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.pass4itsure.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 Microsoft Azure service enables a dedicated and secure connection between an on- premises infrastructure and Azure data centers through a colocation provider?

A. Azure Private Link

B. Azure ExpressRoute

C. Azure Virtual Network

D. Azure Site-to-Site VPN

Correct Answer: B

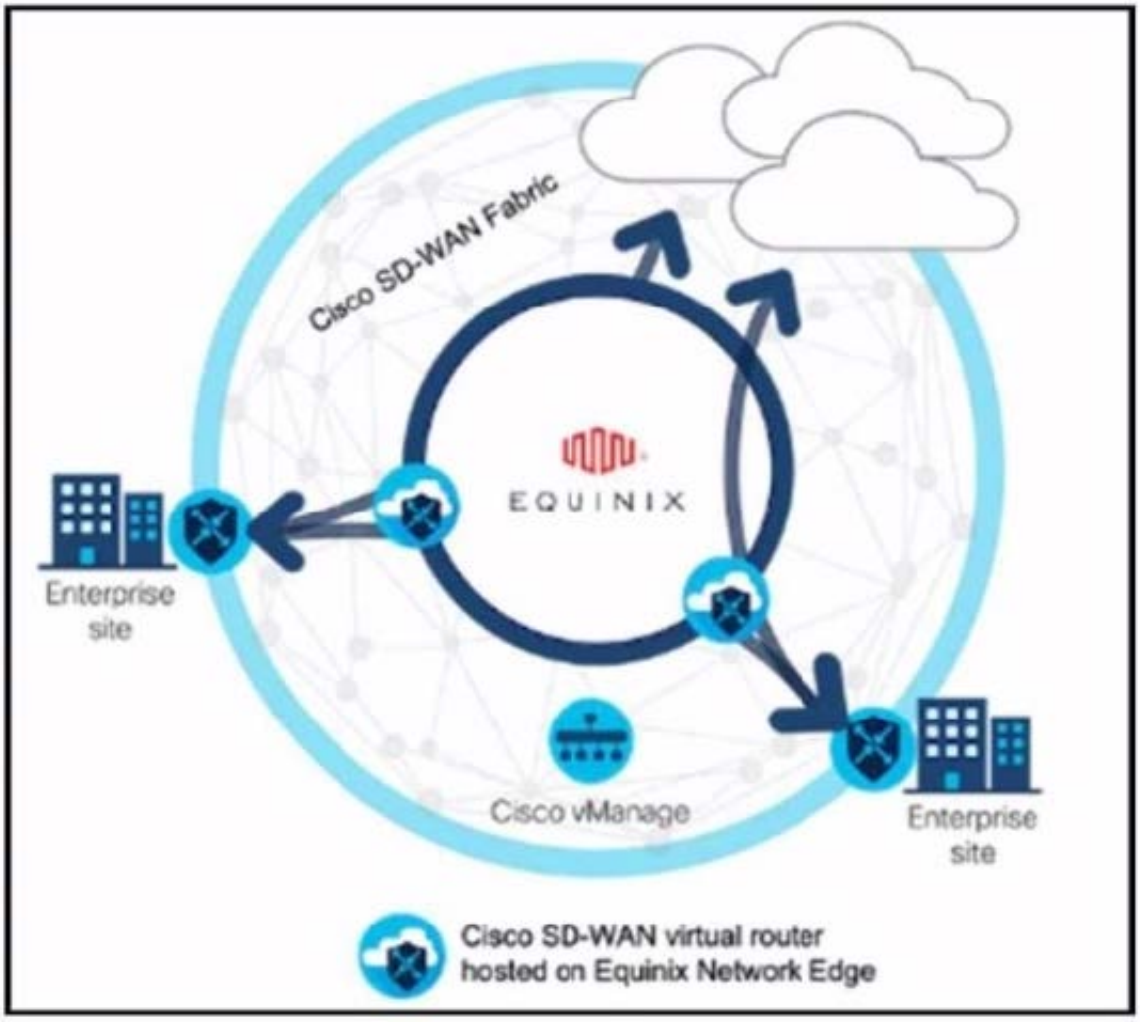
Azure ExpressRoute is a service that enables a dedicated and secure connection between an on-premises infrastructure and Azure data centers through a colocation provider. A colocation provider is a third-party data center that offers network connectivity services to multiple customers. Azure ExpressRoute allows customers to bypass the public internet and connect directly to Azure services, such as virtual machines, storage, databases, and more. This provides benefits such as lower latency, higher bandwidth, more reliability, and enhanced security. Azure ExpressRoute also supports hybrid scenarios, such as connecting to Office 365, Dynamics 365, and other SaaS applications hosted on Azure. Azure ExpressRoute requires a physical connection between the customer\\'s network and the colocation provider\\'s network, as well as a logical connection between the customer\\'s network and the Azure virtual network. The logical connection is established using a Border Gateway Protocol (BGP) session, which exchanges routing information between the two networks. Azure ExpressRoute supports two models: standard and premium. The standard model offers connectivity to all Azure regionswithin the same geopolitical region, while the premium model offers connectivity to all Azure regions globally, as well as additional features such as increased route limits, global reach, and Microsoft peering.

