# Oracle

## 1Z0-1124-25 Exam

**Oracle Cloud Infrastructure 2025 Networking Professional**

**Questions & Answers**
**Demo**

# Version: 4.0

## Question: 1

You are troubleshooting a connectivity issue between two compute instances within the same VCN. Both instances are in different subnets. Instance A (IPv4: 10.0.1.10, IPv6: fc00:1:1::10) can ping its subnet gateway (10.0.1.1) and can ping the IPv6 address of Instance B (fc00:1:2::20), but cannot ping Instance B's IPv4 address (10.0.2.20). The security lists and network security groups (NSGs) are configured to allow all traffic between the subnets. The route table for Instance A's subnet has a rule to route all traffic destined to 10.0.2.0/24 subnet to the VCN Local Peering Gateway. What is the most probable cause?

A. The VCN does not have IPv6 enabled.
B. The route table for Instance B's subnet is missing a rule to route traffic destined for 10.0.1.0/24 to the VCN Local Peering Gateway.
C. IPv6 traffic cannot be filtered by security lists or NSGs.
D. The "ping" utility is not supported on the IPv6 address.

**Answer: B**

Explanation:

Analyze Connectivity Successes: Instance A can ping its subnet gateway (10.0.1.1), indicating that local subnet routing and security rules are functioning for IPv4. It can also ping Instance B's IPv6 address (fc00:1:2::20), confirming that IPv6 routing and security rules between subnets are operational.
Identify the Failure: Instance A cannot ping Instance B's IPv4 address (10.0.2.20). Since security lists and NSGs allow all traffic, the issue is unlikely to be a security configuration problem.
Examine Routing for Instance A: The route table for Instance A's subnet (10.0.1.0/24) has a rule directing traffic to 10.0.2.0/24 via the VCN Local Peering Gateway (LPG). In OCI, LPGs are used for intra-region VCN peering, but here, both instances are in the same VCN, so this rule is likely a misconfiguration or irrelevant unless peering is involved. However, the successful IPv6 ping suggests basic connectivity exists.
Check Return Path from Instance B: For a ping to succeed, Instance B must send ICMP replies back to Instance A (10.0.1.10). Instance B's subnet (10.0.2.0/24) needs a route table entry to send traffic to 10.0.1.0/24. Without this, replies are dropped, causing the IPv4 ping to fail. The IPv6 success indicates that IPv6 routing is correctly configured both ways, possibly via SLAAC or default routes.
Evaluate Options:
A: Incorrect. IPv6 is enabled, as Instance A pings Instance B's IPv6 address.

B: Correct. Missing route for 10.0.1.0/24 in Instance B's subnet prevents IPv4 replies.
C: Incorrect. Security lists and NSGs can filter IPv6 traffic in OCI.
D: Incorrect. Ping supports IPv6, as evidenced by the successful IPv6 ping.
The most probable cause is a missing route in Instance B's subnet route table. In OCI, each subnet has its own route table, and for instances in different subnets within the same VCN to communicate, both subnets must have appropriate routes. The successful IPv6 ping suggests that IPv6 routing is intact (likely due to default behavior or SLAAC), but IPv4 requires explicit routing. Per the Oracle Networking Professional study guide, "Route tables must be configured to direct traffic to the appropriate next hop for inter-subnet communication within a VCN" (OCI Networking Documentation, Section: Virtual Cloud Networks).
Reference: Oracle Cloud Infrastructure Documentation - Networking Overview, Route Tables.

## Question: 2

You are designing a backup solution in OCI. Compute instances in a private subnet need to back up data to OCI Object Storage. Security policy mandates that data transfer must not traverse the public internet. You need to choose the most secure and cost-effective method for accessing Object Storage. Which endpoint/gateway configuration should you implement?

A. Configure an Internet Gateway and use public Object Storage endpoints.
B. Configure a NAT Gateway and use public Object Storage endpoints with HTTPS enabled.
C. Configure a Service Gateway with the Oracle Services Network service CIDR label for your region, and use regional Object Storage endpoints.
D. Configure a Dynamic Routing Gateway (DRG) and FastConnect to a remote region and use public Object Storage endpoints.

Product Questions:
Version:

**Answer: C**

Explanation:

Requirement Analysis: The solution must ensure private access to Object Storage without public internet traversal, while being cost-effective.
Evaluate OCI Components:
Internet Gateway: Provides public internet access, unsuitable for private connectivity.
NAT Gateway: Allows outbound internet access from private subnets, but traffic still exits OCI.
Service Gateway: Enables private access to OCI services like Object Storage within the same region.
DRG with FastConnect: Used for on-premises connectivity, not intra-OCI service access.
Option Assessment:
A: Uses public internet, violating the security policy.
B: HTTPS encrypts data, but traffic traverses the internet via NAT, violating the policy.
C: Service Gateway keeps traffic within OCI's private network, meeting security and cost goals.
D: Overly complex and costly, with public endpoints contradicting the requirement.

Conclusion: Service Gateway with regional Object Storage endpoints ensures private, secure, and cost-effective access.
The Service Gateway is designed for private access to OCI services like Object Storage, avoiding the public internet. The Oracle Networking Professional study guide states, "A Service Gateway allows instances in a private subnet to access supported OCI services without an Internet Gateway or NAT Gateway, ensuring traffic remains within the Oracle network" (OCI Networking Documentation, Section: Service Gateway). Using the Oracle Services Network service CIDR label for the region ensures compatibility with Object Storage endpoints, optimizing cost and security.
Reference: Oracle Cloud Infrastructure Documentation - Service Gateway.

