

## WEB APPLICATION FIREWALL ON LOAD-BALANCER(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 WEB APPLICATION FIREWALL?

- A Web Application Firewall (WAF) in Oracle Cloud Infrastructure (OCI) is a security solution that protects web applications from various online threats and attacks by monitoring, filtering, and blocking malicious traffic before it reaches the application.

### 4. Importance of the WEB APPLICATION FIREWALL?

- **Protection**
- **Security Compliance**
- **Threat Detection**
- **Performance Optimization**
- **Mitigation of DDoS Attacks**
- **Customization Security Policies**

STEP 1 :- We will work with 2 tenancy in this, at our first tenancy we have a VM in german

The screenshot shows the Oracle Cloud console interface. The top navigation bar indicates the region is "Germany Central (Frankfurt)". The left sidebar shows the "Compute" section with "Instances" selected. The main content area displays "Instances in WAF Compartment". A table lists one instance: "WindowsVM" with a state of "Running". A red arrow points to the "WindowsVM" entry in the table. The "List Scope" section shows the compartment as "WAF".

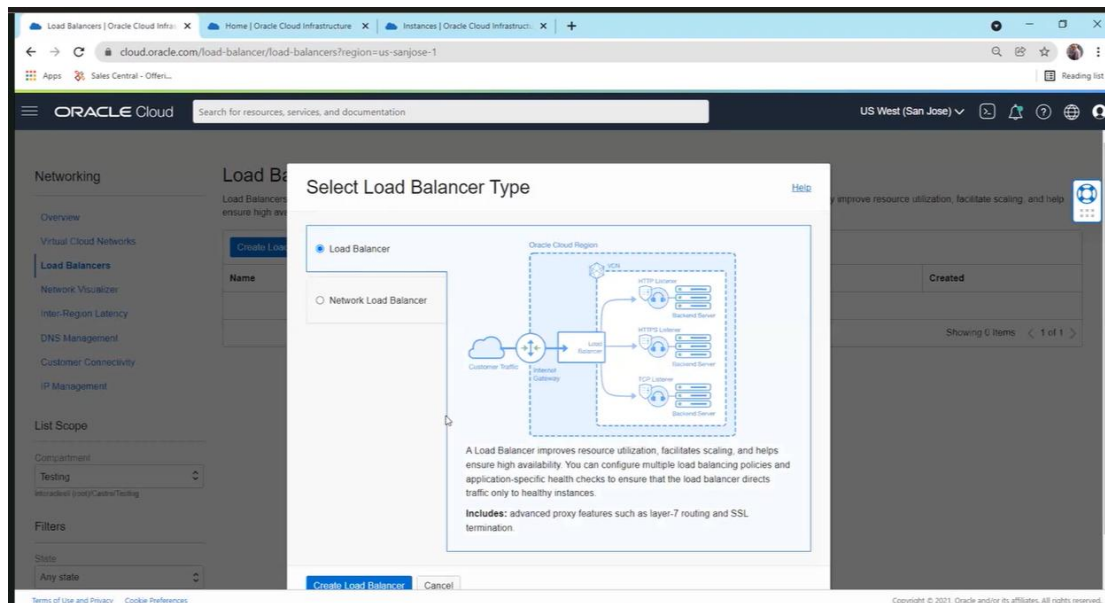
Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Availability domain	Fault domain	Created
WindowsVM	Running			VM.Standard.E4.Flex	1	16	AD-3	FD-1	Wed, Oct 13, 2021, 23:34:33 UTC

