ORACLE

Deploying Fortinet's FortiGate Next-Generation HA Clusters on Oracle Compute Cloud@Customer and Oracle Private Cloud Appliance

Designing Resilient Multi-VCN Topologies within Oracle Compute Cloud@Customer and Oracle Private Clould Appliance X9-2 Platforms using Fortinet's FortiGate Next-Generation HA Clusters

June 2025, Version 1.9

Introduction

Oracle and Fortinet are proud to announce the test certification and associated required configuration documentation to install the Fortinet NGFW on Oracle Compute Cloud@Customer and Oracle Private Cloud Appliance.

Overview

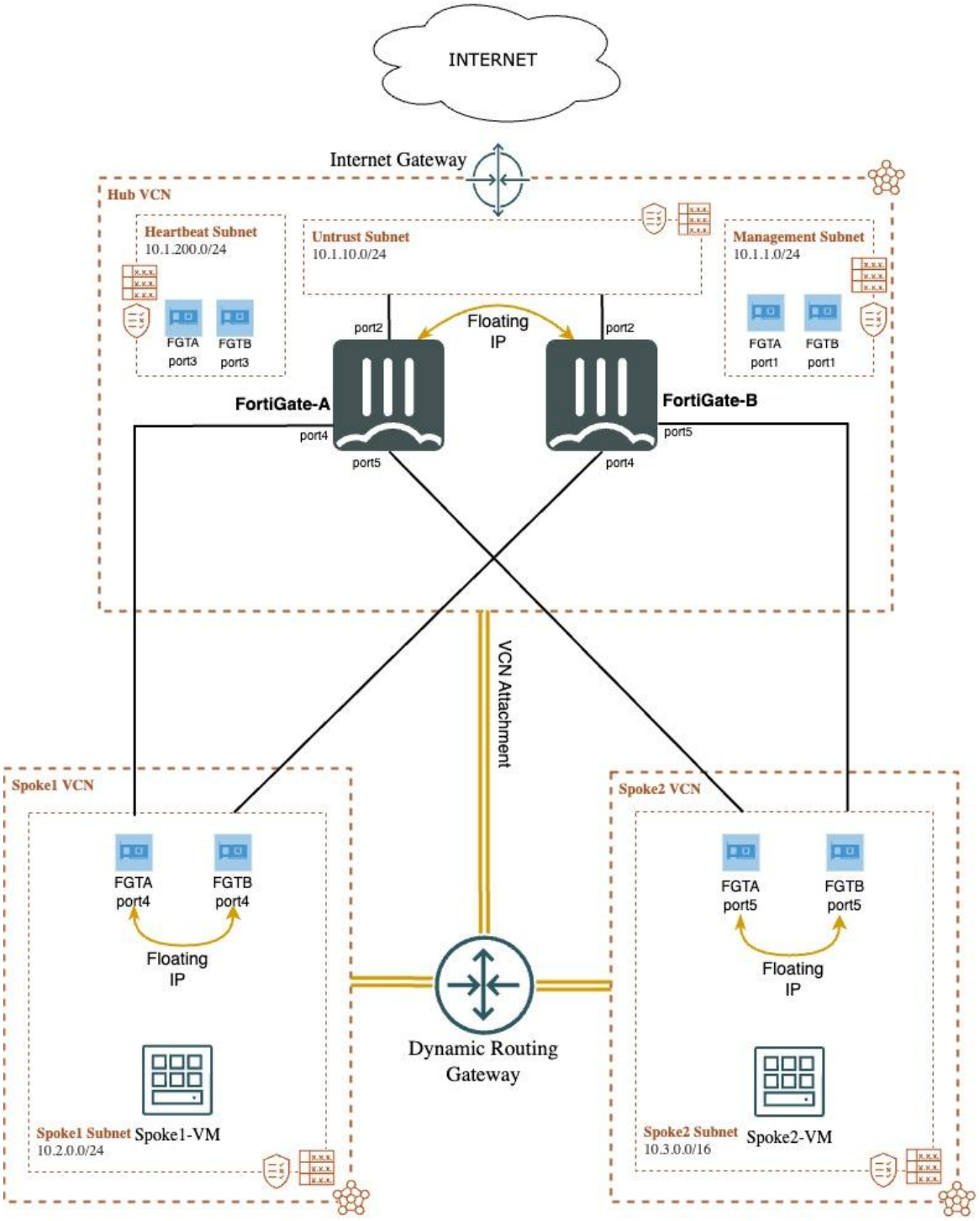
Fortinet's Next-Generation Firewall (NGFW) is a security solution designed to protect networks and data from advanced cyber threats. It extends beyond traditional firewalls by incorporating deep packet inspection, application control, intrusion prevention, and threat intelligence.

