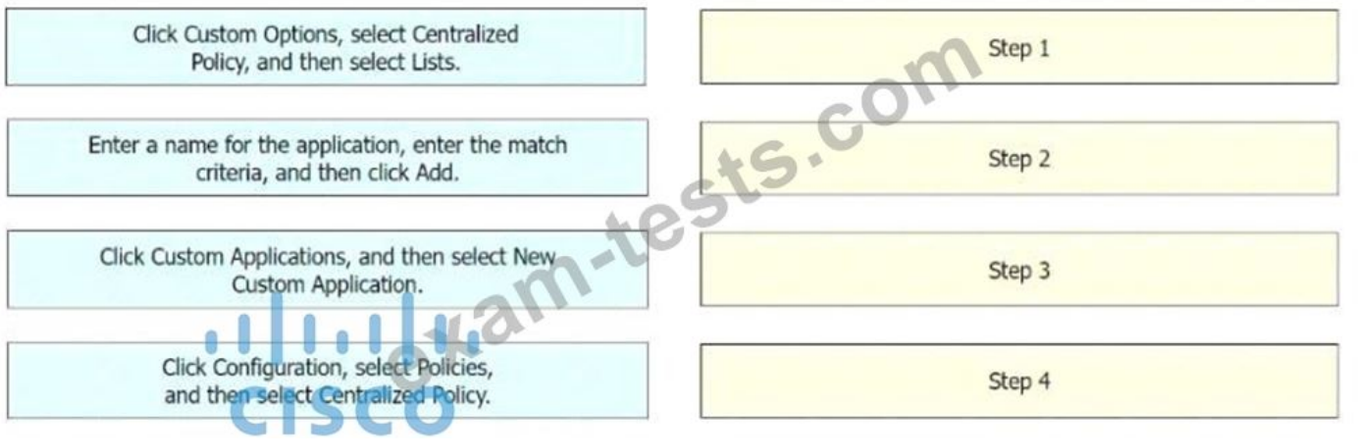
Cisco.300-440.v2024-07-16.q13

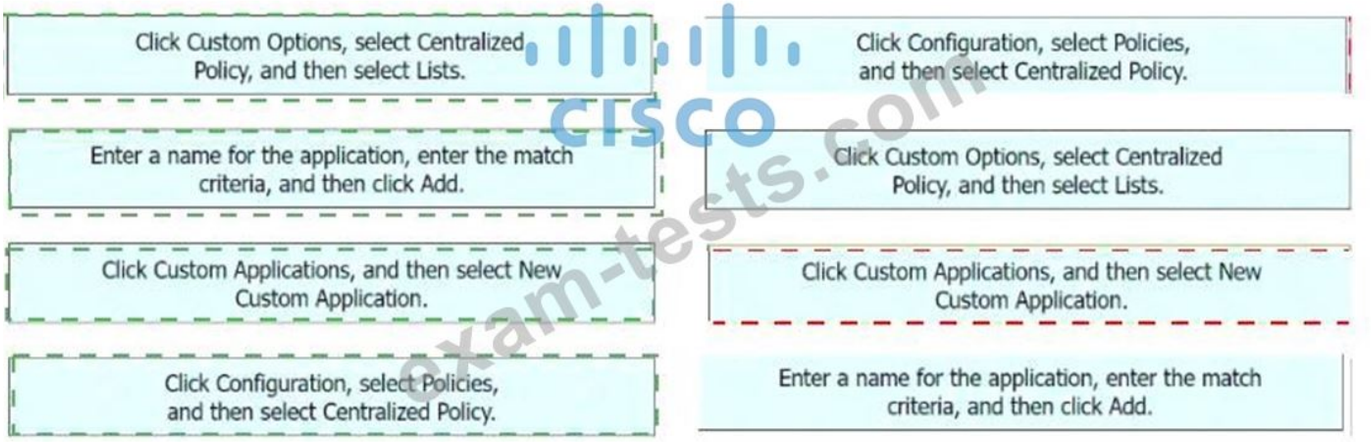
Exam Code:	300-440
Exam Name:	Designing and Implementing Cloud Connectivity
Certification Provider:	Cisco
Free Question Number:	13
Version:	v2024-07-16
# of views:	216
# of Questions views:	130
https://www.exam-tests.com/300-440-exam/Cisco.300-440.v2024-07-16.q13.html	

NEW QUESTION: 1

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:



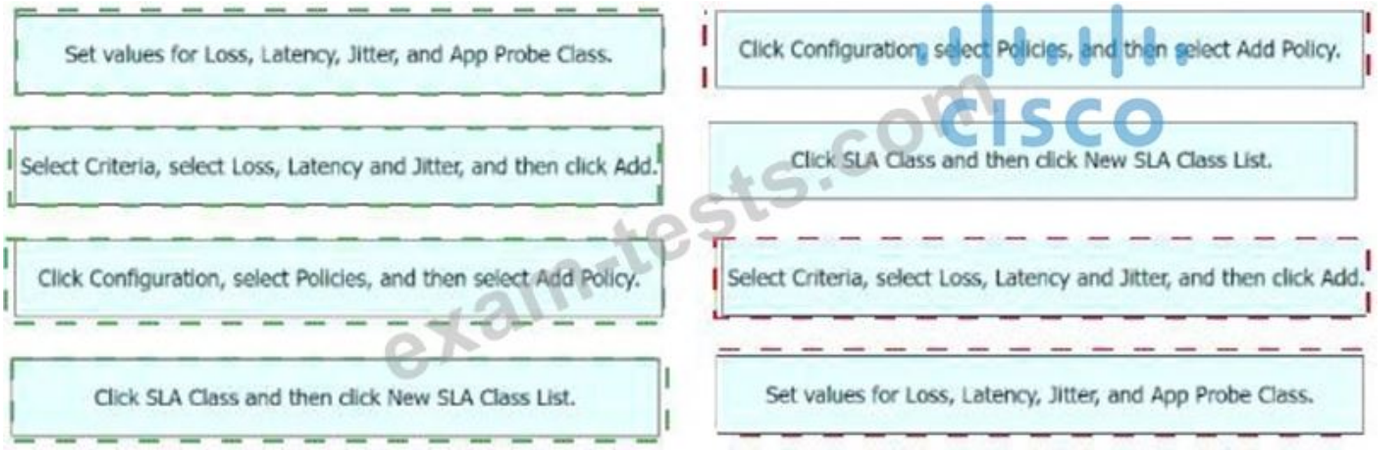
Explanation:

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

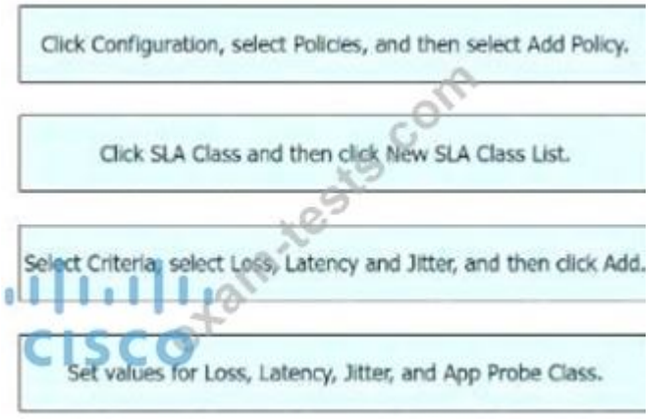
Click Configuration, select Policies, and then select Centralized Policy.
Click Custom Options, select Centralized Policy, and then select Lists.
Click Custom Applications, and then select New Custom Application.
Enter a name for the application, enter the match criteria, and then click Add.
The process 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.
References :=
Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE

NEW QUESTION: 2
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.

Answer:



Explanation:



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 steps12.

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 vManage1.

Click SLA Class and then click New SLA Class List: In this step, you create a new SLA Class List1.

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 Jitter1.

Set values for Loss, Latency, Jitter, and App Probe Class: Finally, you set the values for Loss, Latency, Jitter, and App Probe Class1.

