300-440 Q&As

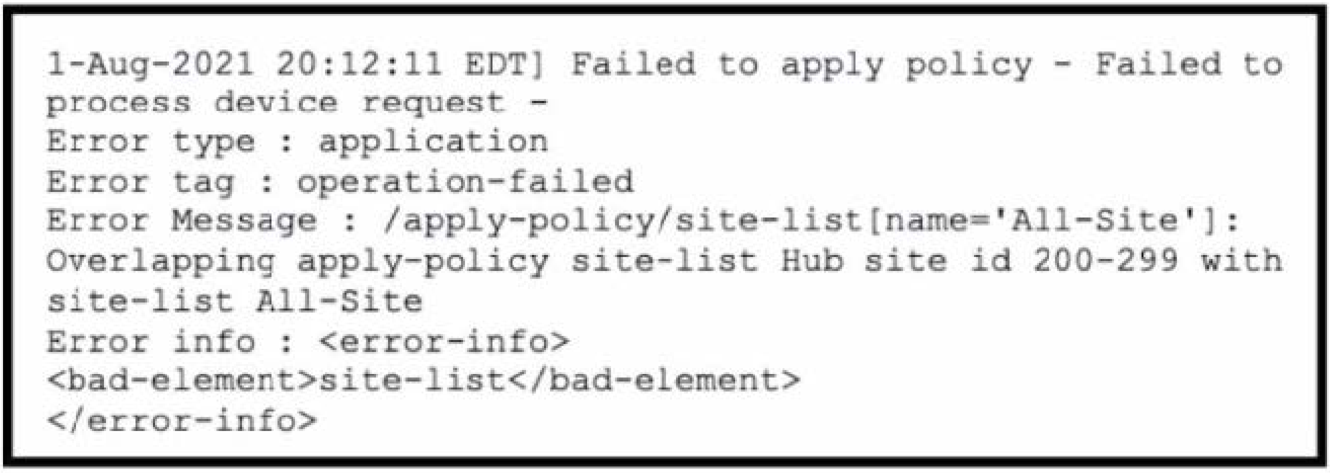
Designing and Implementing Cloud Connectivity (ENCC)

Pass Cisco 300-440 Exam with 100% Guarantee

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

QUESTION 1

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?

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*.

Correct Answer: D

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

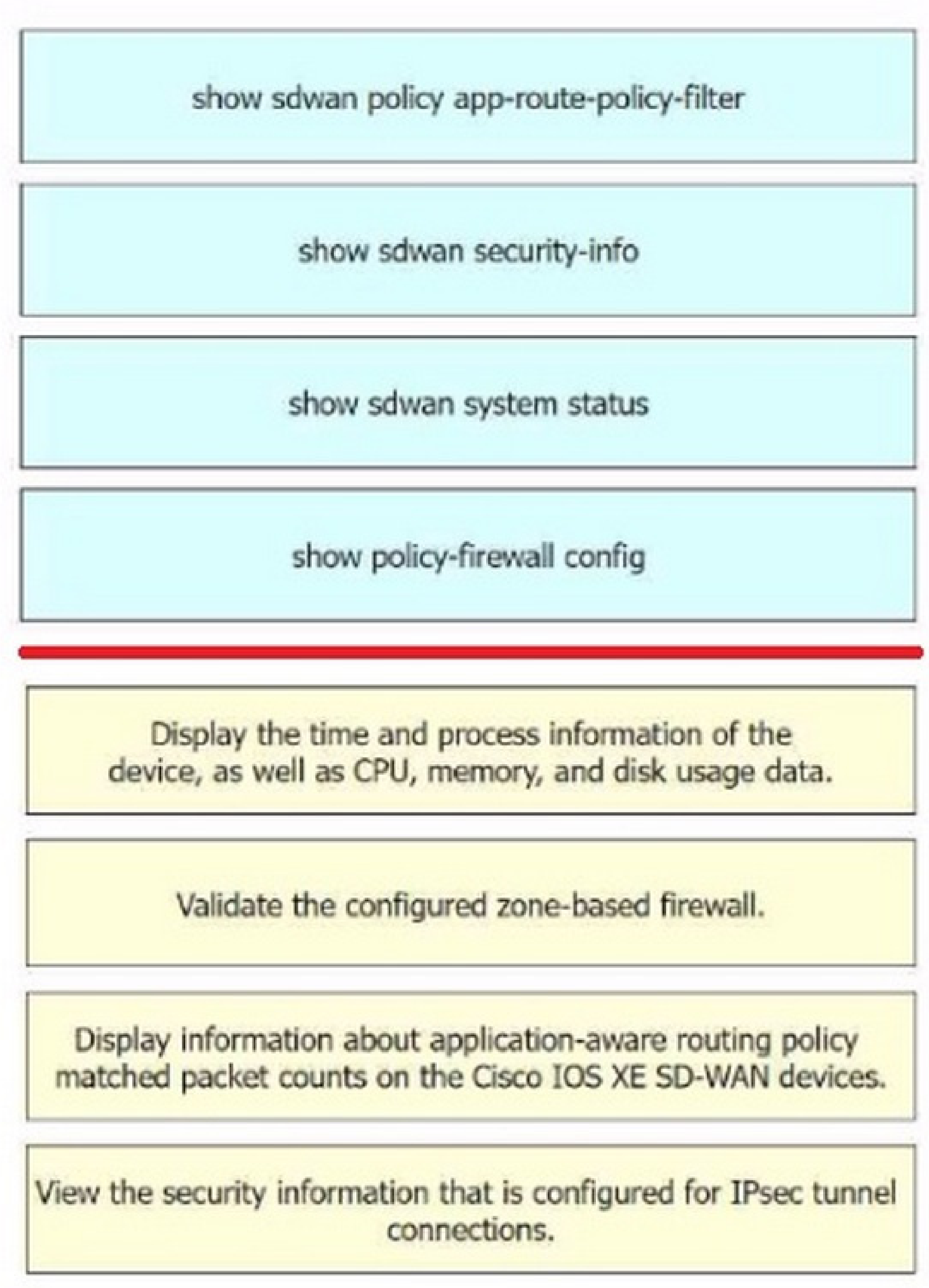
Framework, Section: Policy Configuration Overview

