Oracle Cloud Infrastructure 2026 Networking Professional

Oracle 1z0-1124-25

Version Demo

Total Demo Questions: 13

Total Premium Questions: 134

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Virtual Cloud Network (VCN)	7
Topic 2, Network Security	22
Topic 3, Connectivity	70
Topic 4, Load Balancing	14
Topic 5, DNS	10
Topic 6, Network Monitoring and Troubleshooting	10
Topic 7, Mix Questions	1
Total	134

QUESTION NO: 1

You are designing a hybrid cloud architecture connecting your on-premises network to OCI. You have established a Site-to-Site VPN between your on-premises network and an OCI DRG. You have two VCNs attached to the DRG: VCN-A (10.0.0.0/16) and VCN-B (10.1.0.0/16). You need to ensure that only VCN-A can communicate with the on-premises network (192.168.1.0/24), while VCN-B should remain isolated. What is the MOST effective and secure method to achieve this connectivity requirement using DRG route tables?

A. Create a single DRG route table. Add a route rule to the DRG route table for 192.168.1.0/24 pointing to the VPN attachment. Associate this route table with both the VCN-A and VCN-B attachments. Implement Network Security Groups (NSGs) on VCN-B to block all traffic to and from 192.168.1.0/24.

B. Create a single DRG route table. Add a route rule to the DRG route table for 192.168.1.0/24 pointing to the VPN attachment. Associate this route table with the VCN-A attachment. Associate a default DRG route table that contains no routes for the VPN attachment with the VCN-Battachment.

C. Create two DRG route tables: DRG-RT-A and DRG-RT-B. In DRG-RT-A, add a route rule for 192.168.1.0/24 pointing to the VPN attachment. Associate DRG-RT-A with the VCN-A attachment. In DRG-RT-B, add a route rule for 192.168.1.0/24 pointing to the VPN attachment and associate DRG-RT-B with the VCN-B attachment. Then, use security lists to block all traffic between VCN-B and the on-premises network.

D. Create two DRG route tables: DRG-RT-A and DRG-RT-B. In DRG-RT-A, add a route rule for 192.168.1.0/24 pointing to the VPN attachment. Associate DRG-RT-A with the VCN-A attachment. Associate DRG-RT-B (containing no routes for 192.168.1.0/24) with the VCN-B attachment.

E. Associate separate DRG route tables with VCN-A, VCN-B, and the VPN attachment. Route 192.168.1.0/24 from VCN-A to the VPN and 10.0.0.0/16 from the VPN to VCN-A; do not add corresponding routes for VCN-B or 10.1.0.0/16.

ANSWER: E

Explanation:

Create separate DRG route tables for the VCN attachments and configure the VPN attachment's DRG route table as well. The route table associated with the VCN-A attachment needs a route for `192.168.1.0/24` whose next hop is the VPN attachment, allowing traffic originating in VCN-A to reach the on-premises network. The route table associated with the VCN-B attachment must not contain a route to that on-premises prefix, so traffic from VCN-B has no DRG forwarding path to the VPN. For complete bidirectional isolation, the route table associated with the VPN attachment must route `10.0.0.0/16` to the VCN-A attachment and must not route `10.1.0.0/16` to the VCN-B attachment. This is necessary because a DRG route table governs traffic entering the DRG from its associated attachment; therefore, both the VCN-originated and VPN-originated directions must be controlled. VCN-A's VCN route table must also direct `192.168.1.0/24` to the DRG. This design enforces segmentation at the routing layer rather than depending on security rules as the primary isolation mechanism. See Oracle's Dynamic Routing Gateways documentation and DRG routing documentation.

QUESTION NO: 2

An application team associates an NSG with its compute instances and creates no rules in that NSG because it wants to deny all inbound traffic. The subnet security list, however, contains an existing stateful ingress rule that allows TCP port 443 from `0.0.0.0/0`. Clients can still connect to the instances on port 443. What is the MOST appropriate action to enforce the intended restriction?

A. Remove or narrow the permissive security-list rule, then define only the required allow rules for the workload.

B. Disassociate the NSG from the instance VNICs so that the empty NSG denies all traffic.

C. Add a more specific route rule for the client CIDR block with the Internet Gateway as the target.

D. Create a second empty NSG and associate both NSGs with each instance VNIC.

ANSWER: A

Explanation:

Remove or narrow the permissive security-list rule, then add only the required allow rules in the NSG or in a suitably scoped security list. OCI security rules are allow rules; NSGs and security lists are evaluated cumulatively for a VNIC. An empty NSG does not create a deny override for traffic that a security list already permits.

