Vendor: Cisco

Exam Code:300-440

Exam Name: Designing and Implementing Cloud Connectivity (ENCC)

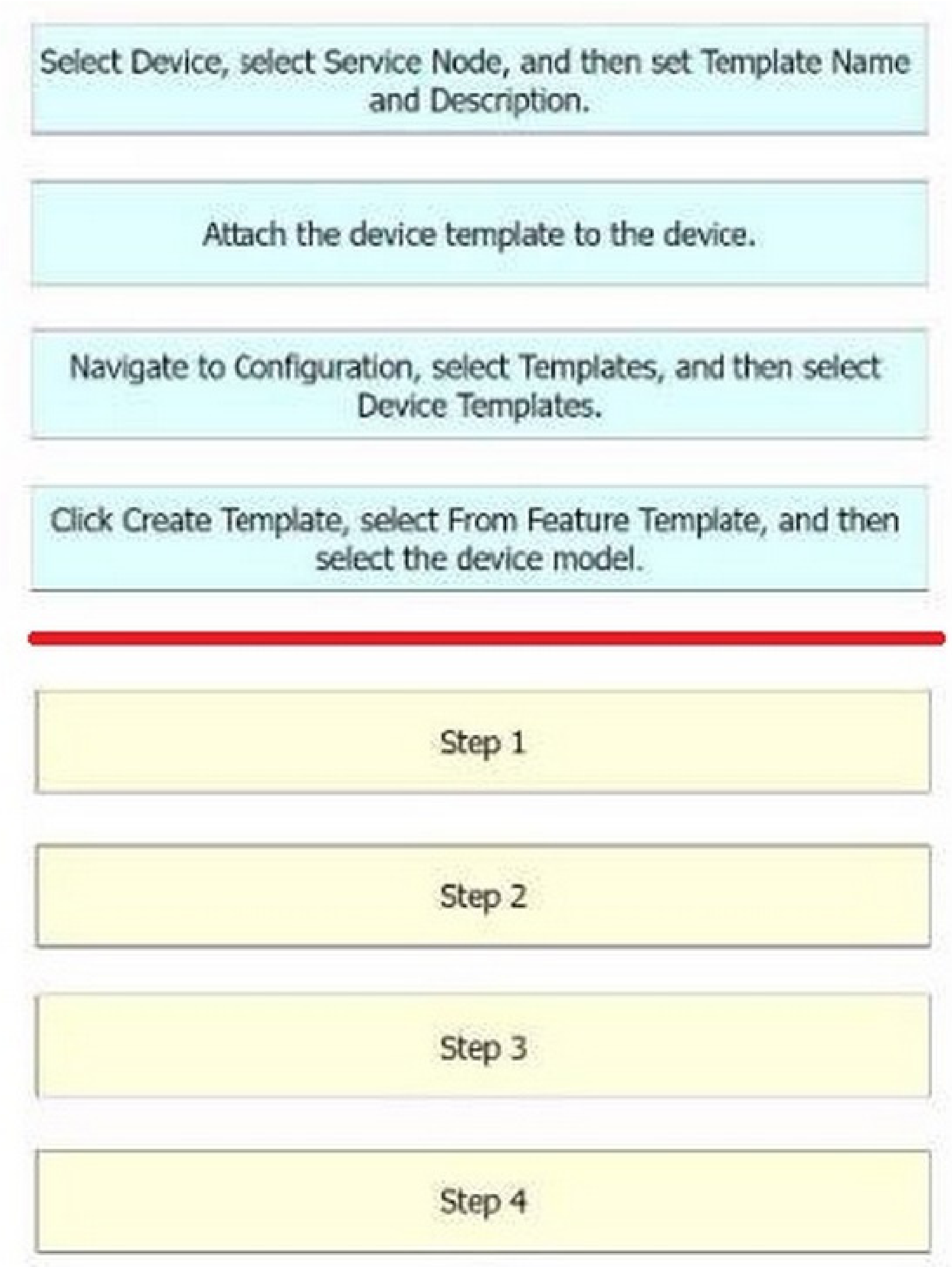
Version: Demo

QUESTION 1

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:



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

Attach the device template to the device.

