CloudGuard Network Security for Oracle Cloud Infrastructure - Reference Architecture

OVERVIEW

Oracle Cloud Infrastructure's security capabilities are designed to let you run your mission-critical workloads and store your data in the cloud with complete control and confidence. Oracle Cloud Infrastructure (OCI) offers best-in-class security technology and operational processes to secure its enterprise cloud services, based on a shared responsibility model. Oracle is responsible for the security of the cloud infrastructure and operations, and you are responsible for securely configuring your workloads to meet your compliance responsibilities.

Check Point is a world-class provider of cyber security solutions to governments and enterprises globally. Check Point CloudGuard Network Security (CGNS) for OCI provides advanced, multilayered security to protect applications from attacks while enabling secure connectivity from enterprise and hybrid cloud networks. It provides consistent security policy management, enforcement, and reporting, allowing customers to move or extend their workloads to OCI painlessly.

Organizations moving or extending their Oracle applications, such as E-Business Suite or PeopleSoft, to OCI can choose Check Point CloudGuard Network Security to inspect traffic and enforce security controls and policies.

This reference architecture provides best practices and recommendations to properly design and segment Oracle applications that an organization plans to migrate or extend into OCI and apply appropriate security controls.

The security controls include the following features:

- Access controls (firewall)
- Logging
- Application control
- Intrusion prevention (IPS)
- Advanced threat prevention
- Site-to-site virtual private network (VPN) for communication with the on-premises network
- Remote access VPN for communication with roaming users
- Network address translation for internet bound traffic

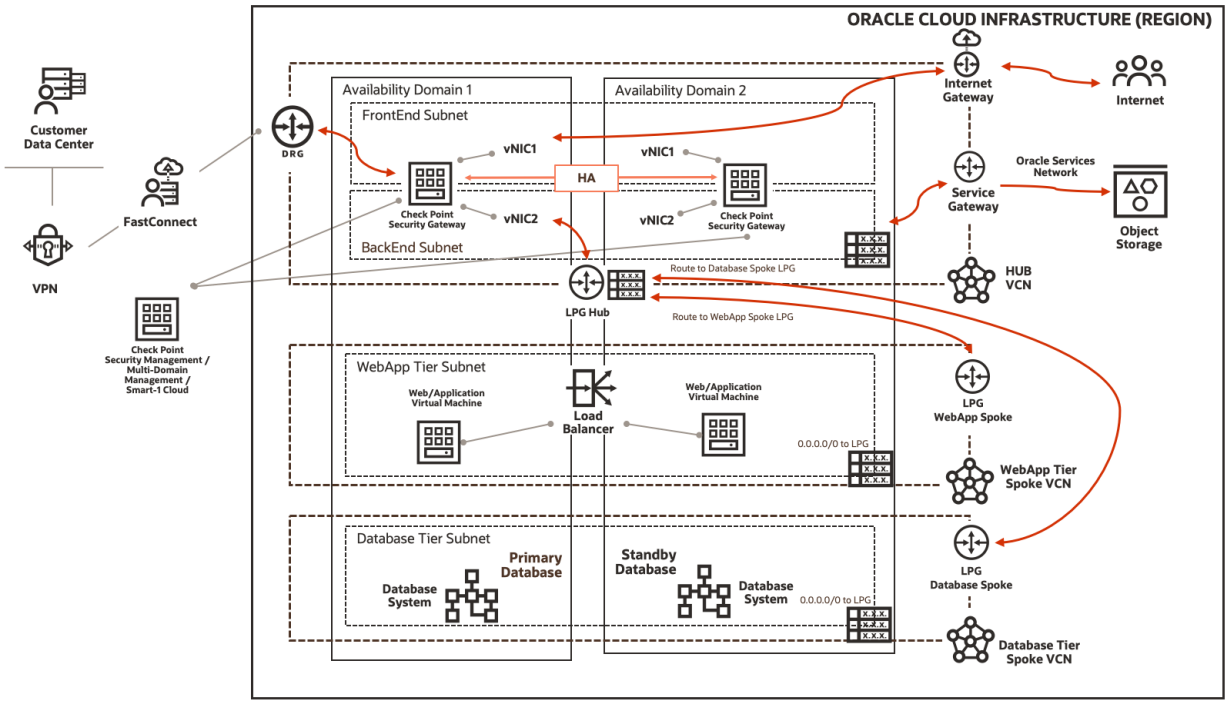
ARCHITECTURE

This reference architecture illustrates how organizations can protect Oracle applications like Oracle E-Business Suite and PeopleSoft deployed in OCI using Check Point CloudGuard Network Security gateways.