STEP 2 :- In our Second tenancy which is in US we will create a Load Balancer

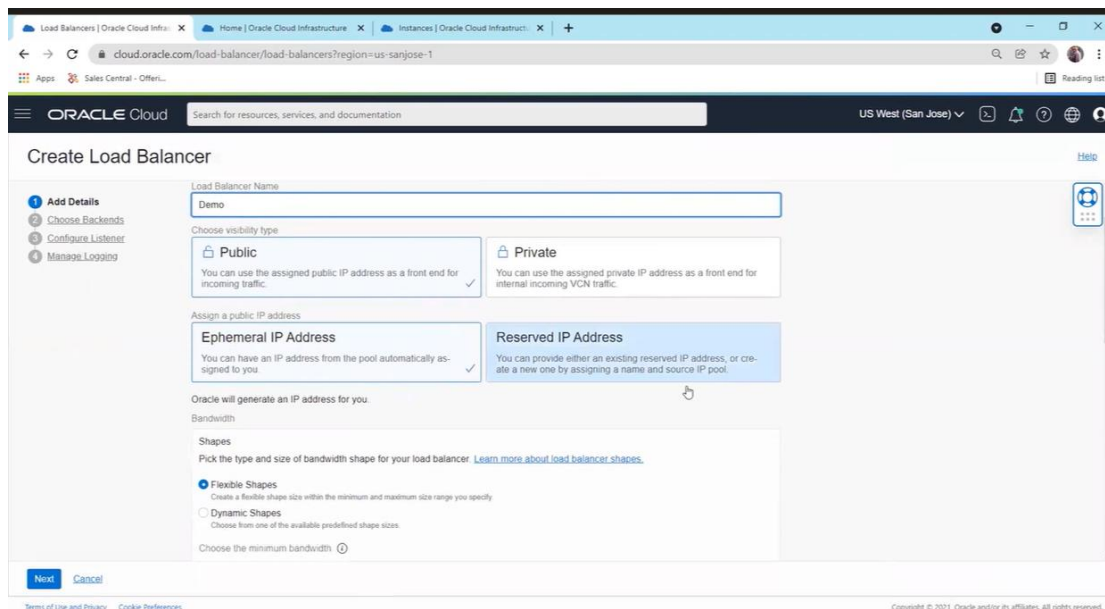
The screenshot shows the Oracle Cloud console interface. The top navigation bar indicates the region is "US West (San Jose)". The left sidebar shows the "Networking" section with "Load Balancers" selected. The main content area displays "Load Balancers in Testing Compartment". A table lists no items found. The "List Scope" section shows the compartment as "Testing".

Name	Type	State	IP Address	Shape	Overall Health	Created
No items found.						

STEP 3 :- Click on create Load balancer and choose the 1<sup>st</sup> option  
 Load balancer = Application layer (layer 7)  
 Network Load balancer = Network Layer (layer 3)



STEP 4 :- Give the name as required, choose between public and private, and assign IP from Ephemeral IP or Reserved IP



### Public vs. Private Load Balancer:

**Public Load Balancer:** This type of load balancer is accessible from the internet, allowing external users to send requests to your applications or services. It's commonly used for public-facing applications or services that need to be accessed by users over the internet.

**Private Load Balancer:** Unlike a public load balancer, a private load balancer is not directly accessible from the internet. It's deployed within a private subnet and is primarily used for internal communication between resources within your virtual cloud network (VCN). Private load balancers are suitable for applications or services that do not need to be exposed to the public internet, enhancing security by limiting external access.

### Ephemeral IP vs. Reserved IP:

**Ephemeral IP:** An ephemeral IP address is dynamically assigned to the load balancer and is temporary in nature. It's typically used for short-term deployments or testing purposes. Ephemeral IPs are released when the associated load balancer is terminated, and they cannot be reserved for long-term use.

**Reserved IP:** A reserved IP address is a static, persistent IP address that you can reserve and assign to your load balancer. Unlike ephemeral IPs, reserved IPs remain associated with the load balancer even if it's terminated and can be reused across different deployments. Reserved IPs are suitable for production environments or scenarios where consistent IP addressing is required for routing traffic.

STEP 5 :- Keep in mind While creating choose **Flexible Shape** cause web application firewall policy will only work with Flexible shape.

The screenshot shows the Oracle Cloud 'Create Load Balancer' console. The 'Ephemeral IP Address' tab is selected, indicating that an IP address will be generated for the load balancer. The 'Reserved IP Address' tab is also visible, showing options for providing an existing reserved IP address or creating a new one. The 'Shapes' section is expanded, showing 'Flexible Shapes' and 'Dynamic Shapes'. A red arrow points to the 'Flexible Shapes' option, which is selected. The 'Flexible Shapes' section allows users to pick the type and size of bandwidth shape for their load balancer, with a link to 'Learn more about load balancer shapes'. The 'Dynamic Shapes' section allows users to choose from one of the available predefined shape sizes. The 'Choose the minimum bandwidth' section shows a range from 10 Mbps to 8000 Mbps, with a selected value of 10 Mbps. The 'Choose the maximum bandwidth' section shows a range from 10 Mbps to 8000 Mbps, with a selected value of 10 Mbps. The 'Next' button is visible at the bottom left, and the 'Cancel' button is visible at the bottom right. The footer includes 'Terms of Use and Privacy' and 'Cookie Preferences' links, and a copyright notice for Oracle.

STEP 6 :- Choose the VCN and Subnet in which we want to create the Load balancer

ORACLE Cloud Search for resources, services, and documentation US West (San Jose)

### Create Load Balancer

- 1 Add Details
- 2 Choose Backends
- 3 Configure Listener
- 4 Manage Logging

10 Mbps 10 Mbps 8000 Mbps

The maximum service limit is currently 5000 Mbps. For more bandwidth, request a service limit increase from the service limits page in the console.

