ORACLE

OCI Web Application Firewall

Increasing cyber attacks

<50%

of companies globally are sufficiently prepared for a cybersecurity attack,
according to a report that surveyed
3,000 business leaders from 80 countries

Source: Eurasia Group, 2019

92%

of IT professionals surveyed feel that immaturity in their cloud security
programs is creating a readiness gap

Source: Oracle and KPMG Cloud Threat Report, 2020

Exploit data
Steal personal data, usernames and passwords to get to more important data

Hold data ransom
Steal records, personal data, usernames and passwords and charge the organization to give it back

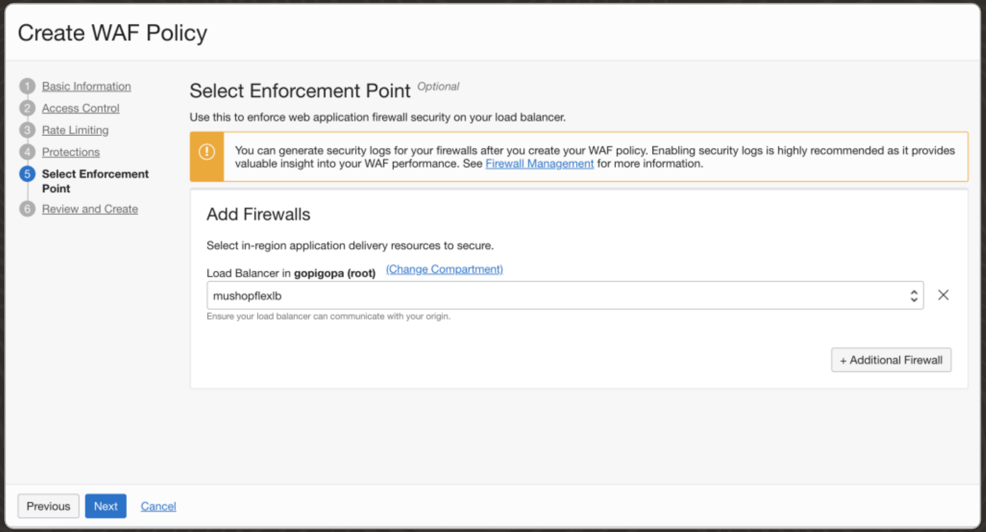
Steal infrastructure
Take control of an organization's compute, storage and network resources so not to pay for them

Deny service
Prevent web services from working to impact organization's reputation or bottom line

OCI Web Application Firewall (WAF)

OCI WAF protects against threats such as OWASP defined top-10 vulnerabilities. It can be used to limit access to the application based on geography or the signature of incoming requests, block unwanted bots.

OCI WAF protects your application infrastructure and workloads no matter where they reside: in OCI, on-premises, multi-cloud and anywhere in between.



Select Enforcement Point *Optional*

Use this to enforce web application firewall security on your load balancer.

You can generate security logs for your firewalls after you create your WAF policy. Enabling security logs is highly recommended as it provides valuable insight into your WAF performance. See Firewall Management for more information.

Add Firewalls

Select in-region application delivery resources to secure.

Load Balancer in **gopigopa (root)** (Change Compartment)