The typical enterprise application consists of multiple tiers, such as a web application tier and database tier.

The following diagram illustrates this reference architecture:

Check Point CloudGuard Network Security on Oracle Cloud Infrastructure



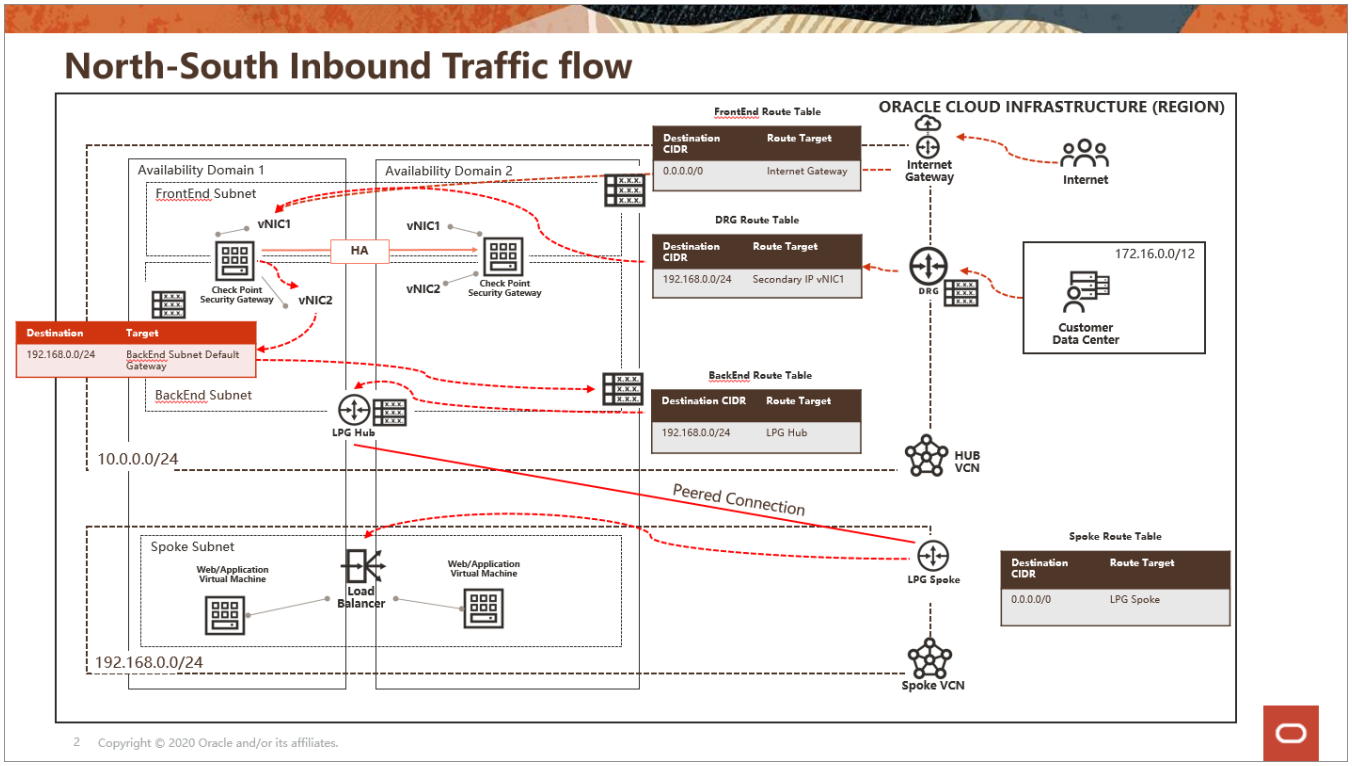
To protect these traffic flows, Check Point recommends segmenting the network using a hub and spoke topology where traffic routes through a central hub and connects to multiple distinct networks (spokes). All traffic between spokes, to and from the internet, to and from on-premises, or to the Oracle Services Network is routed through the hub and inspected with Check Point CloudGuard Network Security's multi-layered threat prevention technologies.

