Free Questions for 300-440 by certsdeals

Shared by Foster on 24-05-2024

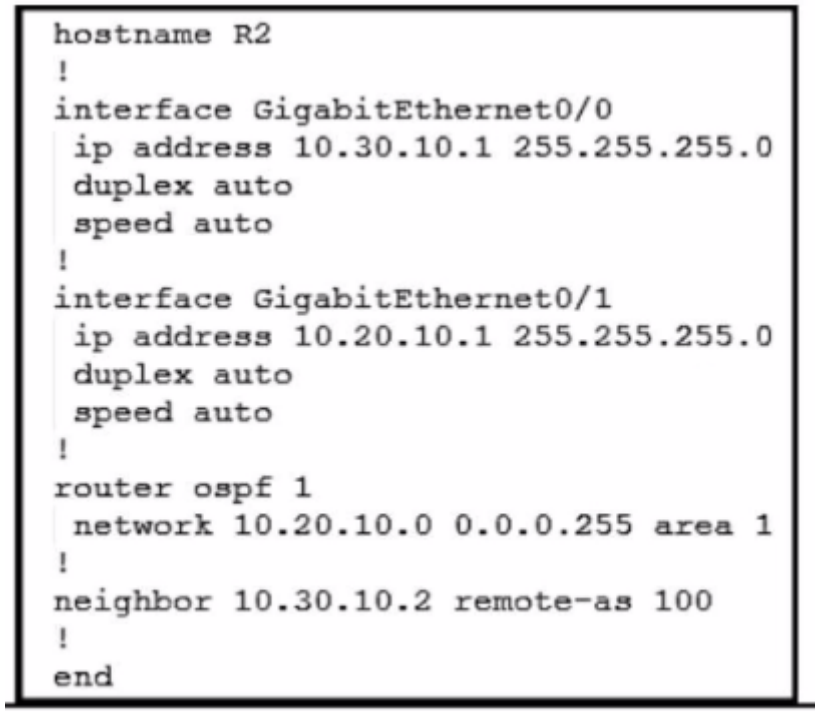
For More Free Questions and Preparation Resources