☐ Enable IPv6 Address Assignment  
Enables a dual-stack IPv4/IPv6 implementation for your load balancer. Learn more about [IPv6 Addresses](#).

Choose Networking

Virtual Cloud Network in Testing [\(Change Compartment\)](#)

VCN4SSL

Specify the subnet to host your load balancer:

Subnet in Testing [\(Change Compartment\)](#)

Select a subnet

☐ Use network security groups to control traffic ⓘ

[Hide Advanced Options](#)

Next Cancel

Terms of Use and Privacy Cookie Preferences Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

STEP 7 :- Click on next and choose from Weighted Round Robin, IP Hash, Least Connections

ORACLE Cloud Search for resources, services, and documentation US West (San Jose)

### Create Load Balancer

- 1 Add Details
- 2 Choose Backends
- 3 Configure Listener
- 4 Manage Logging

#### Choose Backends

A load balancer distributes traffic to backend servers within a backend set. A backend set is a logical entity defined by a load balancing policy, a health check policy, and a list of backend servers (Compute instances).

Specify a Load Balancing Policy

**Weighted Round Robin**

This policy distributes incoming traffic sequentially to each server in a back-end set list. ✓

**IP Hash**

This policy ensures that requests from a particular client are always directed to the same backend server.

**Least Connections**

This policy routes incoming request traffic to the backend server with the fewest active connections.

Select Backend Servers: Optional

No backend servers selected. Click **Add Backends** to select resources from a list of available Compute instances. You can choose instances from one compartment at a time. After you add instances from one compartment, you can choose **Add More Backends** to add instances from another compartment. You can also add backend servers after you create the load balancer.

**Add Backends**

Specify Health Check Policy

A health check is a test to confirm the availability of backend servers. A health check can be a request or a connection attempt. Based on a time interval you specify, the load balancer applies the health check policy to continuously monitor backend servers.

Protocol: HTTP Port: 80 (Optional)

Ensure your backend set's health check port number matches the backend's port.

Previous Next Cancel

## Weighted Round Robin:

This algorithm assigns a weight to each server based on its capacity or performance.

Traffic is distributed to servers in a cyclic manner according to their weights.

Servers with higher weights receive more traffic compared to those with lower weights.

Useful when you want to prioritize certain servers over others based on their capabilities.

## IP Hash:

In this algorithm, the source IP address of the client is used to determine which server will handle the request.

The hash function generates a unique identifier from the client's IP address, and this identifier is used to select the server.

Ensures that requests from the same client are always routed to the same server.

Useful for session persistence or when maintaining state information between the client and server.

## Least Connection:

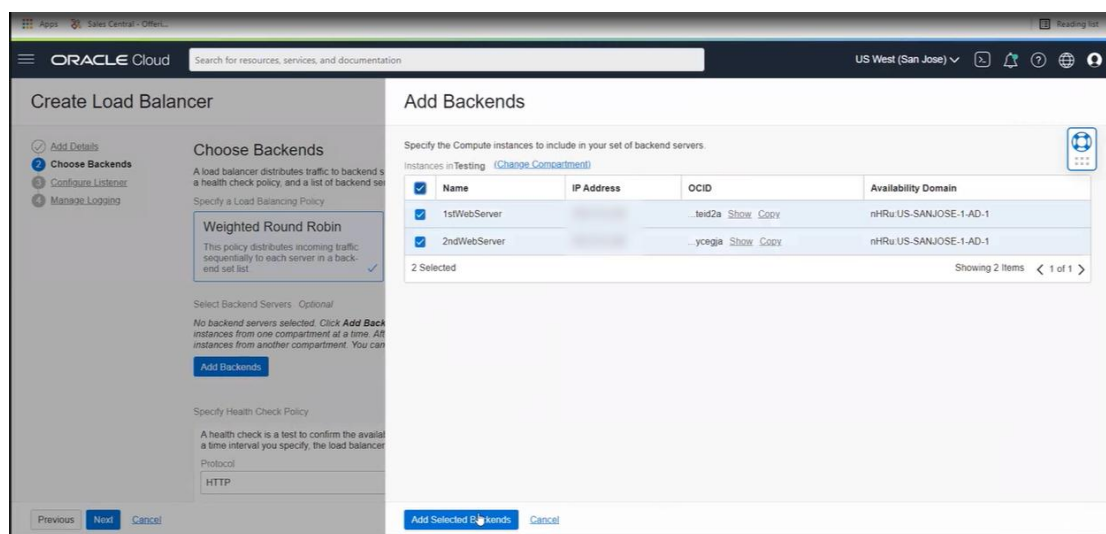
This algorithm directs traffic to the server with the fewest active connections at the time of the request.

