300-440 Q&As

Designing and Implementing Cloud Connectivity (ENCC)

Pass Cisco 300-440 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

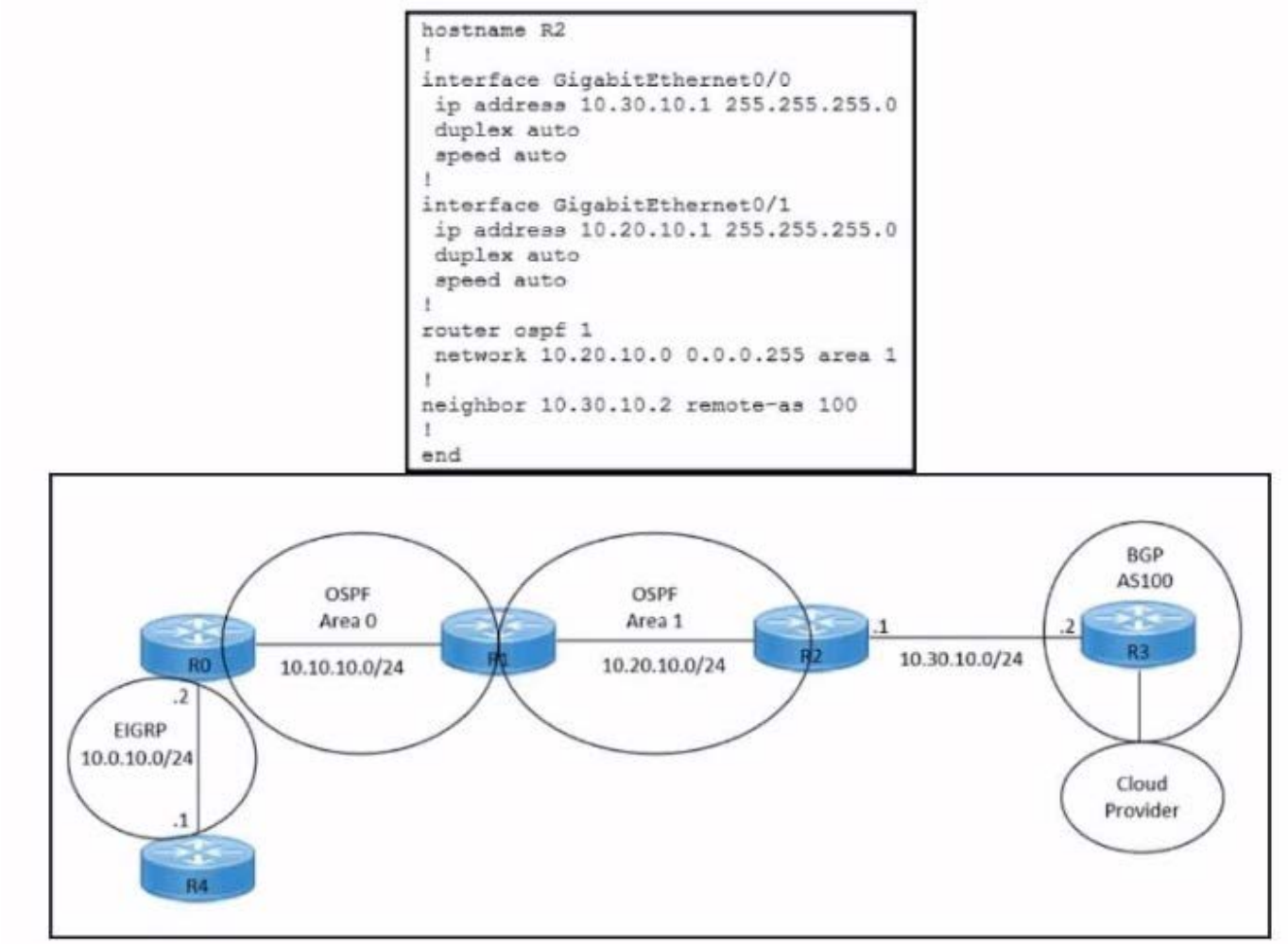
https://www.certbus.com/300-440.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

Correct Answer: BE

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 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:

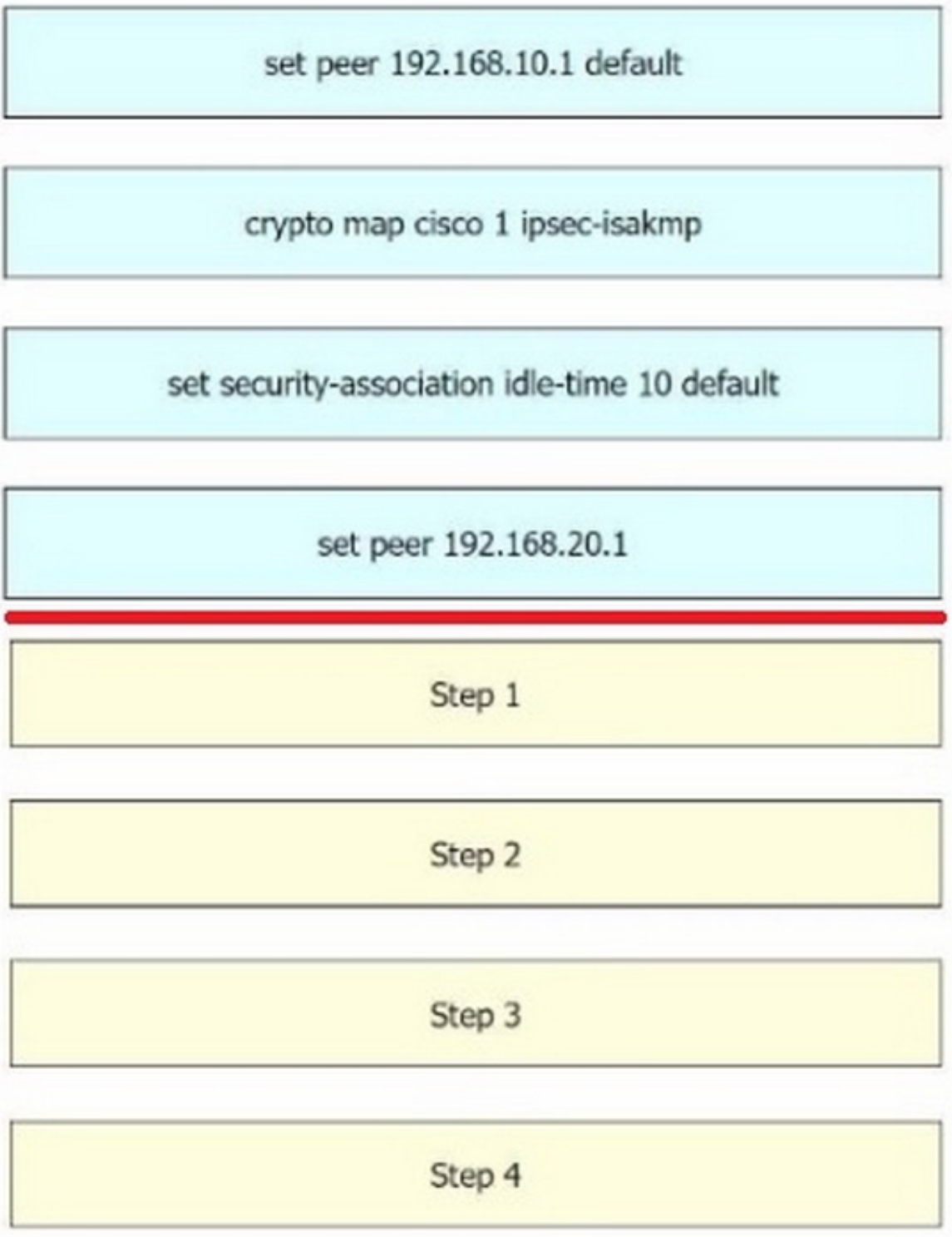
Designing and Implementing Cloud Connectivity (ENCC) v1.0, [ENCC: Configuring IPsec VPN from Cisco IOS XE to AWS], [Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs]