References: Designing and Implementing Cloud Connectivity (ENCC) v1.0, Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300-440) Exam Prep, ENCC | Designing and Implementing Cloud Connectivity | Netec

QUESTION 2

DRAG DROP

Refer to the exhibit.



These configurations are complete:

1.

Create an account in the Equinix portal.

2.

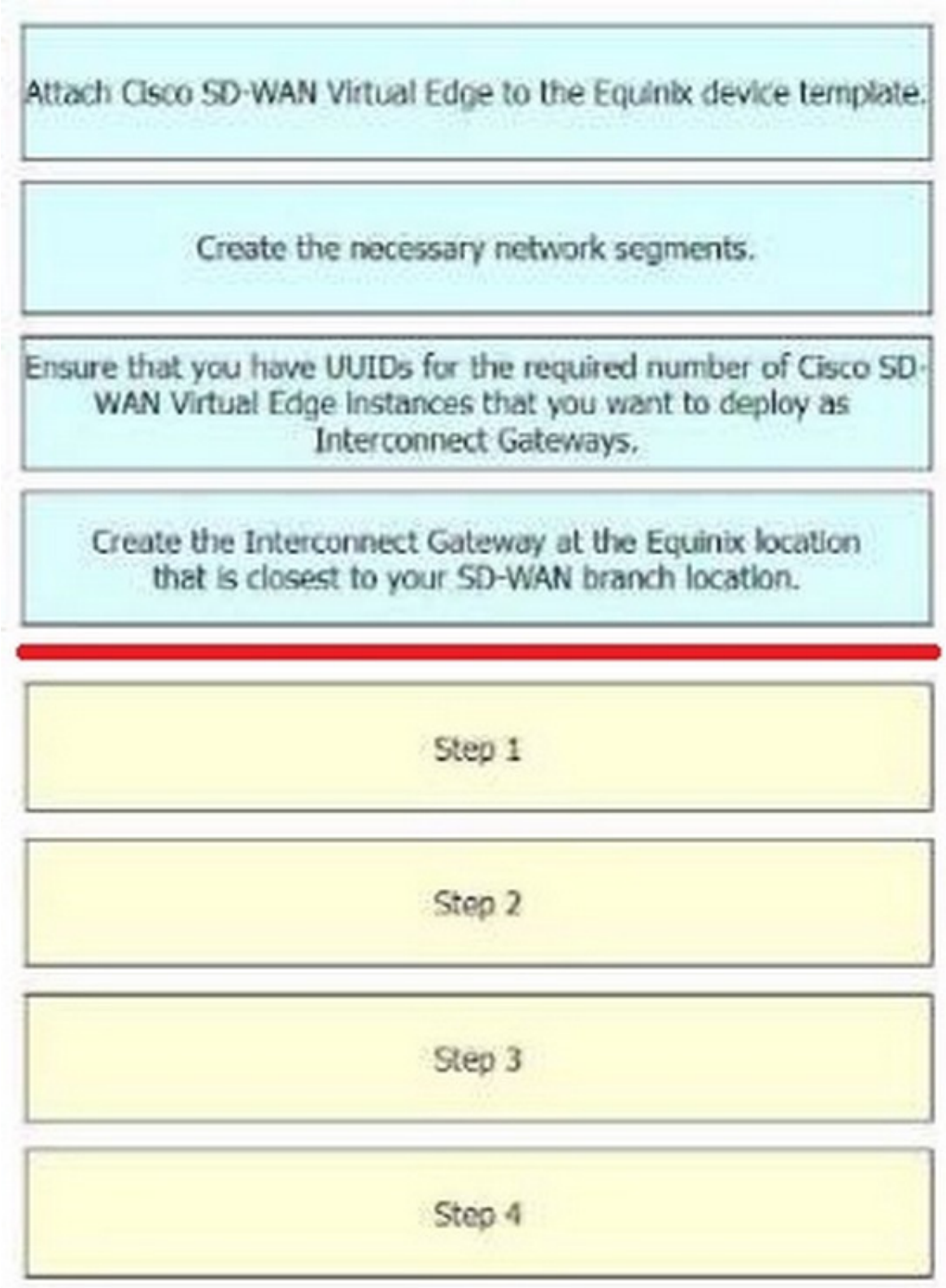
Associate the Equinix account with Cisco vManage.