It dynamically adjusts the load distribution based on the current workload of each server.

New connections are sent to the server with the least number of active connections.

Helpful in evenly distributing the load among backend servers and preventing overloading of any single server.

## STEP 8 :- Add Backend Servers



STEP 9 :- Click on next and choose on which protocol you want to configure Listener

The screenshot shows the 'Create Load Balancer' console in the Oracle Cloud interface. The 'Configure Listener' step is active, indicated by a blue circle with a number 3 in the left-hand navigation pane. The main content area explains that a listener is a logical entity that checks for incoming traffic. It includes a text input for 'Listener Name' with the value 'listener\_lb\_2021-1123-1456'. Below this, there are four buttons for specifying the type of traffic: 'HTTPS', 'HTTP' (which is selected and has a checkmark), 'HTTP/2', and 'TCP'. A text input for 'Specify the port your listener monitors for ingress traffic' has the value '80'. At the bottom of the main content area, there is a link to 'Show Advanced Options'. The footer of the console shows 'Previous', 'Next', and 'Cancel' buttons, along with 'Terms of Use and Privacy' and 'Cookie Preferences' links.

STEP 10 :- Click next and Choose if you want enable or disable log and then click on submit

The screenshot shows the 'Create Load Balancer' console in the Oracle Cloud interface, now at the 'Manage Logging' step. The left-hand navigation pane shows 'Manage Logging' as the active step with a blue circle and number 4. The main content area explains that enabling access and error logs is optional but recommended. It includes a warning box stating that logging is an option in the Load Balancer service and that standard limits, restrictions, and rates apply. Below this, there are two sections: 'Error Logs' and 'Access Logs'. Each section has a toggle switch that is currently 'Not Enabled'. The footer of the console shows 'Previous', 'Submit', and 'Cancel' buttons, along with 'Terms of Use and Privacy' and 'Cookie Preferences' links.

## STEP 11 :- Successfully Created Load Balancer

The screenshot displays the Oracle Cloud console interface for a Load Balancer named 'Demo'. The console shows the 'Load Balancer Information' tab, which includes details such as OCID, creation time, shape, bandwidth, IP address, virtual cloud network, subnet, web application firewall, network security groups, and type. The 'Overall Health' section indicates that the load balancer is 'OK'. The 'Backend Sets Health' section shows that the backend sets are also 'OK'. The 'Backend Sets Drain Status' section shows that the backend sets are 'Drained'.

**Load Balancer Information**

- OCID: [...j32gyq](#) [Show](#) [Copy](#)
- Created: Tue, Nov 23, 2021, 22:57:27 UTC
- Shape: Flexible
- Min Bandwidth: 10 Mbps
- Max Bandwidth: 10 Mbps
- IP Address: [Public](#)
- Virtual Cloud Network: [VCN4SSL](#)
- Subnet: [Public Subnet.VCN4SSL](#)
- Web Application Firewall: None
- Network Security Groups: [None](#) [Edit](#)
- Type: Load Balancer

**Overall Health**

- OK

**Backend Sets Health**

- 0 Critical
- 0 Warning
- 0 Incomplete
- 0 Pending
- 1 OK

**Backend Sets Drain Status**

- 0 Drained

## STEP 12 :- To check the working copy the IP address of the Load balancer

The screenshot displays the Oracle Cloud console interface for the Load Balancer 'Demo'. The 'Load Balancer Information' tab is selected, and the IP address is highlighted. A context menu is open over the IP address, showing options like 'Copy', 'Copy link to highlight', 'Go to', 'Print...', and 'Inspect'. The 'Copy' option is selected, indicating that the IP address has been copied to the clipboard.

**Load Balancer Information**

- OCID: [...j32gyq](#) [Show](#) [Copy](#)
- Created: Tue, Nov 23, 2021, 22:57:27 UTC
- Shape: Flexible
- Min Bandwidth: 10 Mbps
- Max Bandwidth: 10 Mbps
- IP Address: [Public](#)
- Virtual Cloud Network: [VCN4SSL](#)
- Subnet: [Public Subnet.V](#)
- Web Application Firewall: None
- Network Security Groups: [None](#) [Inspect](#)
- Type: Load Balancer