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

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

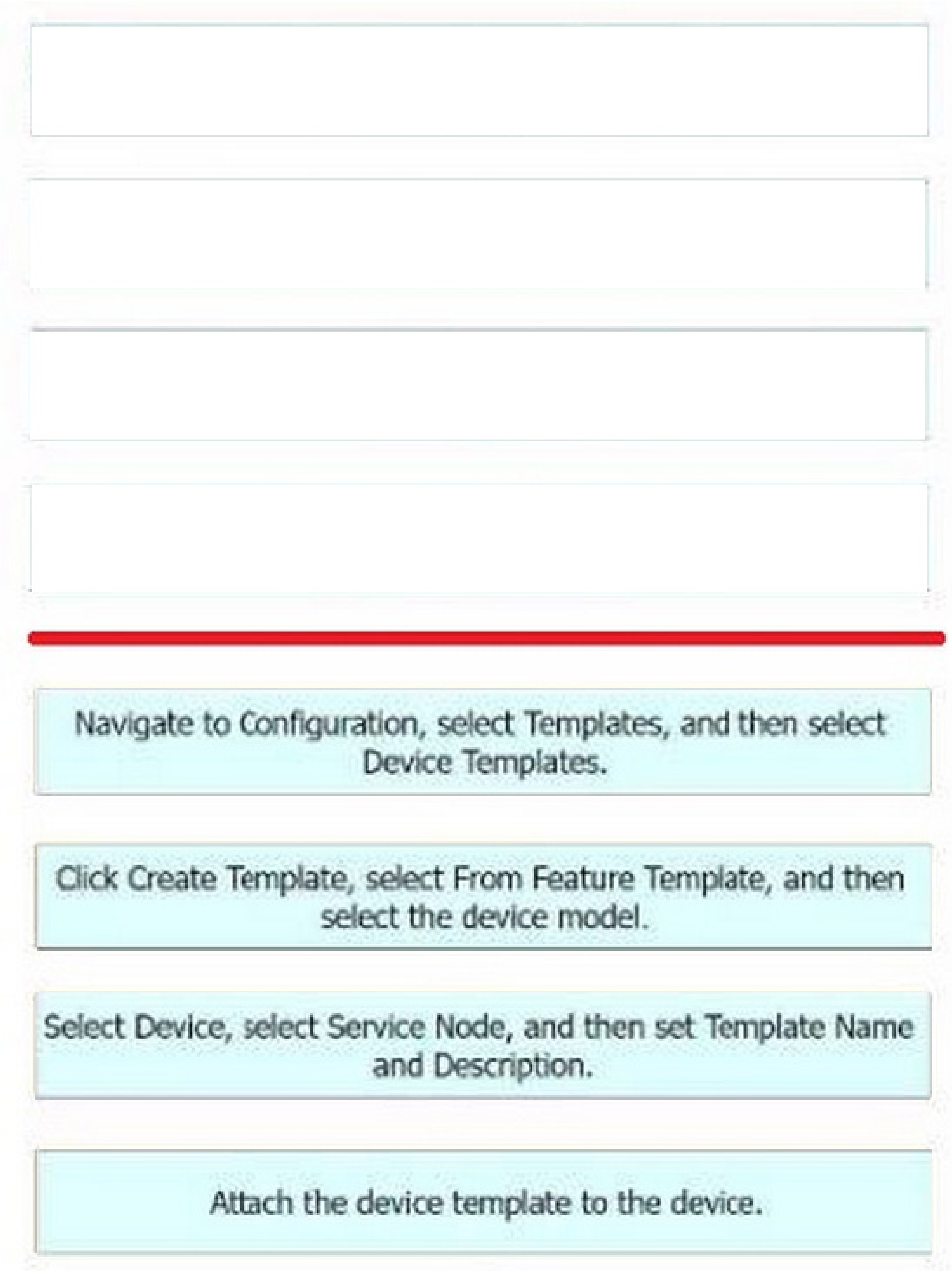
Step 1

Step 2

Step 3

Step 4

Correct Answer:



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

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

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

Attach the device template to the device.

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.

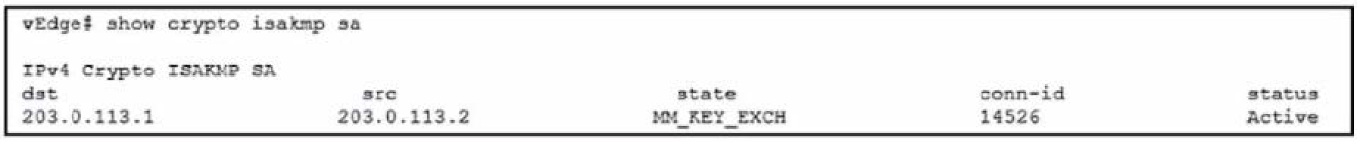
References:

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

---

QUESTION 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:

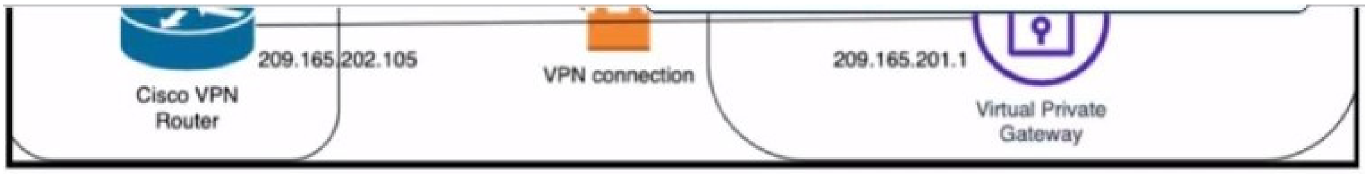
Implementing Cloud Connectivity, Lesson 2: Implementing Cisco SD-WAN Cloud OnRamp for IaaS, Topic: Troubleshooting Cisco SD-WAN Cloud OnRamp for IaaS Cisco IOS Security Configuration Guide, Release 15MandT, Chapter:

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

---

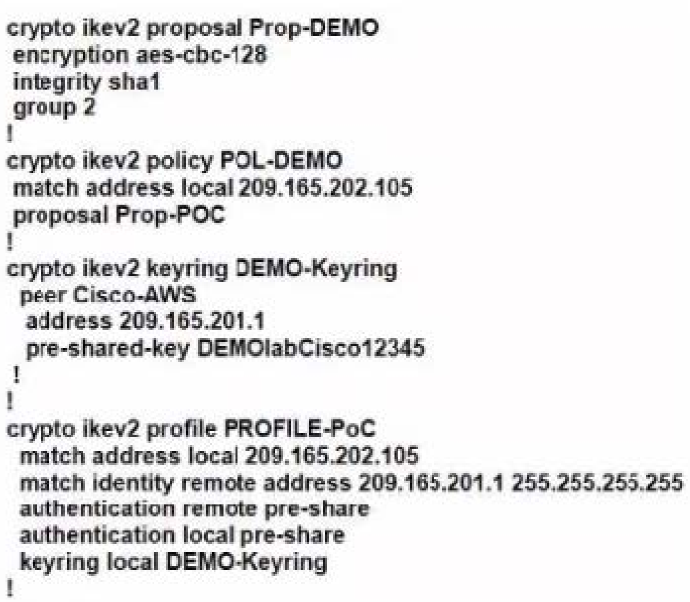
QUESTION 3

Refer to the exhibit.



