DUMPSsheet

Free Questions for 300-440 by dumpssheet

Shared by Short on 29-02-2024

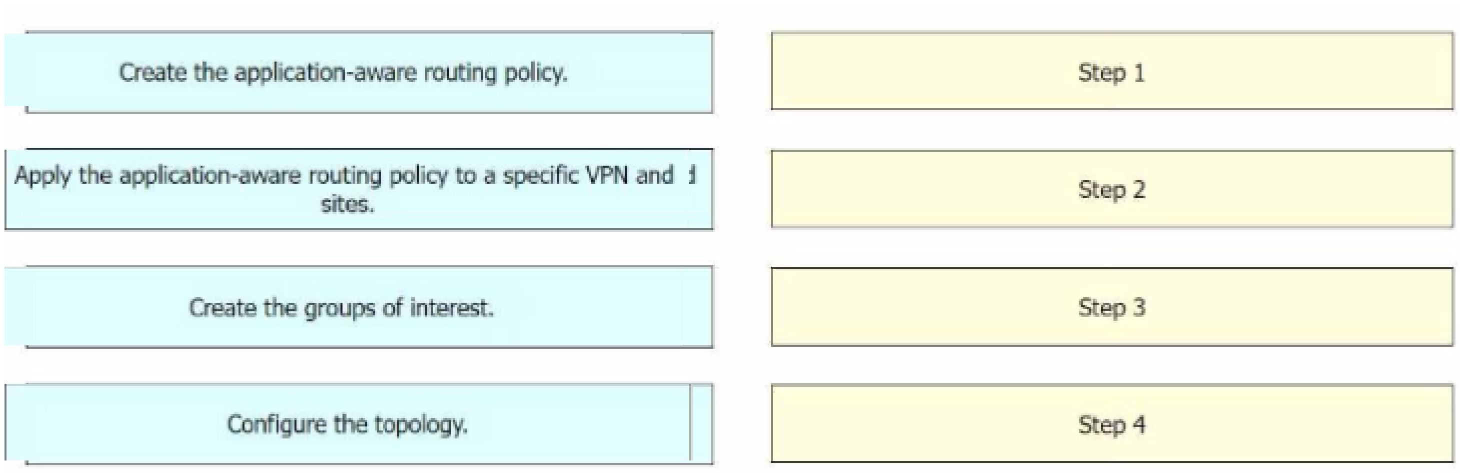
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: DragDrop

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.



Create the application-aware routing policy.

Apply the application-aware routing policy to a specific VPN and 1 sites.

Create the groups of interest.

Configure the topology.

Step 1

Step 2

Step 3

Step 4

Explanation:

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

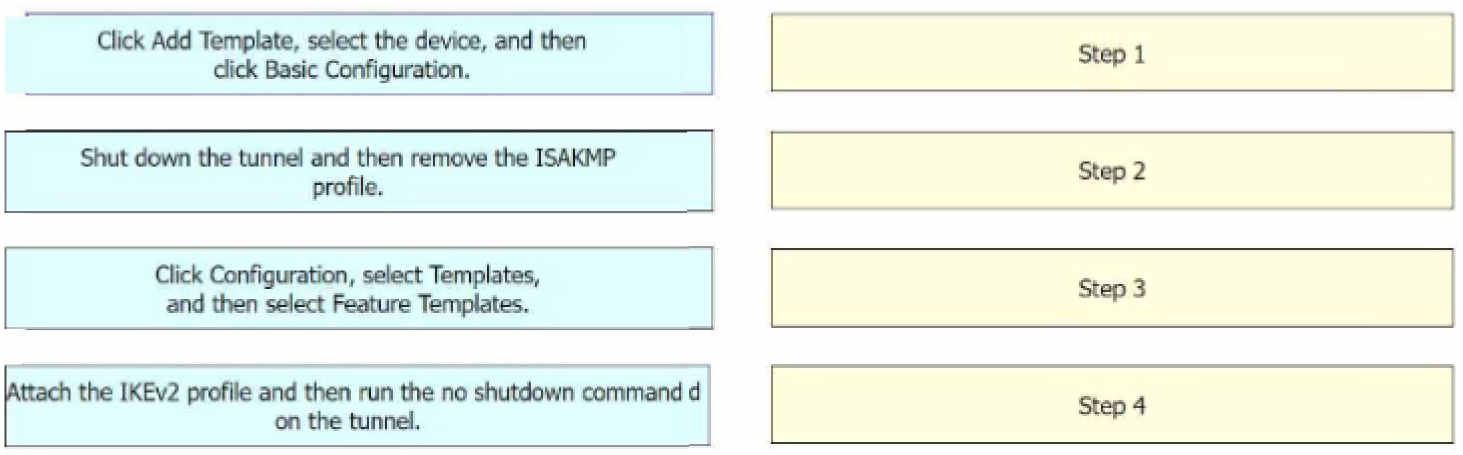
Configuring Application-Aware Routing (AAR) Policies | NetworkAcademy.io