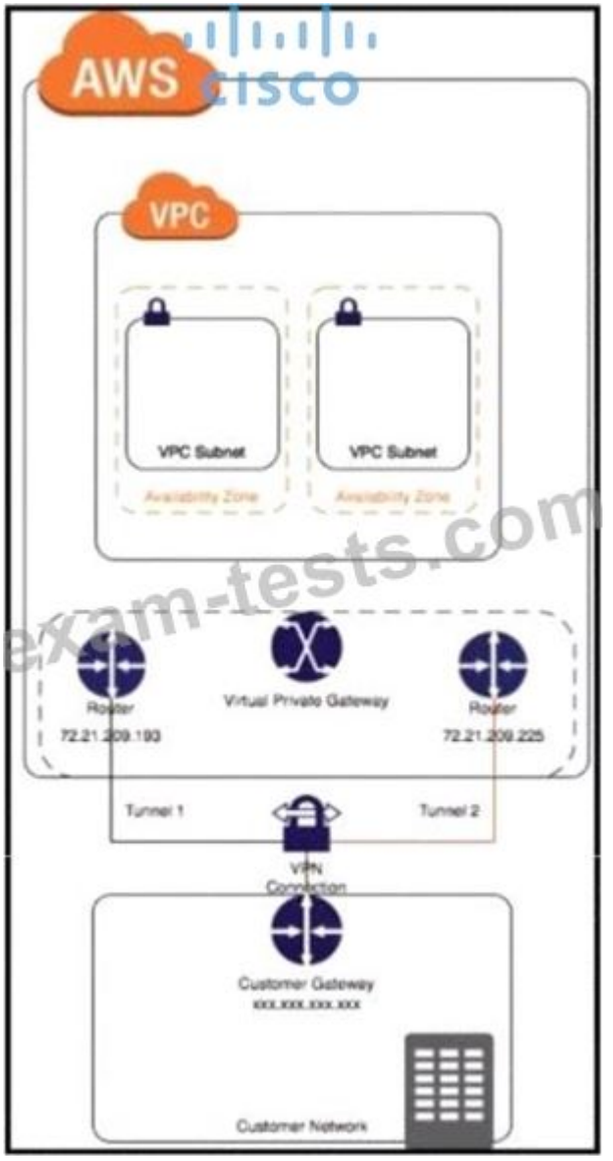
References :=

Information About Application-Aware Routing - Cisco

Policies Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20

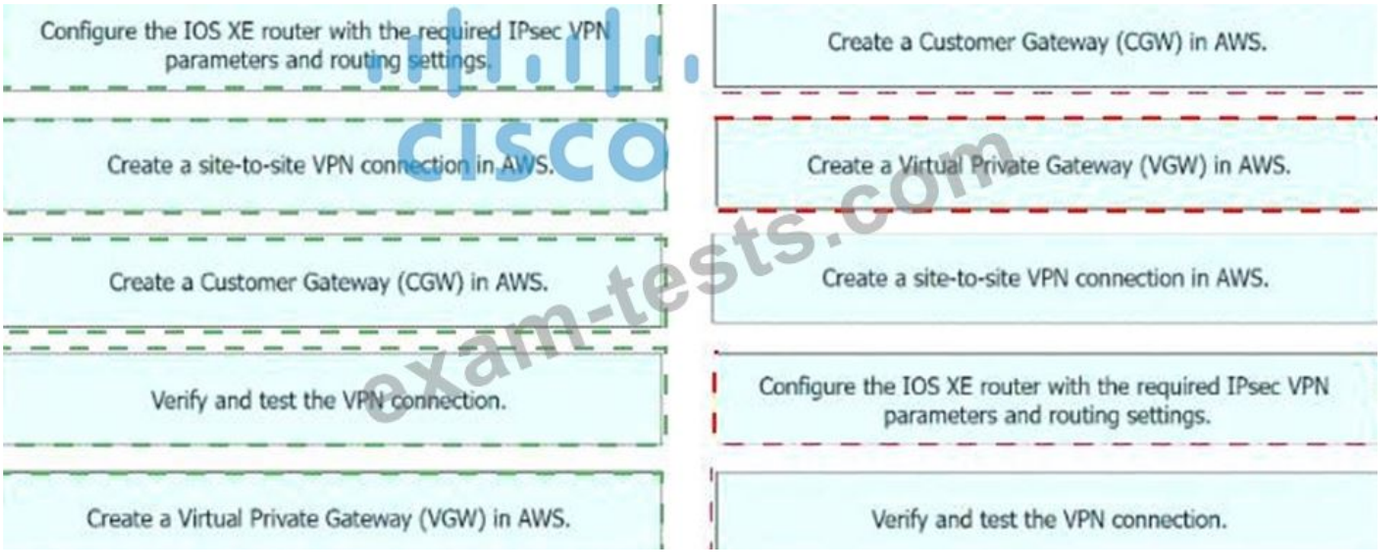
NEW QUESTION: 3

Refer to the exhibit.



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).

Answer:



Explanation:

Step 1 = Create a Customer Gateway (CGW) in AWS. Step 2 = Create a Virtual Private Gateway (VGW) in AWS. Step 3 = Create a site-to-site VPN connection in AWS. Step 4 = Configure the IOS XE router with the required IPsec VPN parameters and routing settings. Step 5 = Verify and test the VPN connection.

The process of configuring a site-to-site VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS) involves several steps12.

Create a Customer Gateway (CGW) in AWS: This is the first step where you define the public IP address of your on-premises Cisco IOS XE router in AWS1.

Create a Virtual Private Gateway (VGW) in AWS: This involves creating a VGW and attaching it to the VPC in AWS1.

Create a site-to-site VPN connection in AWS: After setting up the CGW and VGW, you then create a site-to-site VPN connection in AWS. This involves specifying the CGW, VGW, and the static IP prefixes for your on-premises network1.