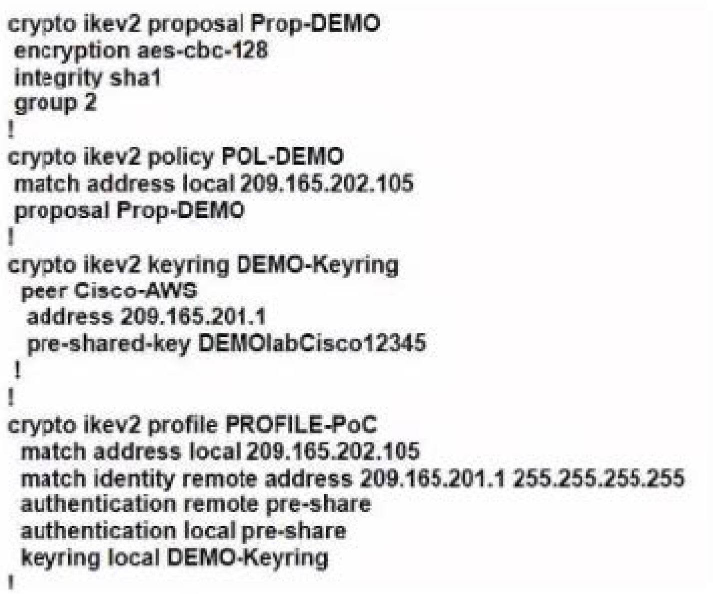
Which Cisco IKEv2 configuration brings up the IPsec tunnel between the remote office router and the AWS virtual private gateway?

A.



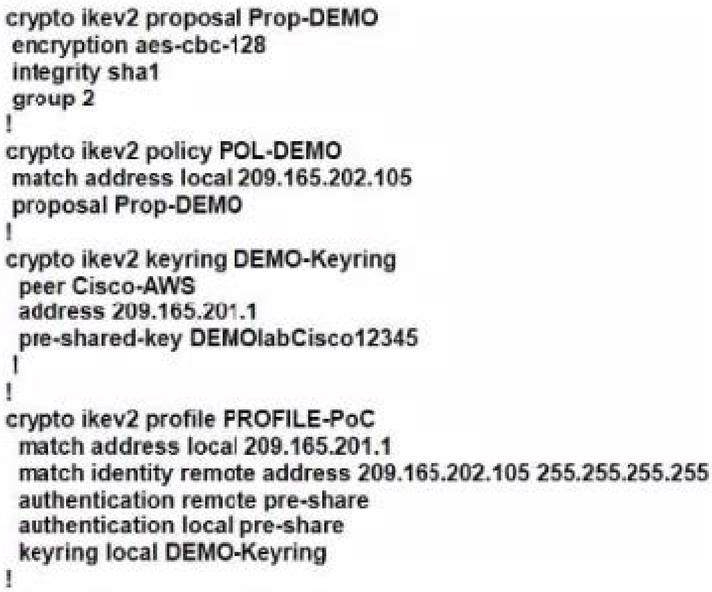
```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-POC
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
   address 209.165.201.1
   pre-shared-key DEMOlabCisco12345
 !
!
crypto ikev2 profile PROFILE-PoC
  match address local 209.165.202.105
  match identity remote address 209.165.201.1 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
!
```

B.



```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-DEMO
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
   address 209.165.201.1
   pre-shared-key DEMOlabCisco12345
 !
!
crypto ikev2 profile PROFILE-PoC
  match address local 209.165.202.105
  match identity remote address 209.165.201.1 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
!
```

C.



```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-DEMO
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
  address 209.165.201.1
  pre-shared-key DEMOlabCisco12345
 !
!
crypto ikev2 profile PROFILE-PoC
  match address local 209.165.201.1
  match identity remote address 209.165.202.105 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
!
```

A. Option A

B. Option B

C. Option C

Correct Answer: C

Option C is the correct answer because it configures the IKEv2 profile with the correct match identity, authentication, and keyring parameters. It also configures the IPsecprofile with the correct transform set and lifetime parameters. Option A is incorrect because it does not specify the match identity remote address in the IKEv2 profile, which is required to match the AWS virtual private gateway IP address. Option B is incorrect because it does not specify the authentication preshare in the IKEv2 profile, which is required to authenticate the IKEv2 peers using a pre-shared key. Option C also matches the configuration example provided by AWS and Cisco for setting up an IKEv2 IPsec site-to- site VPN between a Cisco IOS-XE router and an AWS virtual private gateway.

References:

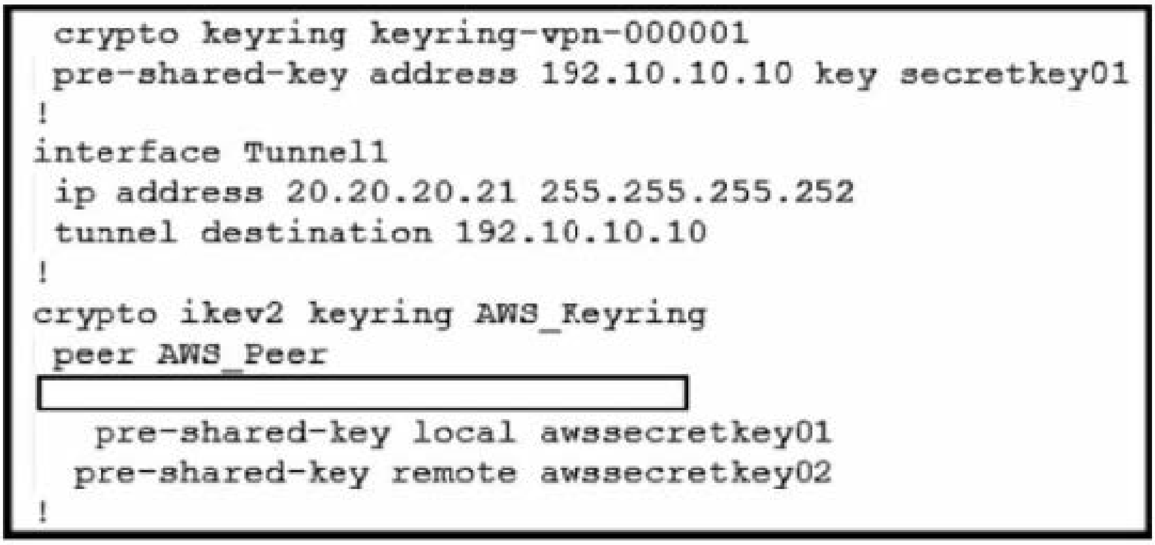
1: AWS VPN Configuration Guide for Cisco IOS-XE