Deploy each tier of your application in its own virtual cloud network (VCN), which acts as a spoke. The hub VCN contains a Check Point CGNS high availability cluster, Oracle internet gateway, dynamic routing gateway (DRG), Oracle Service Gateway, and local peering gateways (LPGs).

The hub VCN connects to the spoke VCNs through LPGs or by attaching secondary virtual network interface cards (VNIC) to the CGNS gateways. All spoke traffic routes to the hub for inspection by the Check Point CGNS high availability cluster through the LPGs using route table rules.

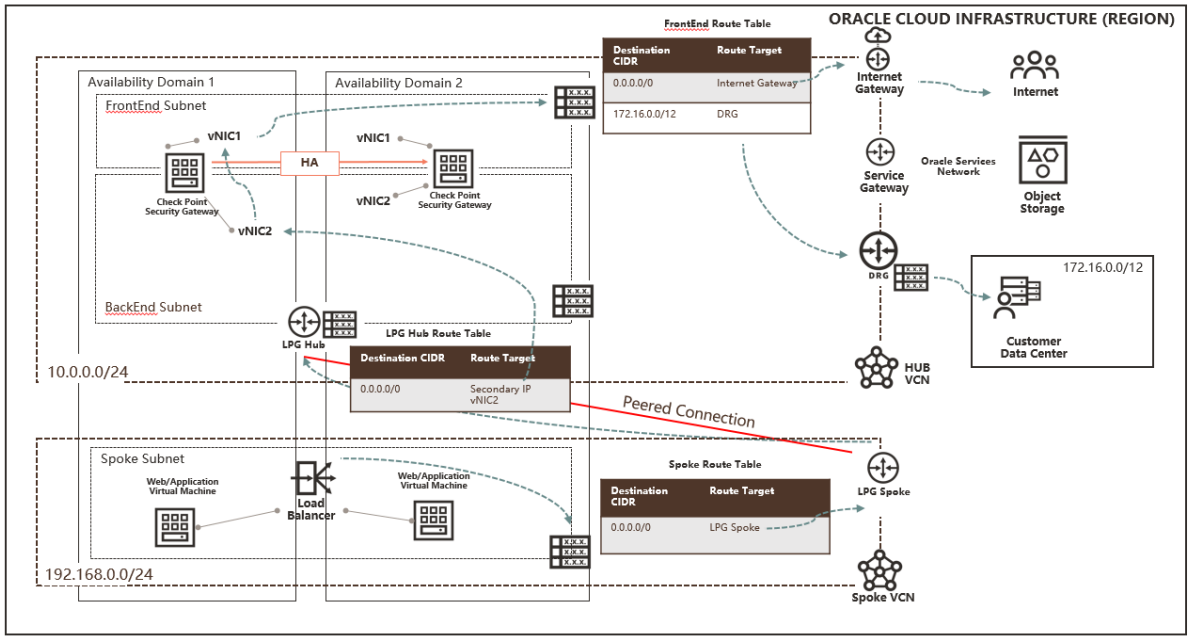
The traffic flows consist of the following aspects:

- Traffic arriving from the internet to the web application tier and for remote user access