3.

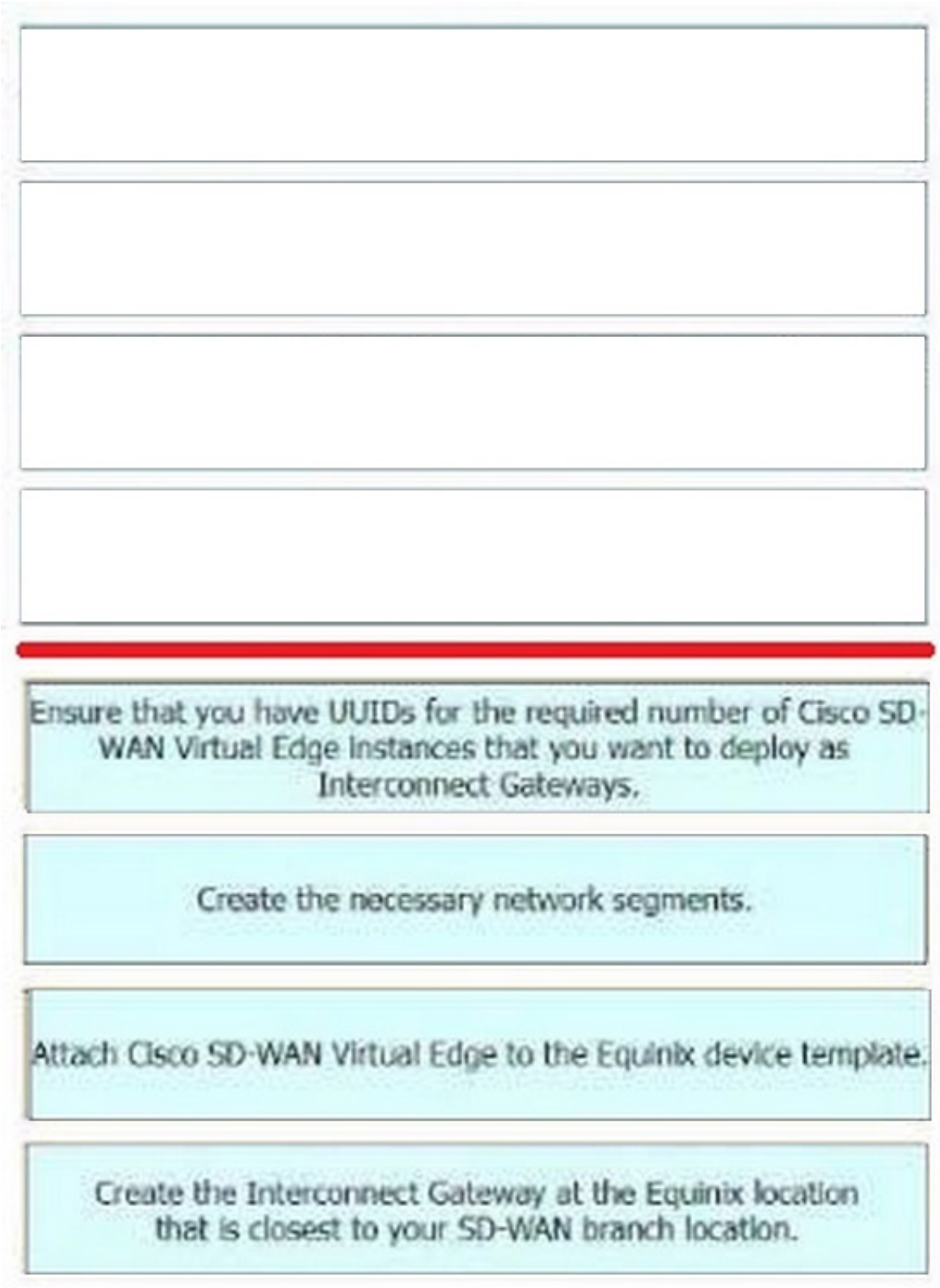
Configure the global settings for Interconnect Gateways.