2: Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services

---

QUESTION 4

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

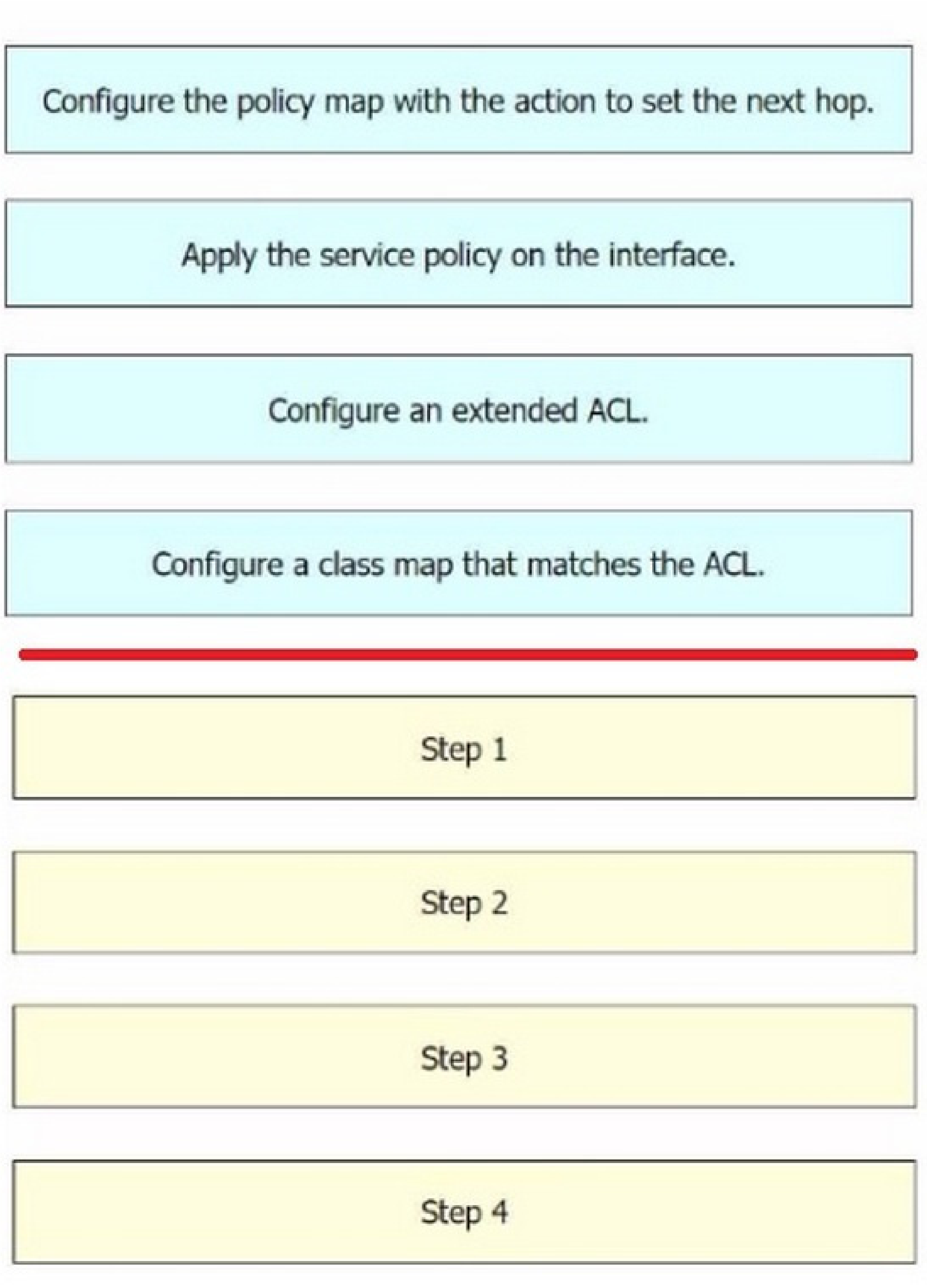
---

QUESTION 5

DRAG DROP

An engineer needs to configure enhanced policy-based routing (ePBR) for IPv4 by using Cisco vManage. Drag and drop the steps from the left onto the order on the right to complete the configuration of the ePBR using the CLI add-on template.

Select and Place:



Configure the policy map with the action to set the next hop.

Apply the service policy on the interface.

Configure an extended ACL.

Configure a class map that matches the ACL.