QUESTION 2

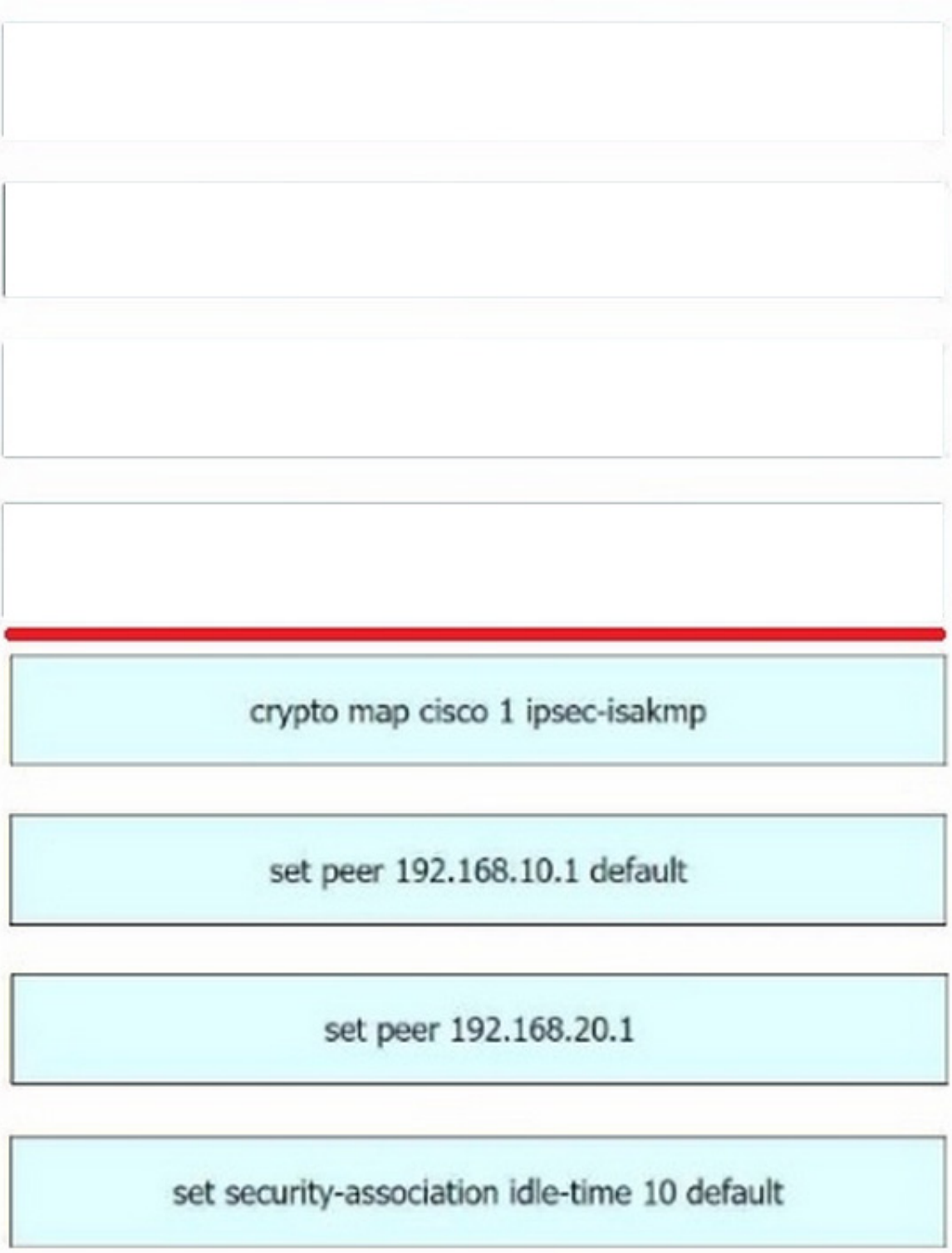
DRAG DROP

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.

Select and Place:



Correct Answer:



Step 1 = crypto map cisco 1 ipsec-isakmp Step 2 = set peer 192.168.10.1 default Step 3 = set peer 192.168.20.1 Step 4 = set security-association idle-time 120 default

The process of editing the settings of a site-to-site IPsec VPN connection between an on- premises Cisco IOS XE router and Amazon Web Services (AWS), and configuring IPsec to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco involves several steps123456. crypto map cisco 1 ipsec-isakmp: This command is used to create a new entry in the crypto map named "cisco". The "1" is the sequence number of the entry, and "ipsec-isakmp" specifies that the IPSec security associations (SAs) should be established using the