Fortinet's security fabric spans data centers and clouds, offering a consolidated view of security posture with a single console for policy management, governance reporting, and event monitoring. This fabric is natively integrated with Oracle Cloud Infrastructure (OCI) and now extends to Oracle Compute Cloud@Customer (C3) and Oracle Private Cloud Appliance (PCA) X9-2. This integration delivers scalable performance, advanced security orchestration, and unified threat protection for workloads across cloud, hybrid, and on-premises (PCA X9-2) environments.

Benefits of FortiGate NGFW on Oracle C3 and PCA X9-2

The FortiGate NGFW enhances enterprise firewall capabilities for organizations of all sizes. This reference architecture deploys a highly available cluster of FortiGate firewalls in a hub-and-spoke topology within Oracle C3 and PCA X9-2 environments.

Architecture



This diagram illustrates a high availability (HA) network setup using FortiGate firewalls in Oracle's C3 and PCA X9-2 platforms. It demonstrates secure and resilient communication across hub-and-spoke topology using cluster FortiGate virtual machines configured with failover and required routing.

Architecture Key Components

Refer to the Architecture diagram shown above.

1. FortiGate Firewalls (FGTA & FGTB)

- Two FortiGate VMs (A and B) are deployed in active/passive HA configuration.
- They are connected using multiple ports and a floating IP for automatic failover.
- Each FortiGate handles specific interfaces:
    - port1: Management Subnet
    - port2: Untrust Subnet (for internet traffic)
    - port3: Heartbeat Subnet (HA sync and status monitoring)
    - port4 / port5: Traffic routing between Hub and Spokes

2. Subnets in Hub VCN

- Management Subnet (10.1.1.0/24) provides management access to FGTA/B (via port1).
- Untrust Subnet (10.1.10.0/24) connects to the Internet Gateway (via port2).
- Heartbeat Subnet (10.1.200.0/24) used for HA status sync between FGTA and FGTB (via port3).

3. Dynamic Routing Gateway (DRG)

- Centralized routing hub that connects Hub VCN to Spoke1 VCN and Spoke2 VCN via VCN attachments.
- Ensures traffic routing between VCNs and facilitates dynamic route exchange.

4. Spoke VCNs

- Each spoke has its own subnet and virtual machines, which connect to the central hub via the DRG.

Spoke1 VCN

- Subnet: 10.2.0.0/24
- Interfaces: FGT A and B use port4 here.
- Floating IP: For redundancy across the firewalls
- VM: A virtual machine deployed in the subnet.

Spoke2 VCN

- Subnet: 10.3.0.0/16
- Interfaces: FGT A and B use port5.
- Floating IP: Ensures failover capabilities.
- VM: Another virtual machine

The network follows a hub-and-spoke topology with FortiGate deployments on C3 and PCA X9-2, providing:

- North-South Traffic Protection controls, inspects, and secures traffic moving between virtual cloud networks (VCNs) and the Internet.
- East-West Traffic Protection controls, inspects, and secures traffic between VCNs.

The hub virtual network serves as the primary connectivity point for both external (North-South) and internal (East-West) traffic. The architecture supports high scalability and modularity for connecting multiple spokes. FortiGate NGFWs are deployed in a HA active/standby configuration to enforce security and traffic inspection.

Use Cases

The FortiGate highly available deployment in Oracle C3 and PCA X9-2 platform enables centralized security enforcement across various traffic flows. By integrating with Oracle's networking constructs such as DRG, route tables, and floating IPs, the solution supports secure inspection of East-West, South-North, and North-South traffic. The following use cases illustrate how FortiGate ensures consistent security controls across different communication patterns within and across VCNs, the internet, and on-premises environments.