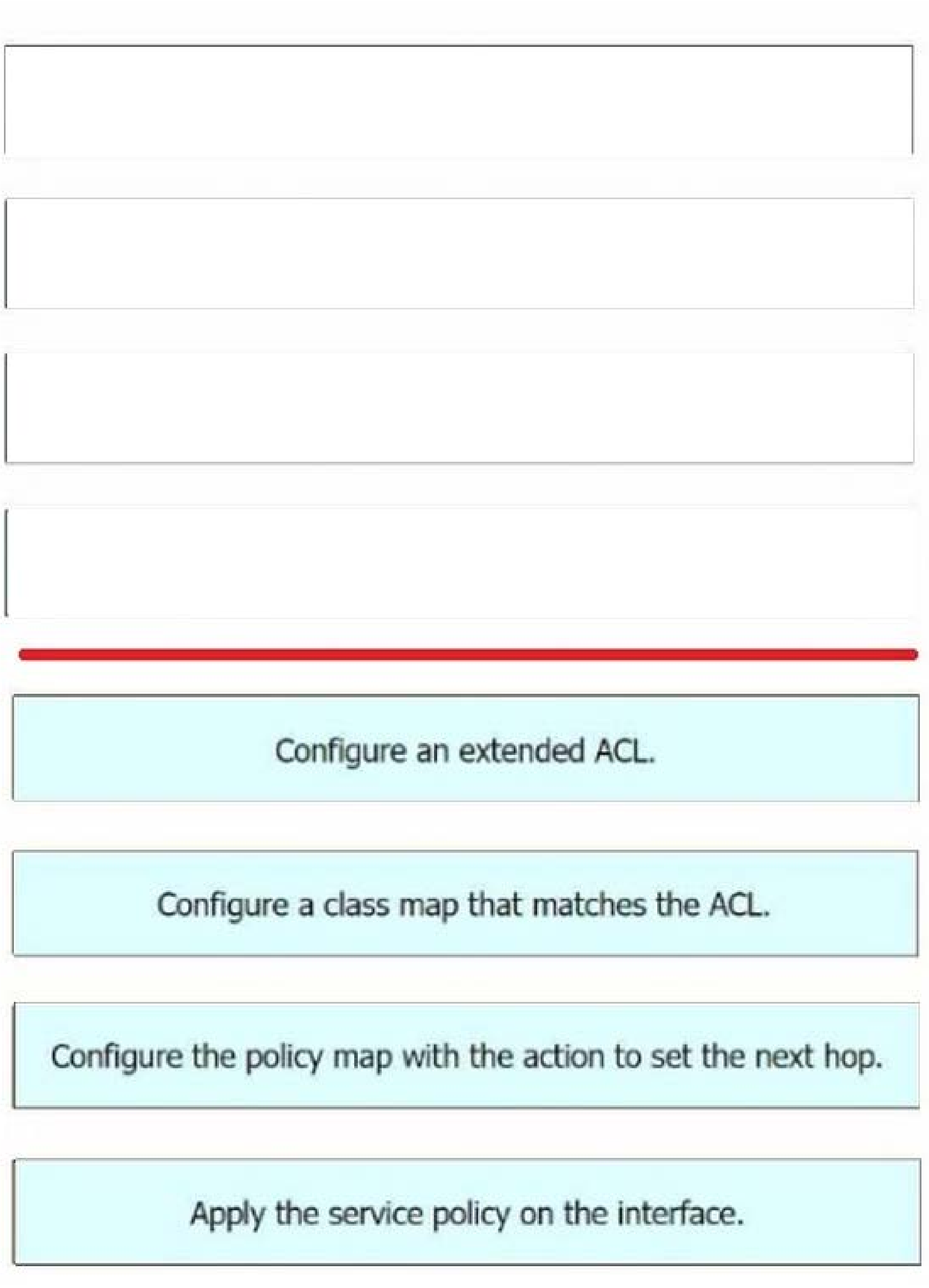
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Configure an extended ACL.

Configure a class map that matches the ACL.

Configure the policy map with the action to set the next hop.

Apply the service policy on the interface.

Enhanced Policy-Based Routing (ePBR) is used to direct packets that arrive at an interface to a specified next-hop. It is very useful in managing a large number of configured access lists more efficiently. In ePBR, the router drops the traffic packets if the next hop configured in the PBR policy is not reachable. To avoid packet loss in such scenarios, you must configure multiple next hops for each access control entry. Here are the steps to configure ePBR for IPv4 using Cisco vManage: Configure an extended ACL: This step involves defining the network or the host. For example, you can permit

IPv4 traffic from any source to specific hosts. Configure a class map that matches the ACL: Class maps match the parameters in the ACLs. For instance, you can create a class map of type traffic and match it with the previously created ACL. Configure the policy map with the action to set the next hop: Policy maps with ePBR then take detailed actions based on the set statements configured. You can configure an ePBR policy map with the class map and set the next hop. Apply the service policy on the interface: Finally, you apply the ePBR policy map to the interface. For example, you can apply the policy map to a GigabitEthernet interface. References : Implementing Enhanced Policy Based Routing - Cisco Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE How to configure PBR - Cisco Community

---

QUESTION 6

Which feature is unique to Cisco SD-WAN IPsec tunnels compared to native IPsec VPN tunnels?

A. real-time dynamic path selection

B. tunneling protocols

C. end-to-end encryption

D. authentication mechanisms

Correct Answer: A

Cisco SD-WAN IPsec tunnels are different from native IPsec VPN tunnels in several ways. One of the unique features of Cisco SD-WAN IPsec tunnels is that they support real-time dynamic path selection, which means that they can

automatically choose the best path for each application based on the network conditions and policies. This feature improves the performance, reliability, and efficiency of the network traffic. Native IPsec VPN tunnels, on the other hand, do not

have this capability and rely on static routing or manual configuration to select the path for each tunnel. This can result in suboptimal performance, increased latency, and higher costs.

References:

Traditional IPsec Versus Cisco SD-WAN IPsec, SD-WAN vs IPsec VPN\\'s - What\\'s the difference?, SD-WAN vs. VPN: How Do They Compare?, Traditional IPSEC Versus SD-WAN IPSEC

QUESTION 7

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 8

An engineer must configure an IPsec tunnel to the cloud VPN gateway. Which Two actions send traffic into the tunnel? (Choose two.)

A. Configure access lists that match the interesting user traffic.

B. Configure a static route.

C. Configure a local policy in Cisco vManage.

D. Configure an IPsec profile and match the remote peer IP address.

E. Configure policy-based routing.

Correct Answer: AE

To send traffic into an IPsec tunnel to the cloud VPN gateway, the engineer must configure two actions:

Configure access lists that match the interesting user traffic. This is the traffic that needs to be encrypted and sent over the IPsec tunnel. The access lists are applied to the crypto map that defines the IPsec parameters for the tunnel.

Configure policy-based routing (PBR). This is a technique that allows the engineer to override the routing table and forward packets based on a defined policy. PBR can be used to send specific traffic to the IPsec tunnel interface, regardless

of the destination IP address. This is useful when the cloud VPN gateway has a dynamic IP address or when multiple cloud VPN gateways are available for load balancing or redundancy.

References:

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

Implementing Cloud Connectivity, Lesson 3: Implementing IPsec VPNs to the Cloud, Topic: Configuring IPsec VPNs on Cisco IOS XE Routers Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter:

Configuring IPsec VPNs, Topic: Configuring Crypto Maps [Cisco IOS XE Gibraltar 16.12.x Feature Guide], Chapter: Policy-Based Routing, Topic: Policy-Based Routing Overview

---

QUESTION 9

A cloud engineer is setting up a new set of nodes in the AWS EKS cluster to manage database integration with Mongo Atlas. The engineer set up security to Mongo but now wants to ensure that the nodes are also secure on the network side. Which feature in AWS should the engineer use?

