HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **300-440**

Title : Designing and Implementing Cloud Connectivity

Version : DEMO

1.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

Answer: B

Explanation:

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.

Reference: = 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 15M&T, Chapter: Configuring IPsec Network Security, Topic: Configuring IPsec Identity and Peer Addressing

2.Refer to the exhibit.

```
vedge1# show policy from-vsmart
apply-policy
 site-list site1
  control-policy prefer_local out
 !
 policy
  lists
   site-list site1
    site-id 100
   tloc-list prefer_site1
     tloc 10.1.1.1 color mpls encap ipsec preference 100
   control-policy prefer_local
    sequence 10
     match route
      site-list site1
    !
    action accept
     set
       tloc-list prefer_site1
```

A network engineer discovers that the policy that is configured on an on-premises Cisco WAN edge router affects only the route tables of the specific devices that are listed in the site list.
What is the problem?
A. An inbound policy must be applied.
B. The action must be set to deny
C. A localized data policy must be configured.
D. A centralized data policy must be configured
Answer: D
Explanation:
A centralized data policy is a policy that is applied to all devices in the overlay network, regardless of the site list. A localized data policy is a policy that is applied only to the devices that are listed in the site list. In this case, the network engineer wants to apply the policy to all devices in the overlay network, not just the specific devices in the site list. Therefore, a centralized data policy must be configured on the on-premises Cisco WAN edge router.
Reference: = Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3: Implementing Cloud Connectivity, Lesson 3: Implementing Cisco SD-WAN Cloud OnRamp for Colocation, Topic: Centralized Data Policy [Cisco SD-WAN Cloud OnRamp for Colocation Deployment Guide], Chapter: Configuring Centralized Data Policy

3.A company with multiple branch offices wants a connectivity model to meet its network architecture requirements. The company focuses on ensuring low latency and efficient routing for its critical business applications.
Which connectivity model meets these requirements?

A. hub-and-spoke topology with SD-WAN technology, using dynamic routing and OSPF as the routing protocol
B. fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol
C. point-to-point topology using dedicated leased lines and static routing
D. star topology with internet-based VPN connections and static routing

Answer: B

Explanation:

A fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol, meets the requirements of the company because it provides the following benefits:

It allows direct and secure connectivity between any two branch offices, without the need for a central hub or intermediary devices12. This reduces the latency and improves the performance of the critical business applications.

It leverages SD-WAN technology to optimize the traffic flow and application quality of service (QoS) across the WAN13. SD-WAN can dynamically select the best path for each application based on the network conditions and policies13. SD-WAN can also provide redundancy, security, and visibility for the WAN13.

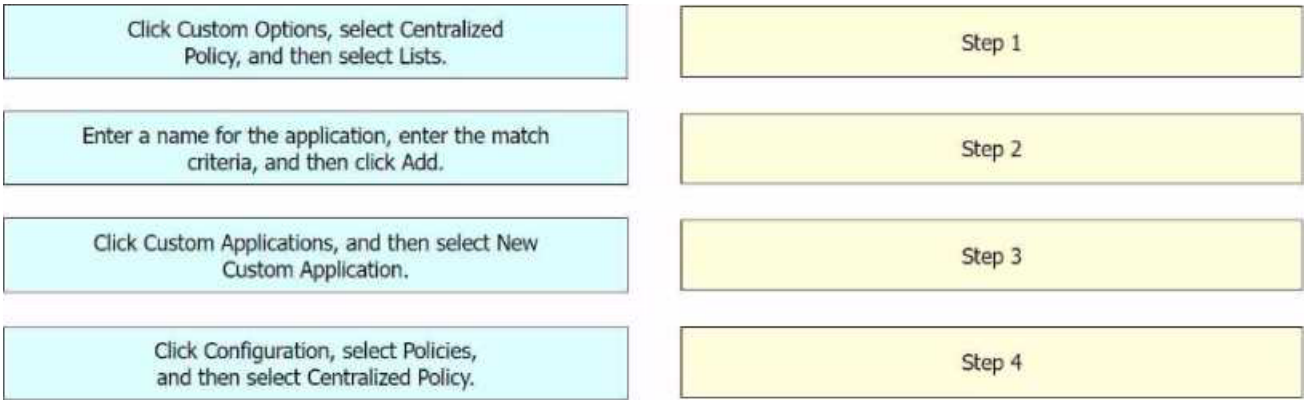
It uses dynamic routing and BGP as the routing protocol to exchange routing information and establish connectivity between the branch offices14. BGP is a scalable and flexible protocol that can support multiple address families, such as IPv4 and IPv6, and multiple routing policies, such as local preference and route filtering14. BGP can also enable seamless integration with the cloud service providers (CSPs) and internet service providers (ISPs)14.

Reference: = 1: Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5) (Cisco U. login required) 2: Cisco SD-WAN Design Guide

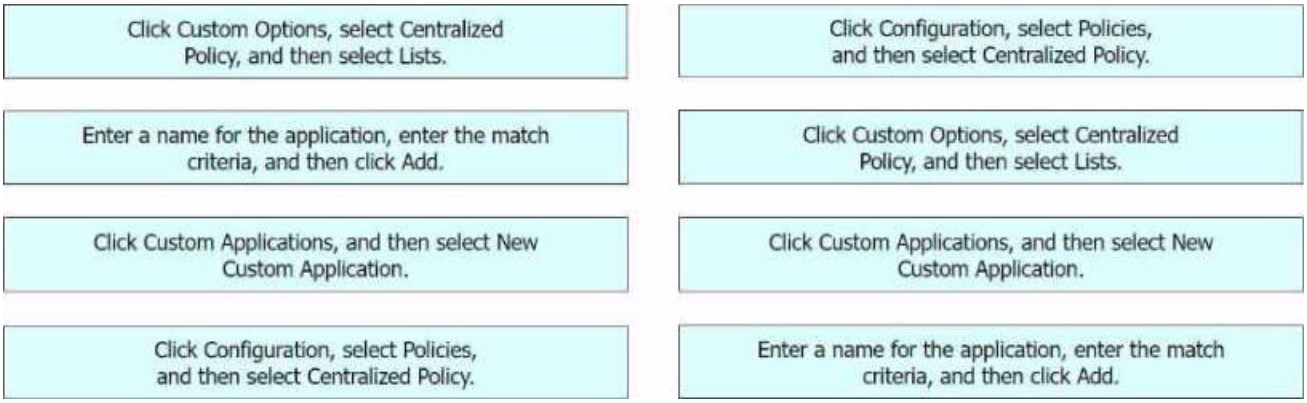
4.DRAG DROP

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.



Answer:



Explanation:

To configure a custom application with Cisco SD-WAN centralized policy, you need to follow these steps25:

Click Configuration, select Policies, and then select Centralized Policy.

Click Custom Options, select Centralized Policy, and then select Lists.

Click Custom Applications, and then select New Custom Application.

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

The process of configuring a custom application with a Cisco SD-WAN centralized policy using Cisco vManage involves several steps1.

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 vManage1.

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 Lists1.

Click Custom Applications, and then select New Custom Application: After setting up the Lists, you click on Custom Applications and then select New Custom Application1.

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 configuration1.

Reference: = Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE

5.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

Answer: B

Explanation:

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 regions within 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.
Reference: 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