NETWORK FIREWALL IN OCI

1. What is OCI?

- OCI, or Oracle Cloud Infrastructure, is Oracle's cloud computing platform. It offers a range of services for deploying and scaling applications with high performance and security. OCI is known for its global presence, robust infrastructure, and support for diverse workloads, making it a preferred choice for enterprises.

2. What is OCI Security?

- OCI security involves protective measures in Oracle Cloud Infrastructure to safeguard data and resources from unauthorized access and cyber threats, using features like encryption and identity management.

3. What is Network Firewall in the OCI?

- Network Firewall in Oracle Cloud Infrastructure (OCI) is a security service that regulates incoming and outgoing traffic within a virtual cloud network, protecting against unauthorized access.

Technical Example:

Configures rules to permit specific IP addresses to access a database, enhancing security.

Non-Technical Example:

Acts like a digital bouncer, allowing only authorized network traffic akin to a club bouncer permitting only invited guests.

4. Importance of Network Firewall in the OCI?

-Network Firewall in Oracle Cloud Infrastructure is crucial for:

Security: Safeguarding against unauthorized access and potential threats.

Control: Regulating traffic within a virtual cloud network based on defined rules.

Compliance: Ensuring adherence to security policies and preventing unauthorized activities.

Order to follow

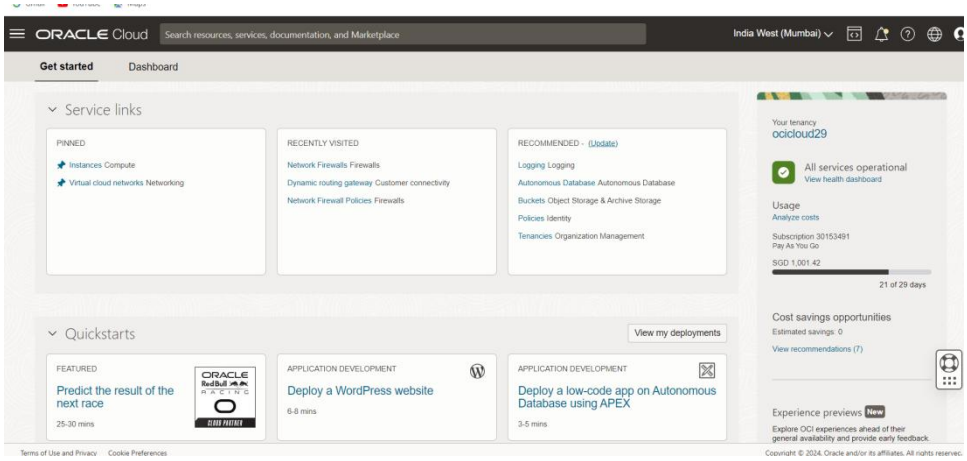
1) Network Firewall policy

- Lists
  - Service List
  - Application List
  - URL List
  - IP Address List
- Mapped Secret and Decryption Profile (Option)
  - Mapped Secret
  - Decryption