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:

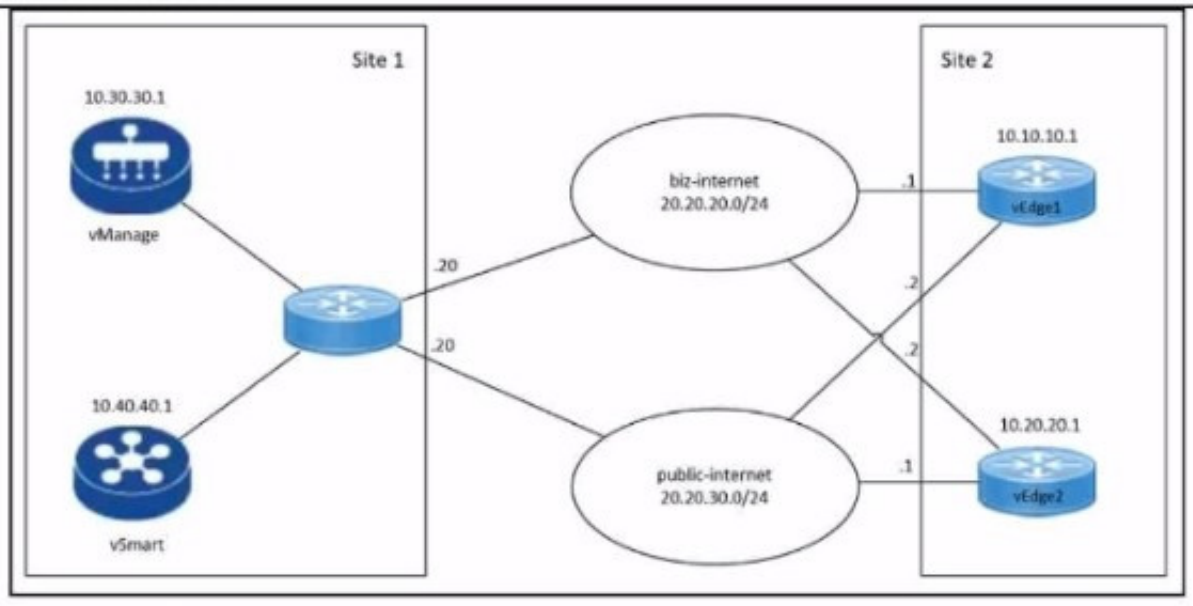
[Cisco SD-WAN Cloud Interconnect with Equinix]

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

QUESTION 3

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.

