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

Which approach does a centralized internet gateway use to provide connectivity to SaaS applications?

A. A cloud-based proxy server routes traffic from the on-premises infrastructure to the SaaS provider data center.

B. Internet traffic from the on-premises infrastructure is routed through a centralized gateway that provides access controls for SaaS applications.

C. VPN connections are used to provide secure access to SaaS applications from the on- premises infrastructure.

D. A dedicated, private connection is established between the on-premises infrastructure and the SaaS provider data center using colocation services.

Correct Answer: B

A centralized internet gateway is a network design that routes all internet- bound traffic from the on-premises infrastructure through a single point of egress, typically located at the data center or a regional hub1. This approach allows the enterprise to apply consistent security policies and access controls for SaaS applications, as well as optimize the bandwidth utilization and performance of the WAN links. A centralized internet gateway can use various technologies to provide connectivity to SaaS applications, such as proxy servers, firewalls, web filters, and WAN optimizers. However, a cloud-based proxy server (option A) is not a part of the centralized internet gateway, but rather a separate service that can be used to route traffic from the on-premises infrastructure to the SaaS provider data center4. VPN connections (option C) and dedicated, private connections (option D) are also not related to the centralized internet gateway, but rather alternative ways of providing secure and reliable access to SaaS applications from the on- premises infrastructure5. Therefore, the correct answer is option B, which describes the basic function of a centralized internet gateway.

QUESTION 2

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.

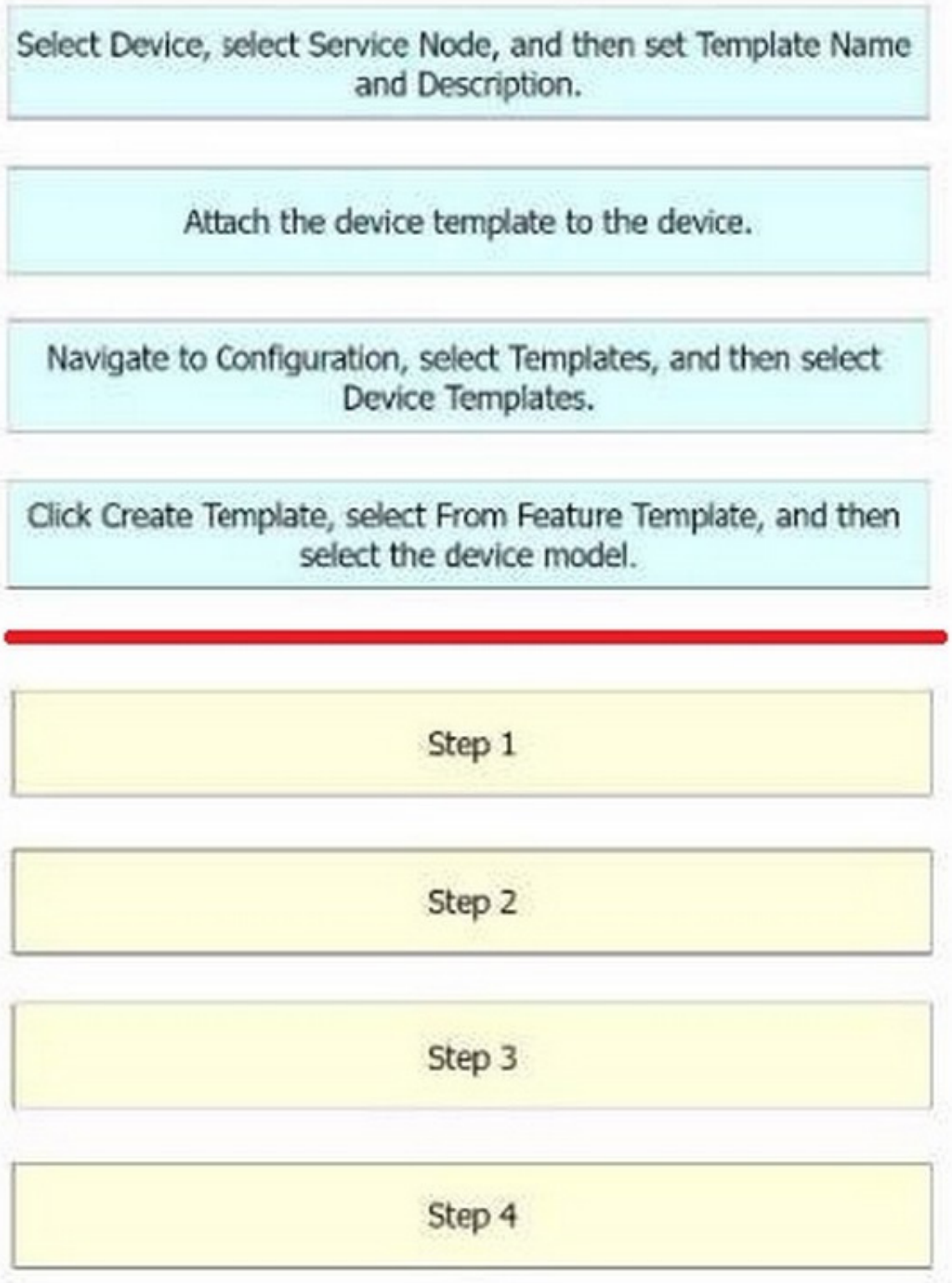
References: FedRAMP Authorization Boundary Guidance document