Policies Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12

Question 2

Question Type: **DragDrop**

An engineer must configure a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router In Controller mode and AWS. The IKE version must be changed from IKEv1 to IKEv2 in Cisco vManage. Drag and drop the steps from the left onto the order on the right to complete the configuration.



Click Add Template, select the device, and then click Basic Configuration.

Shut down the tunnel and then remove the ISAKMP profile.

Click Configuration, select Templates, and then select Feature Templates.

Attach the IKEv2 profile and then run the no shutdown command d on the tunnel.

Step 1

Step 2

Step 3

Step 4

Answer:

Explanation:

Configuring Internet Key Exchange Version 2 (IKEv2) - Cisco

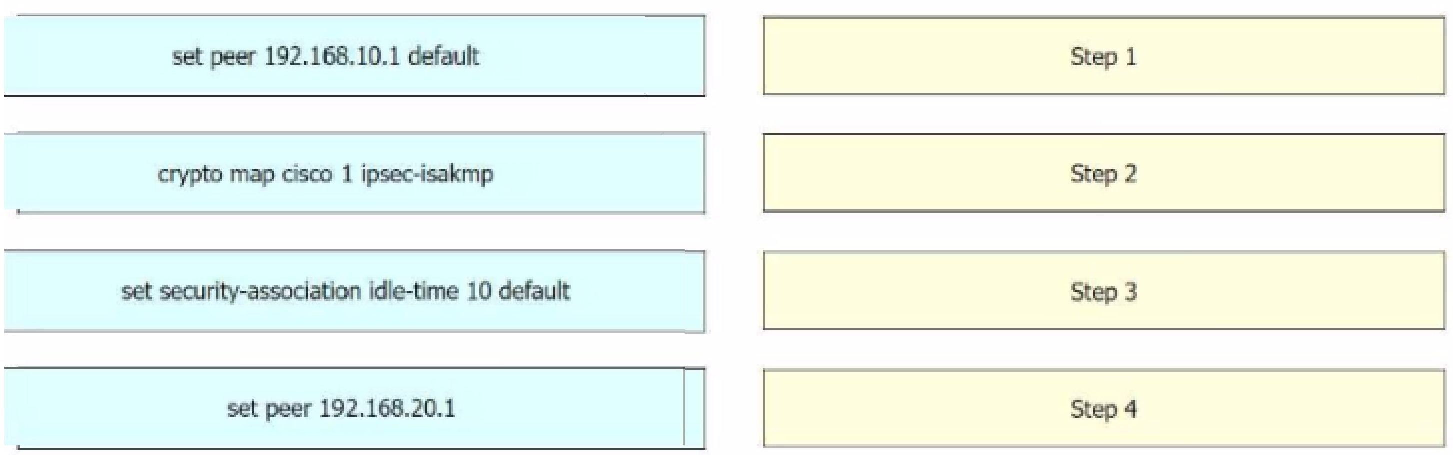
Switch from IKEv1 to IKEv2 on Cisco Routers - Cisco Community

Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

Question 3

Question Type: **DragDrop**

An engineer must edit the settings of a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS). IPsec must be configured to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco. Drag and drop the commands from the left onto the order on the right.



set peer 192.168.10.1 default

crypto map cisco 1 ipsec-isakmp

set security-association idle-time 10 default

set peer 192.168.20.1

Step 1

Step 2

Step 3

Step 4

Explanation:

Configure a Site-to-Site IPSec IKEv1 Tunnel Between an ASA and a Cisco IOS Router - Cisco

Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

Configuring Site to Site IPSec VPN Tunnel Between Cisco Routers

Configure Failover for IPSec Site-to-Site Tunnels with Backup ISP Links on FTD Managed by FMC - Cisco

Does Setting Multiple Peers in a Crypto Map Also Support Parallel IPSec Connections - Cisco Community

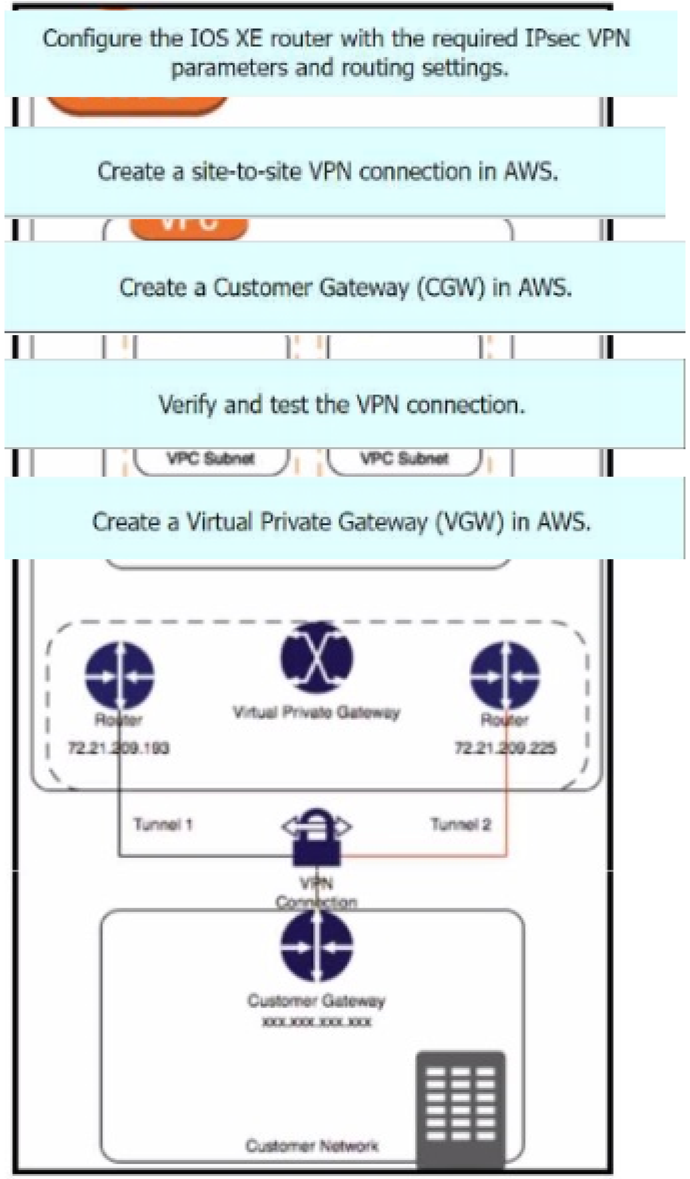
Multiple WAN Connections --- IPsec in Multi-WAN Environments | pfSense Documentation

Multiple Set Peer for VPN Failover - Server Fault

Question 4

Question Type: **DragDrop**

Refer to the exhibit.



Configure the IOS XE router with the required IPsec VPN parameters and routing settings.