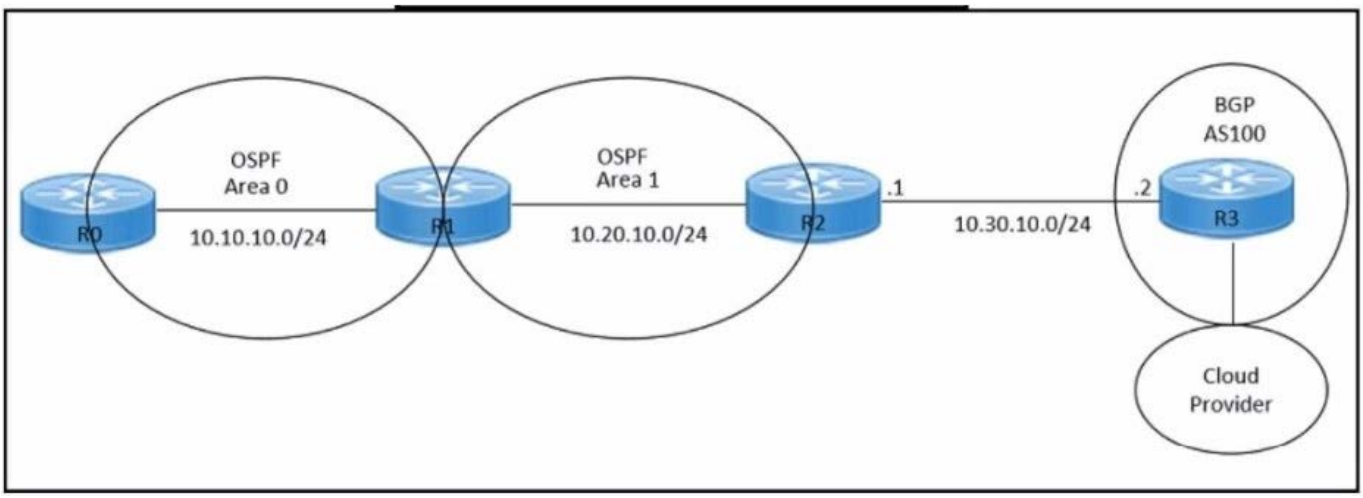
Internet Key Exchange (IKE) protocol13. set peer 192.168.10.1 default: This command is used to specify the IP address of the default peer for the crypto map entry. In this case, the default peer is at IP address 192.168.10.115. set peer 192.168.20.1: This command is used to add an additional peer to the crypto map entry. In this case, the additional peer is at IP address 192.168.20.1. This allows the IPsec VPN to support multiple peers56. set security-association idle-time 120 default: This command is used to set the idle time for the security association. If no traffic is detected over the VPN for the specified idle time (in this case, 120 seconds), the security association is deleted, and the VPN connection fails over to the next peer46.

References: 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 3