QUESTION 3

DRAG DROP

An engineer must configure an AppGoE service node for WAN optimization for applications that are hosted in the cloud using Cisco vManage for C8000V or C8500L-8S4X devices. 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 = Navigate to Configuration, select Templates, and then select Device Templates.

Step 2 = Click Create Template, select From Feature Template, and then select the device model.

Step 3 = Select Device, select Service Node, and then set Template Name and Description.

Step 4 = Attach the device template to the device.

The process of configuring an AppGoE service node for WAN optimization for applications that are hosted in the cloud using Cisco vManage for C8000V or C8500L-8S4X devices involves several steps.

Navigate to Configuration, select Templates, and then select Device Templates:

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

Click Create Template, select From Feature Template, and then select the device model: In this step, you create a new template for the device model from the feature template.

Select Device, select Service Node, and then set Template Name and Description:

After setting up the template, you select the device and the service node, and then set the template name and description.

Attach the device template to the device: Finally, you attach the created device template to the device.

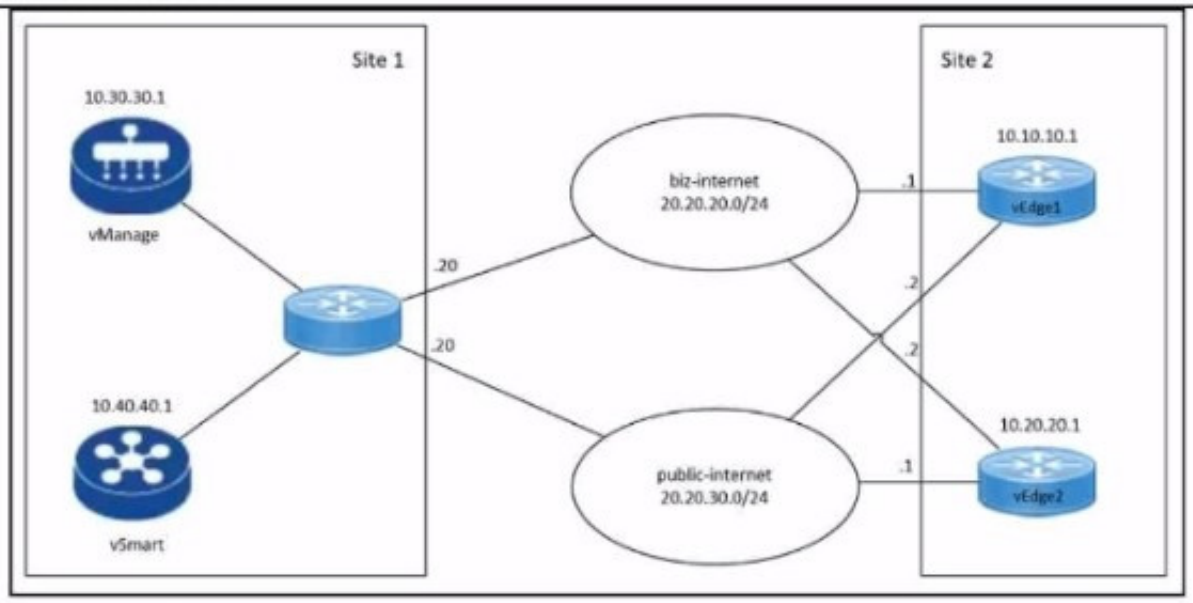
References:

AppQoE - Step-by-Step Configuration - Cisco Community Cisco Catalyst SD-WAN AppQoE Configuration Guide, Cisco IOS XE Catalyst SD- WAN Release 17.x