Configure the IOS XE router with the required IPsec VPN parameters and routing settings: After the AWS side is set up, you configure the on-premises Cisco IOS XE router with the required IPsec VPN parameters and routing settings2.

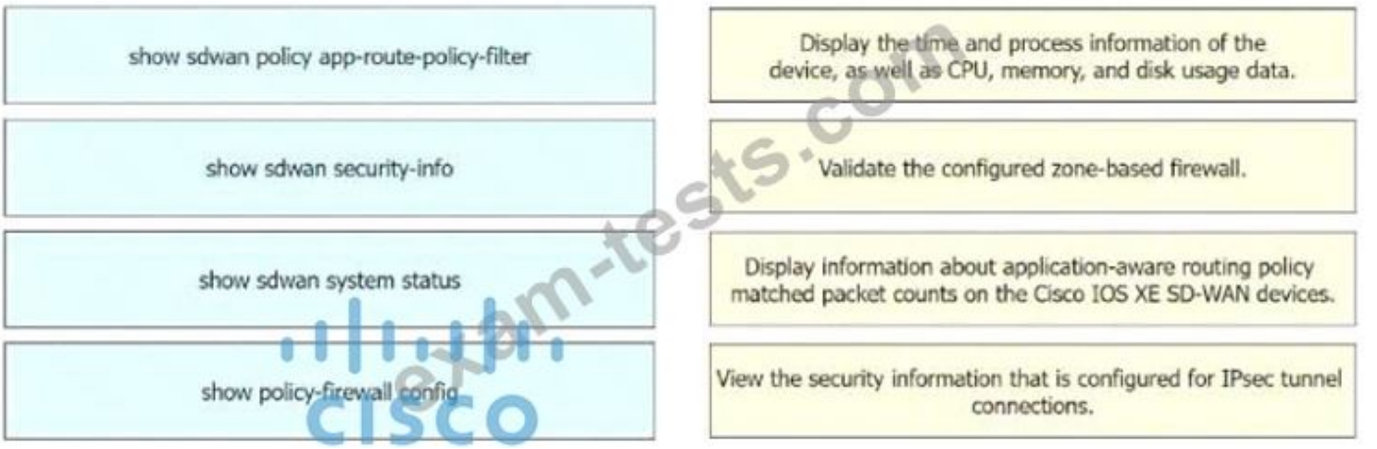
Verify and test the VPN connection: Finally, you verify and test the VPN connection to ensure that it is working correctly12.

References :=

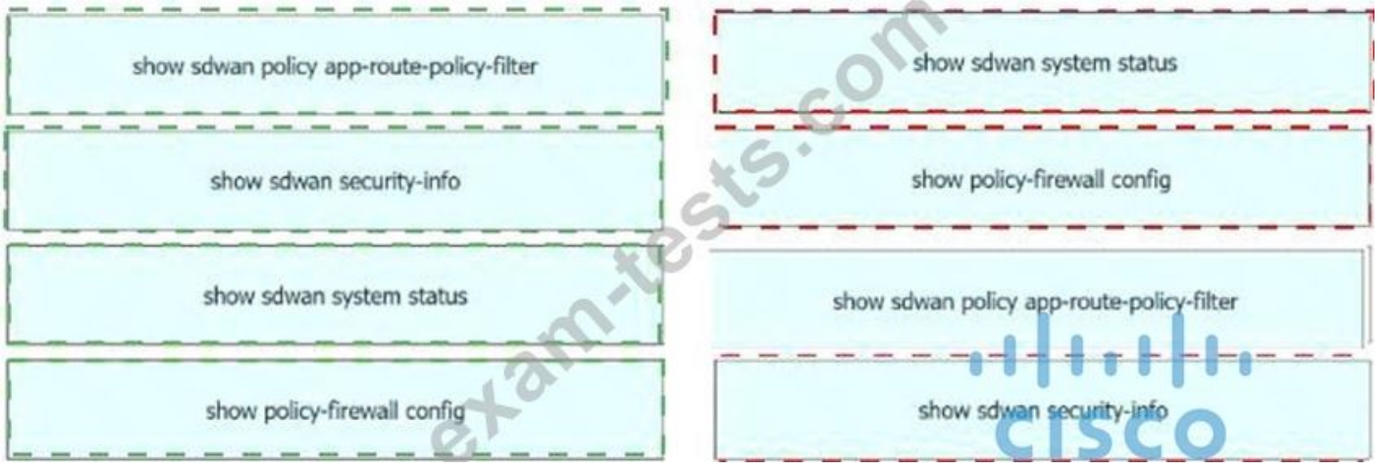
Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community SD-WAN Configuration Example: Site-to-site (LAN to LAN) IPSec between vEdge and Cisco IOS - Cisco Community