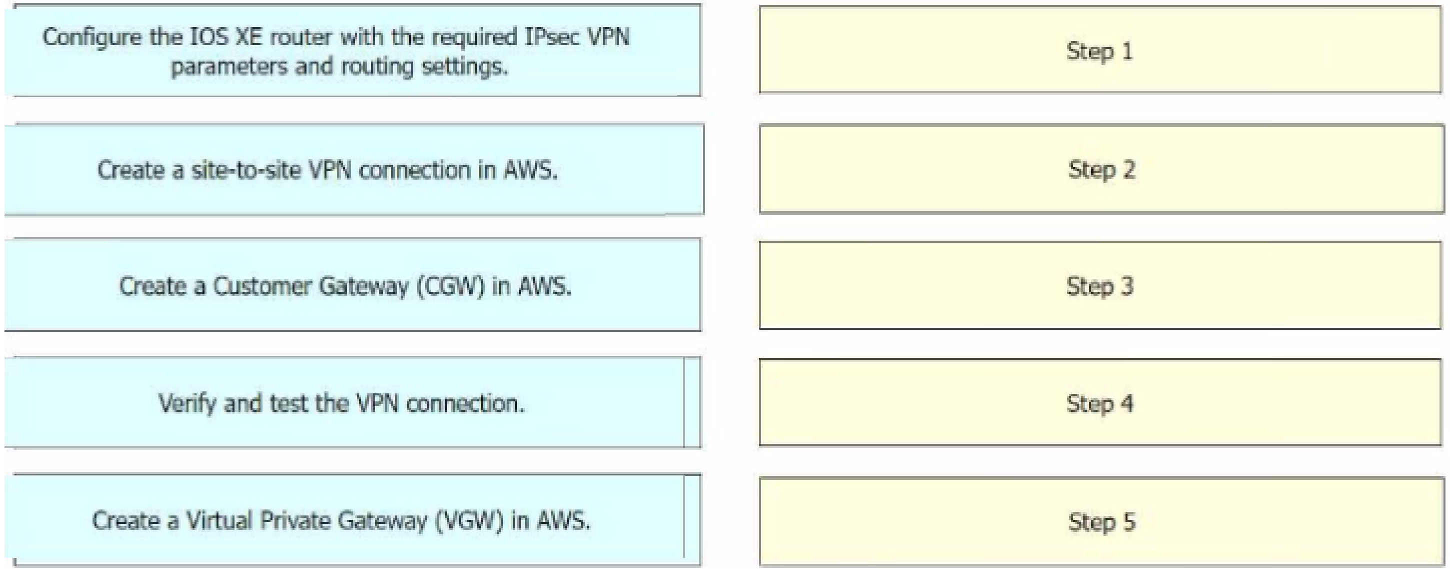
Create a site-to-site VPN connection in AWS.

Create a Customer Gateway (CGW) in AWS.

Verify and test the VPN connection.

Create a Virtual Private Gateway (VGW) in AWS.

Drag and drop the steps from the left onto the order on the right to configure a site-to-site VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS).



Configure the IOS XE router with the required IPsec VPN parameters and routing settings.

Create a site-to-site VPN connection in AWS.

Create a Customer Gateway (CGW) in AWS.

Verify and test the VPN connection.

Create a Virtual Private Gateway (VGW) in AWS.

Step 1

Step 2

Step 3

Step 4

Step 5

Explanation:

Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

SD-WAN Configuration Example: Site-to-site (LAN to LAN) IPSec between vEdge and Cisco IOS - Cisco Community

Question 5

Question Type: MultipleChoice

Which method is used to create authorization boundary diagrams (ABDs)?

Options:

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

Answer:

C

Explanation:

According to the FedRAMP Authorization Boundary Guidance document1, the method used to create authorization boundary diagrams (ABDs) is to identify all tools as either external or internal 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 customer1.The other options are incorrect because they do not capture the full scope and details of the authorization boundary as required by FedRAMP.Reference:= FedRAMP Authorization Boundary Guidance document1

Question 6

Question Type: MultipleChoice

A company has multiple branch offices across different geographic locations and a centralized data center. The company plans to migrate Its critical business applications to the public cloud infrastructure that is hosted in Microsoft Azure. The company requires high availability, redundancy, and low latency for its business applications. Which connectivity model meets these requirements?

Options:

A- ExpressRoute with private peering using SDCI

B- hybrid connectivity with SD-WAN

C- AWS Direct Connect with dedicated connections

D- site-to-site VPN with Azure VPN gateway

Answer:

A

Explanation:

The connectivity model that meets the requirements of high availability, redundancy, and low latency for the company's business applications isExpressRoute with private peering using SDCI.

ExpressRoute is a service that provides a dedicated, private, and high-bandwidth connection between the customer's on-premises network and Microsoft Azure cloud network1.

Private peering is a type of ExpressRoute circuit that allows the customer to access Azure services that are hosted in a virtual network, such as virtual machines, storage, and databases2.