Disassociating the NSG would not remove the subnet-level allow rule. Adding a route-table rule does not provide packet filtering, and an Internet Gateway route affects reachability rather than authorization on TCP port 443.

QUESTION NO: 3

You are inserting OCI Network Firewall between an application subnet and a database subnet to inspect all east-west traffic. The application subnet route table sends database-subnet traffic to the Network Firewall. TCP connections reach the database, but return traffic bypasses the firewall. Which change is REQUIRED to maintain a symmetric inspected path?

A. Add a route rule in the database subnet route table that sends traffic for the application subnet CIDR block to the Network Firewall.

B. Add a default route in the database subnet route table that sends all traffic to a NAT Gateway.

C. Add a security-list ingress rule on the database subnet allowing all traffic from the application subnet.

D. Associate the database instances with public IP addresses and route return traffic through an Internet Gateway.

ANSWER: A

Explanation:

The database subnet route table must also route traffic destined for the application subnet through the same Network Firewall. A stateful firewall must observe both directions of a session so that it can apply policy consistently and maintain session state. Routing only the forward path through the firewall creates asymmetric routing and can cause response traffic to bypass inspection or be dropped.

Security rules remain necessary to permit the intended application traffic, but they do not control the next-hop path. Adding a route to a NAT Gateway or Internet Gateway would not provide east-west inspection between the private subnets.

QUESTION NO: 4

You have successfully enabled DNSSEC on your OCI DNS zone and provided the DS record to your domain registrar. However, when you test your DNS configuration using online DNSSEC validation tools, you are still seeing errors indicating that DNSSEC validation is failing. What is the most likely reason for this failure?

A. The Time To Live (TTL) value for your DNS records is too low, causing validation errors.

B. The domain registrar has not yet published the DS record in the parent zone, preventing the chain of trust from being established.

C. The OCI DNS resolver is not configured to validate DNSSEC signatures.

D. The DNSSEC algorithm used by OCI DNS is not supported by the validation tools.

ANSWER: B

Explanation:

The domain registrar has not yet published the DS record in the parent zone, preventing the chain of trust from being established. Enabling DNSSEC in an OCI-managed zone causes OCI DNS to sign the zone and makes Delegation Signer information available. That alone does not establish a publicly verifiable DNSSEC chain. The DS record must be added to and served by the domain's parent zone, typically through the registrar or registry. A validating resolver starts with a trust anchor, follows the signed delegation from the parent, and uses the published DS record to authenticate the child zone's DNSKEY. Until the parent-zone delegation is actually visible in public DNS, validators cannot establish that authenticated link to the OCI zone, so they report DNSSEC validation failure. There can also be normal propagation and caching time after the registrar accepts the submission; the important check is whether an authoritative lookup of the parent zone returns the expected DS record. Oracle's DNSSEC guidance describes configuring the parent-zone DS record as the required external delegation step after DNSSEC is enabled for an OCI DNS zone. See the Oracle Cloud Infrastructure DNSSEC documentation and ICANN's overview of the DNSSEC chain of trust.

QUESTION NO: 5

Your company is migrating several applications to OCI and requires a highly available and resilient VPN connection between your on-premises network and OCI. You need to ensure that if one VPN tunnel fails, traffic automatically fails over to a backup tunnel with minimal disruption. Which configuration would BEST achieve high availability and automatic failover for your OCI Site-to-Site VPN connection?

A. Configure a single VPN connection with a single tunnel and rely on the underlying OCI infrastructure for automatic failover.

B. Configure a single VPN connection with two tunnels, ensuring that both tunnels use different CPE IP addresses on the on-premises side.

C. Configure two separate VPN connections, each terminating on a different CPE IP address and using redundant tunnels. Advertise the same prefixes over both VPN connections using BGP.

D. Configure a single VPN connection with two tunnels using the same CPE IP address.

ANSWER: C

Explanation:

Configure two separate VPN connections, each terminating on a different CPE IP address and using redundant tunnels. Advertise the same prefixes over both VPN connections using BGP. This design removes the on-premises CPE public address and device path as a single point of failure while also providing redundant IPSec tunnel paths. Each OCI IPSec connection is associated with a CPE object, which represents the on-premises VPN device's public IP address. Consequently, using distinct CPE IP addresses requires separate IPSec connections rather than distinct tunnels within one connection. For strong end-to-end availability, the CPE endpoints should ideally be independent devices and, where feasible, use separate upstream network paths.