NEW QUESTION: 4

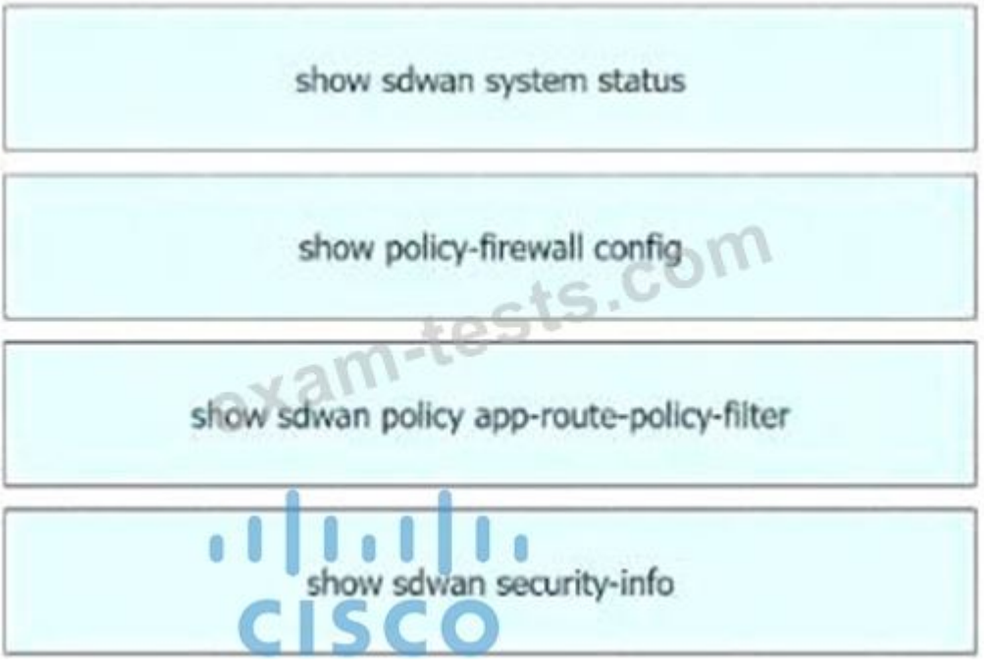
Drag and drop the commands from the left onto the purposes on the right to identify issues on a Cisco IOS XE SD-WAN device.



Answer:



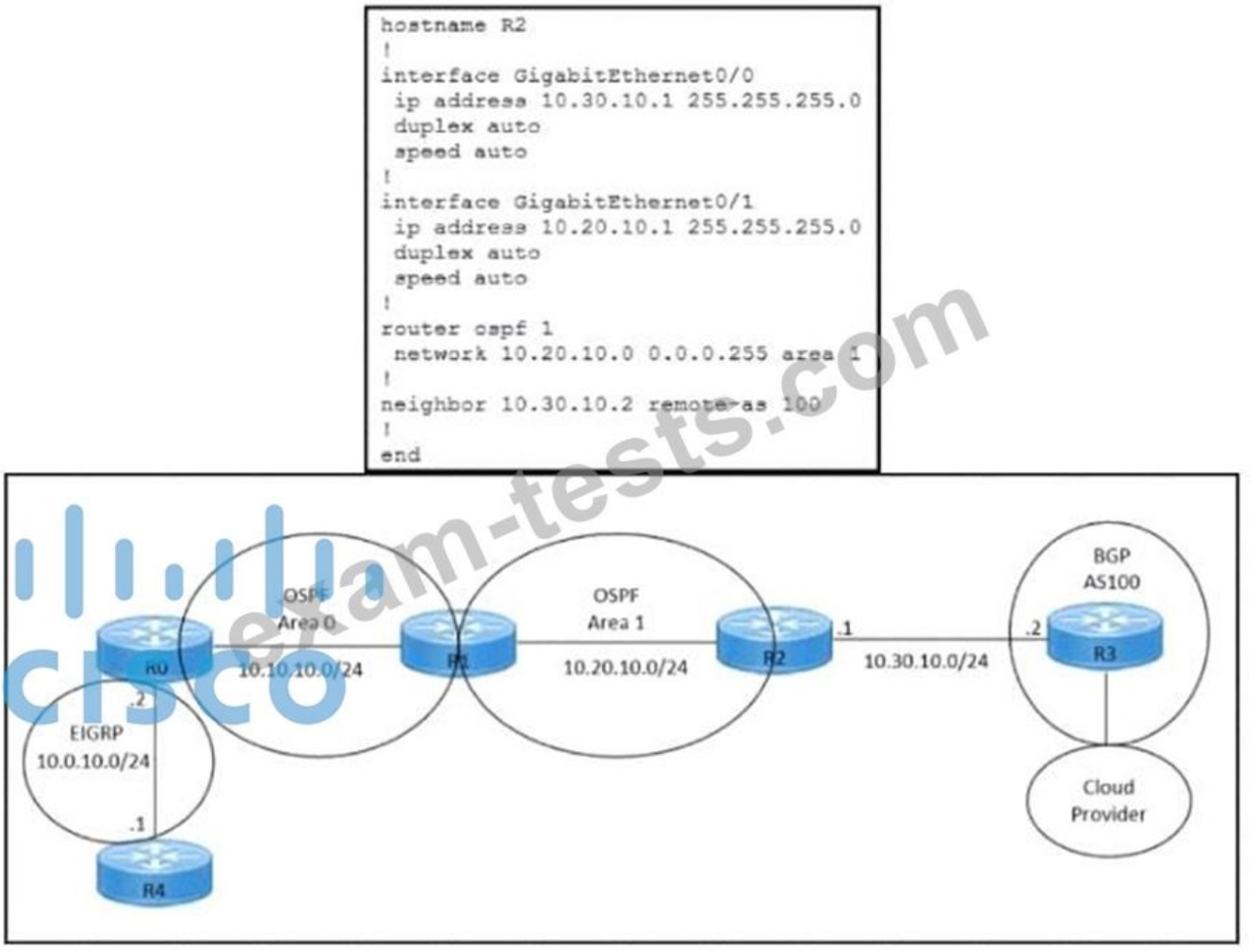
Explanation:



Display the time and process information of the device, as well as CPU, memory, and disk usage data. = show sdwan system status1 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-filter1 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 follows1:
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 data1.
show policy-firewall config: This command is used to validate the configured zone-based firewall1.
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 devices1.
show sdwan security-info: This command is used to view the security information that is configured for IPsec tunnel connections1.
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

NEW QUESTION: 5



Refer to the exhibits. An engineer must redistribute OSPF internal routes into BGP to connect an on-premises network to a cloud provider without introducing extra routes. Which two commands must be configured on router R2? (Choose two.)

A. router ospf 1

B. router bgp 100

C. redistribute ospf 1

D. redistribute bgp 100

E. redistribute ospf 1 match internal external

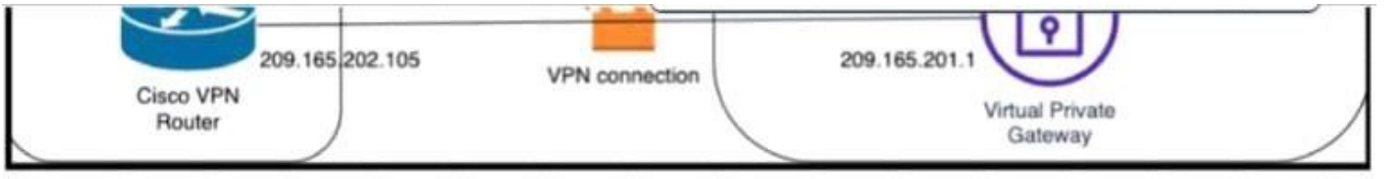
Answer: B,E (LEAVE A REPLY)

To redistribute OSPF internal routes into BGP, the engineer needs to configure two commands on router R2.

The first command is router bgp 100, which enables BGP routing process and specifies the autonomous system number of 100. The second command is redistribute ospf 1 match internal external, which redistributes the routes from OSPF process 1 into BGP, and matches both internal and external OSPF routes. This way, the engineer can avoid introducing extra routes that are not part of OSPF process 1, such as the default route or the connected routes. References: = Designing and Implementing Cloud Connectivity (ENCC) v1.0, [ENCC:
Configuring IPsec VPN from Cisco IOS XE to AWS], [Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs]

NEW QUESTION: 6

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
!
```

```
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
```

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 209.165.201.1
  match identity remote address 209.165.202.105 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
```

C.

Answer: C (LEAVE A REPLY)