East-West Traffic Flow

- Traffic between spoke VCNs is routed through the FortiGate cluster for inspection.
- To enable this traffic flow, DRG and VCN attachments are required, allowing the DRG to facilitate inter-VCN communication.
- Each FortiGate virtual machine is provisioned with dedicated virtual network interface cards (VNICs) within its respective spoke Virtual Cloud Network (VCN) to support interconnectivity.
- The FortiGate HA cluster leverages Oracle's floating IP feature, enabling seamless failover by shifting the floating IP between cluster members
- Spoke VCN route tables are configured to direct traffic to the FortiGate HA floating IP—either for reaching other spoke VCN classless inter-domain routings (CIDRs) or routing to the internet via a default route.

South-North Traffic Flow

- Outbound traffic from the Spoke VM to the internet is routed through the FortiGate cluster's floating IP in the spoke subnet, as defined in the Spoke VCN's route table.
- The FortiGate cluster receives the traffic and inspects it according to the configured outbound firewall policy.
- Outbound traffic can be network address translated (NATd) depending on the network topology and the logical placement of the Oracle C3/PCA X9-2 solution within the customer's on-premises environment.

North-South Traffic Flow

- Inbound traffic from the internet or the customer's on-premises network is directed to the FortiGate cluster's floating IP in the public subnet.

- The FortiGate cluster inspects the incoming traffic based on the configured inbound firewall policies.
- Source NAT (SNAT) might be required for return traffic from the Spoke VM to ensure it is routed back to the original source via the FortiGate cluster

Terminology

Oracle Cloud@Customer

Oracle Dedicated Region Cloud@Customer brings Oracle's second-generation cloud services and SaaS applications into enterprise data centers. It offers autonomous operations, high performance, and cost efficiency while meeting stringent latency requirements.

Oracle PCA X9-2

Oracle Private Cloud Appliance (PCA) X9-2 is an engineered system providing a resilient and scalable environment for modern applications. It pairs with Oracle Exadata for multi-tier applications, offering cloud-like operational benefits. Using a separate firewall appliance with PCA X9-2 enhances network security between the appliance and external networks.

Virtual Cloud Network (VCN) and Subnets

A VCN is a software-defined network in C3 or PCA X9-2, providing complete control over network environments. Each VCN can have multiple non-overlapping CIDR blocks and be segmented into subnets with public or private accessibility.

Security Lists

Security lists define inbound and outbound traffic rules for each subnet, specifying allowed traffic sources, destinations, and protocols.

Fortinet FortiGate NGFW

FortiGate provides advanced security services, including threat protection, SSL inspection, and ultra-low latency security enforcement. Available on Oracle Cloud Marketplace, it supports single root I/O virtualization (SR-IOV) for enhanced performance.

FortiGate Clustering Protocol (FGCP)

FGCP ensures high availability and redundancy through clustering, enabling seamless failover, load balancing, and session synchronization. It supports both active-passive and active-active configurations.

Bring Your Own License (BYOL)

Deploying FortiGate-VM using a license that the customer has already purchased separately, allowing for greater flexibility and cost control across cloud or hybrid environments**.**