QUESTION 4

Refer to the exhibit.

```
local7.debug: Mar 11 11:31:11 VEDGE-1 VDAEMON[1136]: vdaemon_disable_my_tloc[1308]:
%VDAEMON_DBG_EVENTS-1: Disabling tloc ge0_1.
local7.info: Mar 11 11:31:11 VEDGE-1 VDAEMON[1136]: %Viptela-VEDGE-1-vdaemon-6-INFO-1400002:
Notification:
 3/11/2023 11:31:11 control-connection-state-change severity-level:major host-name:"VEDGE-1"
 system-ip:10.10.10.1
 personality:vEdge peer-type:vmanage peer-system-ip:10.30.30.1 peer-vmanage-system-ip:0.0.0.0
 public-ip:20.20.20.20
 public-port:12947 src-color:biz-internet remote-color:public-internet uptime:"0:01:36:34" new-
 state:down
local7.info: Mar 11 11:31:11 VEDGE-1 FTMD[1126]: %Viptela-VEDGE-1-ftmd-6-INFO-1400002:
Notification:
 3/11/2023 11:31:11 bfd-state-change severity-level:major host-name:"VEDGE-1" system-
 ip:10.10.10.1 src-ip:20.20.30.2
dst-ip:20.20.30.20   proto:ipsec src-port:12406 dst-port:12347 local-system-ip:10.10.10.1 local-
color:"biz-internet"
  emote-system-ip:10.10.10.4 remote-color:"public-internet" new-state:down deleted:false flap-
  reason:bfd-deleted
```



An engineer troubleshoots a Cisco SD-WAN connectivity issue between an on-premises data center WAN Edge and a public cloud provider WAN Edge. The engineer discovers that BFD is Dapping on vEdge1. What is the problem?