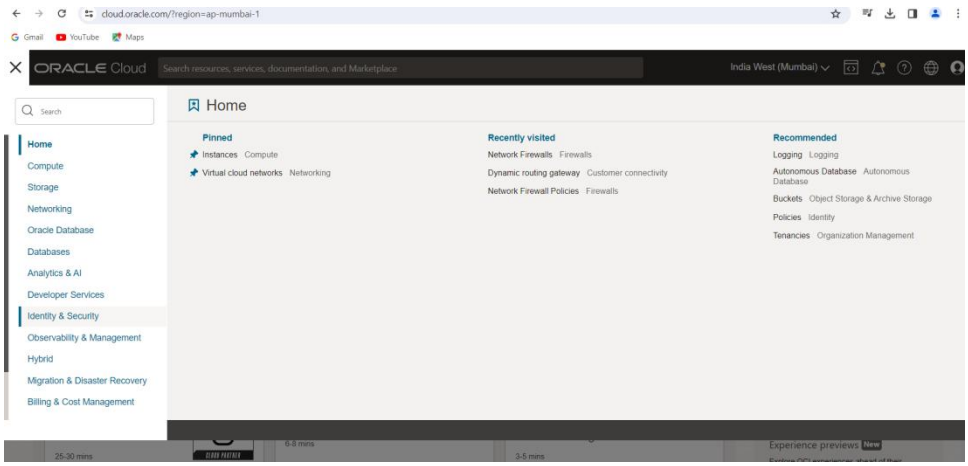
2) Create a Network Firewall

3) Configure Route table rules

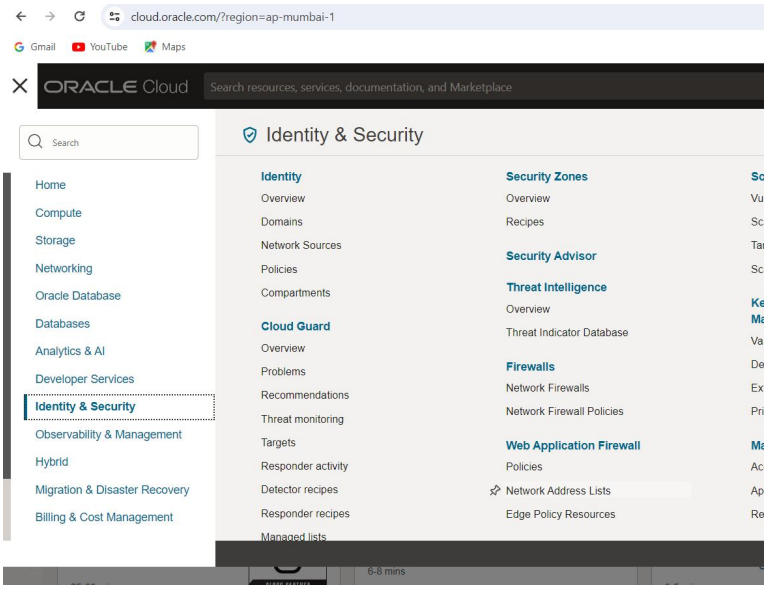
Step 1:- Put the credentials and login to the OCI account