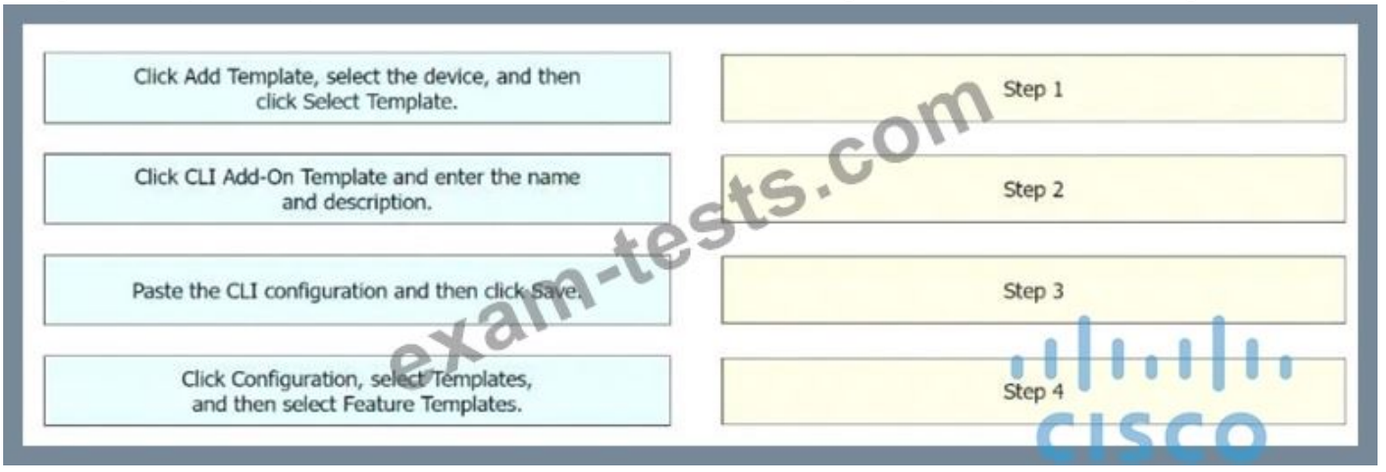
Option C is the correct answer because it configures the IKEv2 profile with the correct match identity, authentication, and keyring parameters. It also configures the IPsecprofile with the correct transform set and lifetime parameters. Option A is incorrect because it does not specify the match identity 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 pre-share 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 AWS1 and Cisco2 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

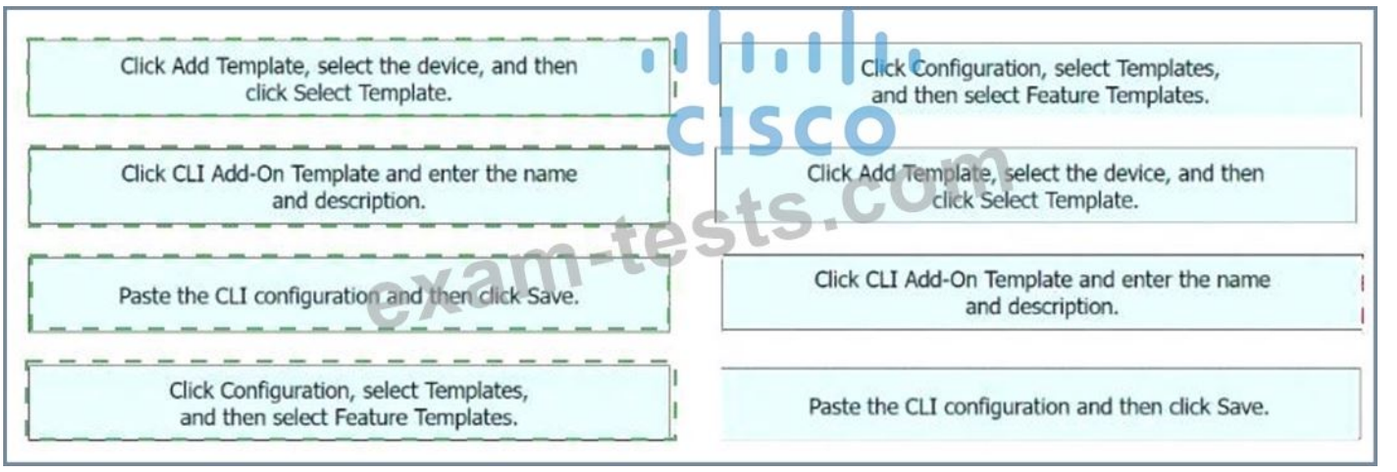
2: Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services

NEW QUESTION: 7
An engineer must enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device. What should be configured after the global address-family ipv4 is configured?
A. Set the VRF-specific route advertisements.
B. Enable bgp advertisement.
C. Enter sdwan mode.
D. Disable bgp advertisement.
Answer: B (LEAVE A REPLY)
To enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device, the engineer must first configure the global address-family ipv4 and then enable bgp advertisement under the vrf definition. This will allow the device to advertise the BGP routes learned from the cloud provider to the OMP control plane, which will then distribute them to the other SD-WAN devices in the overlay network1 References := 1: Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3: Implementing Cloud Connectivity, Lesson 3: Configuring IPsec VPN from Cisco IOS XE to AWS, Topic: Configuring BGP on the Cisco IOS XE Device, Page 3-24.

