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

QUESTION 1

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

Correct Answer: C

According to the FedRAMP Authorization Boundary Guidance document, the method used to create authorization boundary diagrams (ABDs) is to identify all tools as either external orinternal 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.

References: FedRAMP Authorization Boundary Guidance document

QUESTION 2

Refer to the exhibit.

```
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
```

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?

A. wrong ISAKMP policy

B. identity mismatch

C. wrong encryption

D. IKE version mismatch

Correct Answer: B

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.

References: Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services, Topic:Troubleshooting

Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:

Implementing Cloud Connectivity, Lesson 2: Implementing Cisco SD-WAN Cloud OnRamp for IaaS, Topic: Troubleshooting Cisco SD-WAN Cloud OnRamp for IaaS Cisco IOS Security Configuration Guide, Release 15MandT, Chapter:

Configuring IPsec Network Security, Topic: Configuring IPsec Identity and Peer Addressing

---

QUESTION 3

DRAG DROP

An engineer must configure a CLI add-on feature template in Cisco vManage for enhanced policy-based routing (ePBR) for IPv4. These configurations were deleted:

1.

licensing config enable false

2.

licensing config privacy hostname true

3.

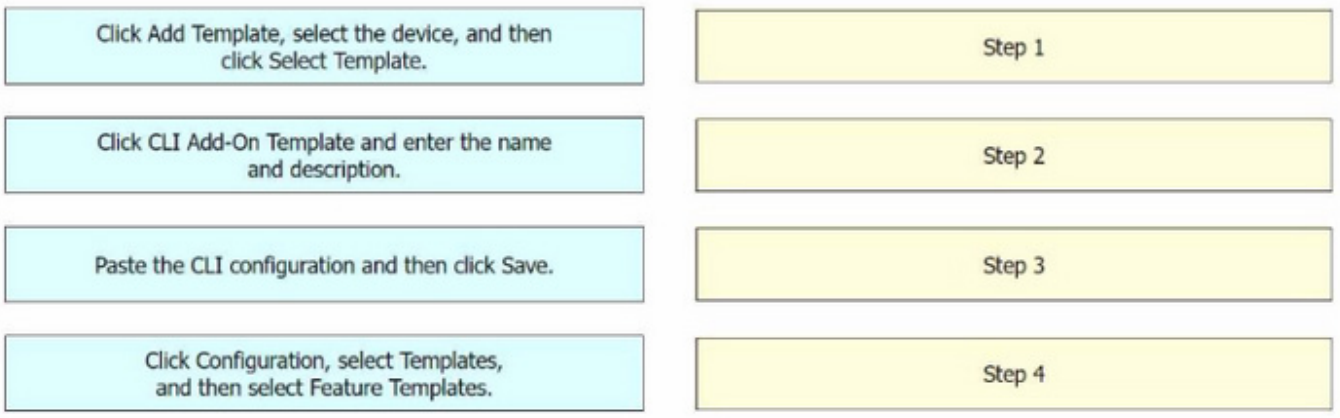
licensing config privacy version false

4.

licensing config utility utility-enable true

Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:

Step 1 = Click Configuration, select Templates, and then select Feature Templates.

Step 2 = Click Add Template, select the device, and then click Select Template.

Step 3 = Click CLI Add-On Template and enter the name and description.

Step 4 = Paste the CLI configuration and then click Save.

The process of configuring a CLI add-on feature template in Cisco vManage for enhanced policy-based routing (ePBR) for IPv4 involves several steps1234. Click Configuration, select Templates, and then select Feature Templates: This is the

first step where you navigate to the Templates section in the Configuration menu of Cisco vManage.

Click Add Template, select the device, and then click Select Template: In this step, you add a new template for the device.

Click CLI Add-On Template and enter the name and description: After setting up the template, you select the CLI Add-On Template option, and then enter the name and description for the template.

Paste the CLI configuration and then click Save: Finally, you paste the CLI configuration into the template and save the changes.

References:

CLI Add-On Feature Templates - Cisco

Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - CLI Add-On Feature Templates Cisco SD-WAN vSmart CLI Template - NetworkLessons.com CLI Templates for Cisco XE

SD-WAN Routers

QUESTION 4

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 CloudFrontfor caching and distributing content globally and uses HTTPS for secure data transfer.

Correct Answer: A

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. The other options are not correct because they do not establish internet-based connectivity between on-premises networks and AWS cloud resources. Option B relies on AWS Elastic Load Balancing (ELB) for traffic distribution and uses SSL/TLS encryption for secure data transmission. However, ELB is a service that distributes incoming traffic across multiple targets within a VPC, not across different networks. Option C employs AWS Direct Connect for a dedicated network connection and uses private IP addresses for secure communication. However, AWS Direct Connect is a service that establishes a private connection between on-premises networks and AWS, bypassing the public internet. Option D uses Amazon CloudFront for caching and distributing content globally and uses HTTPS for secure data transfer. However, Amazon CloudFront is a service that delivers static and dynamic web content to end users, not to on-premises networks.