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
```



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.)

A. router bgp 100

B. redistribute bgp 100

C. router ospf 1

D. redistribute ospf 1

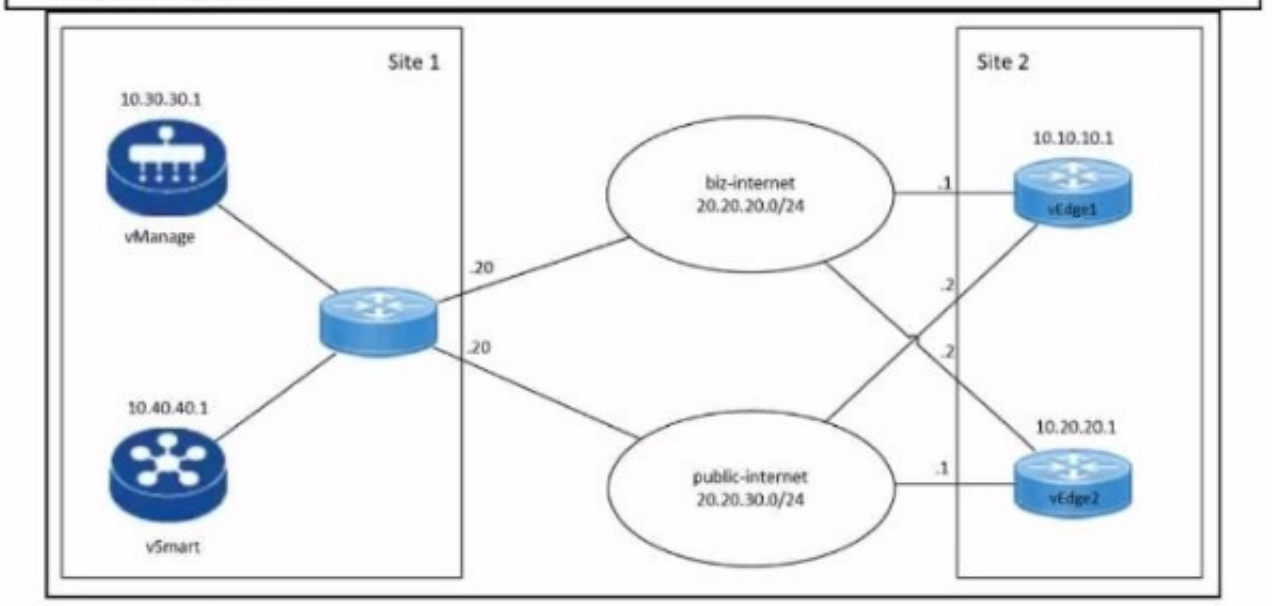
E. redistribute ospf 100

Correct Answer: AD

QUESTION 4

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.

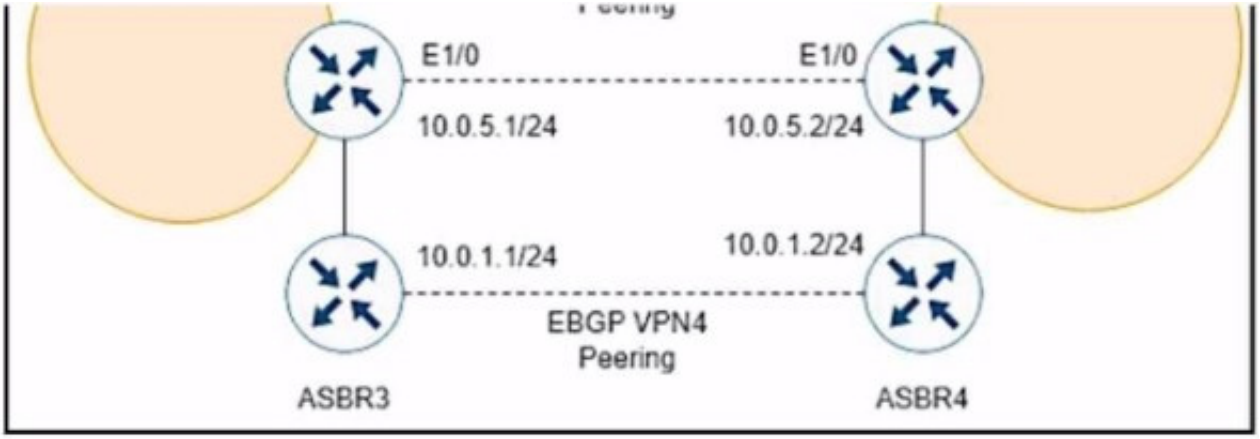
C. The remote Edge device has a duplicate IP address.

D. The control plane deleted the BFD session.

Correct Answer: B

QUESTION 5

Refer to the exhibits.



While troubleshooting, a network engineer discovers that the backup path fails between ASBR3 and ASBR4 for traffic between BGP AS6000 and BGP AS6500 when the connection between ASBR1 and ASBR2 goes down. The following configurations were performed on ASBR1:

```
ASBR1(config)# router bgp 6000
ASBR1 (config-router)# address-family vpn4
ASBR1 (config-router-af)# neighbor 10.0.5.2 remote-as 6500
ASBR1 (config-router-af)# neighbor 10.0.5.2 activate
ASBR1 (config-router-af)# neighbor 10.0.5.2 fall-over bfd
ASBR1 (config-router-af)# end
```

Which command is missing?

A. bgp additional-paths Install

B. bgp additional-paths select

C. redistribute static

D. bgp advertise-best-external

Correct Answer: D

The bgp advertise-best-external command is used to enable the advertisement of the best external path to internal BGP peers. This command is useful when there are multiple exit points from the local AS to other ASes, and the local AS wants to use the closest exit point for each destination. By default, BGP only advertises the best path to its peers, and the best path is usually the one with the lowest IGP metric to the next hop. However, this may not be the optimal path for traffic leaving the local AS, as it may result in suboptimal hot-potato routing or MED oscillations. The bgp advertise-best-external command allows BGP to advertise the best external path, which is the path with the lowest MED among the paths from different neighboring ASes, in addition to the best path. This way, the internal BGP peers can choose the best exit point based on the MED value, rather than the IGP metric. In this scenario, ASBR1 is configured to receive additional paths from ASBR2, which is a route reflector. ASBR2 receivestwo paths for the same prefix from AS6500, one from ASBR3 and one from ASBR4. ASBR2 selects the best path based on the IGP metric to the next hop, and advertises it to ASBR1. However, this path may not be the best external path, as it may have a higher MED value than the other path. If the connection between ASBR1 and ASBR2 goes down, ASBR1 will not have any backup path to reach AS6500, as it does not know the other path from ASBR4. To prevent this situation, ASBR1 should be configured with the bgp advertise-best-external command, so that it can receive the best external path from ASBR2, along with the best path. This way, ASBR1 will have a backup path to reach AS6500, in case the primary path fails.