Pay As You Go (PAYG) - Paid license

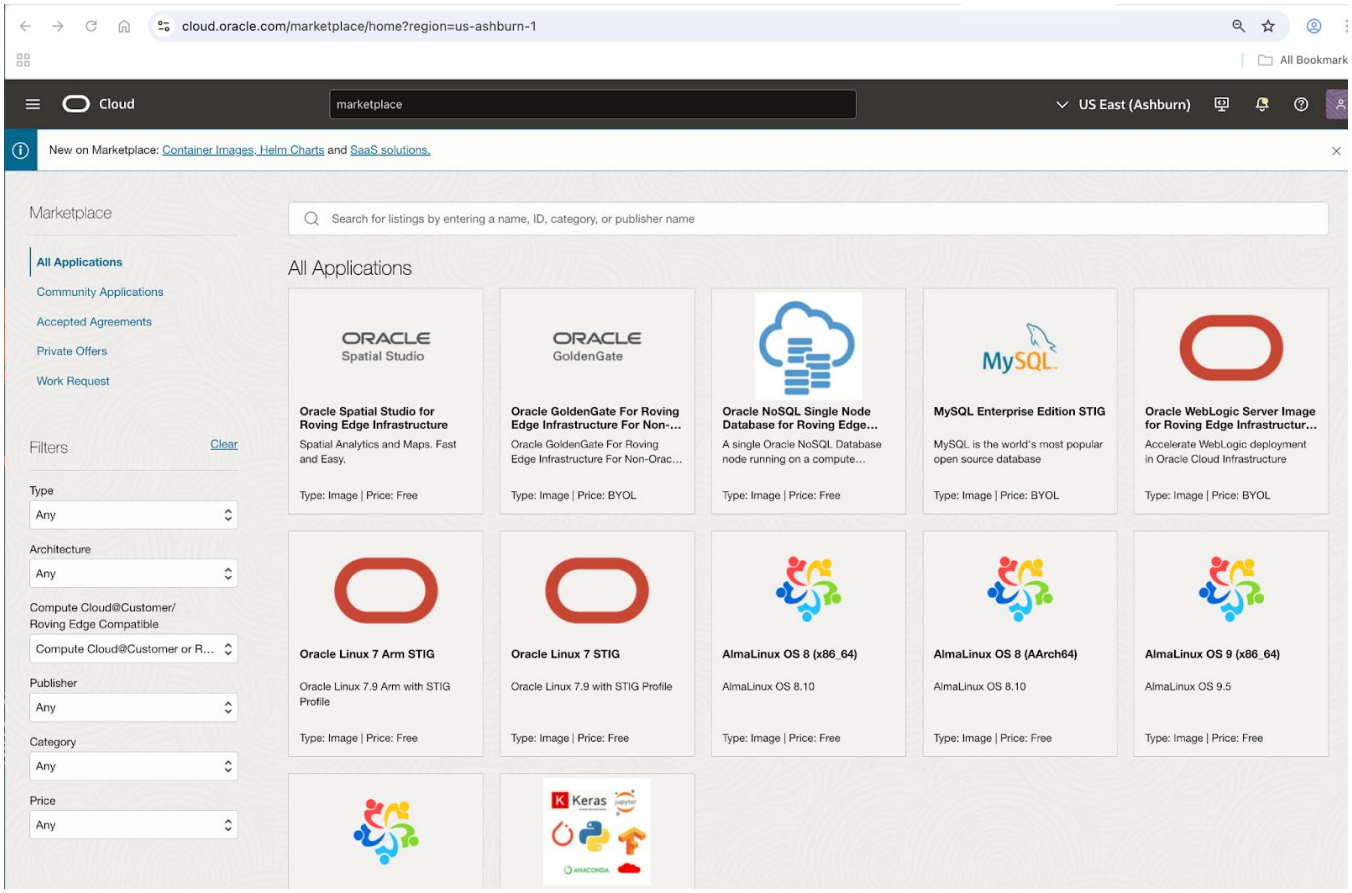
Deploying FortiGate-VM with a license that is automatically included and billed through the cloud provider’s marketplace, offering a flexible, usage-based pricing model without the need for separate license management.

Getting Started

You can download the Fortinet NGFW (BYOL version) from Oracle's OCI Marketplace.

Due to current delays in deploying the FortiGate BYOL Image on Oracle's Marketplace, an image can be obtained directly from the following Fortinet site: https://support.fortinet.com/

In the left-hand filter panel, be sure to update the "Compute Cloud@Customer / Roving Edge Compatible" filter from "Any" to "Compute Cloud@Customer or Roving Edge Compatible" to ensure C3/PCA compatible images are provided.



Fortigate PCA/C3 Configuration Guide

To download, import to C3 or PCA and deploy the Fortinet NGFW,Oracle Compute@Customer or Private Cloud Appliance, access the following Documentation:

- **Creating a Fortigate instance on PCA-X9-2 and Cloud@Customer**

Additional Resources

Explore more about this reference architecture and related materials:

- **Oracle Cloud Edge Infrastructure Documentation:**
  - Oracle Compute Cloud@Customer
  - Oracle Private Cloud Appliance

- **Fortinet FortiGate Documentation:**
  - Initial Fabric connector configuration
  - About FortiGate-VM for OCI
  - Fortinet Community

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Acknowledgments

Authors: Ozan Oguz (Fortinet), Robert Murphy (Oracle C3/PCA Solution Engineering)
Contributors: Thomas Guan (Fortinet QA), Feng Hua (Fortinet QA), Hien Nguyen (Oracle Solution Center)