References:

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

2: Cisco ASA Site-to-Site VPN

3: What Is Elastic Load Balancing?

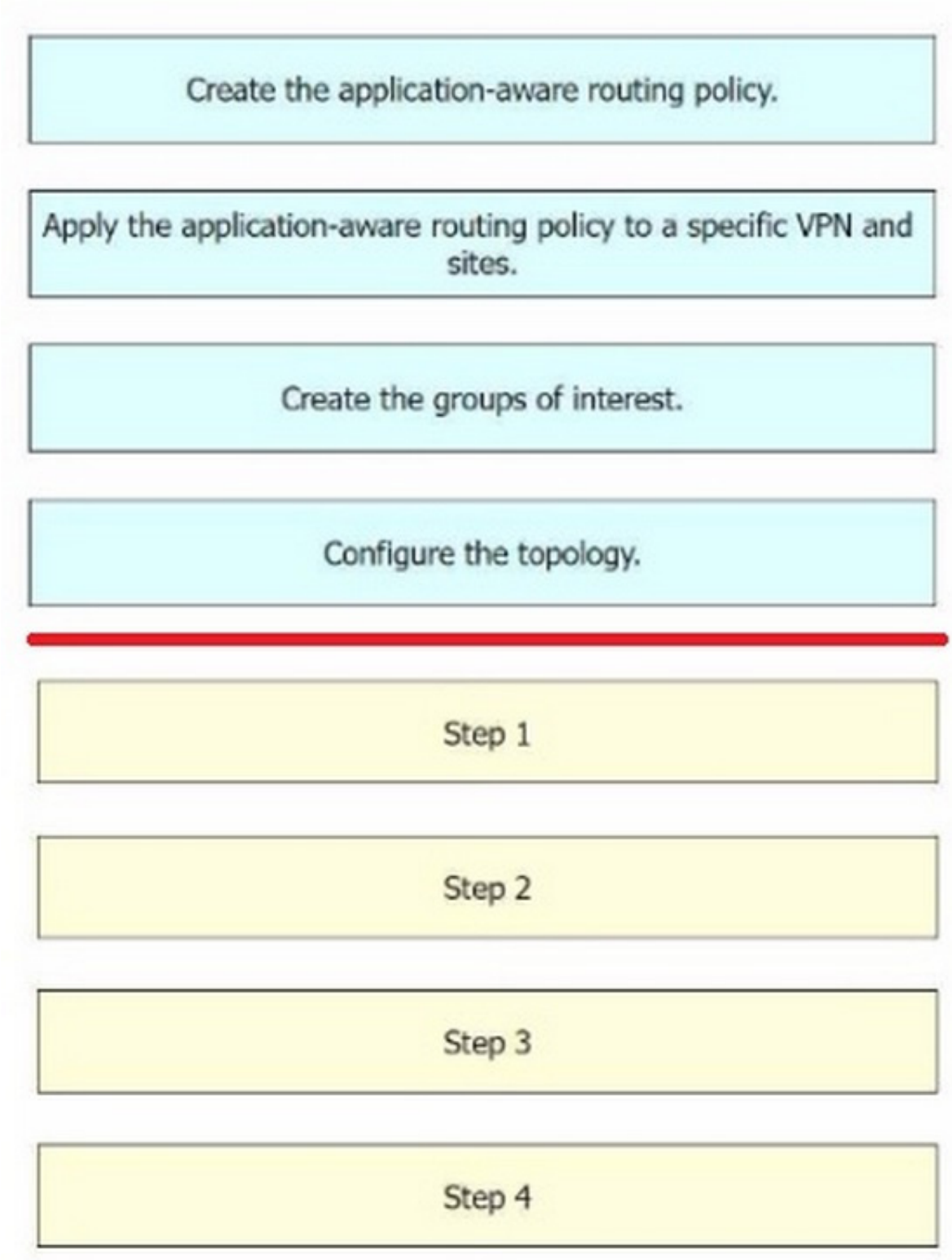
4: What is AWS Direct Connect?

