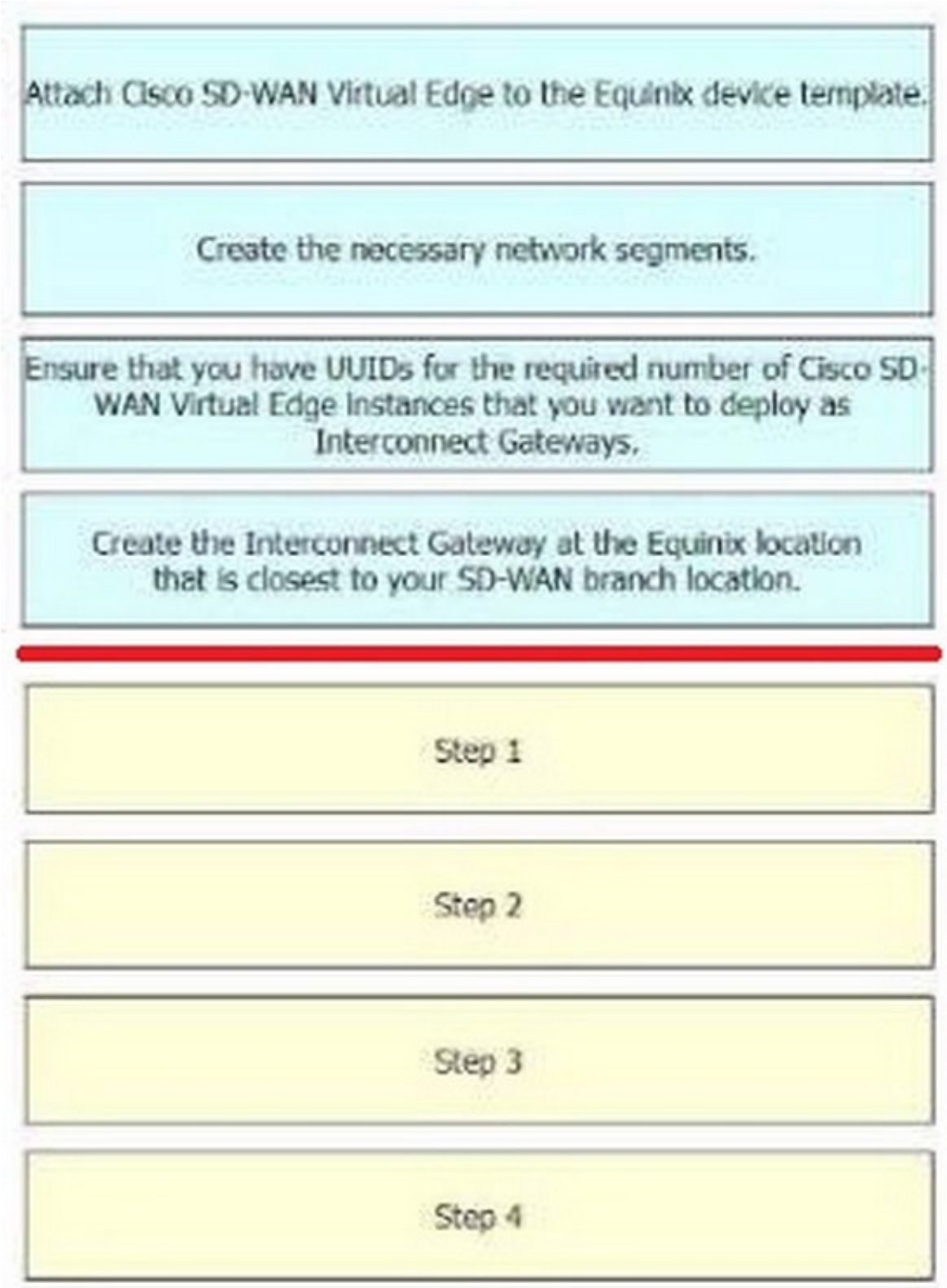
Associate the Equinix account with Cisco vManage.

3.