QUESTION 2

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

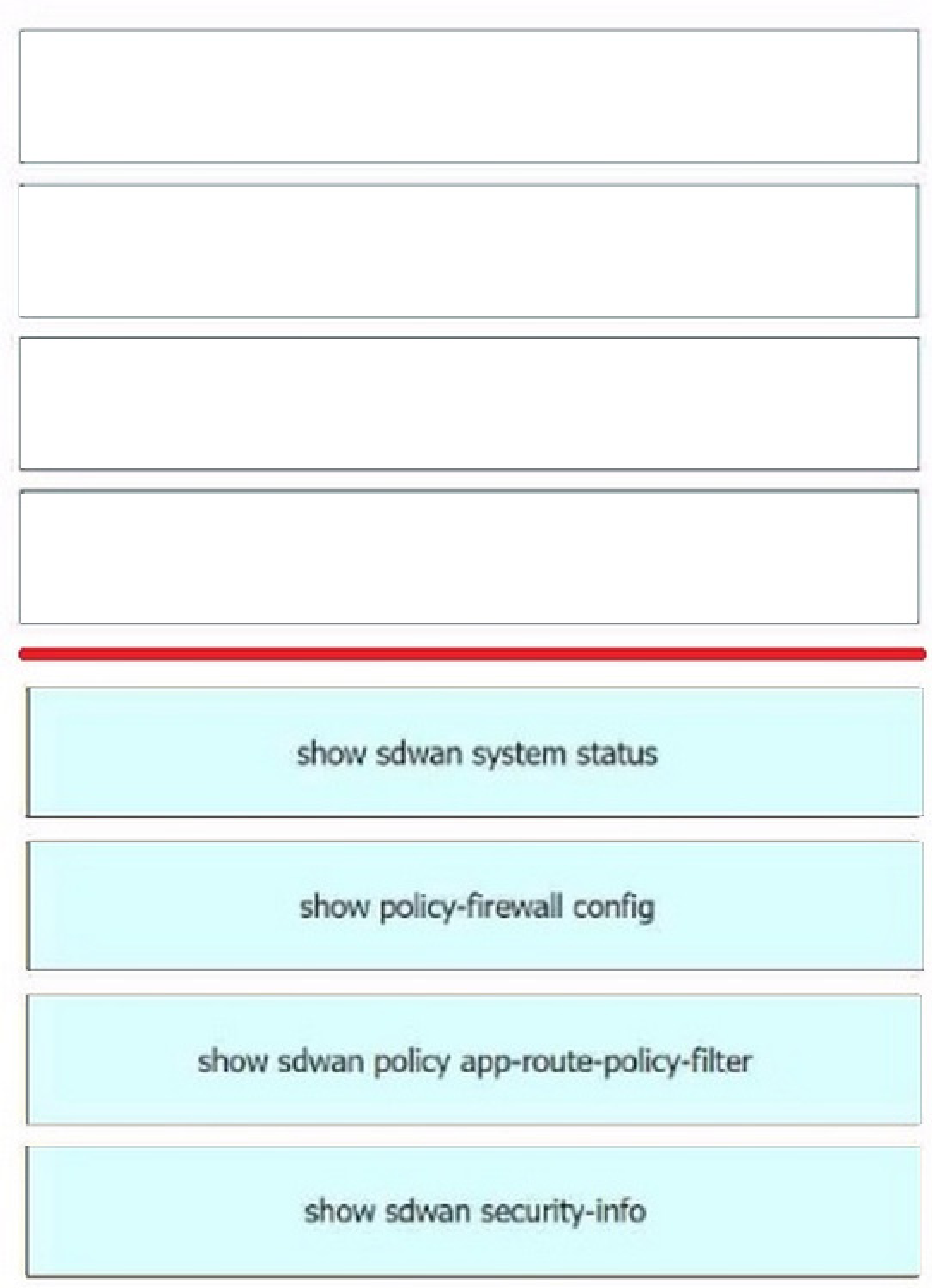
Display the time and process information of the device, as well as CPU, memory, and disk usage data.