Step 2:- Click on the Identity & Security

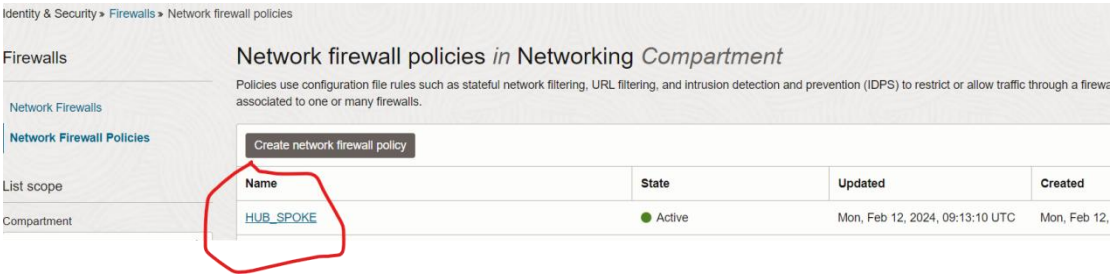


Step 3:- Click on Network Firewall Policy

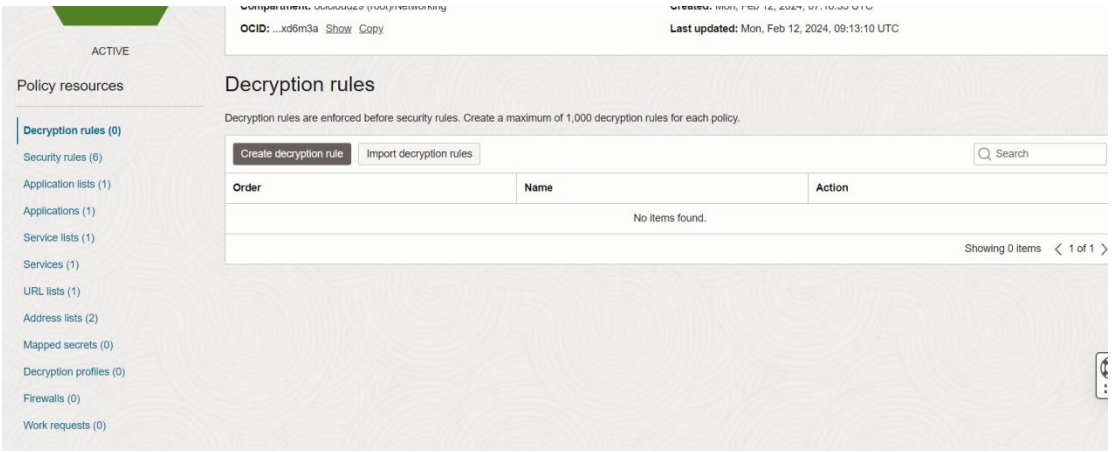


Step 4:-Click on Create Network Firewall Policy

Step 5:- Created a Network Firewall Policy

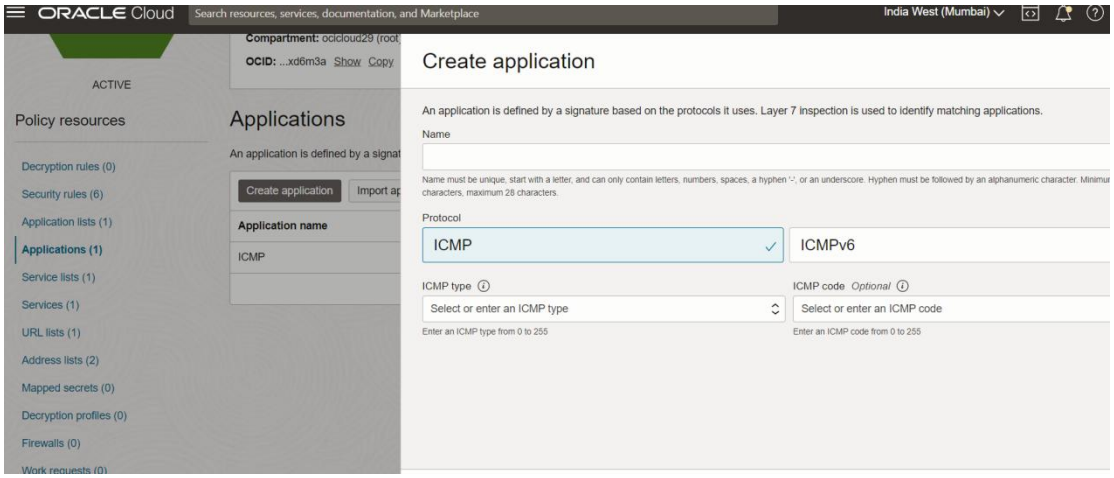


Step 6:- This will be the Interface where we have to create policy and Rules for the Network Firewall

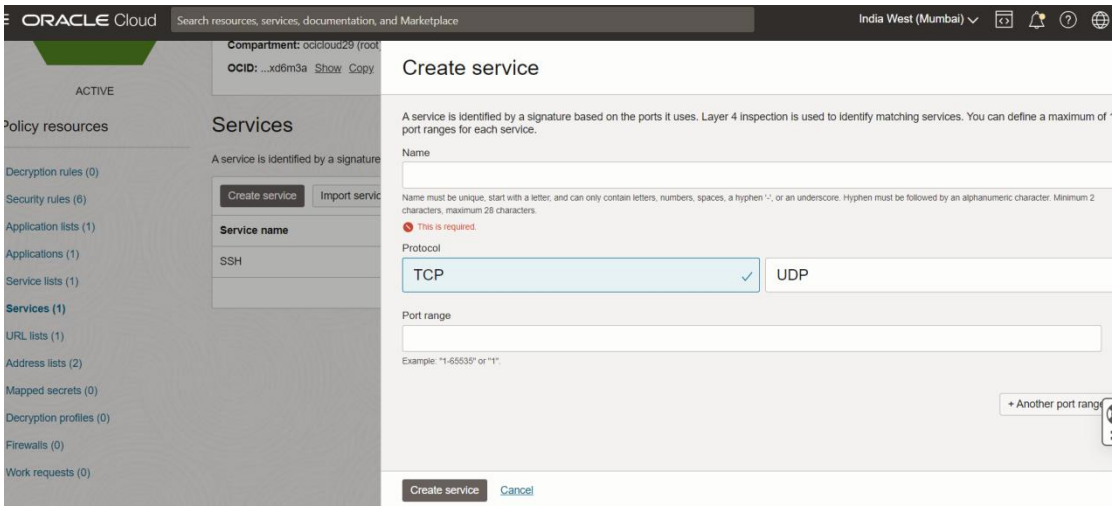


Step 7:- Add ICMP, SSH, URL policy to the selected IP address in the Network Firewall