**Overall Health**

- OK

**Backend Sets Health**

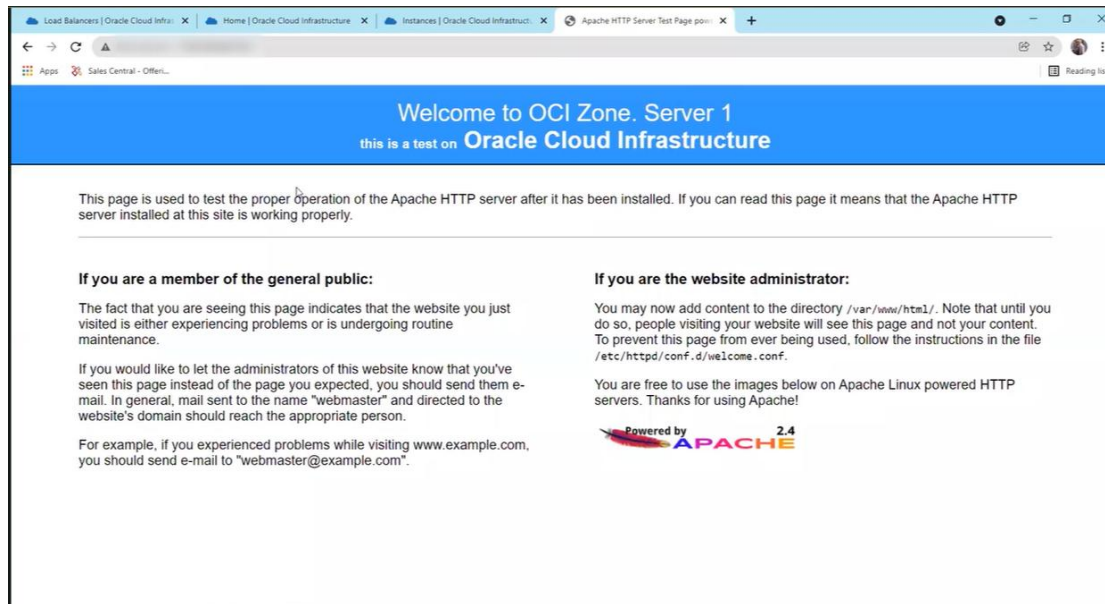
- 0 Critical
- 0 Warning
- 0 Incomplete
- 0 Pending
- 1 OK