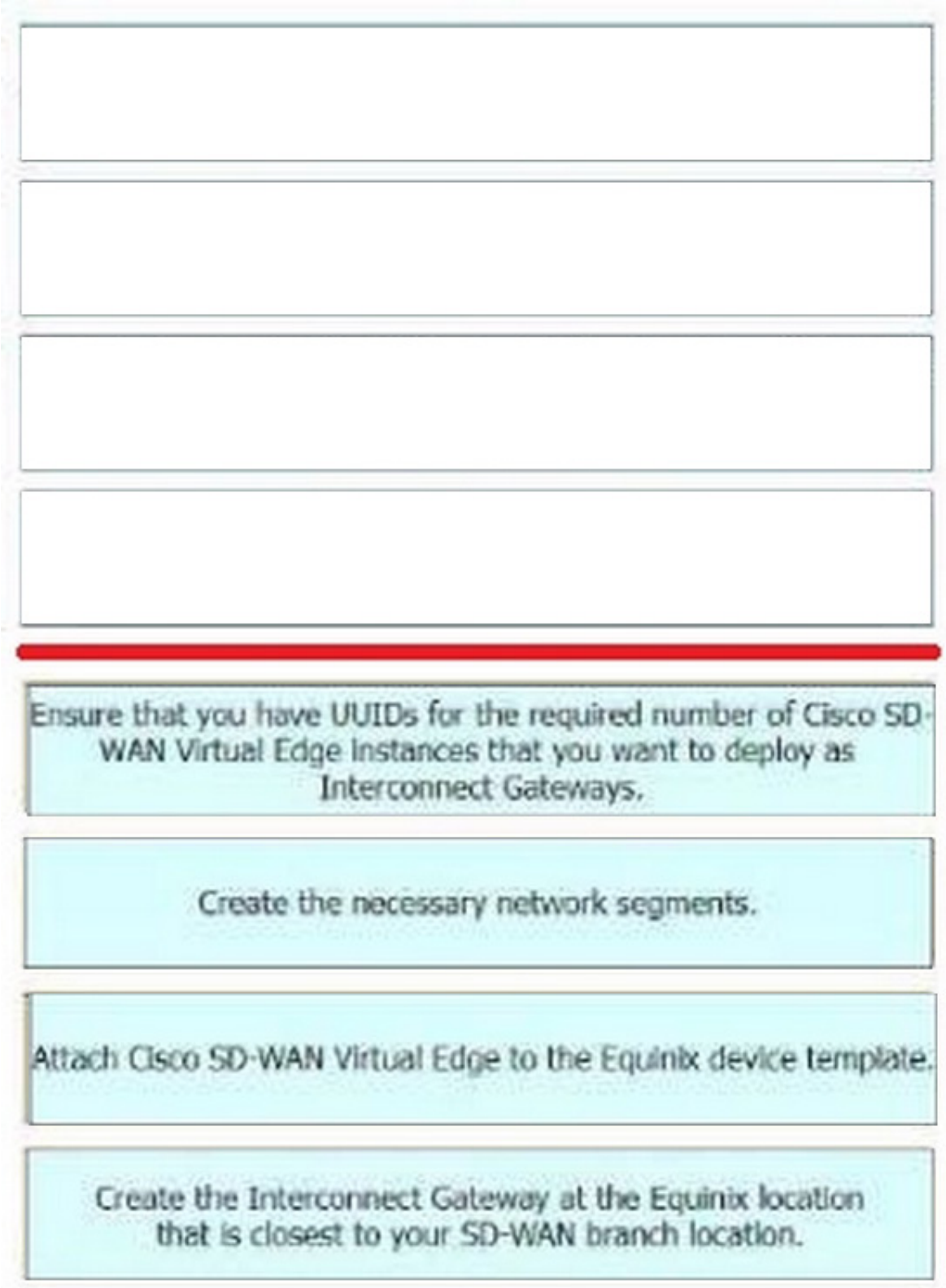
Configure the global settings for Interconnect Gateways.

Drag the prerequisite steps from the left onto the order on the right to configure a Cisco SD-WAN Cloud Interconnect with Equinix

Select and Place:



Correct Answer:



The process of configuring a Cisco SD-WAN Cloud Interconnect with Equinix involves several steps.

Ensure that you have UUIDs for the required number of Cisco SD WAN Virtual Edge instances that you want to deploy as Interconnect Gateways: This is the first step where you ensure that you have the necessary UUIDs for the Cisco SDWAN Virtual Edge instances that you want to deploy.

Create the necessary network segments: After ensuring the availability of UUIDs, you create the necessary network segments.

Attach Cisco SD-WAN Virtual Edge to the Equinix device template: After setting up the network segments, you attach the Cisco SD-WAN Virtual Edge to the Equinix device template.

Create the Interconnect Gateway at the Equinix location that is closest to your SD- WAN branch location: Finally, you create the Interconnect Gateway at the Equinix location that is closest to your SD-WAN branch location.