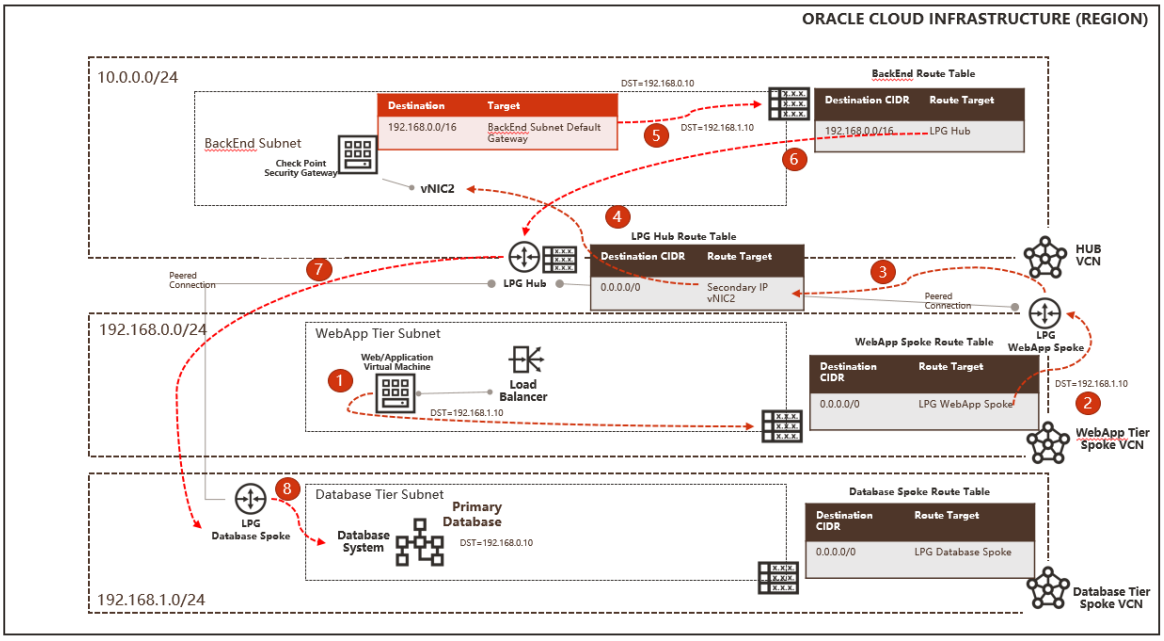
- Outgoing connections from the web application and database tiers to the internet for software updates and access to external web services. Ensure that the hide NAT is configured in your Check Point security policy for the relevant networks.

North-South Outbound Traffic flow

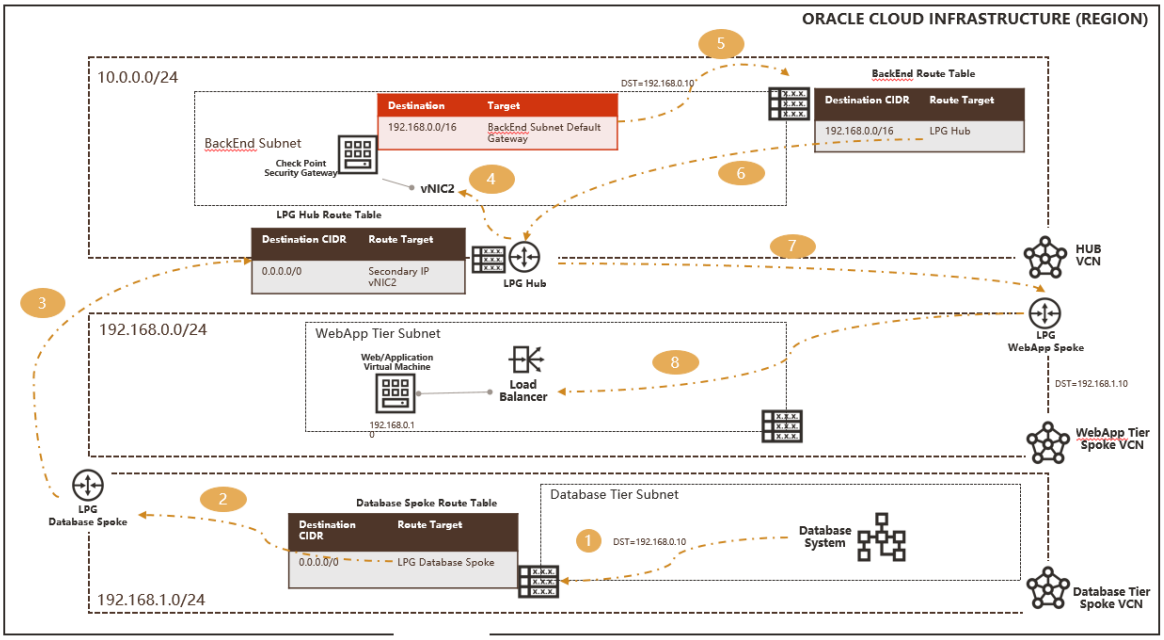


- Traffic to and from the web application and database tiers

East-West Traffic Flow (Web to Database)