Using BGP on both connections lets the Dynamic Routing Gateway and the on-premises routers exchange equivalent route advertisements dynamically. If a tunnel or an entire CPE path becomes unavailable, BGP withdraws the affected routes and traffic can converge to the remaining healthy VPN connection automatically. OCI provisions redundant tunnels for an IPSec connection, and Oracle recommends redundant connections to distinct CPE devices for higher availability. This combines OCI tunnel redundancy with CPE and connectivity redundancy, providing the resilient failover architecture required. See Oracle's Site-to-Site VPN overview and IPSec connection configuration documentation.

QUESTION NO: 6

In a multi-tier architecture with multiple application instances across different private subnets, which Bastion service approach minimizes the need for continuous maintenance of individual session configurations?

A. Creating individual Bastion sessions for each application instance.

B. Using dynamic port forwarding with SOCKS5 sessions allowing users to define their own targets.

C. Implementing a centralized Bastion service with managed sessions and predefined target resource configurations.

D. Deploying separate Bastion hosts in each private subnet.

ANSWER: B

Explanation:

Using dynamic port forwarding with SOCKS5 sessions allowing users to define their own targets is the best fit because one OCI Bastion dynamic port-forwarding session creates a SOCKS5 proxy through which an authorized user can reach multiple private targets, rather than creating and maintaining a distinct managed SSH session configuration for every application instance. This is especially useful when the instances are distributed across private subnets but are reachable through the Bastion target virtual cloud network and the applicable routing and security rules. The session is established to the Bastion service, and the user's SOCKS5-capable client directs traffic for the desired private host and port through that encrypted channel. As a result, adding, replacing, or changing individual application instances generally does not require administrators to continually create or update separate Bastion session target definitions. OCI still enforces the Bastion's network scope, session lifetime, identity policies, and network-security controls, so this reduced configuration effort does not remove access governance. Oracle documents dynamic port forwarding as a Bastion session type designed to provide SOCKS5 proxy access to resources in a private network. See the OCI Bastion overview and OCI Bastion session connection documentation.

QUESTION NO: 7

You are responsible for managing the network infrastructure of a multi-tenant SaaS application deployed on OCI. Each tenant has their own dedicated VCN. To simplify management and provide a centralized point for connectivity to your on-premises network via FastConnect, you are using a DRG. However, you need to ensure that tenants are logically isolated from each other, and no traffic can flow directly between tenant VCNs through the DRG. How can you achieve tenant isolation while still allowing each tenant to connect to your on-premises network through the centralized DRG?

A. Create a separate DRG for each tenant and attach the respective tenant VCN to its DRG. Configure static routes on each DRG to direct traffic appropriately.

B. Utilize a single DRG and attach all tenant VCNs to it. Implement Network Security Groups (NSGs) on each tenant VCN to explicitly block all traffic to and from other tenant VCNs.

C. Utilize a single DRG and attach all tenant VCNs to it. Associate each tenant VCN attachment with a DRG route table that permits only the FastConnect attachment, and configure the FastConnect attachment's DRG route table with routes to the tenant VCN attachments.

D. Utilize a single DRG and attach all tenant VCNs to it. Create a separate compartment for each tenant VCN. This will automatically isolate tenant traffic at the DRG level.

ANSWER: C

Explanation:

Utilize a single DRG and attach all tenant VCNs to it. Associate each tenant VCN attachment with a dedicated DRG route table that permits forwarding only to the FastConnect attachment, and configure the FastConnect attachment's DRG route table with routes to the tenant VCN attachments. This implements hub-and-spoke routing at the DRG: traffic originating in a tenant VCN can be sent to the on-premises network through FastConnect, while that VCN's attachment route table contains no path to another tenant VCN attachment. As a result, the DRG does not forward traffic directly between tenants.

The FastConnect attachment requires routes back to the tenant VCN CIDR ranges so that return traffic from on premises can reach the appropriate tenant. These routes can be maintained through DRG route rules and, where appropriate, route distributions that import attachment route information. The essential isolation control is the route table associated with each VCN attachment: it limits the reachable next-hop attachment to FastConnect rather than allowing lateral VCN-to-VCN forwarding. Oracle DRG route tables are specifically designed to control routing between attached networks, enabling centralized connectivity without granting all attachments transitive connectivity. See Oracle Cloud Infrastructure: Managing DRGs and Oracle Cloud Infrastructure: DRG Routing.

QUESTION NO: 8

An application subnet uses stateless security rules. Application instances initiate TCP connections to database instances on port 1521. The database subnet has an ingress rule allowing TCP port 1521 from the application subnet, but connections still fail because no return traffic rule exists. Which additional rule configuration is required?