QUESTION 6

What is the role of service providers to establish private connectivity between on-premises networks and Google Cloud resources?

A. facilitate direct, dedicated network connections through Google Cloud Interconnect

B. enable intelligent routing and dynamic path selection using software-defined networking

C. provide end-to-end encryption for data transmission using native IPsec

D. accelerate content delivery through integration with Google Cloud CDN

Correct Answer: A

The role of service providers to establish private connectivity between on- premises networks and Google Cloud resources is to facilitate direct, dedicated network connections through Google Cloud Interconnect. Google Cloud Interconnect is

a service that allows customers to connect their on-premises networks to Google Cloud through a service provider partner. This provides low latency, high bandwidth, and secure connectivity to Google Cloud services, such as Google

Compute Engine, Google Cloud Storage, and Google BigQuery. Google Cloud Interconnect also supports hybrid cloud scenarios, such as extending on-premises networks to Google Cloud regions, or connecting multiple Google Cloud

regions together. Google Cloud Interconnect offers two types of connections: Dedicated Interconnect and Partner Interconnect. Dedicated Interconnect provides physical connections between the customer\\'s network and Google\\'s network at

a Google Cloud Interconnect location. Partner Interconnect provides virtual connections between the customer\\'s network and Google\\'s network through a supported service provider partner. Both types of connections use VLAN attachments

to establish private connectivity to Google Cloud Virtual Private Cloud (VPC) networks.

References:

Designing and Implementing Cloud Connectivity (ENCC) v1.0 [Google Cloud Interconnect Overview] [Google Cloud Interconnect Documentation]

QUESTION 7

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

1.

high availability

2.

quality of service (QoS)

3.

multihoming

4.

specific routing needs

Which connectivity model meets these requirements?

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