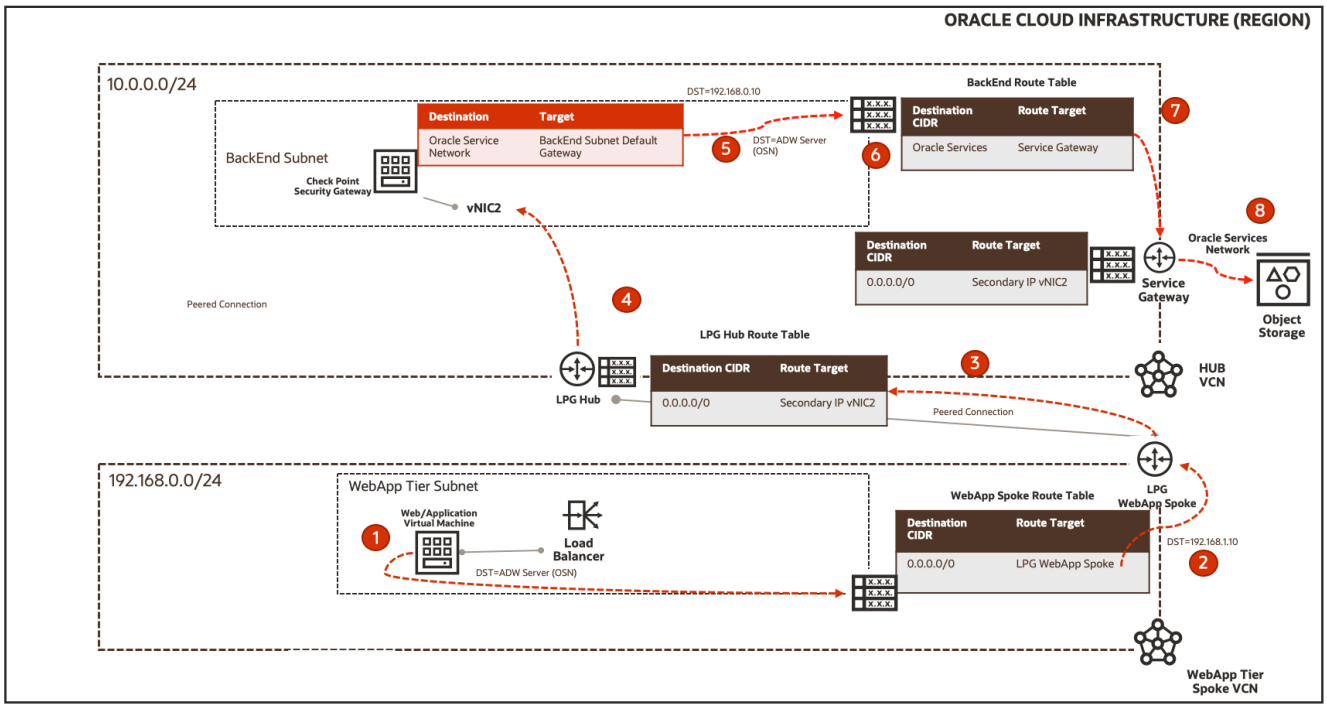


East-West Traffic Flow (Database to Web)