References:

[Cisco SD-WAN Cloud Interconnect with Equinix]

[Cisco SD-WAN Cloud OnRamp for CoLocation Deployment Guide]

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

Correct Answer: C

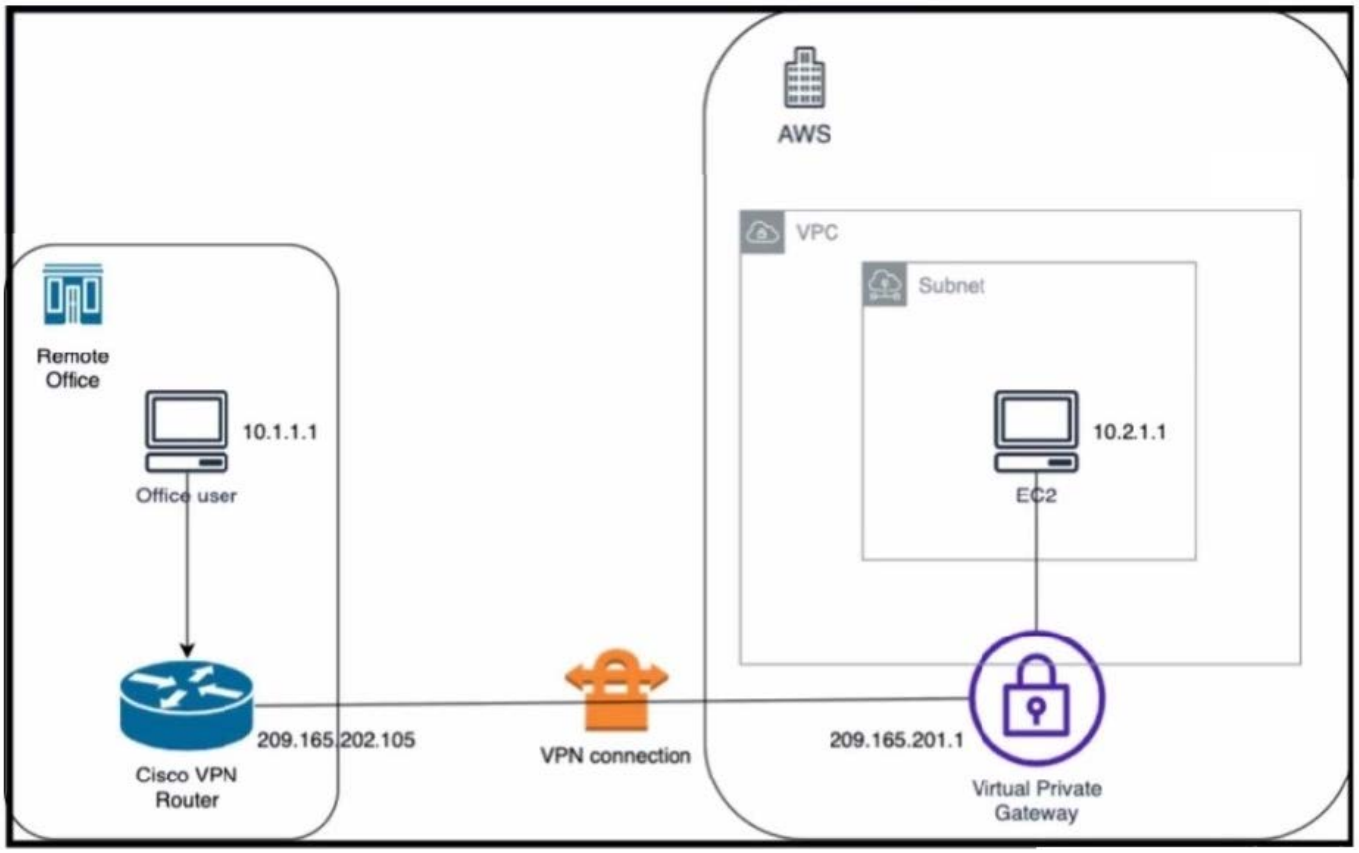
In the given scenario, an engineer is configuring a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router and AWS. The correct command to complete the tunnel configuration is "tunnel source 20.20.20.21". This command specifies the source IP address for the tunnel, which is essential 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 3

