

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.

<u>Order to follow</u>

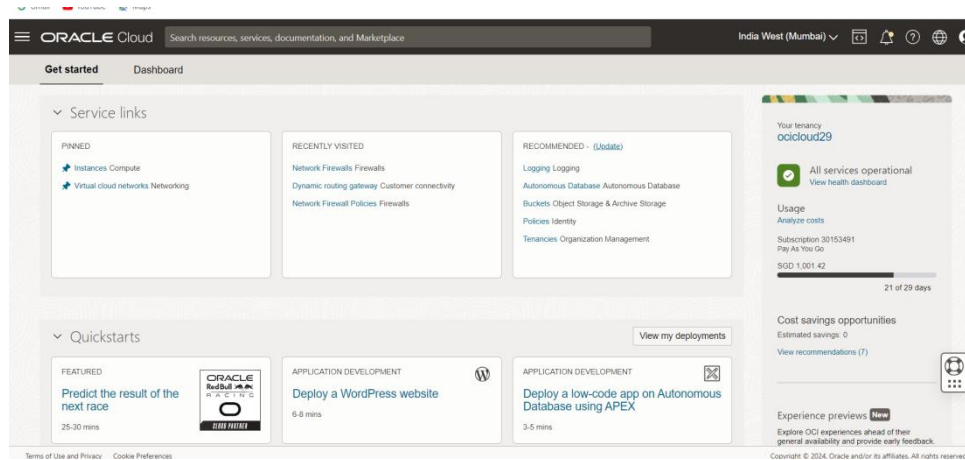
1) Network Firewall policy

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

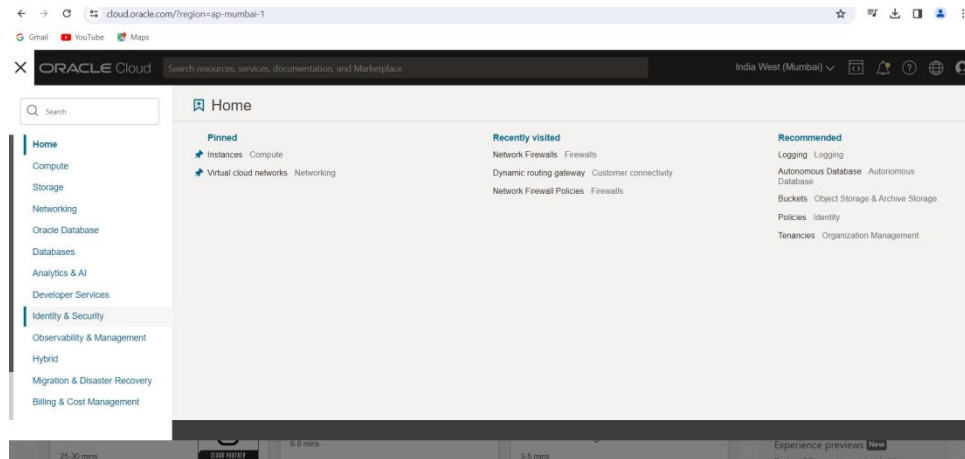
2) Create a Network Firewall

3) Configure Route table rules

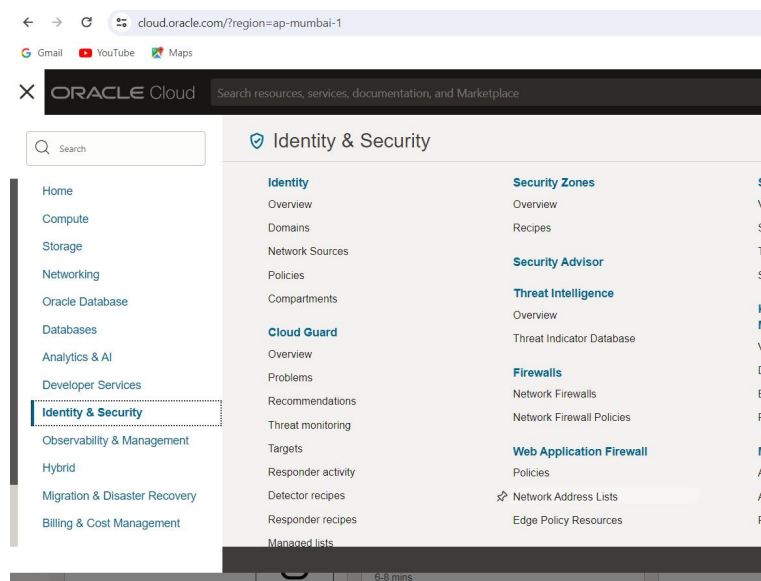
Step 1:- Put the credentials and login to the OCI account



Step 2:- Click on the Identity & Security



Step 3:- Click on Network Firewall Policy



Step 4:-Click on Create Network Firewall Policy

Identity & Security » Firewalls » Network firewall policies

Firewalls

Network Firewalls

Network Firewall Policies

List scope

Network firewall policies *in* Networking

Policies use configuration file rules such as stateful network filtering, URL filtering, and intrusion detection and prevention (IDPS) to restrict or allow traffic through a firewall associated to one or many firewalls.