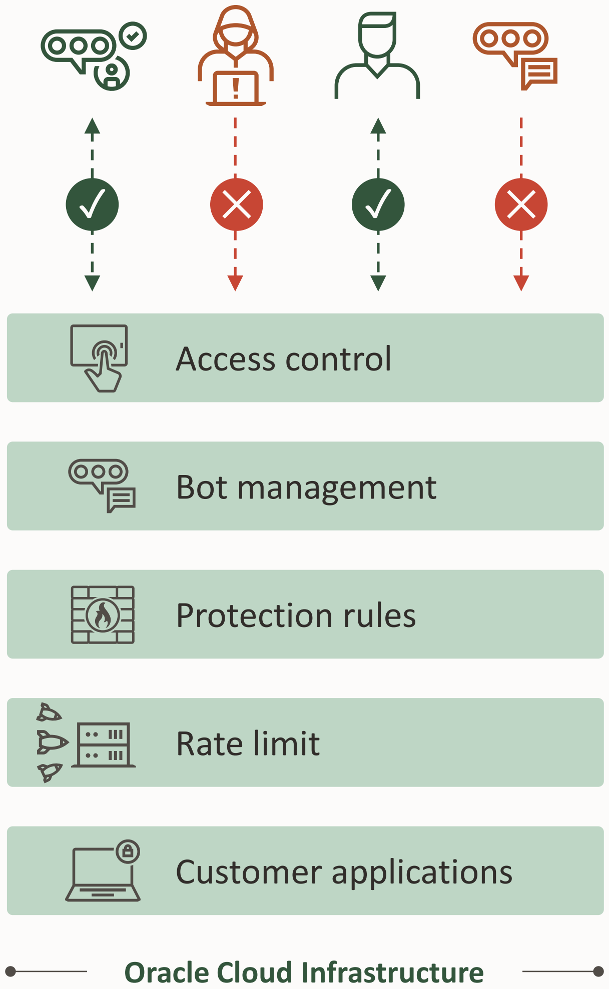
mushopflexlb

Ensure your load balancer can communicate with your origin.

Customer benefits

- Layered defense and flexibility to enforce security at the edge closest to users as well as in-region closest to the application on flexible load balancers (New!)
- WAF policies can be enforced on internet facing web applications, and/or (public/private) flexible load balancer instances
- Protects internet facing and internal applications against both external and insider threats
- Supports access rules, protection rules, rate limiting and bot management*

OCI WAF features



Access control

Bot management

Protection rules

Rate limit

Customer applications

Oracle Cloud Infrastructure

Restrict or control access to critical web applications, data and service

Identifies whether request are from a human or a machine

Controls or blocks non-human suspicious requests

Hides the origin server

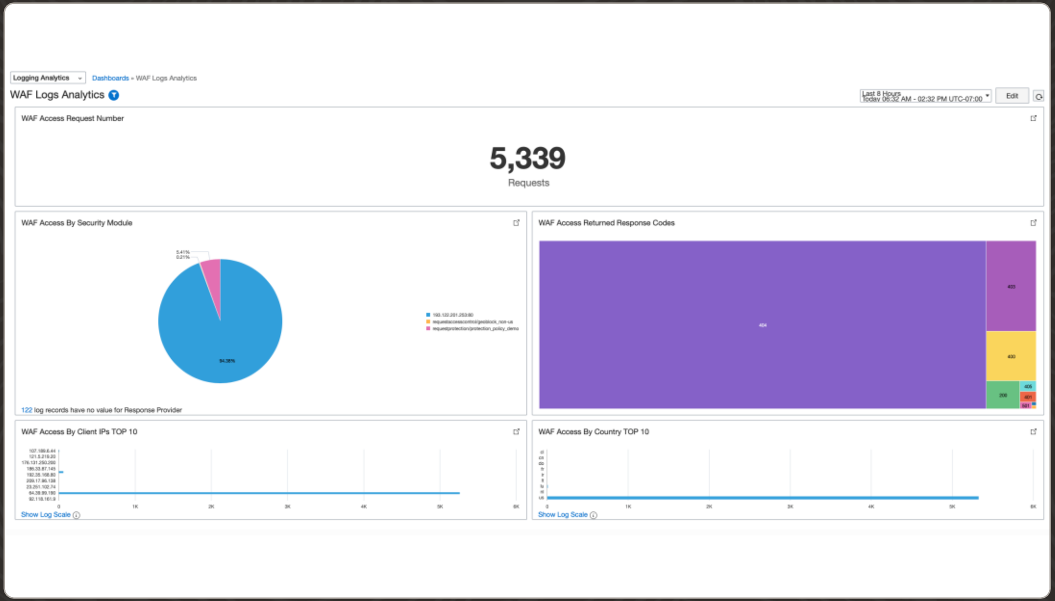
Inspects traffic as it tries to access the server or as it leaves the server

Provides protection against L7 DDOS

Access controls

Use the access controls to restrict or control access to your critical web applications, data and services.