Check the Links on Last Page

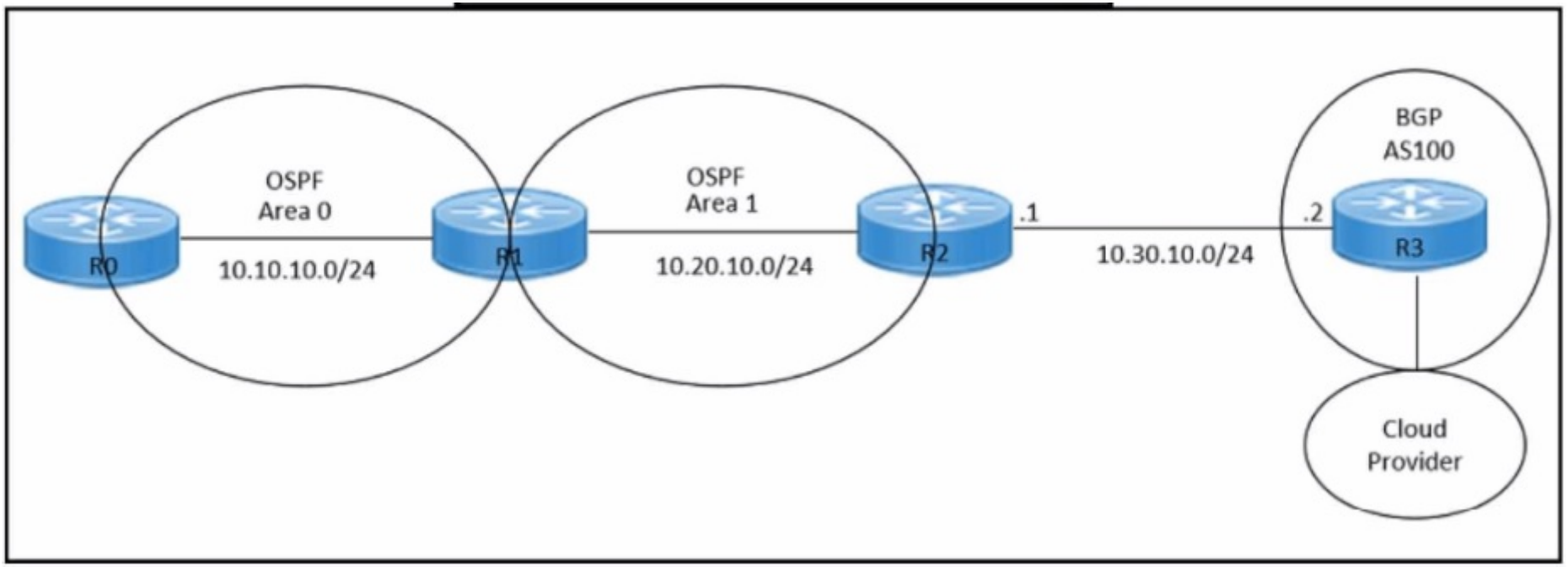
Question 1

Question Type: MultipleChoice

Refer to the exhibits.



```
hostname R2
!
interface GigabitEthernet0/0
 ip address 10.30.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 network 10.20.10.0 0.0.0.255 area 1
!
neighbor 10.30.10.2 remote-as 100
!
end
```



Refer to the exhibits. An engineer must redistribute OSPF internal routes into BGP to connect an on-premises network to a cloud provider. Which two commands should the engineer run on router R2? (Choose two.)

Options:

A- router bgp 100

B- redistribute bgp 100

C- router ospf 1

D- redistribute ospf 1

E- redistribute ospf 100

Answer:

A, D

Explanation:

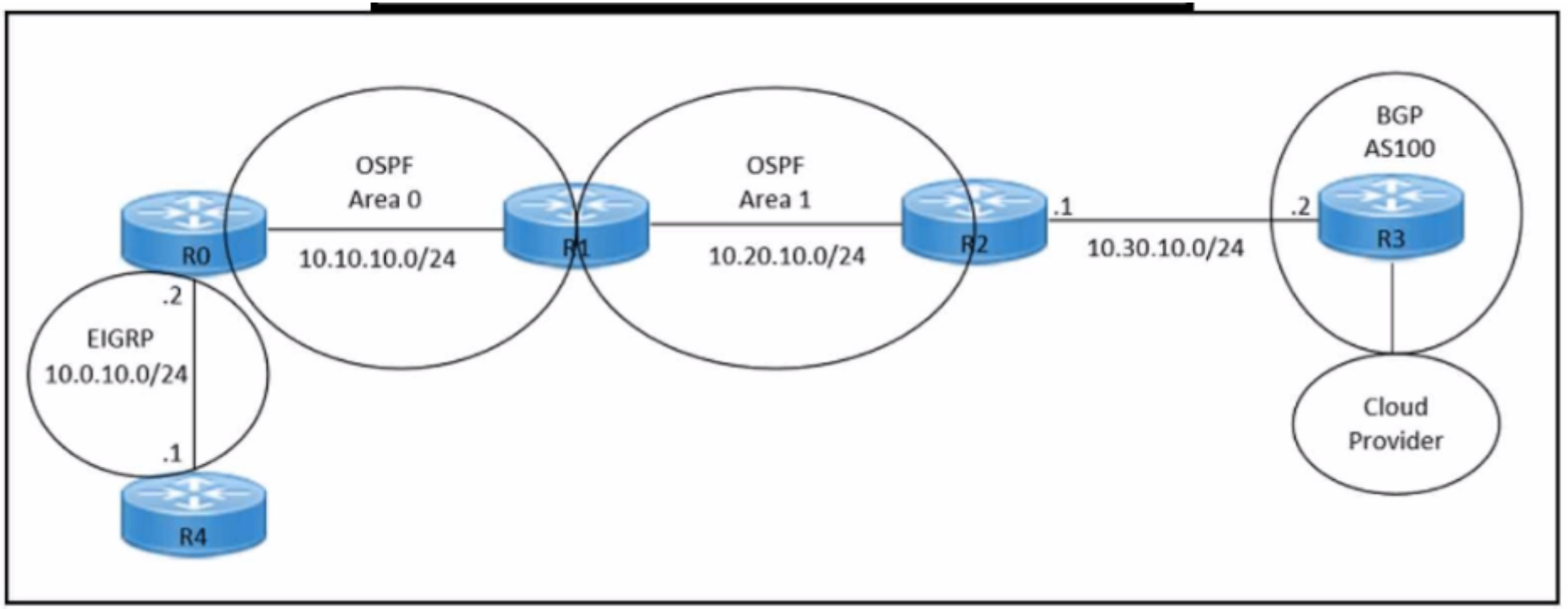
To redistribute OSPF internal routes into BGP for connecting an on-premises network to a cloud provider, the engineer should run the commands "router bgp 100" and "redistribute ospf 1" on router R2. The command "router bgp 100" is used to create a BGP routing process with AS number 100. The command "redistribute ospf 1" is used to redistribute OSPF routes from process ID 1 into BGP.Reference: = I need to access the specific content of Designing and Implementing Cloud Connectivity (ENCC) v1.0 from Cisco's official resources to provide exact references. However, I don't have direct access to external databases or resources, including the Cisco ENCC course materials. I recommend referring to the ENCC course materials for the most accurate and detailed information. Please note that this answer is based on general networking principles and may not reflect the specific content of the ENCC course. Always refer to the official course materials for the most accurate information.