Correct Answer: D

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 SDWAN technology can also support specific routing needs, such as segment routing, policy-based routing, or application-aware routing.

References:

Designing and Implementing Cloud Connectivity (ENCC) v1.0 [Cisco SD-WAN Design Guide]

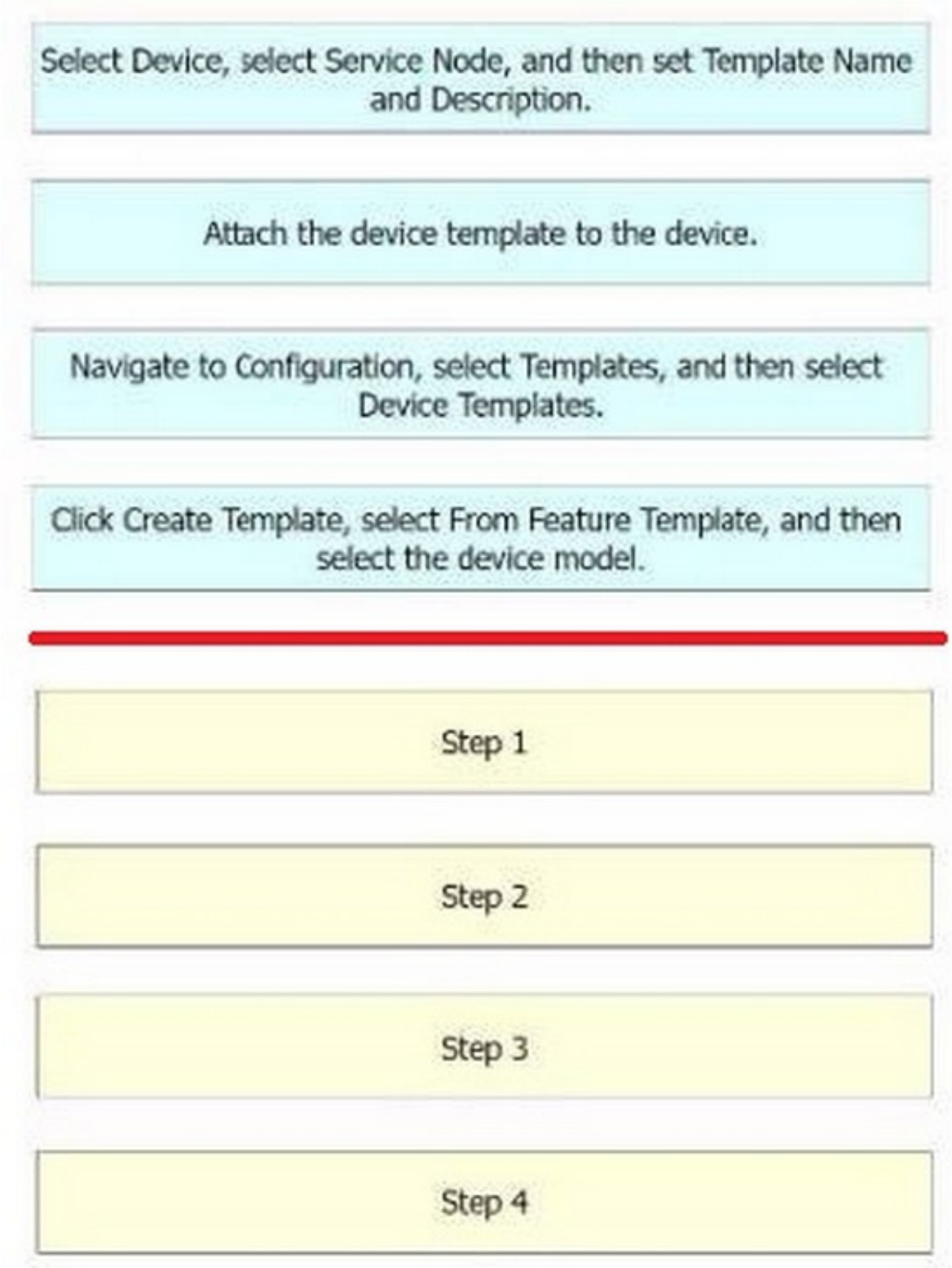
[Cisco SD-WAN Configuration Guide]

QUESTION 8

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:



Correct Answer:

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 9

An engineer is implementing a highly securemultitierapplication in AWS that includes S3. RDS, and some additional private links. What is critical to keep the traffic safe?

A. VPC peering and bucket policies

B. specific routing and bucket policies

C. EC2 super policies and specific routing policies

D. gateway load balancers and specific routing policies

Correct Answer: B

A highly secure multitier application in AWS that includes S3, RDS, and some additional private links requires specific routing and bucket policies to keep the traffic safe. The reasons are as follows:

Specific routing policies are needed to ensure that the traffic between the tiers is routed through the private links, which provide secure and low-latency connectivity between AWS services and on-premises resources12. The private links can

also prevent the exposure of the data and the application logic to the public internet12. Bucket policies are needed to control the access to the S3 buckets that store the application data34. Bucket policies can specify the conditions under

which the requests are allowed or denied, such as the source IP address, the encryption status, the request time, etc.34. Bucket policies can also enforce encryption in transit and at rest for the data in S334.

References:

1: AWS PrivateLink

2: AWS PrivateLink FAQs

3: Using Bucket Policies and User Policies

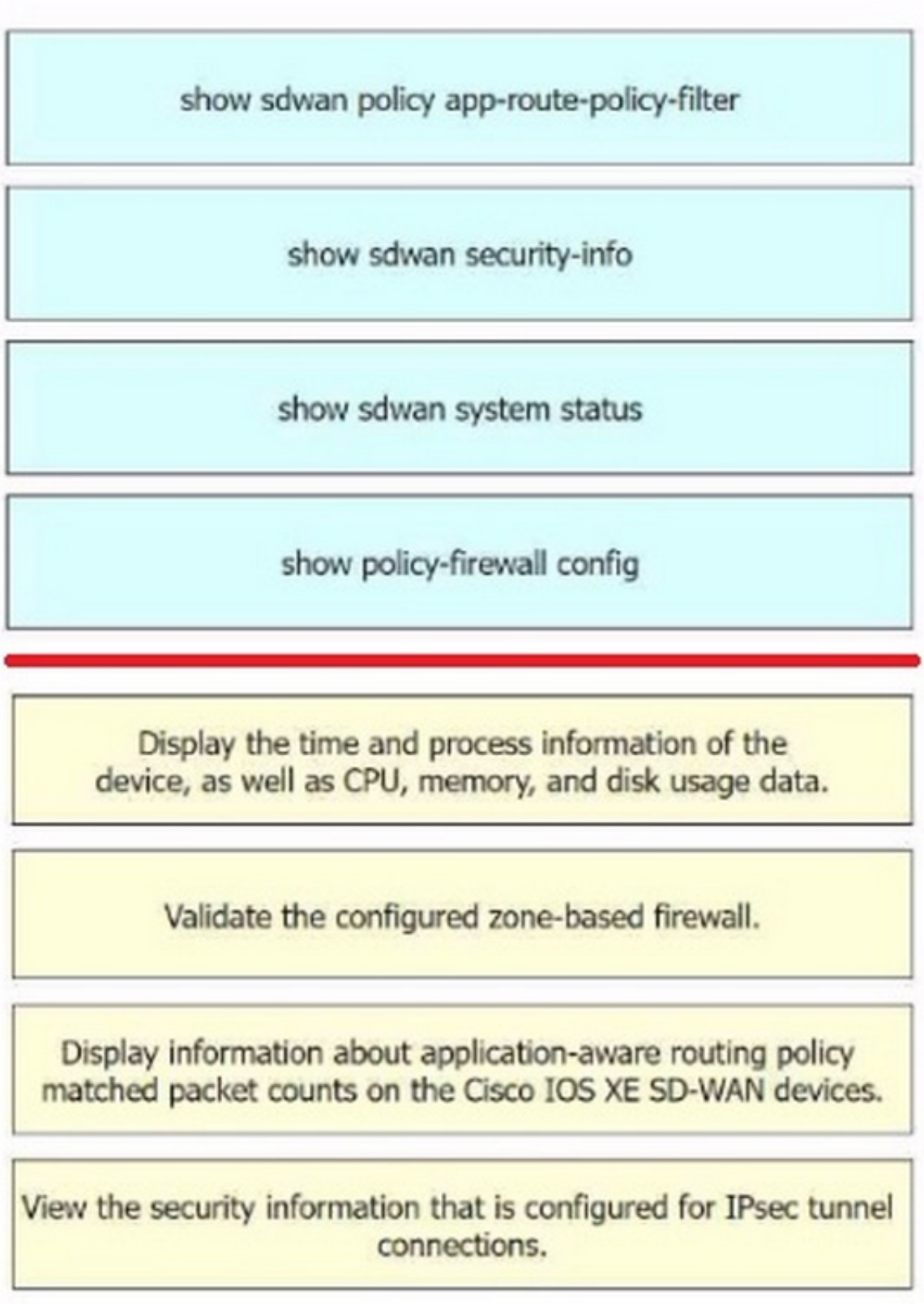
4: Bucket Policy Examples

QUESTION 10

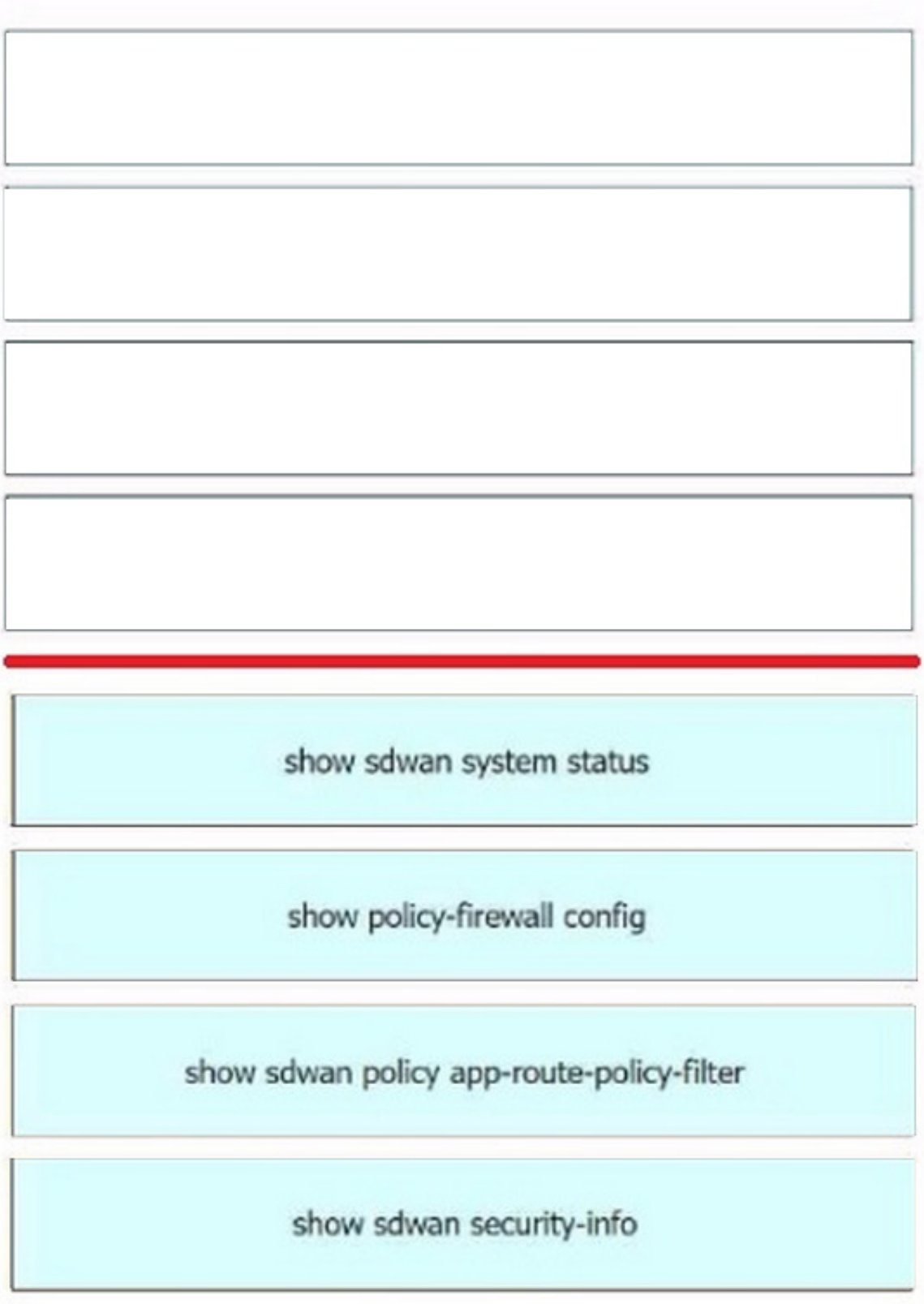
DRAG DROP

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:



Correct Answer:



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