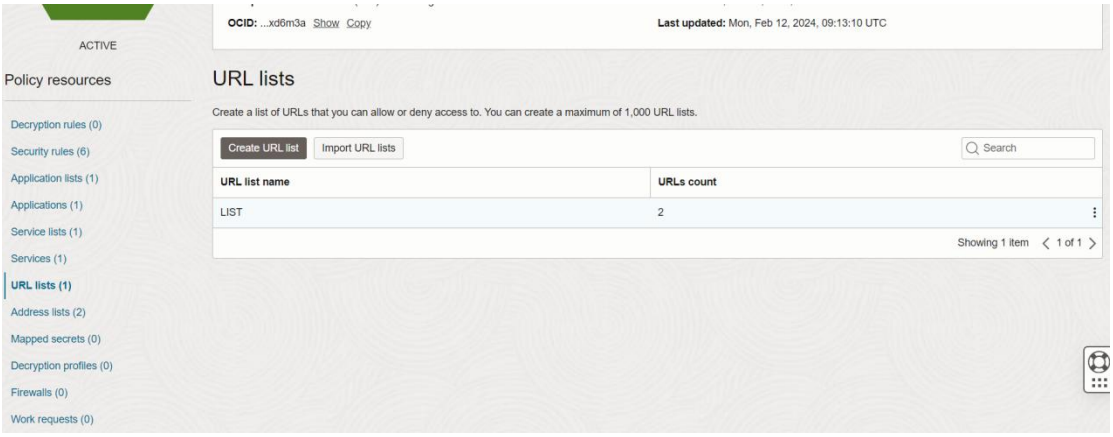
- Application List



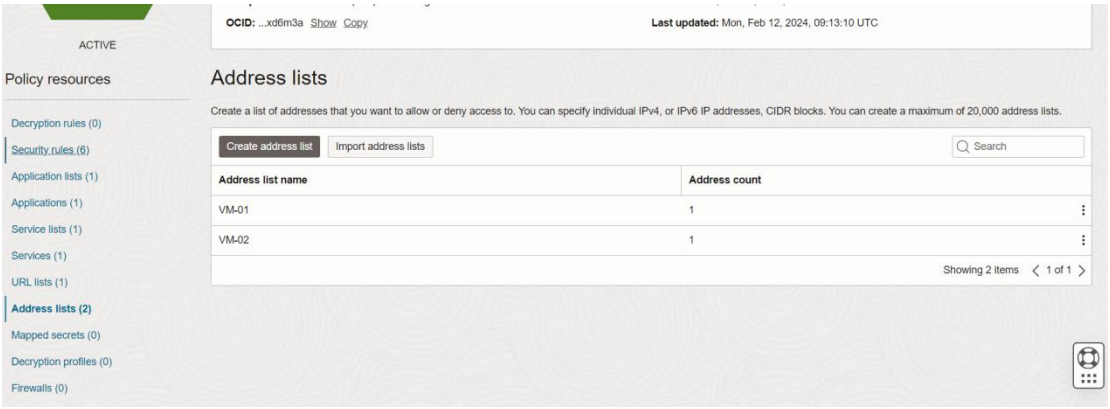
- Service List



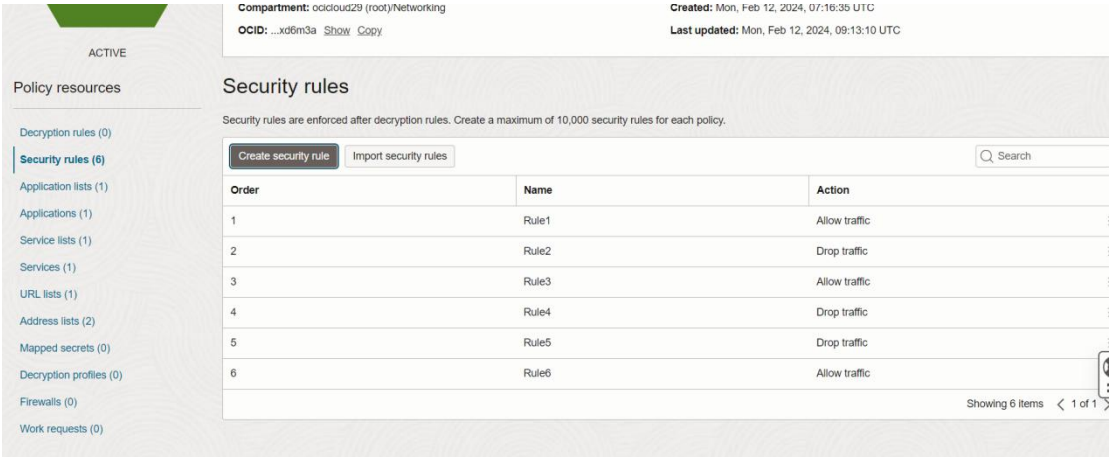
- URL List



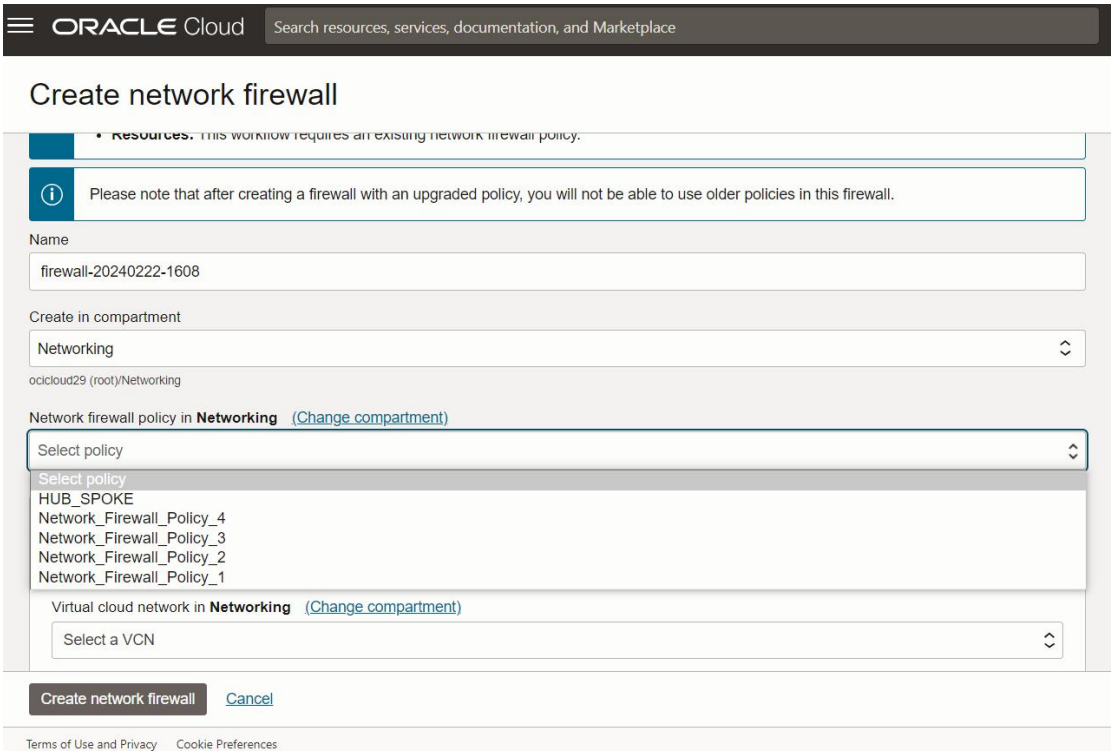
- IP address List



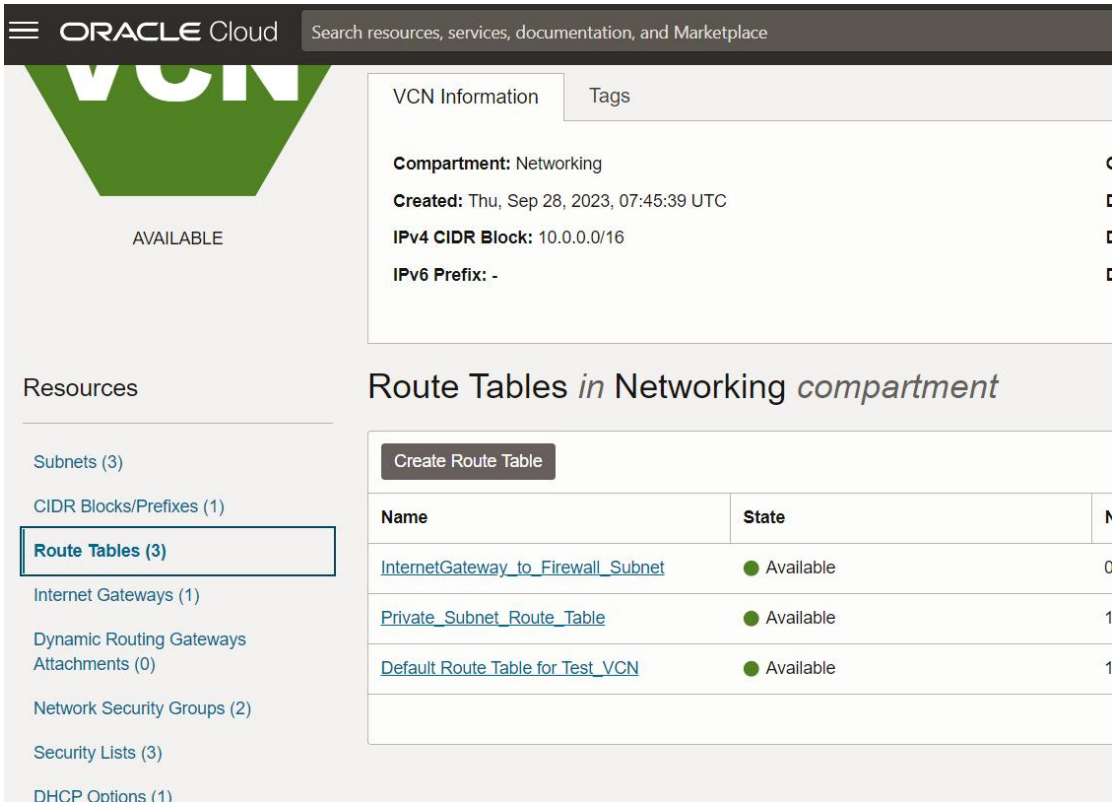
Step 8 - Create Security Rules based on Policy



Step 9:- Create Firewall in the Selected Subnet and attach the Firewall Policy which we have Created (It will take around 30-45 minutess)



Step 10:- After creating the Network Firewall go to the Networking > VCN > (choose the VCN in which we have created the firewall) > Route table and then attach the route table to the following subnets



Explanation of topics

1) Network Firewall Policy:

- **Lists:**
  - Service List: Enumerates allowed services (e.g., HTTP, SSH).
  - Application List: Specifies permitted applications (e.g., Oracle Database).
  - URL List: Defines acceptable URLs (e.g., example.com).
  - IP Address List: Specifies allowed IP addresses or ranges.
- **Mapped Secret and Decryption Profile (Option):**
  - Mapped Secret: Establishes secure communication using cryptographic keys.
  - Decryption: Configures decryption profiles for specific traffic types, enhancing visibility.

2) Create a Network Firewall:

- Follow OCI documentation steps for creating a Network Firewall. This typically involves:
  - Defining rules based on the lists created in the Network Firewall Policy.
  - Setting up parameters like allowed services, applications, and IP addresses.
  - Configuring Mapped Secrets and Decryption Profiles if needed.

3) Configure Route Table Rules:

- Utilize OCI documentation for configuring route table rules:
  - Specify how traffic should flow within the virtual network.
  - Ensure proper routing for resources protected by the Network Firewall.
  - Associate the route table with the appropriate subnets to enforce traffic control.