Question 2

Question Type: MultipleChoice

Refer to the exhibits.

```
hostname R2
!
interface GigabitEthernet0/0
 ip address 10.30.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 network 10.20.10.0 0.0.0.255 area 1
!
router bgp 100
 neighbor 10.30.10.2 remote-as 100
 redistribute ospf 1
!
```



Refer to the exhibits. An engineer must redistribute only the 10.0.10.0/24 network into BGP to connect an on-premises network to a public cloud provider. These routes are currently redistributed:

***10.10.10.0/24**
***10.20.10.0/24**

Which command is missing on router R2?

Options:

A- neighbor 10.0.10.2 remote-as 100

B- redistribute ospf 1 match internal

C- redistribute ospf 1 match external

D- neighbor 10.0.10.0/24 remote-as 100

Answer:

C

Explanation:

The commandredistribute ospf 1 match externalis missing on router R2. This command is needed to redistribute only the external OSPF routes into BGP. The external OSPF routes are those that are learned from another routing protocol or redistributed into OSPF. In this case, the 10.0.10.0/24 network is an external OSPF route, as it is redistributed from EIGRP into OSPF on router R1. The other commands are either already present or not relevant for this scenario.Reference:=

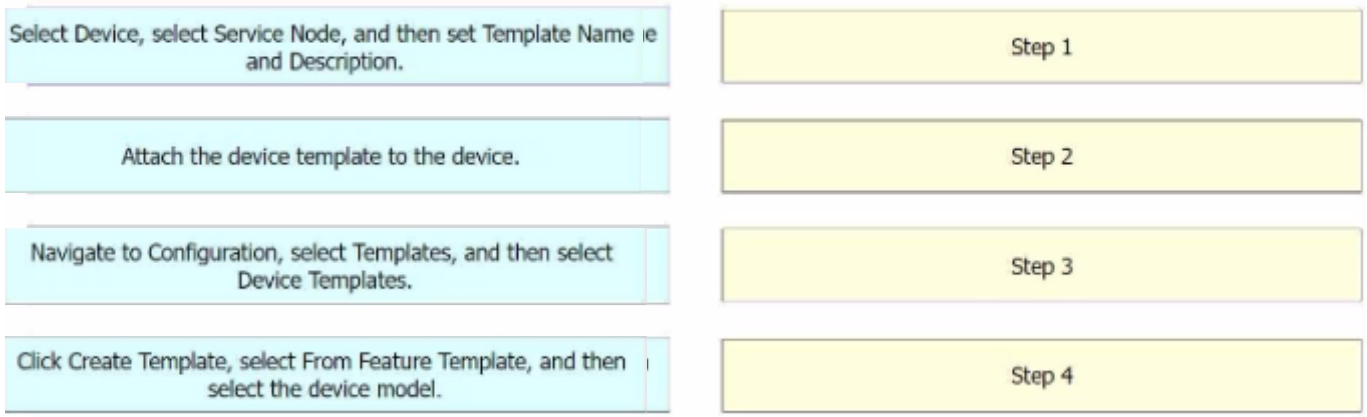
Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3: Implementing Cloud Connectivity, Lesson 3.1: Implementing IPsec VPN from Cisco IOS XE to AWS, Topic 3.1.2: Configure BGP on the Cisco IOS XE Router

Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter: Configuring IPsec VPNs with Dynamic Routing Protocols, Section: Configuring BGP over IPsec VPNs

Question 3

Question Type: DragDrop

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.



Explanation:

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

Question Type: DragDrop

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:

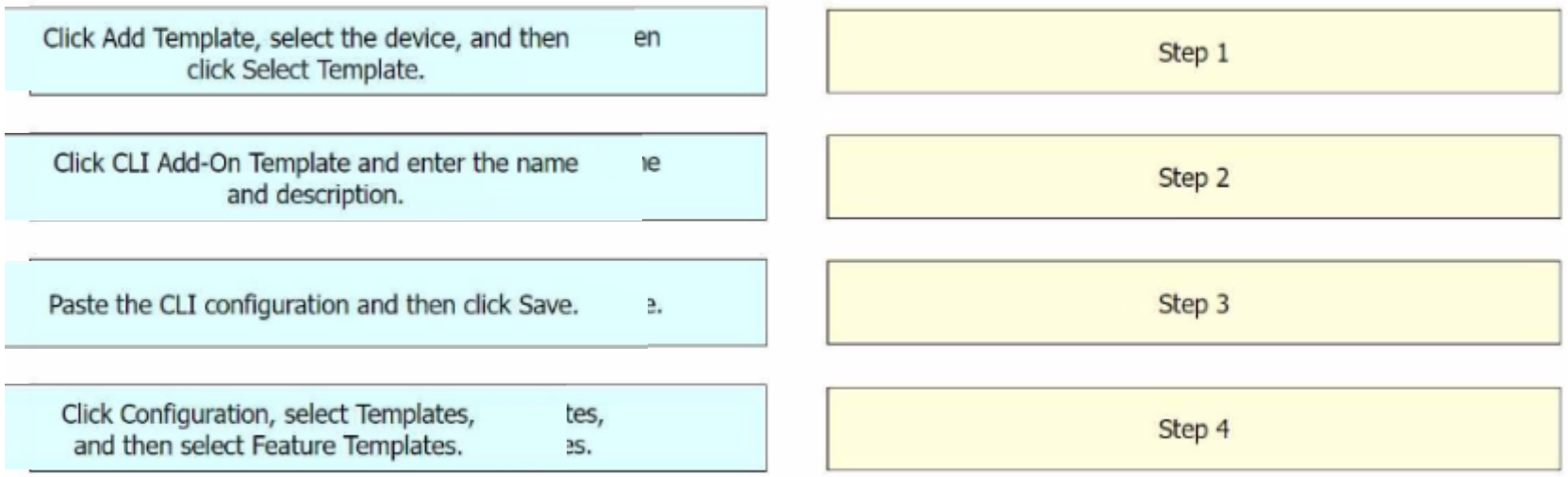
* licensing config enable false

* licensing config privacy hostname true

* licensing config privacy version false

* licensing config utility utility-enable true

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



Explanation:

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

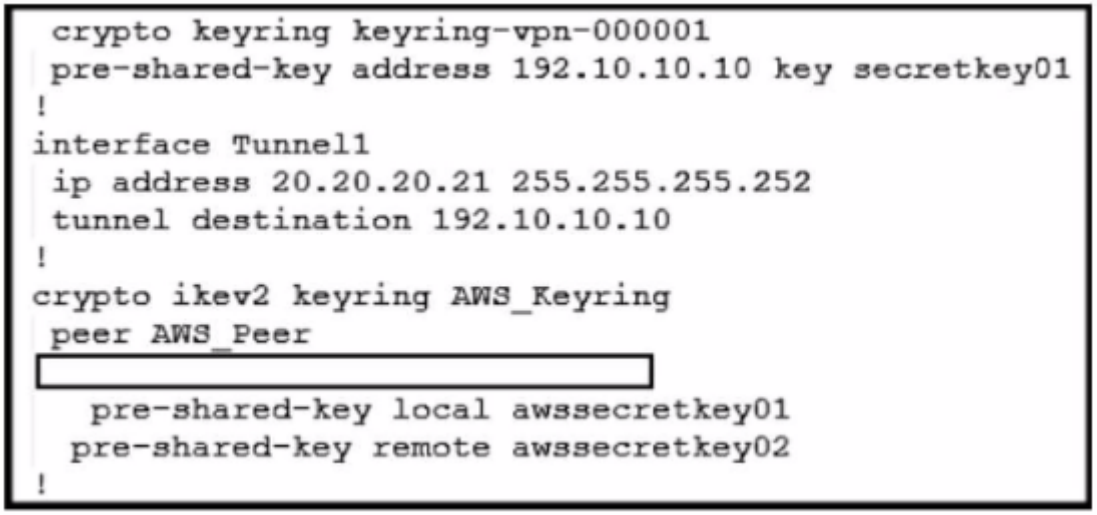
Cisco SD-WAN vSmart CLI Template - NetworkLessons.com

CLI Templates for Cisco XE SD-WAN Routers

Question 5

Question Type: MultipleChoice

Refer to the exhibits.



Refer to the exhibit. 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?

Options:

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

Answer:

C

Explanation:

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 network1.Reference:

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 6

Question Type: MultipleChoice

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

Options:

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.

Answer:

B

Explanation:

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 links2.A centralized internet gateway can use various technologies to provide connectivity to SaaS applications, such as proxy servers,

firewalls, web filters, and WAN optimizers3.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.Reference:=1: Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 1: Cloud Connectivity Overview, Lesson 1: Cloud Connectivity Concepts, Topic: Centralized Internet Gateway2: Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Release 17.3.1a and Later, Topic: Centralized Internet Gateway3: Architect and optimize your internet traffic with Azure routing preference, Microsoft Azure Blog, Topic: Routing via the premium Microsoft global network4: What is SaaS?Software as a Service, Microsoft Azure, Topic: How SaaS works5: How an application gateway works, Microsoft Learn, Topic: Application gateway components

Question 7

Question Type: MultipleChoice

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

Options:

A- real-time dynamic path selection

B- tunneling protocols

C- end-to-end encryption

D- authentication mechanisms

Answer:

A

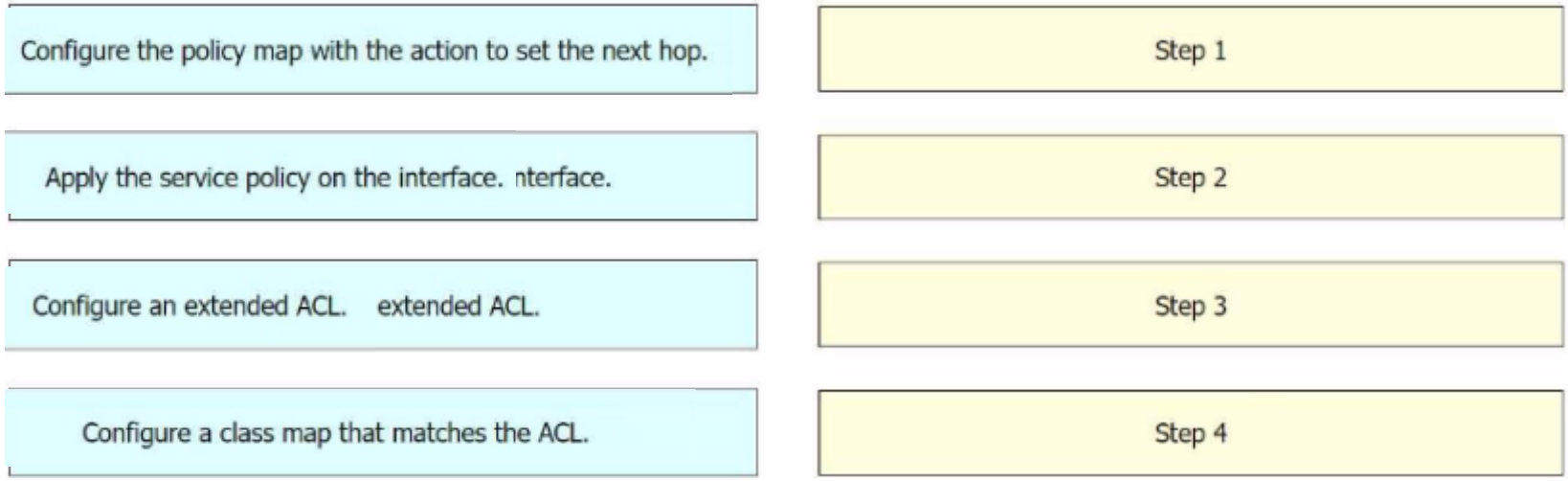
Explanation:

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.Reference:=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 8

Question Type: DragDrop

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.



Explanation:

Implementing Enhanced Policy Based Routing - Cisco

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

How to configure PBR - Cisco Community

Question 9

Question Type: MultipleChoice

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?

Options:

A- EC2 Trust Lock

B- security groups

C- tagging

D- key pairs

Answer:

B

Explanation:

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. You can also use security groups to isolate your nodes from other instances in the same VPC or subnet, or to allow communication between nodes in different clusters or regions.Reference:=

AWS Security Groups

Security Groups for Your VPC

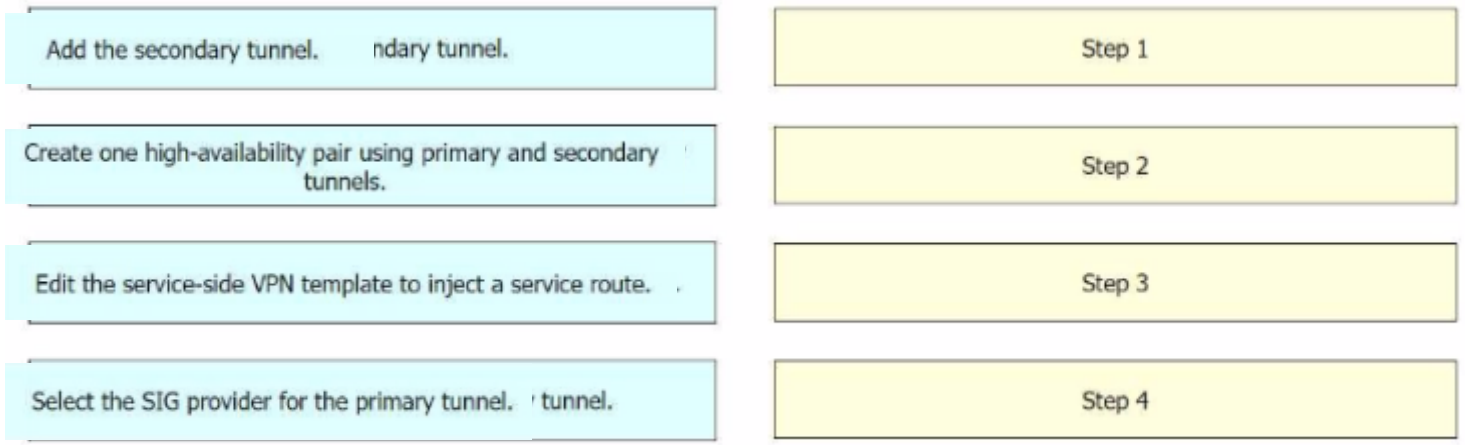
Security Groups for Your Amazon EC2 Instances

Security Groups for Your Amazon EKS Cluster

Question 10

Question Type: **DragDrop**

An engineer must configure cloud connectivity with Cisco Umbrella Secure Internet Gateway (SIG) in active/backup mode. The engineer already configured the SIG Credentials and SIG Feature Templates. Drag and drop the steps from the left onto the order on the right to complete the configuration.



Explanation:

Designing and Implementing Cloud Connectivity (ENCC) v1.01

Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300-440) Exam Prep2

Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios - Cisco3