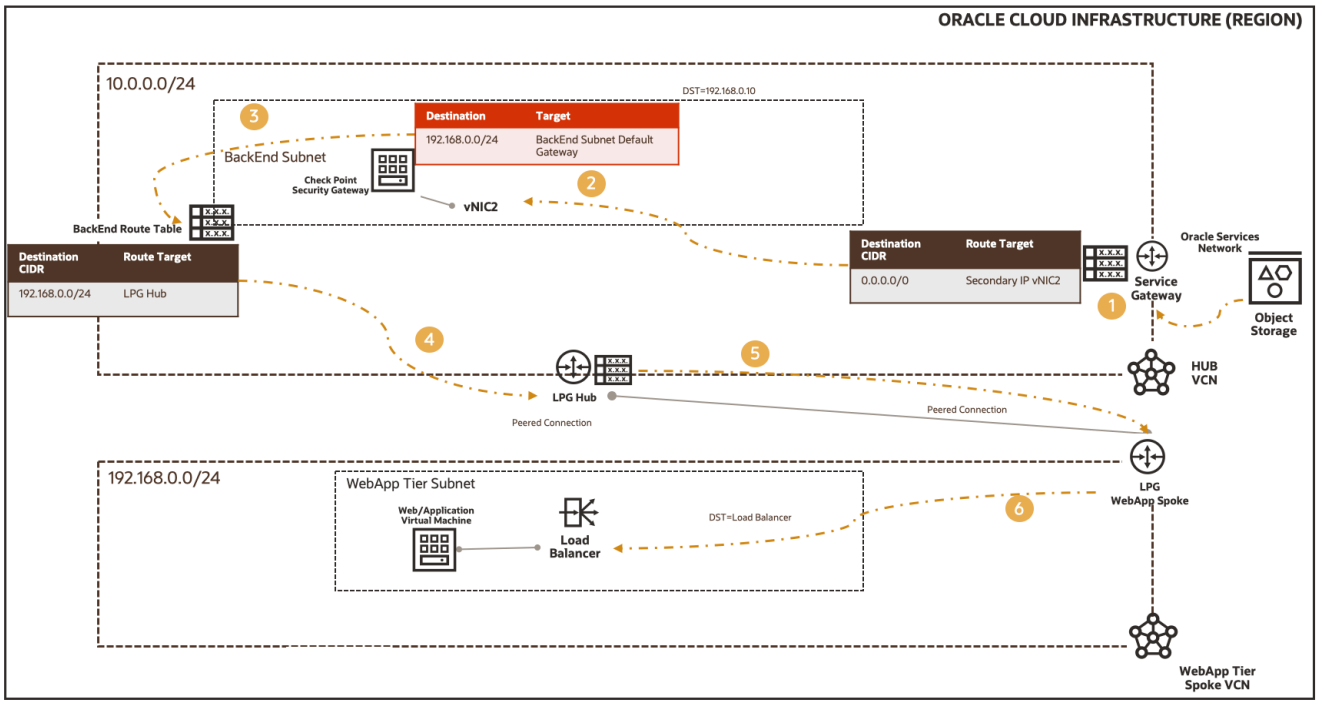


- Traffic to and from the ebApp tier and Oracle Services Network

East-West Traffic Flow (WebApp to Oracle Services Network)



East-West Traffic Flow (Oracle Services Network to WebApp)



Managing the environment can be accomplished by one of the following methods:

- Centrally managed with a Check Point Security Management server or multidomain management server
    - Deployed in its own subnet in the hub VCN
    - Preexisting customer Check Point security management server deployment accessible to the hub
- Centrally managed from Check Point's Smart-1 Cloud Management-as-a-Service

This architecture has the following components:

- **Check Point CloudGuard network security gateways**
- **Check Point Security Management**
    - Security Management Server
    - Multi-Domain Management
    - Smart-1 Cloud Management-as-a-Service
- **Oracle E-Business Suite or PeopleSoft application tier**

  Oracle E-Business Suite or PeopleSoft application servers and file system
- **Oracle E-Business Suite or PeopleSoft database tier**

  Composed of Oracle Database, but not limited to Oracle Exadata Database Cloud service or Oracle Database services.
- **Region**

A region is a localized geographic area composed of one or more availability domains. Regions are independent of other regions, and vast distances can separate them (across countries or continents).

- **Availability domains**

  Availability domains are standalone, independent data centers within a region. The physical resources in each availability domain are isolated from the resources in the other availability domains, which provides fault tolerance. Availability domains do not share infrastructure, such as power or cooling, or the internal availability domain network. Therefore, a failure at one availability domain is unlikely to affect the other availability domains in the region.

- **Fault domains**

  A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain has three fault domains with independent power and hardware. When you place Compute instances across multiple fault domains, applications can tolerate physical server failure, system maintenance, and many common networking and power failures inside the availability domain.

- **Virtual cloud network (VCN) and subnets**

  A VCN is a customizable, private network that you set up in an OCI region. Like traditional data center networks, VCNs give you complete control over your network environment. You can segment VCNs into subnets, which can be scoped to a region or an availability domain. Both regional subnets and availability domain-specific subnets can coexist in the same VCN. A subnet can be public or private.