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

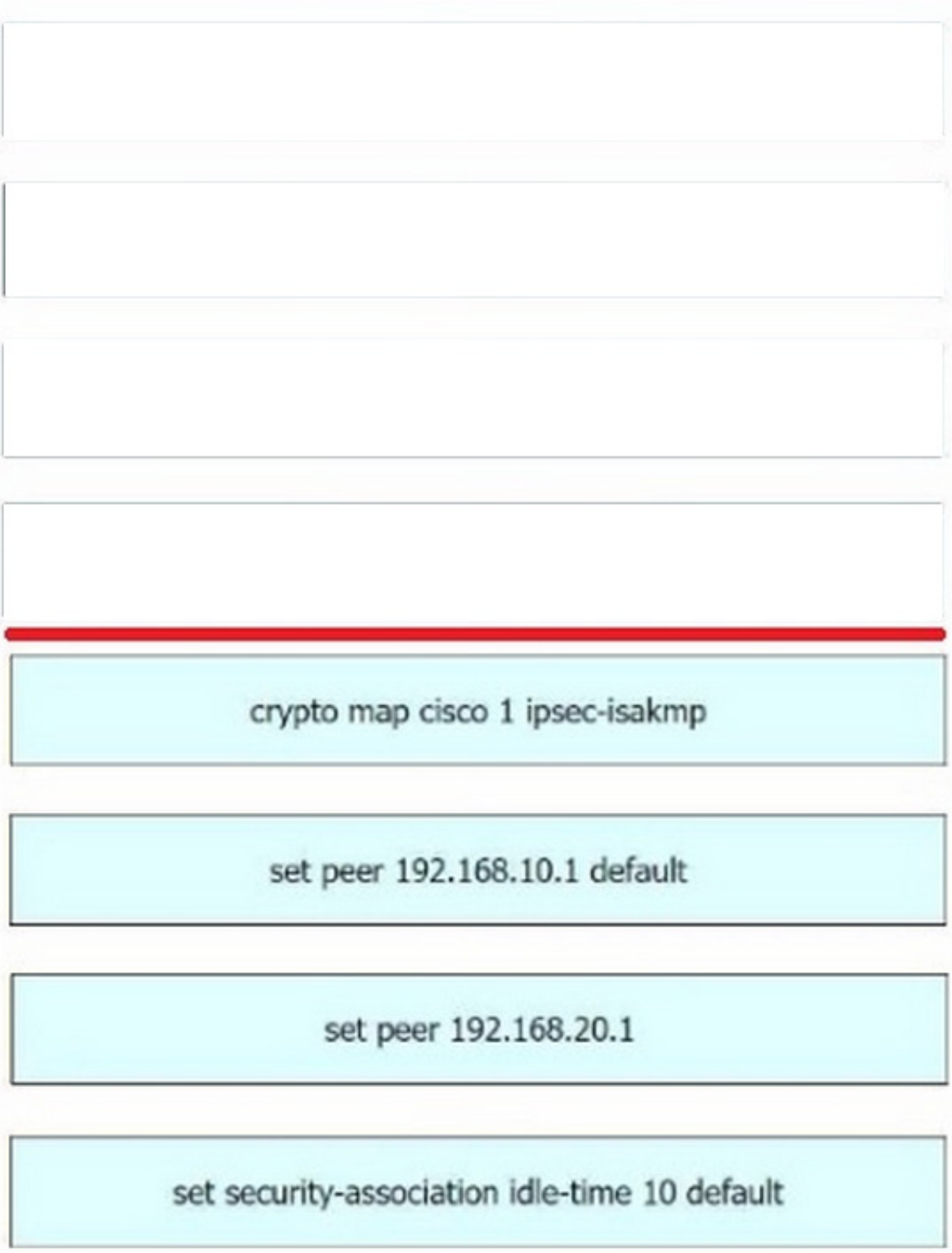
QUESTION 4

DRAG DROP

An engineer must edit the settings of a site-to-site IPsec VPN connection between an on- premises Cisco IOS XE router and Amazon Web Services (AWS). IPsec must be configured to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco. Drag and drop the commands from the left onto the order on the right.

Select and Place:

Correct Answer:



Step 1 = crypto map cisco 1 ipsec-isakmp Step 2 = set peer 192.168.10.1 default Step 3 = set peer 192.168.20.1 Step 4 = set security-association idle-time 120 default

The process of editing the settings of a site-to-site IPsec VPN connection between an on- premises Cisco IOS XE router and Amazon Web Services (AWS), and configuring IPsec to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco involves several steps123456. crypto map cisco 1 ipsec-isakmp: This command is used to create a new entry in the crypto map named "cisco". The "1" is the sequence number of the entry, and "ipsec-isakmp" specifies that the IPSec security associations (SAs) should be established using the

Internet Key Exchange (IKE) protocol13. set peer 192.168.10.1 default: This command is used to specify the IP address of the default peer for the crypto map entry. In this case, the default peer is at IP address 192.168.10.115. set peer 192.168.20.1: This command is used to add an additional peer to the crypto map entry. In this case, the additional peer is at IP address 192.168.20.1. This allows the IPsec VPN to support multiple peers56. set security-association idle-time 120 default: This command is used to set the idle time for the security association. If no traffic is detected over the VPN for the specified idle time (in this case, 120 seconds), the security association is deleted, and the VPN connection fails over to the next peer46.

References: Configure a Site-to-Site IPSec IKEv1 Tunnel Between an ASA and a Cisco IOS Router - Cisco Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community Configuring Site to Site IPSec VPN Tunnel Between Cisco Routers Configure Failover for IPSec Site-to-Site Tunnels with Backup ISP Links on FTD Managed by FMC - Cisco Does Setting Multiple Peers in a Crypto Map Also Support Parallel IPSec Connections - Cisco Community Multiple WAN Connections -- IPsec in Multi-WAN Environments | pfSense Documentation Multiple Set Peer for VPN Failover - Server Fault

QUESTION 5

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

Correct Answer: B

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

[300-440 VCE Dumps](#) [300-440 Practice Test](#) [300-440 Braindumps](#)