**Backend Sets Drain Status**

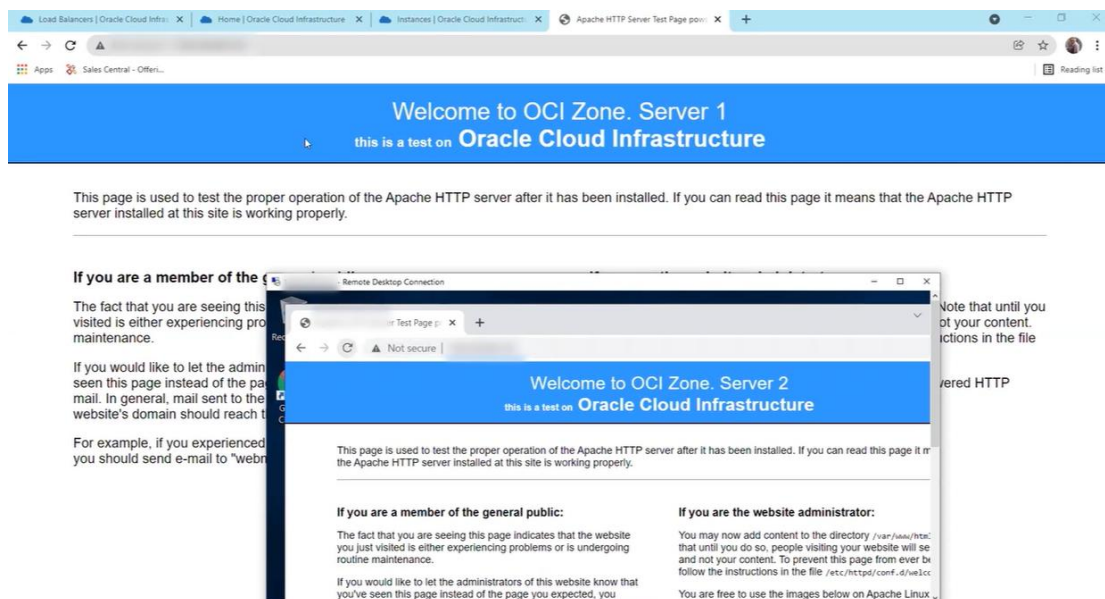
- 0 Drained



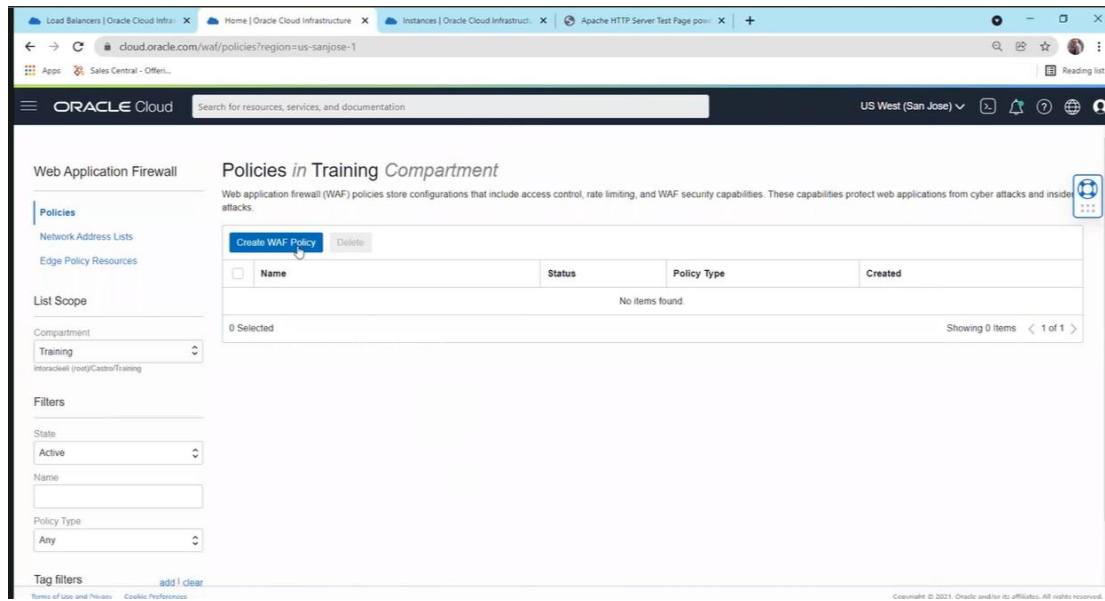
STEP 13 :- Paste it in the browser from US



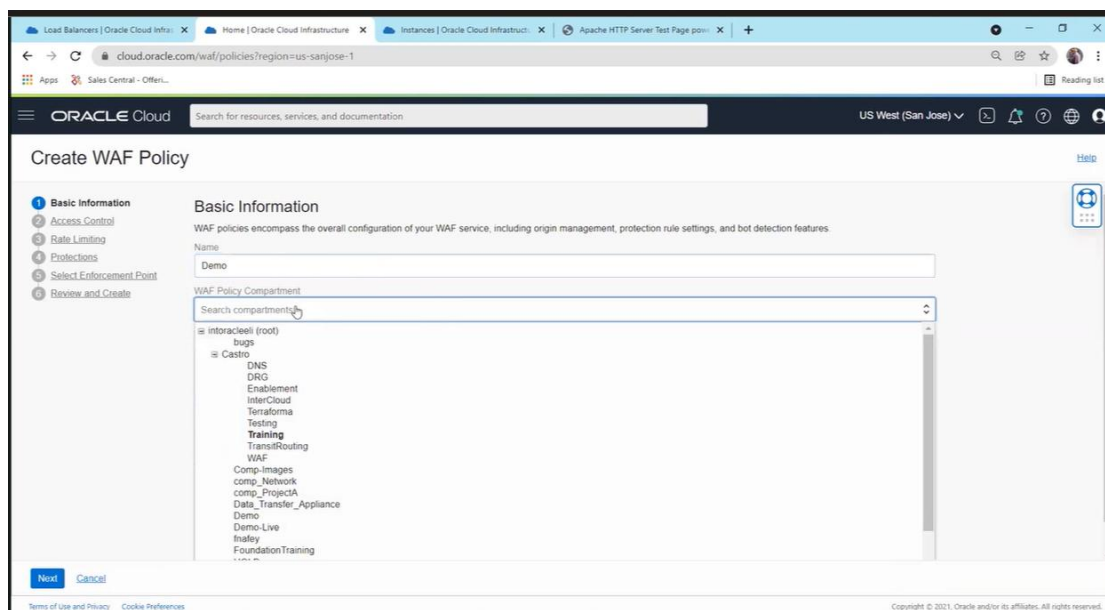
STEP 14 :- Paste it in the browser from German



## STEP 15 :- Now Creating a Web-Application Firewall policy



## STEP 16 :- First the Basic Information Section Fill the name according to the requirement and same goes with the compartment



STEP 17 :- This are the Action we have Check, Allow and Detect, write now we don't have any rule  
So we will just click on the Next

STEP 18 :- Will Click on the Access Control

## Access Control:

Access control refers to setting rules and policies to control who can access your web application. This involves defining whitelist and blacklist rules to allow or block specific IP addresses or ranges from accessing your application. Access control helps in preventing unauthorized access and protecting your web application from malicious users or bots.