A. Add a stateful ingress rule on the database subnet allowing TCP port 1521 from the application subnet.

B. Add stateless egress rules on the database subnet and stateless ingress rules on the application subnet for TCP response traffic to the application instances' ephemeral ports.

C. Add an Internet Gateway route rule to the database subnet route table for the application subnet CIDR block.

D. Add a stateless ingress rule on the database subnet allowing TCP port 1521 from 0.0.0.0/0.

ANSWER: B

Explanation:

Stateless security rules do not automatically allow return traffic. In addition to allowing the application-tier request to reach TCP port 1521 on the database tier, the database tier must allow egress responses to the ephemeral source ports used by the application client, and the application tier must allow ingress responses to those ephemeral ports.

A typical configuration allows stateless egress from the application subnet to TCP port 1521 on the database subnet, stateless ingress to TCP port 1521 on the database subnet, stateless egress from the database subnet to the application subnet ephemeral-port range, and corresponding stateless ingress on the application subnet. Stateful rules would automatically allow response traffic for an established session, but that behavior does not apply to stateless rules.

QUESTION NO: 9

Your security team has mandated that all traffic to Oracle Cloud Infrastructure Object Storage must be encrypted end-to-end and must not be routed over the public internet. You are designing asolution where compute instances within a private subnet will frequently upload and download data from Object Storage. Which of the following options provides the most secure and compliant solution?

A. Configure a Service Gateway to Object Storage and enable encryption at rest on the Object Storage bucket.

B. Configure a NAT Gateway for the instances and enable encryption in transit using HTTPS for all Object Storage API calls.

C. Configure a Service Gateway to Object Storage and ensure all API calls to Object Storage are made over HTTPS.

D. Configure a Private Endpoint to Object Storage and ensure all API calls to Object Storage are made over HTTPS.

ANSWER: C

Explanation:

Configure a Service Gateway to Object Storage and ensure all API calls to Object Storage are made over HTTPS. A service gateway gives resources in a VCN private access to supported Oracle services, including Oracle Cloud Infrastructure Object Storage, without requiring an internet gateway, NAT gateway, or public IP address. Traffic takes the Oracle services network path rather than traversing the public internet, which directly satisfies the network-routing requirement for compute instances in a private subnet.

HTTPS uses TLS to encrypt the connection between the instance and the Object Storage service endpoint. This protects Object Storage API requests and responses, including uploads and downloads, while in transit. Combining HTTPS with a service gateway therefore addresses both independent controls in the mandate: private service access that avoids the public internet and encryption for the data path. The subnet route table must include a route for the Oracle Services Network service CIDR label with the service gateway as its target, and security rules must permit the required HTTPS egress. Oracle documents service gateways at Service Gateway and describes Object Storage security and HTTPS access at Securing Object Storage.

QUESTION NO: 10

You are designing a multi-tier application in OCI, deploying the application tier in a public subnet and the database tier in a private subnet within the same VCN. The application tier requires access to specific external internet resources for software updates and third-party API calls. However, the database tier should not have direct internet access. Which of the following is the most secure and efficient method to achieve this configuration?

A. Configure a NAT Gateway for the private subnet and a Service Gateway for the public subnet.

B. Configure a NAT Gateway for both the public and private subnets.

C. Configure a NAT Gateway for the public subnet and a Service Gateway for the private subnet.

D. Configure a NAT Gateway for the private subnet and an Internet Gateway for the public subnet.

E. Configure an Internet Gateway for the public subnet and no Internet Gateway or NAT Gateway route for the private database subnet.

ANSWER: E

Explanation:

Configure an Internet Gateway for the public subnet and do not configure an internet egress route for the private database subnet. This meets the stated separation requirement with the smallest necessary exposure: the application tier, which is intentionally placed in a public subnet, can use a route rule whose destination is `0.0.0.0/0` and whose target is the Internet Gateway to reach approved external update repositories and third-party APIs. Security lists or network security groups can then restrict ingress and egress to only the required protocols, addresses, and ports.

The database subnet remains private by having no route rule to an Internet Gateway or NAT Gateway. Consequently, instances in that subnet have no direct path to public internet destinations, while they can still communicate with the application tier through private VCN addressing. This is more secure and efficient than provisioning a NAT Gateway for a database tier that has no stated outbound internet requirement: a NAT Gateway is specifically an outbound internet access mechanism for private resources. If the database later needs Oracle Cloud service access, a Service Gateway and narrowly scoped route rule can be added without enabling public-internet connectivity. Oracle describes public-subnet Internet Gateway routing and private-subnet routing in its Internet Gateway documentation and explains private access to supported OCI services through a Service Gateway.