Create network firewall policy

Name

Step 5:- Created a Network Firewall Policy

Identity & Security » Firewalls » Network firewall policies

Firewalls

Network Firewalls

Network Firewall Policies

List scope

Compartment

Network firewall policies *in* Networking *Compartment*

Policies use configuration file rules such as stateful network filtering, URL filtering, and intrusion detection and prevention (IDPS) to restrict or allow traffic through a firewall associated to one or many firewalls.

Create network firewall policy

Name	State	Updated	Created
HUB_SPOKE	Active	Mon, Feb 12, 2024, 09:13:10 UTC	Mon, Feb 12,

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

ACTIVE

Policy resources

- Decryption rules (0)
- Security rules (6)
- Application lists (1)
- Applications (1)
- Service lists (1)
- Services (1)
- URL lists (1)
- Address lists (2)
- Mapped secrets (0)
- Decryption profiles (0)
- Firewalls (0)
- Work requests (0)

Compartment: ocid1.ocm3a... (not refreshing)

OCID: ...x08m3a Show Copy

Created: Mon, Feb 12, 2024, 09:13:10 UTC

Last updated: Mon, Feb 12, 2024, 09:13:10 UTC

Decryption rules

Decryption rules are enforced before security rules. Create a maximum of 1,000 decryption rules for each policy.

Create decryption rule Import decryption rules Search

Order	Name	Action
No items found.		

Showing 0 items < 1 of 1 >

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

- Application List

The screenshot shows the Oracle Cloud console interface. On the left, a sidebar lists 'Policy resources' including 'Applications (1)'. The main content area is titled 'Create application'. It includes a 'Name' field, a 'Protocol' dropdown set to 'ICMP', and an 'ICMP type' dropdown. Below these are instructions for naming and selecting ICMP types. The 'ICMP code' field is optional and set to 'ICMPv6'.

Oracle Cloud Search resources, services, documentation, and Marketplace India West (Mumbai)

Compartment: odccloud29 (root) OCID: ...xd6m3a [Show](#) [Copy](#)

ACTIVE

Policy resources

- Decryption rules (0)
- Security rules (6)
- Application lists (1)
- Applications (1)**
- Service lists (1)
- Services (1)
- URL lists (1)
- Address lists (2)
- Mapped secrets (0)
- Decryption profiles (0)
- Firewalls (0)
- Work requests (0)

Applications

An application is defined by a signature based on the protocols it uses. Layer 7 inspection is used to identify matching applications.

[Create application](#) [Import application](#)

Application name

ICMP

Create application

An application is defined by a signature based on the protocols it uses. Layer 7 inspection is used to identify matching applications.

Name

Name must be unique, start with a letter, and can only contain letters, numbers, spaces, a hyphen '-', or an underscore. Hyphen must be followed by an alphanumeric character. Minimum 2 characters, maximum 28 characters.

Protocol

ICMP

ICMPv6

ICMP type

Select or enter an ICMP type

Enter an ICMP type from 0 to 255

ICMP code *Optional*

Select or enter an ICMP code

Enter an ICMP code from 0 to 255

- Service List

The screenshot shows the Oracle Cloud console interface. On the left, a sidebar lists 'Policy resources' including 'Services (1)'. The main content area is titled 'Create service'. It includes a 'Name' field, a 'Protocol' dropdown set to 'TCP', and a 'Port range' field. Below these are instructions for naming and selecting protocols. The 'Port range' field has an example: '11-65535' or '11'.

Oracle Cloud Search resources, services, documentation, and Marketplace India West (Mumbai)

Compartment: odccloud29 (root) OCID: ...xd6m3a [Show](#) [Copy](#)

ACTIVE

Policy resources

- Decryption rules (0)
- Security rules (6)
- Application lists (1)
- Applications (1)
- Service lists (1)
- Services (1)**
- URL lists (1)
- Address lists (2)
- Mapped secrets (0)
- Decryption profiles (0)
- Firewalls (0)
- Work requests (0)

Services

A service is identified by a signature based on the ports it uses. Layer 4 inspection is used to identify matching services. You can define a maximum of 1 port ranges for each service.