- **Hub VCN**

  A centralized network where the Check Point CloudGuard NSGs are deployed. It provides secure connectivity to all spoke VCNs, OCI services, public endpoints and clients, and on-premises data center networks.

- **Web application tier spoke VCN**

  The web application tier spoke VCN contains a private subnet to host Oracle E-Business Suite or PeopleSoft components.

- **Database tier spoke VCN**

  The database tier spoke VCN contains a private subnet for hosting Oracle databases.

- **Load balancer**

  The Oracle Cloud Infrastructure Load Balancing service provides automated traffic distribution from a single entry point to multiple servers in the backend.

- **Security list**

  For each subnet, you can create security rules that specify the source, destination, and traffic type that must be allowed in and out of the subnet.

- **Route tables**

  Virtual route tables contain rules to route traffic from subnets to destinations outside a VCN, typically through gateways.

  In each spoke VCN, one defined route table routes all traffic to the hub VCN through the spoke LPG.

  In the hub VCN, you have the following route tables:

- A route table attached to the frontend subnet or default VCN for routing traffic from the hub VCN to the internet, on-premises, or Oracle Services Network.
- A route table attached to the backend subnet pointing to the CIDR block of the spoke VCNs through the associated LPGs.
- For each spoke attached to the hub, a separate route table is defined and attached to an associated LPG. That route table forwards all traffic (0.0.0.0/0) from the associated spoke LPG through the Check Point CGNS backend floating IP.
- A route table attached to the Oracle service gateway for Oracle Services Network communication. That route forwards all traffic (0.0.0.0/0) to the Check Point CGNS backend floating IP.
- To maintain traffic symmetry, routes are also added to each Check Point CGNS cluster member (Gaia OS) to point the CIDR block of Spoke traffic to the backend (internal) subnet's default gateway IP (first IP available in the backend subnet on Hub VCN).

- **Internet gateway**

  The internet gateway allows traffic between the public subnets in a VCN and the public internet.

- **NAT gateway**

  The NAT gateway enables private resources in a VCN to access hosts on the internet without exposing those resources to incoming internet connections.

- **Local peering gateways (LPG)**

  An LPG enables you to peer one VCN with another VCN in the same region. Peering means the VCNs communicate using private IP addresses, without the traffic traversing the internet or routing through your on-premises network.

- **Dynamic routing gateway (DRG)**

  The DRG is a virtual router that provides a path for private network traffic between a VCN and a network outside the region, such as a VCN in another Oracle Cloud Infrastructure region, an on-premises network, or a network in another cloud provider.

- **Service gateway**

  A service gateway is required for communicating with Oracle services, such as infrastructure, PaaS, SaaS, from the hub VCN, or on-premises network.

- **FastConnect**

  Oracle Cloud Infrastructure FastConnect provides an easy way to create a dedicated, private connection between your data center and OCI. FastConnect provides higher-bandwidth options and a more reliable networking experience when compared with internet-based connections.

- **Virtual network interface card (VNIC)**

  The services in Oracle Cloud Infrastructure data centers have physical network interface cards (NICs). Virtual machine (VM) instances communicate using virtual NICs (VNICs) associated with the physical NICs. Each instance has a primary VNIC that is automatically created, attached during launch, and is available during the instance's lifetime. Dynamic host configuration protocol is offered to the primary VNIC only. You can add secondary VNICs after instance launch. Set static IPs for each interface.

- **Private IPs**

A private IPv4 address and related information for addressing an instance. Each VNIC has a primary private IP, and you can add and remove secondary private IPs. The primary private IP address on an instance is attached during instance launch and does not change during the instance's lifetime. Secondary IPs also belong to the same CIDR of the VNIC's subnet. The secondary IP is used as a floating IP because it can move between different VNICs on different instances within the same subnet. You can also use it as a different endpoint to host different services.

- **Public IPs**

  The networking services define a public IPv4 address chosen by Oracle that is mapped to a private IP.

  - Ephemeral: This address is temporary and exists for the lifetime of the instance.
  - Reserved: This address persists beyond the lifetime of the instance. It can be unassigned and reassigned to another instance.

- **Source and destination check**

  Every VNIC performs the source and destination check on its network traffic. This flag must be disabled to allow CloudGuard to inspect traffic between the hub and spokes.