SDCI (Secure Data Center Interconnect) is a Cisco solution that enables secure and scalable connectivity between multiple data centers and cloud providers, using technologies such as MPLS, IPsec, and SD-WAN3.

By using ExpressRoute with private peering and SDCI, the company can achieve the following benefits:

High availability: ExpressRoute circuits are redundant and resilient, and can be configured with multiple service providers and locations for failover and load balancing1.SDCI also provides high availability by using dynamic routing protocols and encryption mechanisms to ensure optimal and secure path selection3.

Redundancy: ExpressRoute circuits can be paired together to form a redundant connection between the customer's network and Azure4.SDCI also supports redundancy by allowing multiple connections between data centers and cloud providers, using different transport technologies and service levels3.

Low latency: ExpressRoute circuits offer lower latency than public internet connections, as they bypass the congestion and variability of the internet1.SDCI also reduces latency by using MPLS and SD-WAN to optimize the performance and quality of service for the traffic between data centers and cloud providers3.

What is Azure ExpressRoute?

Azure ExpressRoute peering

Cisco Secure Data Center Interconnect

ExpressRoute circuit and routing domain

Question 7

Question Type: **MultipleChoice**

A company with multiple branch offices wants a suitable connectivity model to meet these network architecture requirements:

* high availability

* quality of service (QoS)

* multihoming

* specific routing needs

Which connectivity model meets these requirements?

Options:

A- hub-and-spoke topology using MPLS with static routing and dedicated bandwidth for QoS

B- star topology with internet-based VPN connections and BGP for routing

C- hybrid topology that combines MPLS and SD-WAN

D- fully meshed topology with SD-WAN technology using dynamic routing and prioritized traffic for QoS

Answer:

D

Explanation:

A fully meshed topology with SD-WAN technology using dynamic routing and prioritized traffic for QoS meets the network architecture requirements of the company. A fully meshed topology provides high availability by eliminating single points of failure and allowing multiple paths between branch offices. SD-WAN technology enables multihoming by supporting multiple transport options, such as MPLS, internet, LTE, etc. SD-WAN also provides QoS by applying policies to prioritize traffic based on application, user, or network conditions. Dynamic routing allows the SD-WAN solution to adapt to changing network conditions and optimize the path selection for each traffic type. A fully meshed topology with SD-WAN technology can also support specific routing needs, such as segment routing, policy-based routing, or application-aware routing.Reference:

Designing and Implementing Cloud Connectivity (ENCC) v1.0

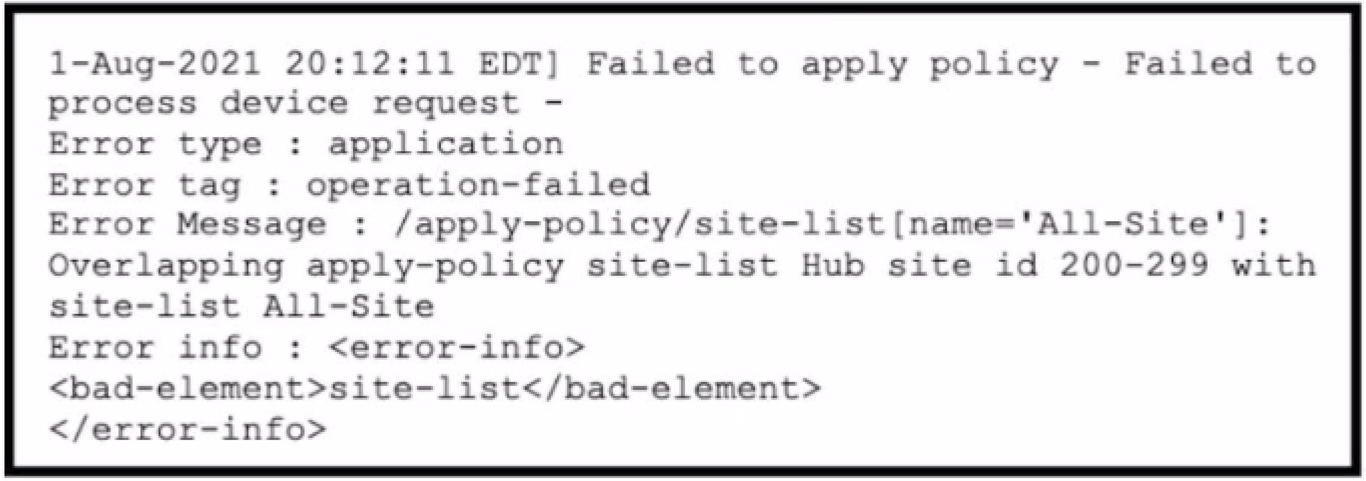
[Cisco SD-WAN Design Guide]