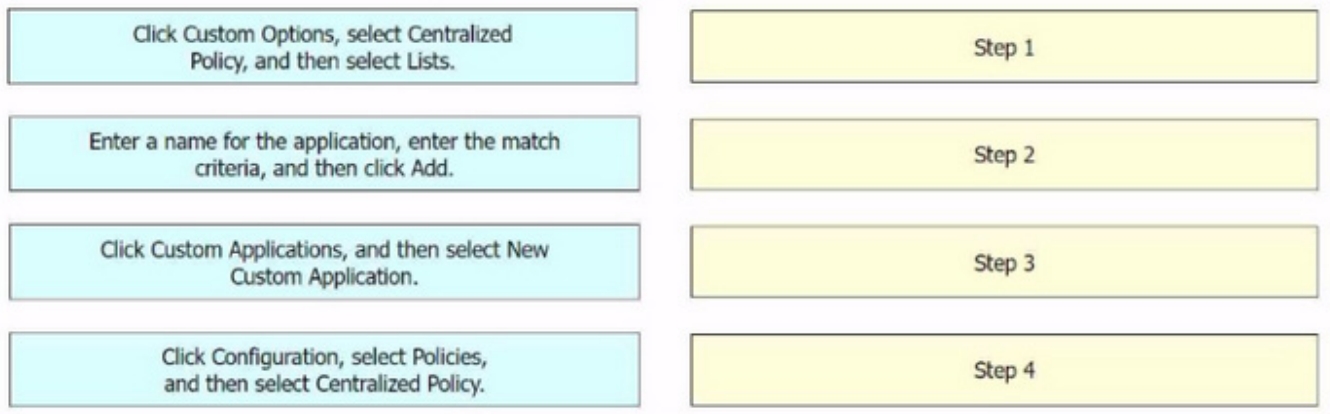
Correct Answer: B

QUESTION 4

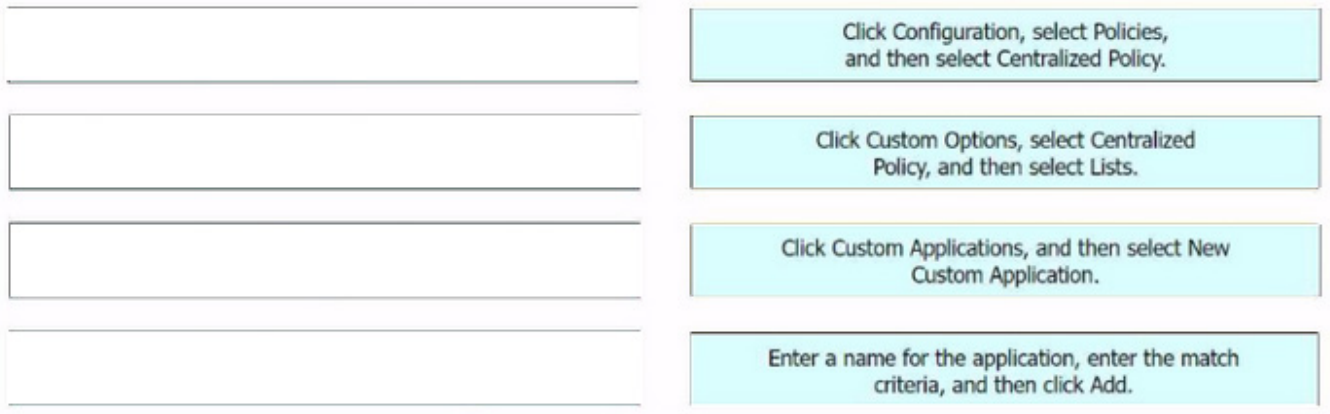
DRAG DROP

An engineer signs in to Cisco vManage and needs to configure a custom application with a Cisco SD-WAN centralized policy. Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:



The process of configuring a custom application with a Cisco SD-WAN centralized policy using Cisco vManage involves several steps.