A. EC2 Trust Lock

B. security groups

C. tagging

D. key pairs

Correct Answer: B

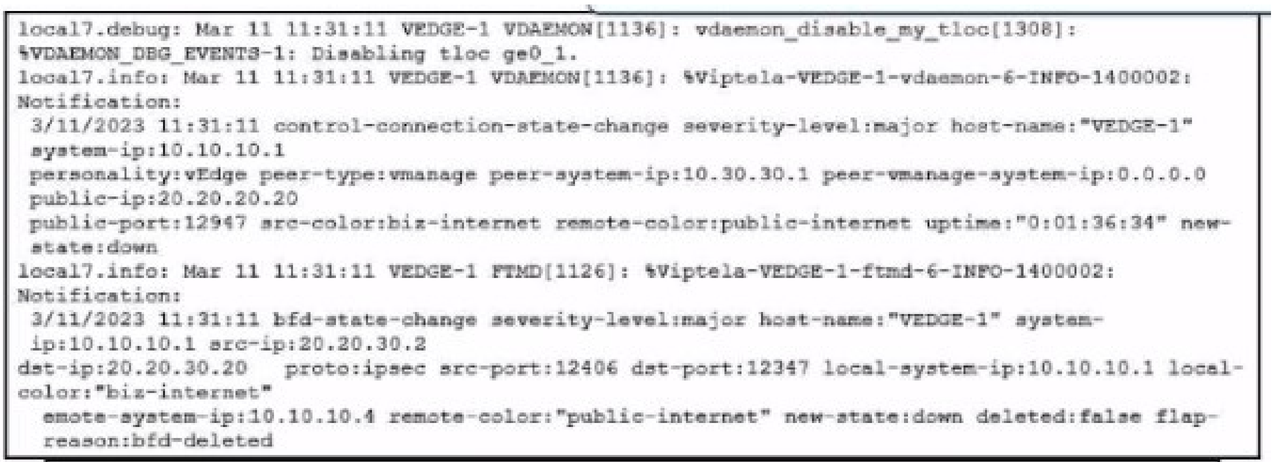
Security groups are a feature in AWS that allow you to control the inbound and outbound traffic to your instances. They act as a virtual firewall that can filter the traffic based on the source, destination, protocol, and port. You can assign one or more security groups to your instances, and each security group can have multiple rules. Security groups are stateful, meaning that they automatically allow the response traffic for any allowed inbound traffic, and vice versa. Security groups are essential for securing your nodes in the AWS EKS cluster, as they can prevent unauthorized access to your Mongo Atlas database or other resources.

References: AWS Security Groups Security Groups for Your VPC Security Groups for Your Amazon EC2 Instances Security Groups for Your Amazon EKS Cluster

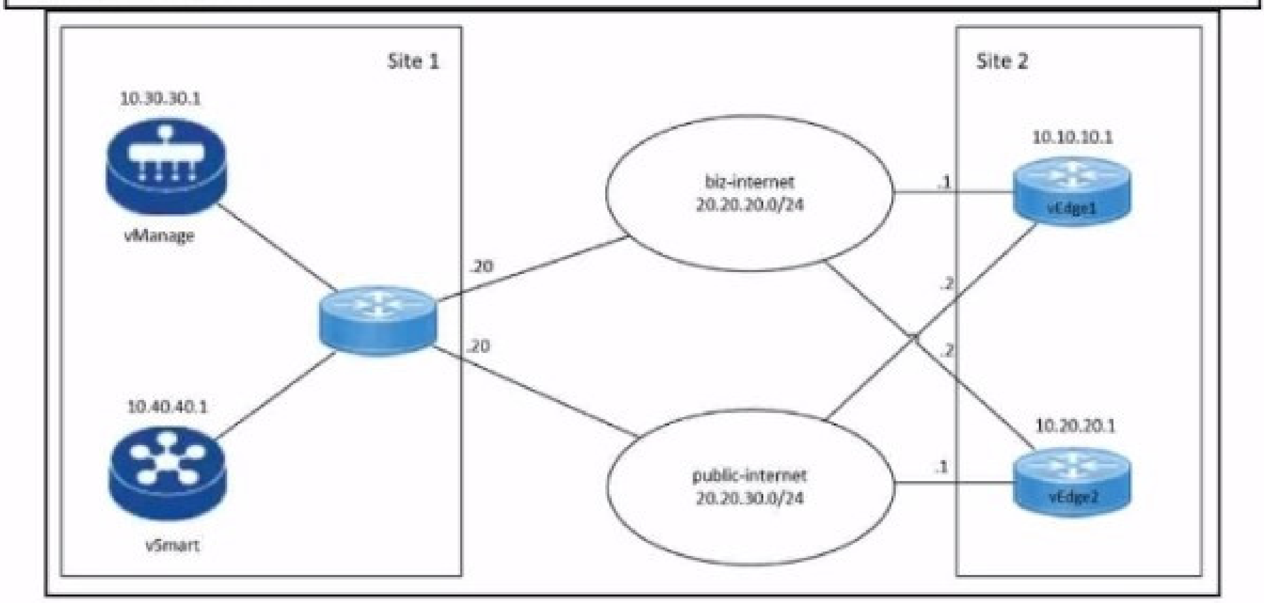
---

QUESTION 10

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.