[Cisco SD-WAN Configuration Guide]

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



```
1-Aug-2021 20:12:11 EDT] Failed to apply policy - Failed to
process device request -
Error type : application
Error tag : operation-failed
Error Message : /apply-policy/site-list[name='All-Site']:
Overlapping apply-policy site-list Hub site id 200-299 with
site-list All-Site
Error info : <error-info>
<bad-element>site-list</bad-element>
</error-info>
```

A company uses Cisco SD-WAN in the data center. All devices have the default configuration. An engineer attempts to add a new centralized control policy in Cisco vManage but receives an error message. What is the problem?

Options:

A- A centralized control policy is already applied to the specific site ID and direction

B- The policy for 'Hub' should be applied in the outbound direction, and the policy for 'All-Site' should be applied inbound.

C- Apply an additional outbound control policy to override the site ID overlaps.

D- Site-list 'All-Site' should be configured with a new match sequence that is lower than the sequence for site-list 'Hub*.

Answer:

D

Explanation:

The problem is that the site-list "All-Site" has a higher match sequence than the site-list "Hub", which means that the policy for "All-Site" will take precedence over the policy for "Hub" for any site that belongs to both lists. This creates a conflict and prevents the engineer from adding a new centralized control policy in Cisco vManage. To resolve this issue, the site-list "All-Site" should be configured with a new match sequence that is lower than the sequence for site-list "Hub", so that the policy for "Hub" will be applied first and then the policy for "All-Site" will be applied only to the remaining sites that are not in the "Hub" list.Reference:=

Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5), Module 3: Cisco SD-WAN Cloud OnRamp for Colocation, Lesson 3: Cisco SD-WAN Cloud OnRamp for Colocation - Centralized Control Policies