QUESTION 5

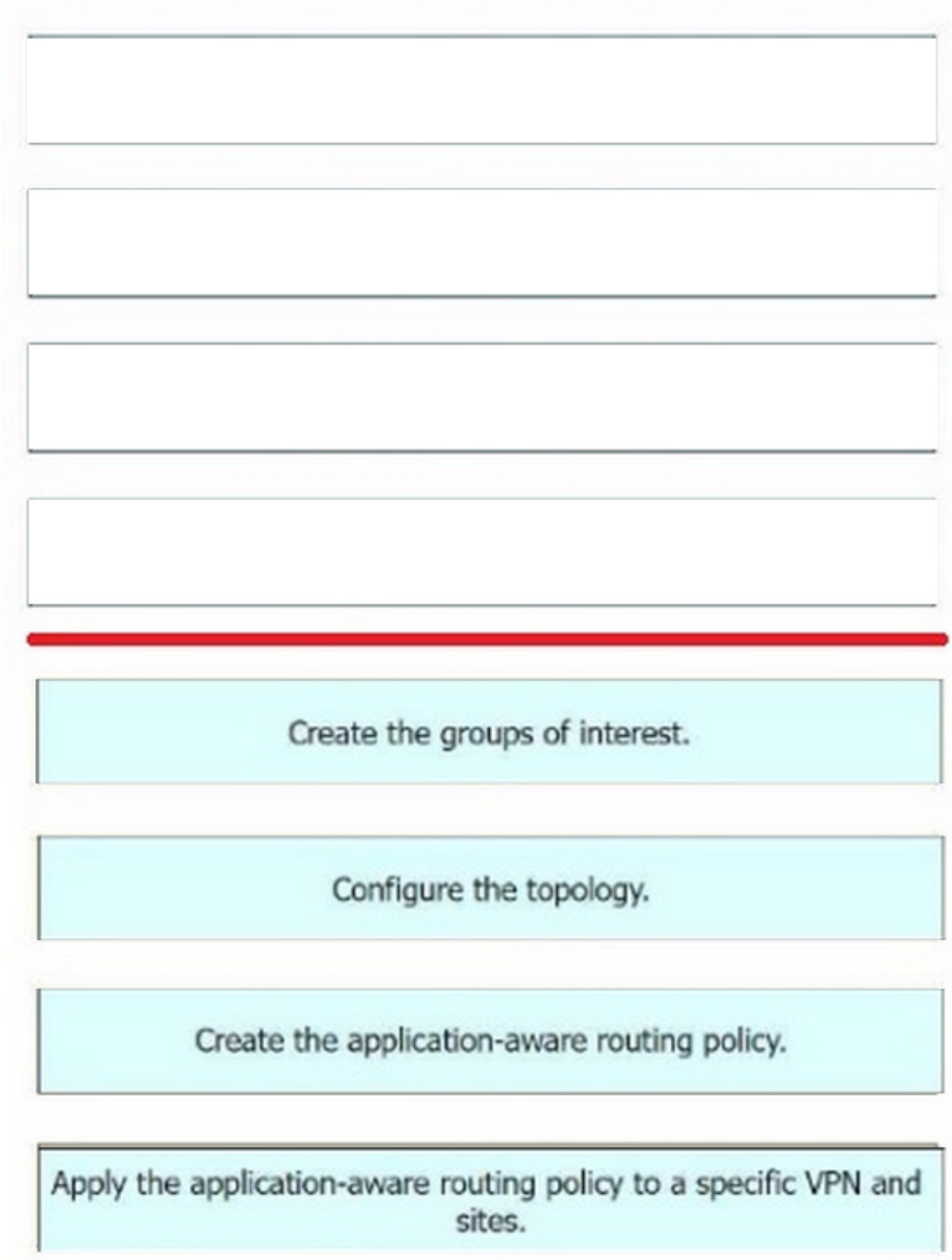
DRAG DROP

An engineer must use Cisco vManage to configure an application-aware routing policy Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:



Step 1 = Create the groups of interest.

Step 2 = Configure the topology.

Step 3 = Create the application-aware routing policy.

Step 4 = Apply the application-aware routing policy to a specific VPN and sites.

The process of configuring an application-aware routing policy in Cisco vManage involves several steps.

Create the groups of interest: This is the first step where you define the applications or groups that the policy will affect. Configure the topology: This involves setting up the network topology that the policy will operate within.

Create the application-aware routing policy: After setting up the groups and topology, you then create the application-aware routing policy. This policy tracks network and path characteristics of the data plane tunnels between Cisco SD-WAN

devices and uses the collected information to compute optimal paths for data traffic.

Apply the application-aware routing policy to a specific VPN and sites: Finally, the created policy is applied to a specific VPN and sites. This allows the policy to affect the desired network traffic.

References:

Designing and Implementing Cloud Connectivity (ENCC) v1.0 Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300- 440)

Information About Application-Aware Routing - Cisco Configuring Application-Aware Routing (AAR) Policies | NetworkAcademy.io Policies Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12