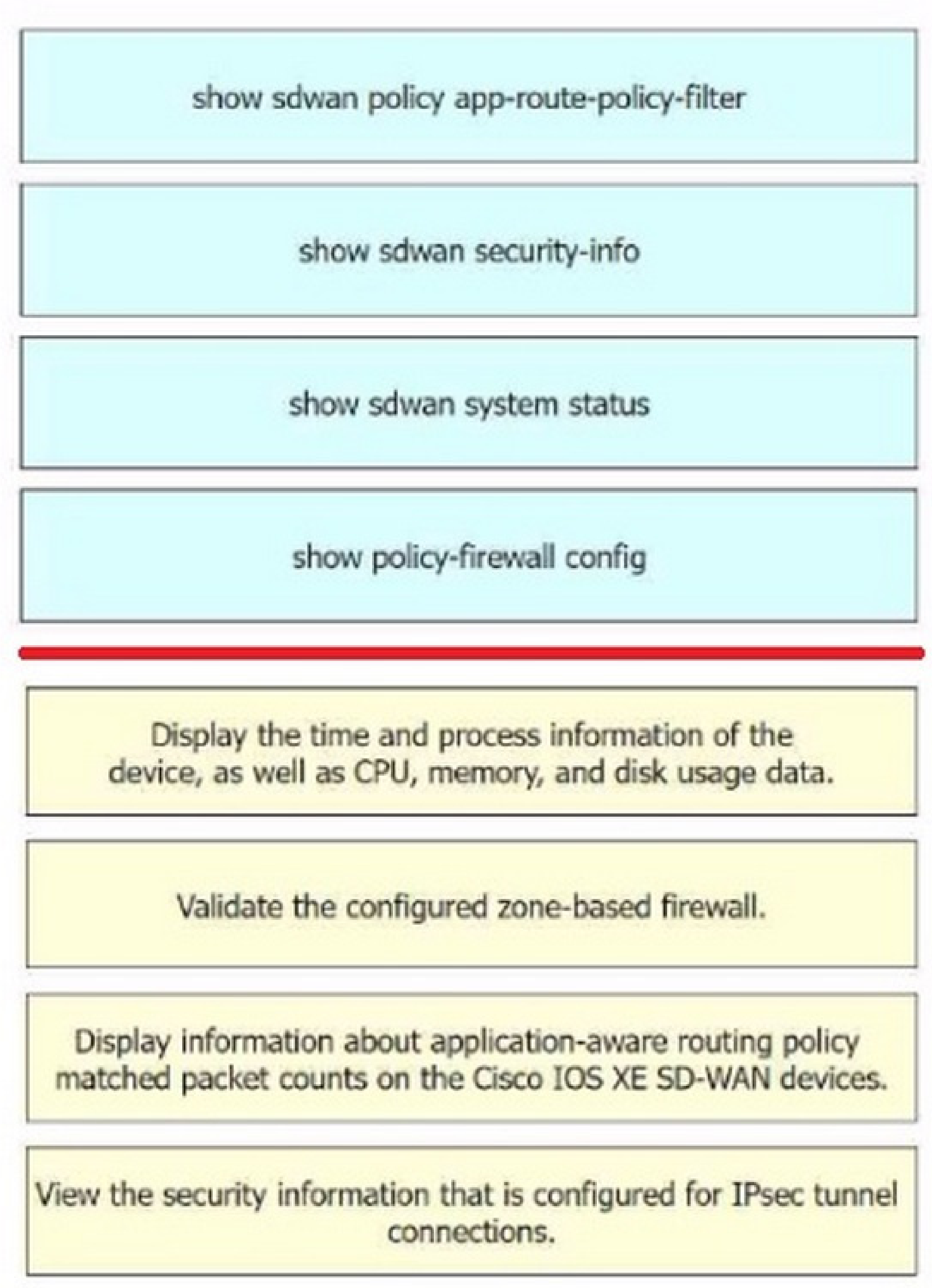
Correct Answer: B

QUESTION 11

DRAG DROP

Drag and drop the commands from the left onto the purposes on the right to identify issues on a Cisco IOS XE SD-WAN device.

Select and Place:



show sdwan policy app-route-policy-filter

show sdwan security-info

show sdwan system status

show policy-firewall config

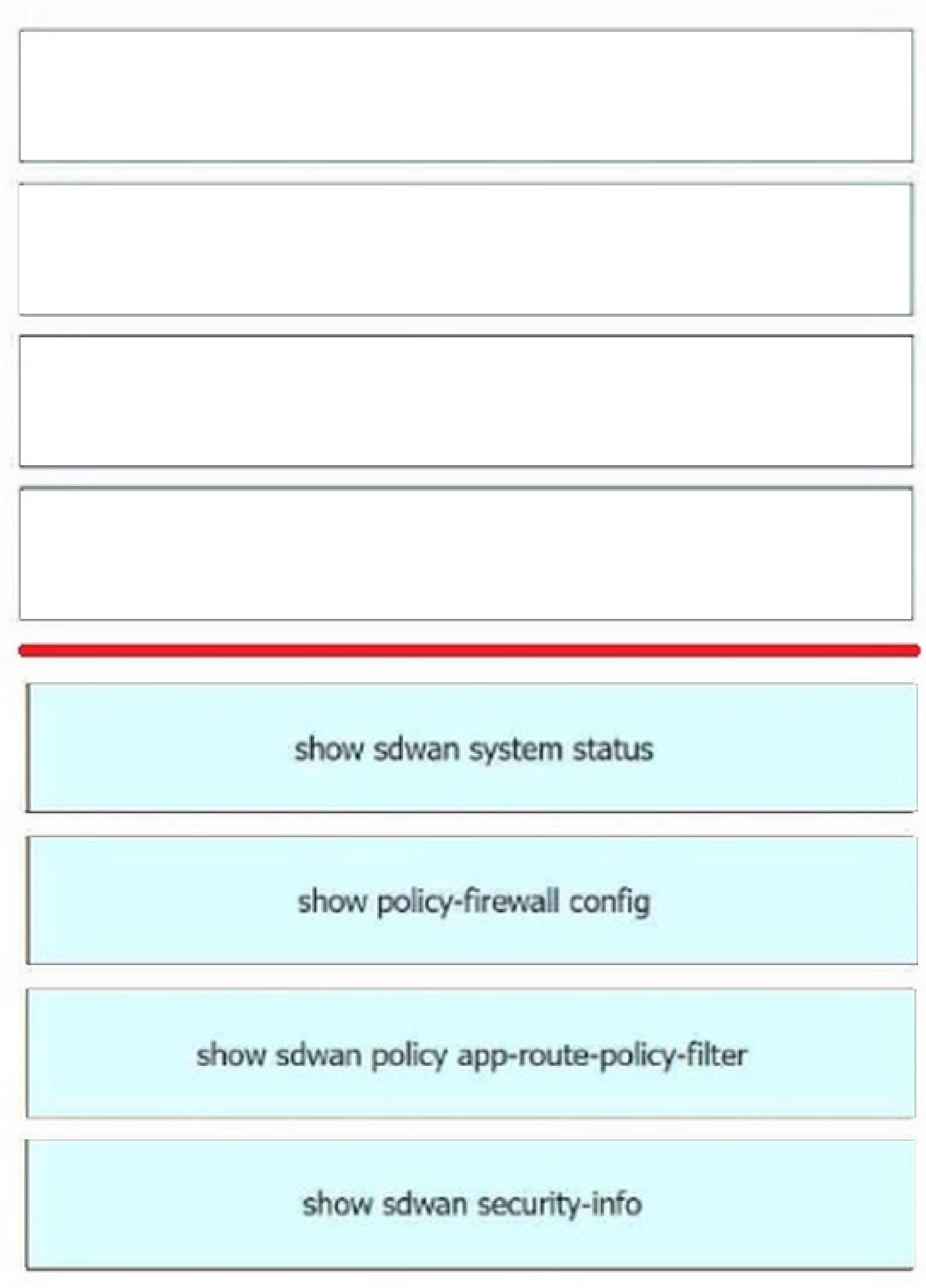
Display the time and process information of the device, as well as CPU, memory, and disk usage data.