A. The remote Edge device BFD is down.

B. The remote Edgedevice failed to respond BFD keepalives.

C. The remote Edge device has a duplicate IP address.

D. The control plane deleted the BFD session.

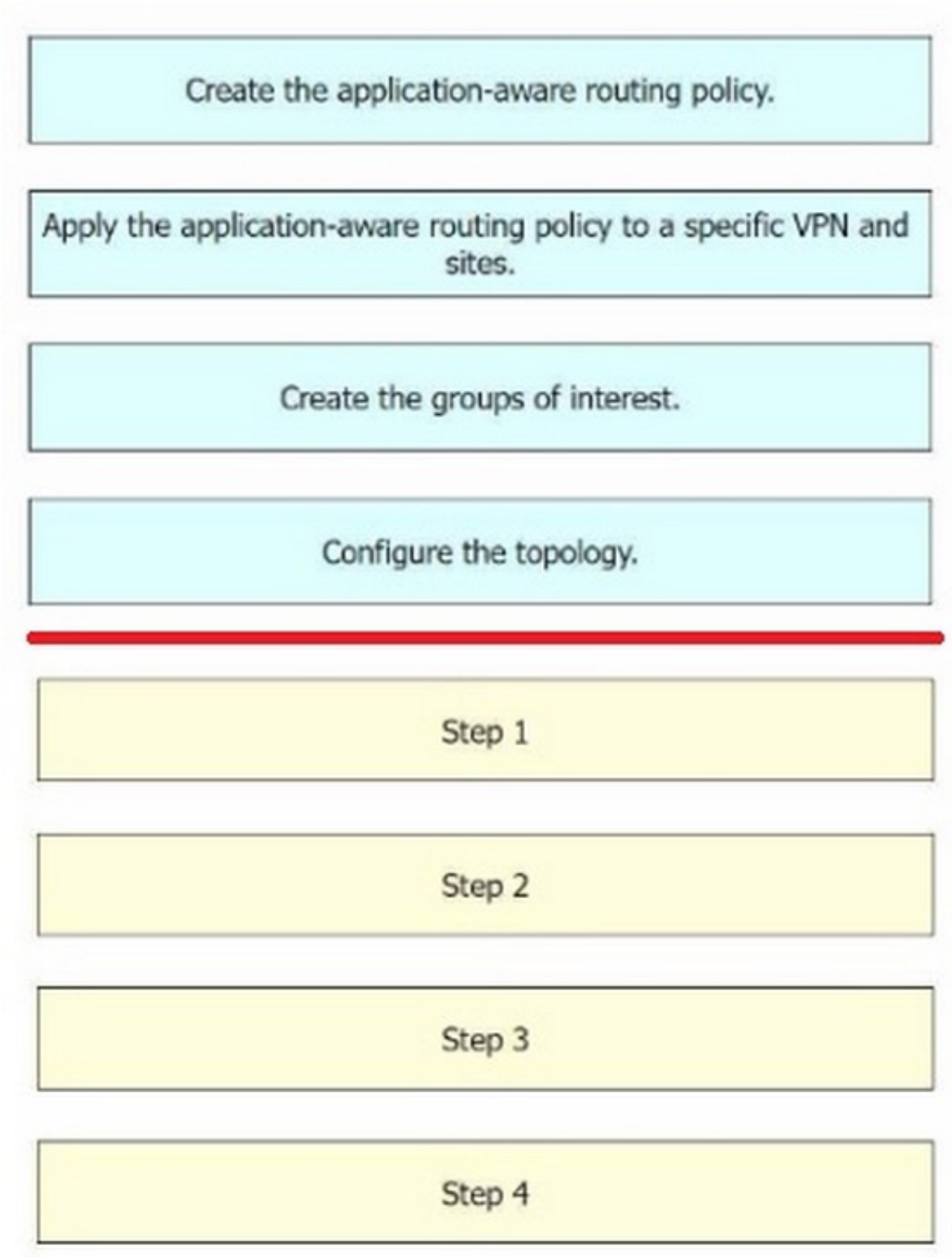
Correct Answer: B

QUESTION 5

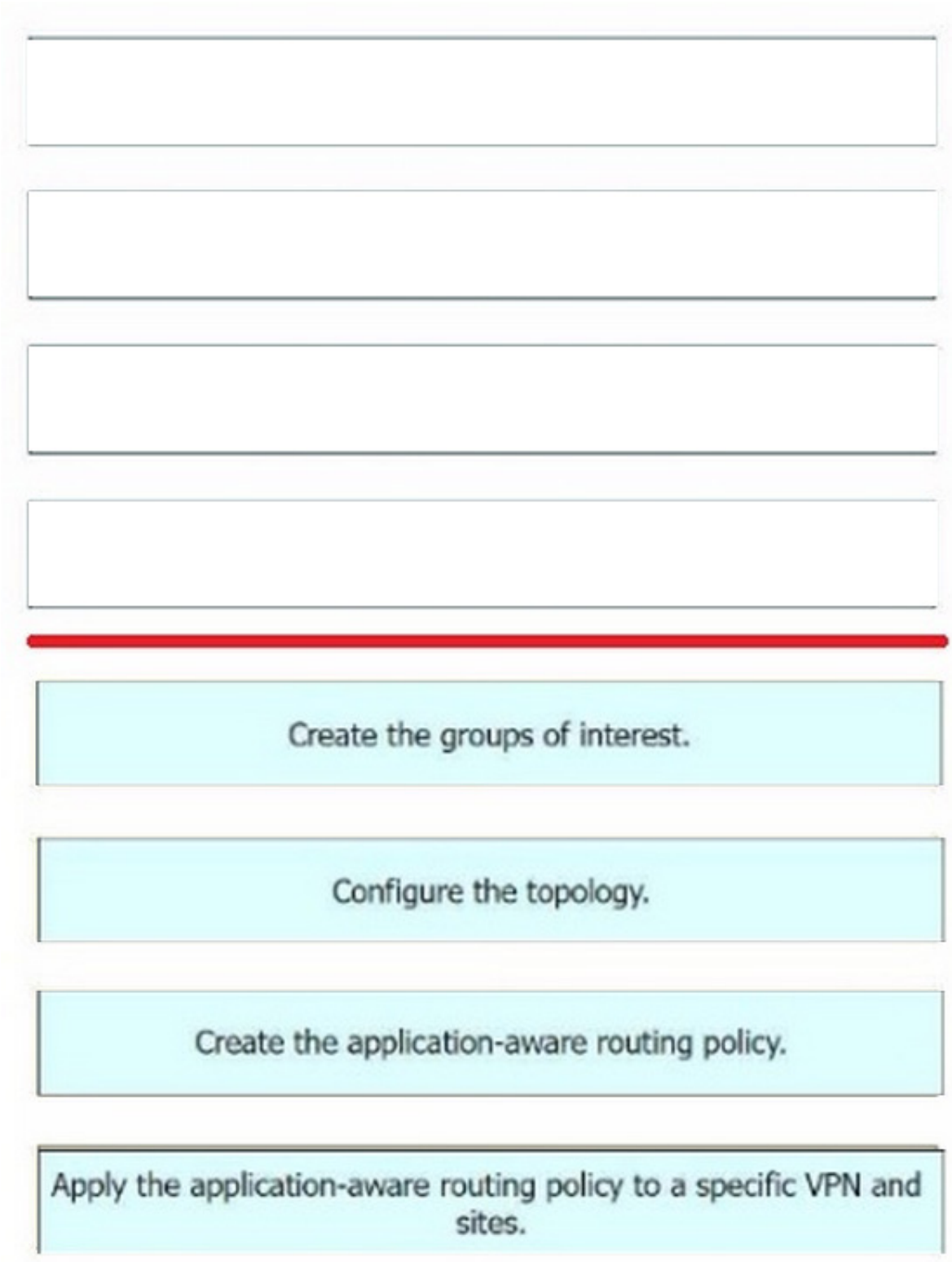
DRAG DROP

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