QUESTION NO: 11

You have configured an IPSec VPN tunnel over your FastConnect circuit to OCI. You are experiencing intermittent connectivity issues and notice that the VPN tunnel is flapping (frequently going up and down). You have verified the IKE and IPSec configuration and confirmed that the security policies are correct. Which is a LESS likely cause of the VPN tunnel flapping when using IPSec over FastConnect, compared to using IPSec over the public internet?

A. Issues with network congestion or packet loss.

B. Mismatched pre-shared keys or incorrect IKE/IPSec parameters.

C. MTU (Maximum Transmission Unit) misconfiguration leading to fragmentation.

D. BGP route flapping or instability.

ANSWER: A

Explanation:

Issues with network congestion or packet loss. is the less likely cause when IPSec is carried over FastConnect. FastConnect provides a private, dedicated connection between the customer environment and Oracle Cloud Infrastructure rather than forwarding VPN traffic across the variable paths of the public internet. This generally gives the IPSec underlay more predictable latency and packet delivery, reducing exposure to internet transit congestion, route changes, and packet loss that can interrupt IKE/IPSec keepalive traffic and make a tunnel appear to flap.

FastConnect does not make packet loss impossible: a problem in the customer edge, provider access circuit, cross-connect, or physical interface can still affect the tunnel. However, relative to an IPSec VPN whose outer packets traverse the public internet, broad network congestion and uncontrolled internet packet loss are materially less probable explanations. Troubleshooting should therefore focus on the health and error counters of the FastConnect path, customer-premises equipment, and tunnel monitoring/keepalive behavior, while recognizing the private connectivity advantage of FastConnect. Oracle describes FastConnect as a dedicated private connection to OCI in its FastConnect overview, and documents IPSec VPN connectivity and tunnel behavior in the Site-to-Site VPN documentation.

QUESTION NO: 12

A database subnet uses stateful security rules. Application instances initiate TCP connections to database instances on port 1521, and the database must return response traffic over those established sessions. No database-initiated connections are required. Which security-rule configuration is sufficient?

A. Create a stateful ingress rule on the database instances allowing TCP port 1521 from the application tier.

B. Create an ingress rule on the application instances allowing TCP port 1521 from the database subnet.

C. Create a stateless ingress rule on the database instances allowing TCP port 1521 and no other rules.

D. Create an egress rule on the database instances allowing all protocols and destinations, with no ingress rule.

ANSWER: A

Explanation:

A stateful ingress rule on the database instances that permits TCP port 1521 from the application tier is sufficient for the established session's return traffic. OCI tracks stateful connections and automatically permits response traffic for an allowed flow, so a separate egress rule for the ephemeral response ports is not required.

An ingress rule on the application subnet does not authorize traffic arriving at the database. A stateless database ingress rule would require complementary return-path rules. Allowing all egress traffic is broader than necessary and does not by itself permit the initial connection to the database listener.

QUESTION NO: 13

You are a cloud architect designing a multi-tiered application on OCI. One tier consists of publicly accessible web servers that must be protected from common web exploits. You plan to use OCI Network Firewall to achieve this. You need to configure the Network Firewall to detect and prevent SQL injection attacks against the web servers. Which Network Firewall feature is most suitable for this purpose?

A. Stateful Inspection, configured with default IPS policies.

B. Intrusion Detection and Prevention System (IDPS) signatures with custom rule sets for SQL injection.

C. URL Filtering with predefined categories blocking SQL injection attempts.

D. Geo-location filtering to block traffic from countries known for SQL injection attacks.

ANSWER: B

Explanation:

Intrusion Detection and Prevention System (IDPS) signatures with custom rule sets for SQL injection is the most suitable choice because SQL injection is an application-layer attack pattern carried in HTTP requests, such as malicious SQL syntax embedded in parameters, form fields, or headers. OCI Network Firewall provides intrusion prevention capabilities that inspect traffic against threat signatures and can take preventive action when a matching threat is detected. This enables the firewall policy to identify known exploit patterns and block the session before the malicious request reaches the web-server tier.

For a public-facing web workload, the protection rule should be applied to the traffic path entering the web-server subnet, with an action that blocks or resets sessions associated with SQL-injection signatures. Tailoring the applicable signature rules and severity thresholds helps align protection with the application’s exposure and reduces unnecessary disruption while retaining detection coverage for relevant web threats. Logging should also be enabled so security teams can review matched signatures, source information, and policy actions, then tune the policy based on observed traffic.

OCI documents Network Firewall as a managed next-generation firewall service with intrusion prevention and threat-signature inspection capabilities. See the [OCI Network Firewall overview]() and the [Network Firewall policy documentation]().