Click Configuration, select Policies, and then select Centralized Policy: This is the first step where you navigate to the Policies section in the Configuration menu of Cisco vManage.

Click Custom Options, select Centralized Policy, and then select Lists: In this step, you select the Custom Options, then select Centralized Policy, and finally select Lists.

Click Custom Applications, and then select New Custom Application: After setting up the Lists, you click on Custom Applications and then select New Custom Application.

Enter a name for the application, enter the match criteria, and then click Add:

Finally, you enter a name for the application, specify the match criteria, and then click Add to complete the configuration.

References:

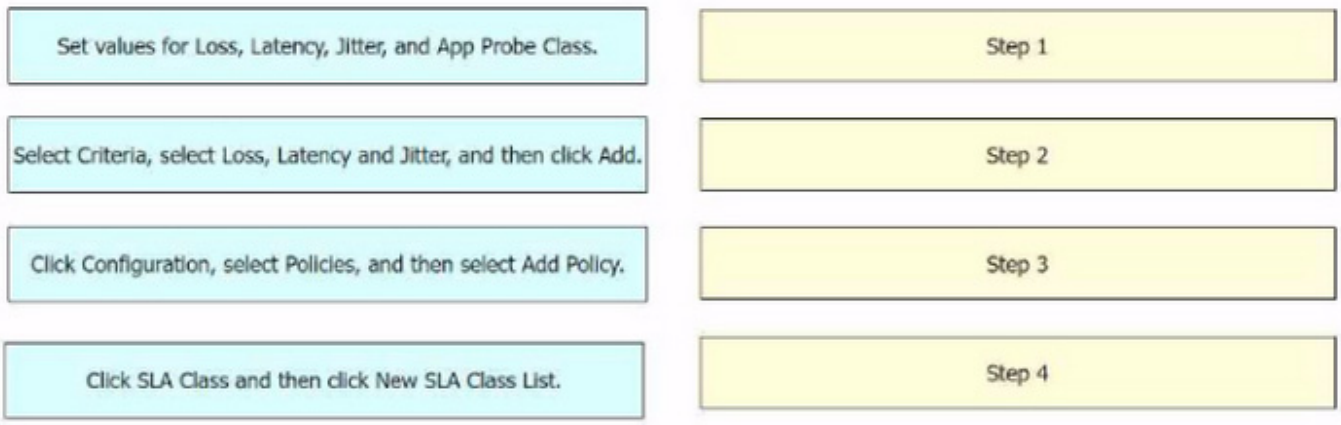
Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE

QUESTION 5

DRAG DROP

An engineer must use Cisco vManage to configure an SLA class to specify the maximum packet loss, packet latency, and jitter allowed on a connection. Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:

The process of configuring an SLA class to specify the maximum packet loss, packet latency, and jitter allowed on a connection using Cisco vManage involves several steps. Click Configuration, select Policies, and then select Add Policy:

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

Click SLA Class and then click New SLA Class List: In this step, you create a new SLA Class List.

Select Criteria, select Loss, Latency and Jitter, and then click Add: After setting up the SLA Class List, you select the criteria for the SLA class. In this case, the criteria are Loss, Latency, and Jitter.

Set values for Loss, Latency, Jitter, and App Probe Class: Finally, you set the values for Loss, Latency, Jitter, and App Probe Class.

References:

Information About Application-Aware Routing - Cisco Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Release