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 3

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.

Correct Answer: B

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.

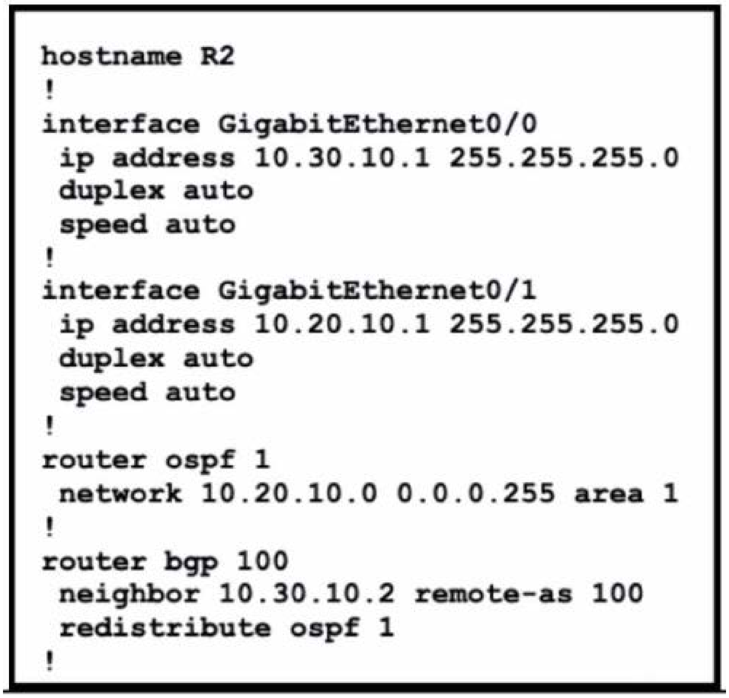
This will allow the device to advertise the BGP routes learned from the cloud provider to the OMP control plane, which will then distribute them to the other SD-WAN devices in the overlay network.

References:

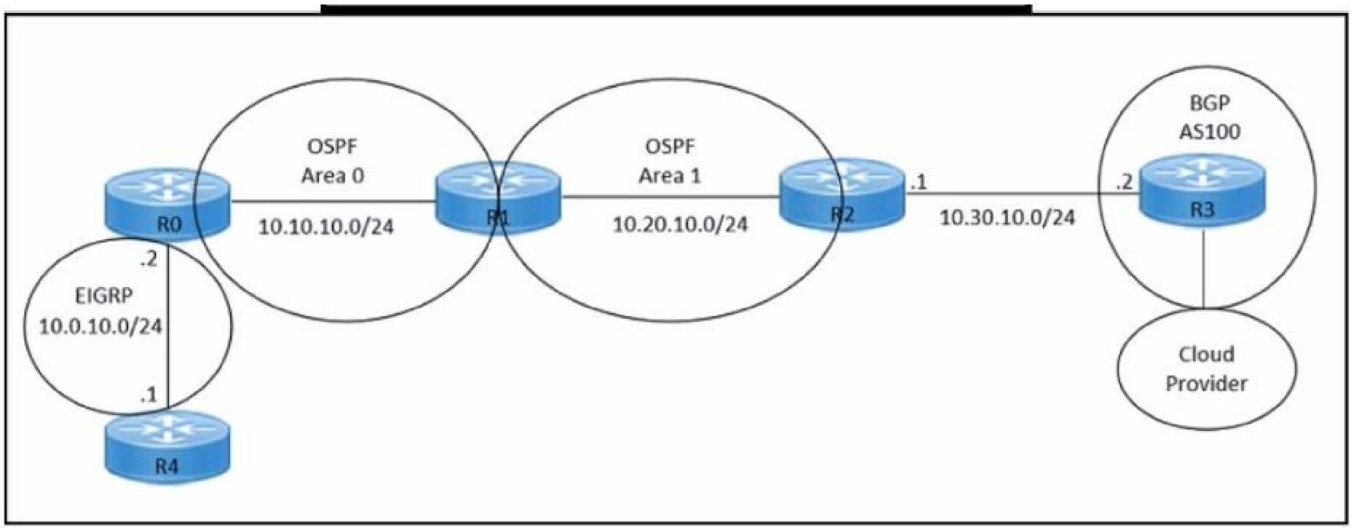
Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:Implementing Cloud Connectivity, Lesson 3: Configuring IPsec VPN from Cisco IOS XE to AWS, Topic: Configuring BGP on the Cisco IOS XE Device, Page 3-24.

QUESTION 4

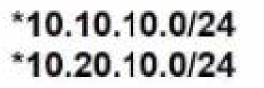
Refer to the exhibits.



```
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
!
```



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?

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

Correct Answer: C

The command redistribute ospf 1 match external is 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.

References:

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 5

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