NEW QUESTION: 8
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.



Answer:



Explanation:

Step 1 = Click Configuration, select Templates, and then select Feature Templates. Step 2 = Click Add Template, select the device, and then click Select Template. Step 3 = Click CLI Add-On Template and enter the name and description. Step 4 = Paste the CLI configuration and then click Save.

The process of configuring a CLI add-on feature template in Cisco vManage for enhanced policy-based routing (ePBR) for IPv4 involves several steps1234.

Click Configuration, select Templates, and then select Feature Templates: This is the first step where you navigate to the Templates section in the Configuration menu of Cisco vManage1.

Click Add Template, select the device, and then click Select Template: In this step, you add a new template for the device1.

Click CLI Add-On Template and enter the name and description: After setting up the template, you select the CLI Add-On Template option, and then enter the name and description for the template1.

Paste the CLI configuration and then click Save: Finally, you paste the CLI configuration into the template and save the changes1.

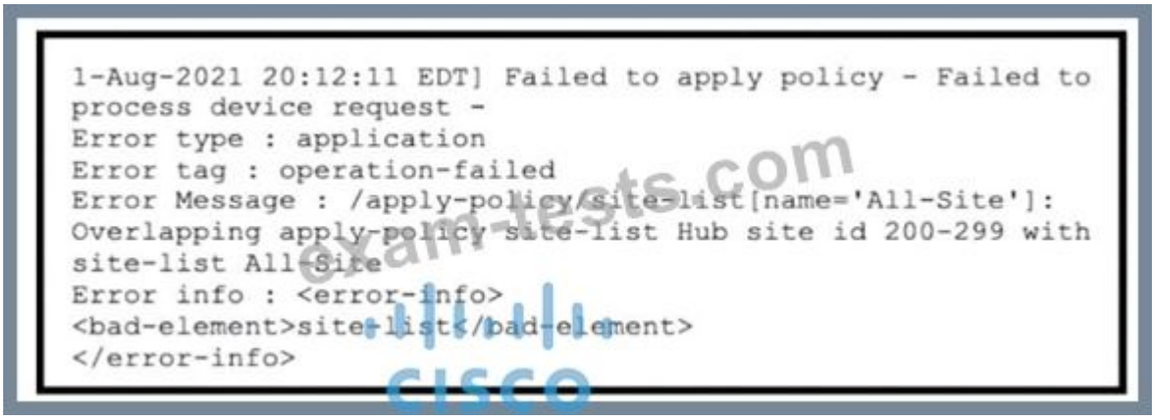
References :=

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

NEW QUESTION: 9

Refer to the exhibit.



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?

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 (LEAVE A REPLY)

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. References := 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

NEW QUESTION: 10

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. point-to-point topology using dedicated leased lines and static routing

B. star topology with internet-based VPN connections and static routing

C. hub-and-spoke topology with SD-WAN technology, using dynamic routing and OSPF as the routing protocol

D. fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol

Answer: D (LEAVE A REPLY)

NEW QUESTION: 11

An engineer must enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device. What should be configured after the global address-family ipv4 is configured?

A. Enable bgp advertisement.

B. Disable bgp advertisement.

C. Enter sdwan mode.

D. Set the VRF-specific route advertisements.

Answer: A (LEAVE A REPLY)

To enable the OMP advertisement of BGP routes for a specific VRF instance on a Cisco IOS XE SD-WAN device, the engineer must first configure the global address-family ipv4 and then enable bgp advertisement under the vrf definition. This will allow the device to advertise the BGP routes learned from the cloud provider to the OMP control plane, which will then distribute them to the other SD-WAN devices in the overlay network1 References := 1: Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3: Implementing Cloud Connectivity, Lesson 3: Configuring IPsec VPN from Cisco IOS XE to AWS, Topic: Configuring BGP on the Cisco IOS XE Device, Page 3-24.

NEW QUESTION: 12

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

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: (SHOW ANSWER)

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 orinternal 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. References := FedRAMP Authorization Boundary Guidance document1

NEW QUESTION: 13
Which approach does a centralized internet gateway use to provide connectivity to SaaS applications?
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 (LEAVE A REPLY)
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. References := 1: Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 1:
Cloud Connectivity Overview, Lesson 1: Cloud Connectivity Concepts, Topic: Centralized Internet Gateway 2: Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Release 17.3.1a and Later, Topic:
Centralized Internet Gateway 3: Architect and optimize your internet traffic with Azure routing preference, Microsoft Azure Blog, Topic: Routing via the premium Microsoft global network 4: What is SaaS? Softwareas a Service, Microsoft Azure, Topic: How SaaS works 5: How an application gateway works, Microsoft Learn, Topic: Application gateway components