Validate the configured zone-based firewall.

Display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices.

View the security information that is configured for IPsec tunnel connections.

Correct Answer:



show sdwan system status

show policy-firewall config

show sdwan policy app-route-policy-filter

show sdwan security-info

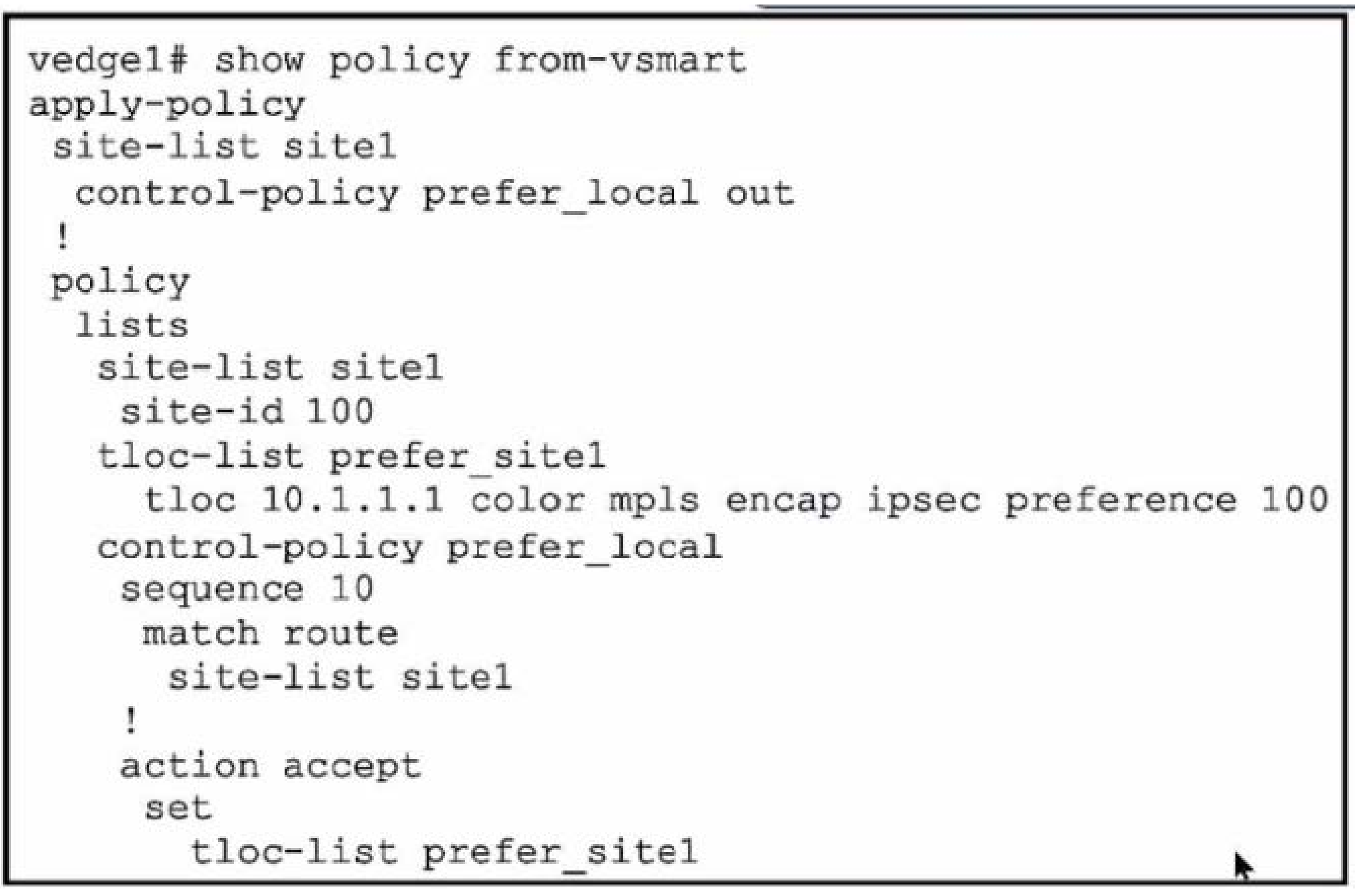
Display the time and process information of the device, as well as CPU, memory, and disk usage data. = show sdwan system status Validate the configured zone-based firewall. = show policy-firewall config1 Display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices. = show sdwan policy app-route-policy- filter View the security information that is configured for IPsec tunnel connections. = show sdwan security-info The commands used to identify issues on a Cisco IOS XE SD-WAN device are as follows show sdwan system status: This command is used to display the time and process information of the device, as well as CPU, memory, and disk usage data. show policy-firewall config: This command is used to validate the configured zone-based firewall. show sdwan policy app-route-policy-filter: This command is used to display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices. show sdwan security-info: This command is used to view the security information that is configured for IPsec tunnel connections

References: Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Cisco Catalyst SD-WAN Command Reference Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE SD-WAN Tunnel Interface Commands - Cisco

---

QUESTION 12

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

Correct Answer: D

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.

References:

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