- **Compute shape**

  The shape of a Compute instance specifies the number of CPUs and amount of memory allocated to the instance. The Compute shape also determines the number of VNICs and maximum bandwidth available for the compute instance.

RECOMMENDATIONS

- **VCN**

  When you create the VCN, determine how many IP addresses your cloud resources in each subnet require. Using Classless Inter-Domain Routing (CIDR) notation, specify a subnet mask and a network address range large enough for the required IP addresses. Use an address space that is within the standard private IP address blocks.

  Select an address range that does not overlap with your on-premises network, so that you can set up a connection between the VCN and your on-premises network later, if necessary.

  When you design the subnets, consider functionality and security requirements. All compute instances within the same tier or role go into the same subnet.

  Use a regional subnet.

  Verify the maximum number of LPGs per VCN in your service limits when you want to extend this architecture for multiple environments and applications.

- **Check Point CloudGuard Network Security**
  - Deploy a high availability cluster. Follow Check Point SecureKnowledge article SK142872 for best practices.
  - Whenever possible, deploy in distinct fault domains at a minimum or different availability domains.
  - Ensure that MTU is set to **9000** on all VNICs.
  - Utilize SRIOV and VFIO interfaces.
  - Create a second hub-spoke topology in a separate region for disaster recovery or geo-redundancy.

- Do not restrict traffic through security lists or NSGs because the security gateway secures all traffic.
- By default, ports `443` and `22` are open on the gateway, and more ports are open based on security policies.

- **Check Point Security Management**
  - If you are doing a new deployment hosted in OCI, create a dedicated subnet for management.
  - Deploy a secondary management server (management for high availability) in a different availability domain or region.
  - Use security lists or NSGs to restrict inbound access to ports `443`, `22`, and `19009` sourced from the internet for administrating the security policy and viewing logs and events.
  - Create either a security list or NSG, allowing ingress and egress traffic to the security gateways from the security management server.
- **Check Point Security Policies**
  - Refer to the following documentation for the most up-to-date information on required ports and protocols that need to be accessible, depending on Oracle application:
    - PeopleSoft on Oracle Cloud Infrastructure
    - Oracle E-Business Suite on Oracle Cloud Infrastructure

CONSIDERATIONS

- **Performance**

  The following factors impact performance:

  - Selecting the proper instance size, determined by the Compute shape, determines the maximum available throughput, CPU, RAM, and the number of interfaces.
  - Organizations need to know what traffic types traverse the environment, determine the appropriate risk levels, and apply proper security controls as required. Different combinations of enabled security controls impact performance.
  - Consider adding dedicated interfaces for FastConnect or VPN services.
  - Consider using large Compute shapes for higher throughput and access to more network interfaces.
  - Run performance tests to validate the design can sustain the required performance and throughput.
- **Security**
  - Deploying Check Point Security Management in OCI allows for centralized security policy configuration and monitoring of all physical and virtual Check Point Security Gateway instances.
  - For existing Check Point customers, migrating Security Management to OCI is also supported.
  - Define distinct Identity and Access Management (IAM) dynamic group or policy per cluster deployment.

- **Availability**

- Deploy your architecture to distinct geographic regions for greatest redundancy.
- Configure site-to-site VPNs with relevant organizational networks for redundant connectivity with on-premises networks.

- **Cost**
  - Check Point CloudGuard is available in bring-your-own-license (BYOL) and pay-as-you-go license models for both Security Management and Security Gateways in the Oracle Cloud Marketplace.
  - Check Point CloudGuard Network Security Gateway licensing is based on the number of vCPUs (one OCPU is equivalent to two vCPUs).
  - Check Point BYOL licenses are portable between instances. For example, if you are migrating workloads from other public clouds that also use BYOL licenses, you do not need to purchase new licenses from Check Point. Check with your Check Point representative if you have questions or need verification of your license status.
  - Check Point Security Management is licensed per managed security gateway. For example, two clusters count as four toward the Security Management license.

MORE INFORMATION

For more information, see the following resources:

- Deploying a Check Point Cluster in Oracle Cloud Infrastructure (OCI)
- CloudGuard for Oracle Cloud Infrastructure (OCI)