[Create service](#) [Import service](#)

Service name

SSH

Create service

A service is identified by a signature based on the ports it uses. Layer 4 inspection is used to identify matching services. You can define a maximum of 1 port ranges for each service.

Name

Name must be unique, start with a letter, and can only contain letters, numbers, spaces, a hyphen '-', or an underscore. Hyphen must be followed by an alphanumeric character. Minimum 2 characters, maximum 28 characters.

Protocol

TCP

UDP

Port range

Example: "11-65535" or "11"

+ Another port range

[Create service](#) [Cancel](#)

- URL List

ACTIVE

Policy resources

Decryption rules (0)

Security rules (6)

Application lists (1)

Applications (1)

Service lists (1)

Services (1)

URL lists (1)

Address lists (2)

Mapped secrets (0)

Decryption profiles (0)

Firewalls (0)

Work requests (0)

OCID: ...xd6m3a Show Copy

Last updated: Mon, Feb 12, 2024, 09:13:10 UTC

URL lists

Create a list of URLs that you can allow or deny access to. You can create a maximum of 1,000 URL lists.

Create URL listImport URL lists

Search

URL list name	URLs count
LIST	2

Showing 1 item < 1 of 1 >

- IP address List

ACTIVE

Policy resources

Decryption rules (0)

Security rules (6)

Application lists (1)

Applications (1)

Service lists (1)

Services (1)

URL lists (1)

Address lists (2)

Mapped secrets (0)

Decryption profiles (0)

Firewalls (0)

OCID: ...xd6m3a Show Copy

Last updated: Mon, Feb 12, 2024, 09:13:10 UTC

Address lists

Create a list of addresses that you want to allow or deny access to. You can specify individual IPv4, or IPv6 IP addresses, CIDR blocks. You can create a maximum of 20,000 address lists.

Create address listImport address lists

Search

Address list name	Address count
VM-01	1
VM-02	1

Showing 2 items < 1 of 1 >

Step 8 - Create Security Rules based on Policy

ACTIVE

Policy resources

Decryption rules (0)

Security rules (6)

Application lists (1)

Applications (1)

Service lists (1)

Services (1)

URL lists (1)

Address lists (2)

Mapped secrets (0)

Decryption profiles (0)

Firewalls (0)

Work requests (0)

Compartment: ocicloud29 (root)/Networking

OCID: ...xd6m3a Show Copy

Created: Mon, Feb 12, 2024, 07:16:35 UTC

Last updated: Mon, Feb 12, 2024, 09:13:10 UTC

Security rules

Security rules are enforced after decryption rules. Create a maximum of 10,000 security rules for each policy.

Create security rule

Import security rules

Order	Name	Action
1	Rule1	Allow traffic
2	Rule2	Drop traffic
3	Rule3	Allow traffic
4	Rule4	Drop traffic
5	Rule5	Drop traffic
6	Rule6	Allow traffic

Showing 6 items < 1 of 1

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

ORACLE Cloud

Search resources, services, documentation, and Marketplace

Create network firewall

Resources. This workflow requires an existing network firewall policy.

Please note that after creating a firewall with an upgraded policy, you will not be able to use older policies in this firewall.

Name

firewall-20240222-1608

Create in compartment

Networking

ocicloud29 (root)/Networking

Network firewall policy in **Networking** (Change compartment)

Select policy

Select policy

HUB_SPOKE

Network_Firewall_Policy_4

Network_Firewall_Policy_3

Network_Firewall_Policy_2

Network_Firewall_Policy_1

Virtual cloud network in **Networking** (Change compartment)

Select a VCN

Create network firewall

Cancel

Terms of Use and Privacy

Cookie Preferences

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

ORACLE Cloud

Search resources, services, documentation, and Marketplace

VCN

AVAILABLE

Resources

Subnets (3)

CIDR Blocks/Prefixes (1)

Route Tables (3)

Internet Gateways (1)

Dynamic Routing Gateways Attachments (0)

Network Security Groups (2)

Security Lists (3)

DHCP Options (1)

VCN Information

Tags

Compartment: Networking

Created: Thu, Sep 28, 2023, 07:45:39 UTC

IPv4 CIDR Block: 10.0.0.0/16

IPv6 Prefix: -

Route Tables in Networking compartment

Create Route Table

Name	State	
InternetGateway_to_Firewall_Subnet	● Available	0
Private_Subnet_Route_Table	● Available	1
Default Route Table for Test_VCN	● Available	1

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.