## Rate Limiting:

Rate limiting involves setting limits on the number of requests that can be sent to your web application within a certain period of time. It helps in mitigating potential DDoS (Distributed Denial of Service) attacks by limiting the rate at which requests are processed. Rate limiting rules can be configured based on various parameters such as IP address, URL path, or HTTP method, allowing you to control the rate of incoming traffic and ensure the availability of your application.

## Protection:

Protection mechanisms in WAF involve implementing rules and policies to protect your web application from common security threats such as SQL injection, cross-site scripting (XSS), and other OWASP (Open Web Application Security Project) top 10 vulnerabilities. These protection rules are designed to inspect incoming requests and block or sanitize malicious payloads before they reach your application servers. By enforcing protection rules, WAF helps in safeguarding your web application and preventing potential security breaches.

## Enforcement Point:

The enforcement point is the location within your network where the WAF is deployed to intercept and inspect incoming traffic destined for your web application. In OCI, the enforcement point typically resides within the network path between the client and your application servers. It acts as a gateway through which all incoming requests must pass before reaching your application, allowing the WAF to inspect, filter, and enforce security policies in real-time.

STEP 19 :- give a Name and choose a Condition

The screenshot displays the Oracle Cloud WAF console interface. On the left, a sidebar titled 'Create WAF Policy' shows a progress list with steps: Basic Information, Access Control (selected), Rate Limiting, Protections, Select Enforcement Point, and Review and Create. The main panel is titled 'Add Access Rule'. It includes a 'Name' field with the value 'US'. Below this, the 'Conditions' section is active, showing a rule where the 'Country/Region' is 'In List'. A dropdown menu for 'Countries' is open, displaying a list of countries including United Arab Emirates, United Kingdom, Réunion, Tunisia, and United States. The 'Rule Action' section below shows the 'Action Name' as 'Pre-configured Check Action' and the 'Action Type' as 'Check'. At the bottom of the main panel, there are 'Add Access Rule' and 'Cancel' buttons. The footer of the console shows 'Terms of Use and Privacy' and 'Cookie Preferences' on the left, and a copyright notice 'Copyright © 2021, Oracle and/or its affiliates. All rights reserved.' on the right.

## STEP 20 :- Choose the Rule Action

The screenshot shows the 'Add Access Rule' configuration page in the Oracle Cloud console. The left sidebar contains a 'Create WAF Policy' section with steps: 1. Basic Information, 2. Access Control (selected), 3. Rate Limiting, 4. Protections, 5. Select Enforcement Point, and 6. Review and Create. The 'Access Control' section includes a checkbox for 'Enable Access Control' which is checked. Below this is the 'Request Control' section with an 'Add Access Rule' button. The main area is titled 'Add Access Rule' and contains a 'Condition Type' dropdown set to 'Country/Region', an 'Operator' dropdown set to 'In List', and a 'Countries' dropdown set to 'United States'. There is a '+ Another Condition' button. Below the conditions is the 'Rule Action' section, which states 'Then perform the following action.' and has an 'Action Name' dropdown set to 'Pre-configured Check Action'. Below this is a 'Create new action' section with a 'Check' dropdown set to 'Pre-configured Check Action'. There are also options for 'Allow' (Pre-configured Allow Action) and 'Return HTTP Response' (Pre-configured 401 Response Code Action). At the bottom are 'Add Access Rule' and 'Cancel' buttons.

## STEP 21 :- After adding the rule we have to choose the Default rule as well

The screenshot shows the 'Default Action' configuration page in the Oracle Cloud console. The left sidebar is the same as in Step 20. The main area is titled 'Default Action' and contains a description: 'You indicate how access rules should handle requests that don't match any rule group that's defined for the policy. You provide this configuration regardless of whether you define rule groups for the policy.' Below this is an 'Action Name' dropdown set to 'Pre-configured Allow Action'. There is a 'Create new action' section with an 'Allow' dropdown set to 'Pre-configured Allow Action'. There are also options for 'Return HTTP Response' (Pre-configured 401 Response Code Action). At the bottom are 'Previous', 'Next', and 'Cancel' buttons.