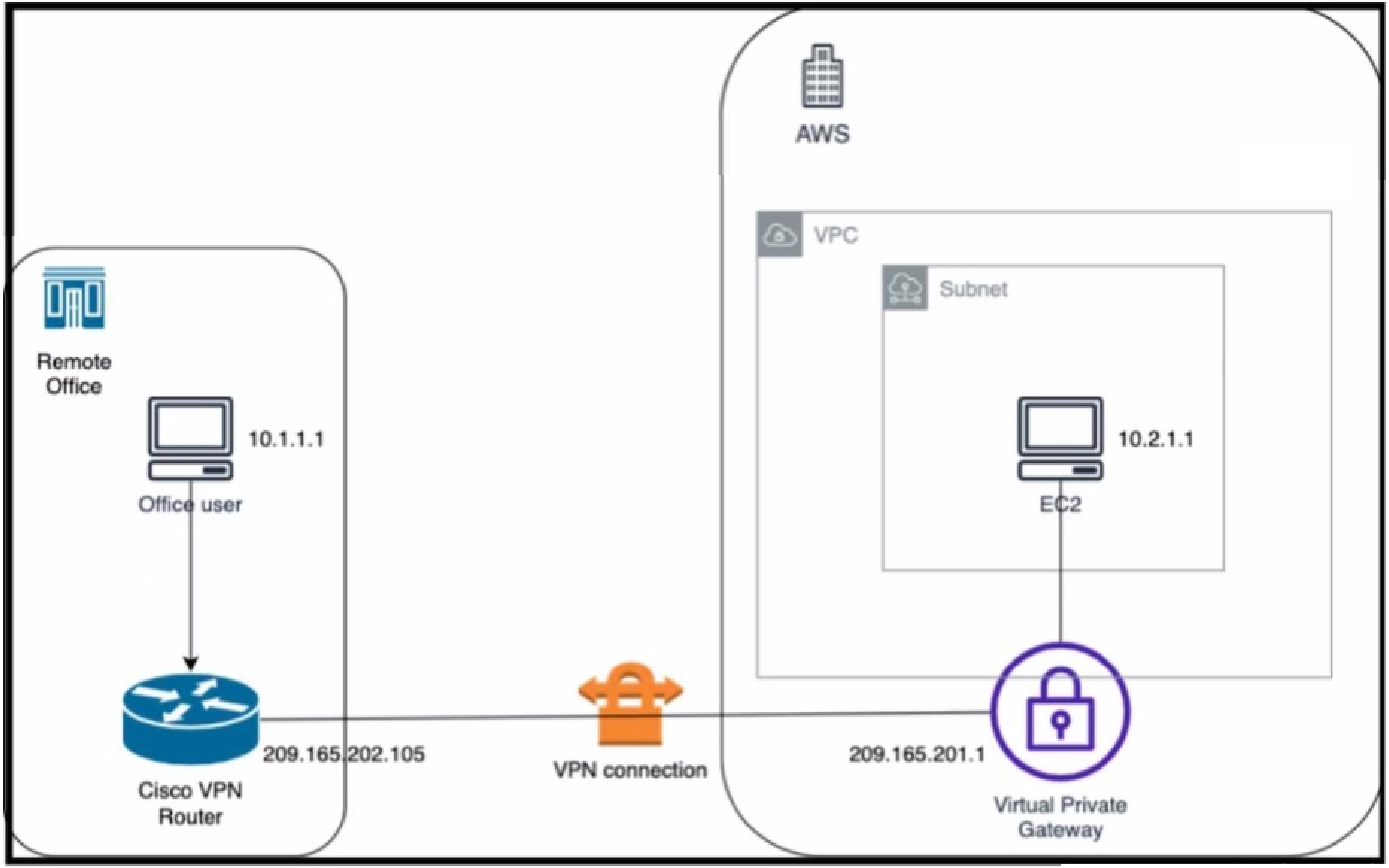
Cisco SD-WAN Cloud OnRamp for Colocation Deployment Guide, Chapter 4: Configuring Centralized Control Policies

Cisco SD-WAN Configuration Guide, Release 20.3, Chapter: Centralized Policy Framework, Section: Policy Configuration Overview

Question 9

Question Type: MultipleChoice

Refer to the exhibits.


AWS
VPC
Subnet
Remote Office
10.1.1.1
Office user
10.2.1.1
EC2
Cisco VPN Router
209.165.202.105
VPN connection
209.165.201.1
Virtual Private Gateway

Refer to the exhibit. An engineer successfully brings up the site-to-site VPN tunnel between the remote office and the AWS virtual private gateway, and the site-to-site routing works correctly. However, the end-to-end ping between the office user PC and the AWS EC2 instance is not working. Which two actions diagnose the loss of connectivity? (Choose two.)

Options:

A- Check the network security group rules on the host VNET.

B- Check the security group rules for the host VPC.

C- Check the IPsec SA counters.

D- On the Cisco VPN router, configure the IPsec SA to allow ping packets.

E- On the AWS private virtual gateway, configure the IPsec SA to allow ping packets.

Answer:

B, C

Explanation:

The end-to-end ping between the office user PC and the AWS EC2 instance is not working because either the security group rules for the host VPC are blocking the ICMP traffic or the IPsec SA counters are showing errors or drops. To diagnose the loss of connectivity, the engineer should check both the security group rules and the IPsec SA counters. The network security group rules on the host VNET are not relevant because they apply to Azure, not AWS. The IPsec SA configuration on the Cisco VPN router and the AWS private virtual gateway are not likely to be the cause of the problem because the site-to-site VPN tunnel is already up and the site-to-site routing works correctly.Reference:=

Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5), Module 3: Configuring IPsec VPN from Cisco IOS XE to AWS, Lesson 3: Verify IPsec VPN Connectivity

Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter: IPsec VPN Overview, Section: IPsec Security Association

AWS Documentation, User Guide for AWS VPN, Section: Security Groups for Your VPC

20%
DISCOUNT