## Question: 3

Your company has established a hybrid cloud environment using FastConnect to connect your on-premises network to your OCI VCN. You are advertising on-premises network prefixes to OCI via BGP. You want to ensure that OCI only learns routes from your on-premises network that are within a specific range, and that any other prefixes advertised are rejected to prevent routing conflicts. Which BGP attribute and configuration on the OCI side should you use to achieve this?

A. AS Path Prepending: Configure AS Path Prepending on the FastConnect virtual circuit to discourage OCI from selecting routes outside the desired range.
B. MED (Multi-Exit Discriminator): Configure MED values on the on-premises BGP router to influence OCI's route selection based on preferred exit points.
C. Route Filtering using Route Distinguisher (RD) and Route Target (RT): Configure RDs and RTs on the FastConnect virtual circuit to filter routes based on tenant isolation.
D. Route Filtering using Prefix Lists: Configure Prefix Lists on the FastConnect virtual circuit to accept only the desired prefix ranges and reject all others.

**Answer: D**

Explanation:

Objective: Filter BGP routes on OCI to accept only specific on-premises prefixes.
BGP Attributes Overview:
AS Path Prepending: Lengthens AS path to influence route preference, not filtering.
MED: Influences exit point selection, not route acceptance.
RD/RT: Used in MPLS VPNs for tenant isolation, not simple prefix filtering.
Prefix Lists: Directly filter prefixes based on IP ranges.
Evaluate Options:
A: AS Path Prepending affects preference, not filtering; unsuitable.
B: MED influences path selection, not route rejection; incorrect.
C: RD/RT is for VPN contexts, not applicable here.
D: Prefix Lists explicitly allow/deny prefixes, meeting the requirement.
Conclusion: Prefix Lists on the FastConnect virtual circuit provide precise control over accepted routes.
Prefix Lists are the most effective BGP tool for filtering routes in OCI. The Oracle Networking Professional study guide notes, "Prefix Lists can be applied to FastConnect virtual circuits to filter BGP advertisements, ensuring only approved prefixes are learned by OCI" (OCI Networking

Documentation, Section: FastConnect and BGP). This prevents routing conflicts by rejecting unwanted prefixes, aligning with the security and control requirements.
Reference: Oracle Cloud Infrastructure Documentation - FastConnect, BGP Configuration.

## Question: 4

Which OCI service or feature enables the enforcement of granular, identity-based access controls for packet routing, crucial for implementing Zero Trust principles?

A. Internet Gateway
B. Service Gateway
C. Network Security Groups (NSGs)
D. Dynamic Routing Gateway (DRG)

**Answer: C**

Explanation:

Zero Trust Principles: Require explicit, identity-based access controls at every network stage.
Evaluate OCI Services:
Internet Gateway: Enables public internet access, no identity-based control.
Service Gateway: Provides private service access, no granular routing control.
NSGs: Offer stateful, identity-based rules at the VNIC level.
DRG: Facilitates routing, not identity-based access control.
NSG Fit: NSGs allow rules based on VNIC identity, source/destination IP, and ports, aligning with Zero Trust.
Conclusion: NSGs are the best fit for granular, identity-based routing control.
NSGs are pivotal for Zero Trust in OCI. The Oracle Networking Professional study guide states, "Network Security Groups provide granular, stateful security rules that can be applied to specific VNICs, enabling identity-based access controls essential for Zero Trust architectures" (OCI Networking Documentation, Section: Network Security Groups). Unlike security lists (subnet-level), NSGs offer instance-level precision.
Reference: Oracle Cloud Infrastructure Documentation - Network Security Groups.

## Question: 5

You are using Terraform to deploy a multi-tier application architecture consisting of a public subnet hosting a load balancer, a private subnet hosting application servers, and another private subnet hosting a database. The Terraform code successfully creates all the required infrastructure, including route tables and security lists. However, after deployment, you realize that the load balancer cannot reach the application servers in the private subnet. You have verified that the load balancer is healthy and the application servers are running. What is the most likely cause of this connectivity problem?

A. The security list associated with the application server subnet does not allow ingress traffic from the load balancer's IP address range.

B. The route table associated with the application server subnet has a default route pointing to the Internet Gateway, which is incorrect for a private subnet.
C. The Network Address Translation (NAT) Gateway is misconfigured, preventing the application servers from initiating connections back to the load balancer.
D. The load balancer's security list is not configured to allow egress traffic to the application server subnet on the required ports (e.g., port 8080).

**Answer: A**

Explanation:

Problem Scope: Load balancer (public subnet) cannot reach application servers (private subnet).
Connectivity Flow: Load balancer initiates traffic to application servers; application servers respond.
Key checkpoints: routing and security rules.
Analyze Routing: Private subnets typically don’t route to an Internet Gateway by default; they use NAT or Service Gateways. Misrouting (Option B) would affect outbound traffic, not inbound from the load balancer.
Security Rules:
Ingress (App Servers): Must allow traffic from the load balancer’s IP range.
Egress (Load Balancer): Must allow traffic to the application servers.
Evaluate Options:
A: Missing ingress rule on application servers’ security list blocks load balancer traffic; most likely.
B: Incorrect default route affects outbound, not inbound; less likely.
C: NAT misconfiguration impacts outbound, not inbound; incorrect.
D: Load balancer egress is necessary but secondary to application server ingress.
Conclusion: Ingress rule absence on the application server subnet is the primary blocker.
Security lists control traffic at the subnet level in OCI. The Oracle Networking Professional study guide explains, "For a load balancer in a public subnet to communicate with instances in a private subnet, the private subnet’s security list must include an ingress rule allowing traffic from the load balancer’s IP range" (OCI Networking Documentation, Section: Security Lists). Since Terraform deployed the infrastructure, a misconfigured security list is a common oversight.
Reference: Oracle Cloud Infrastructure Documentation - Security Lists.