## STEP 22 :- We can add the Rate Limiting Rule

The screenshot shows the Oracle Cloud WAF console interface. On the left, a sidebar titled 'Create WAF Policy' lists steps: Basic Information, Access Control, Rate Limiting (selected), Protections, Select Enforcement Point, and Review and Create. The main content area is titled 'Add Rate Limiting Rule'. It includes a 'Name' field, a 'Conditions (Optional)' section with a table for 'When the following Conditions are met' (Condition Type: Path, Operator: Is, Value: ), and a 'Rate Limiting Configuration' section with fields for 'Requests Limit', 'Period In Seconds', and 'Action Duration in Seconds'. Navigation buttons 'Previous', 'Next', and 'Cancel' are at the bottom.

cloud.oracle.com/waf/policies?region=us-sanjose-1

ORACLE Cloud

US West (San Jose)

Create WAF Policy

- 1 Basic Information
- 2 Access Control
- 3 Rate Limiting
- 4 Protections
- 5 Select Enforcement Point
- 6 Review and Create

Rate Limiting Optional

Rate limiting allows inspection of HTTP connections.

☒ Enable to configure rate limiting rules

Rate Limiting Rules

[Add Rate Limiting Rule](#) [Change Action](#)

☐ Rule Name

0 Selected

Previous Next Cancel

Add Rate Limiting Rule Cancel

Terms of Use and Privacy Cookie Preferences

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

## STEP 23 :- We can add the protection Rule as Well

The screenshot shows the Oracle Cloud WAF console interface. On the left, a sidebar titled 'Create WAF Policy' lists steps: Basic Information, Access Control, Rate Limiting, Protections (selected), Select Enforcement Point, and Review and Create. The main content area is titled 'Add Protection Rule'. It includes a 'Name' field, a 'Conditions (Optional)' section with a table for 'When the following Conditions are met' (Condition Type: Path, Operator: Is, Value: ), and a 'Rule Action' section with a dropdown for 'Action Name' (Pre-configured Check Action) and a radio button for 'Action Type: Check'. Navigation buttons 'Previous', 'Next', and 'Cancel' are at the bottom.

cloud.oracle.com/waf/policies?region=us-sanjose-1

ORACLE Cloud

US West (San Jose)

Create WAF Policy

- 1 Basic Information
- 2 Access Control
- 3 Rate Limiting
- 4 Protections
- 5 Select Enforcement Point
- 6 Review and Create

Protections Optional

Protection rules determine if a network request is malicious.

☒ Enable to configure protection rules

Request Protection Rule

[Add Request Protection Rule](#)

☐ Rule Name

0 Selected

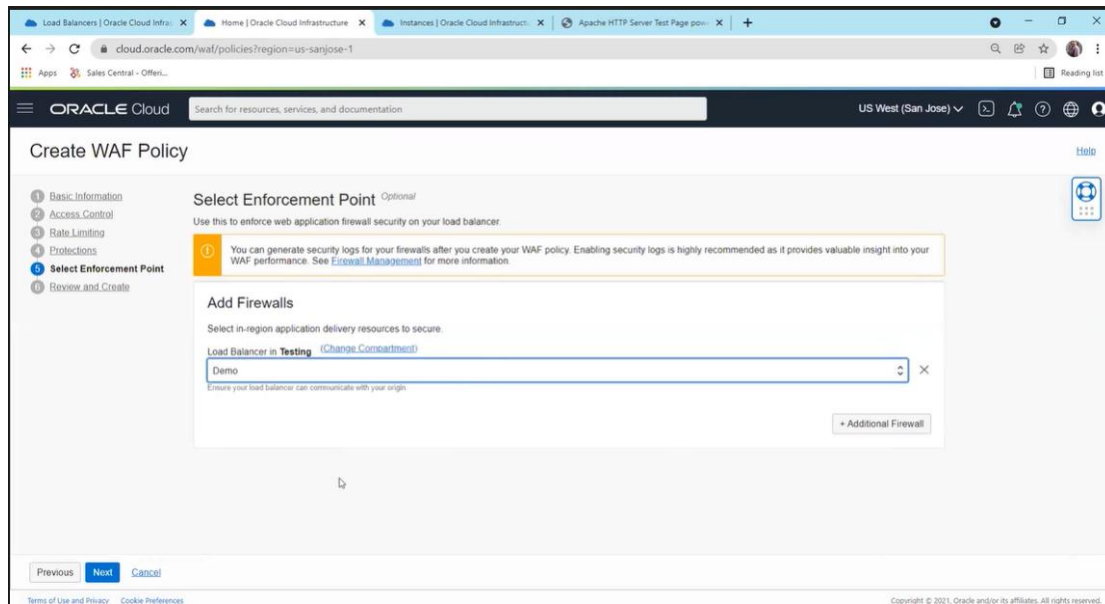
Previous Next Cancel

Add Request Protection Rule Cancel

Terms of Use and Privacy Cookie Preferences

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

STEP 24 :- On the Enforcement Point we can select our Load Balancer



STEP 25 :- Review and create the Web Application Firewall