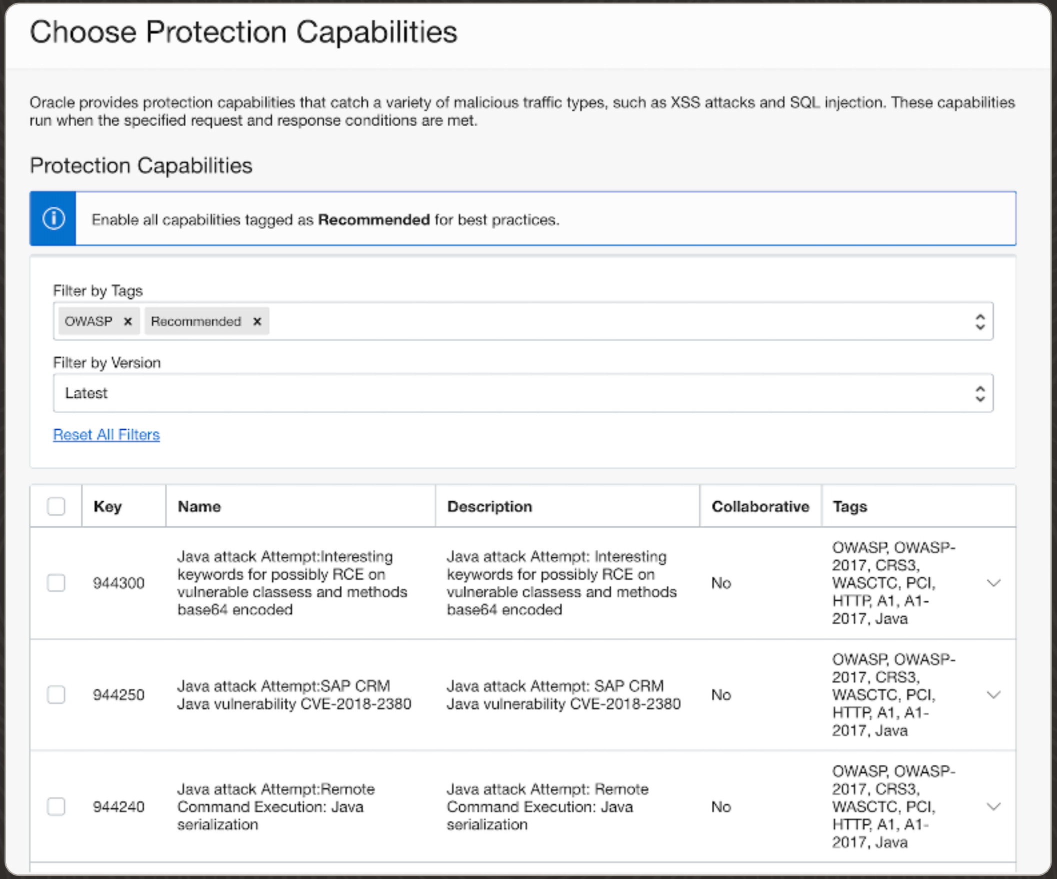
- Control access, based on HTTP header information. Block requests if the HTTP header contains specific names or values or allow traffic with proper HTTP regular expression
- Control access based on URL address matching or partial matching or match proper URL regular expressions
- Regional access control can be used to restrict users from certain geographies


Logging Analytics
Dashboards » WAF Logs Analytics
WAF Logs Analytics
Last 8 Hours
Today 06:32 AM - 02:32 PM UTC-07:00
Edit
WAF Access Request Number
5,339
Requests
WAF Access By Security Module
5.41%
0.21%
94.38%
193.122.201.253:80
requestaccesscontrol/geoblock_non-us
requestprotection/protection_policy_demo
122 log records have no value for Response Provider
WAF Access Returned Response Codes
404
403
400
200
405
401
WAF Access By Client IPs TOP 10
107.189.6.44
121.5.219.20
176.131.250.200
186.33.87.145
192.35.168.80
209.17.96.138
23.251.102.74
64.38.99.180
92.118.161.9
0
1K
2K
3K
4K
5K
6K
Show Log Scale
WAF Access By Country TOP 10
0
1K
2K
3K
4K
5K
6K
Show Log Scale

Protection rules

Use these rules to protect your critical web applications against malicious cyber-attacks from bad actors. Incoming requests are inspected to determine if it contains an attack payload as compared to industry-leading threat feeds.

- Supports over 250 rule sets as well as the Open Web Access Security Project (OWASP) rule sets
- WAF will block and/or alert on the requests: SQL injection, cross-site scripting, HTML injection and many more



Choose Protection Capabilities

Oracle provides protection capabilities that catch a variety of malicious traffic types, such as XSS attacks and SQL injection. These capabilities run when the specified request and response conditions are met.

Protection Capabilities

ⓘ Enable all capabilities tagged as **Recommended** for best practices.

Filter by Tags: OWASP × Recommended ×

Filter by Version: Latest

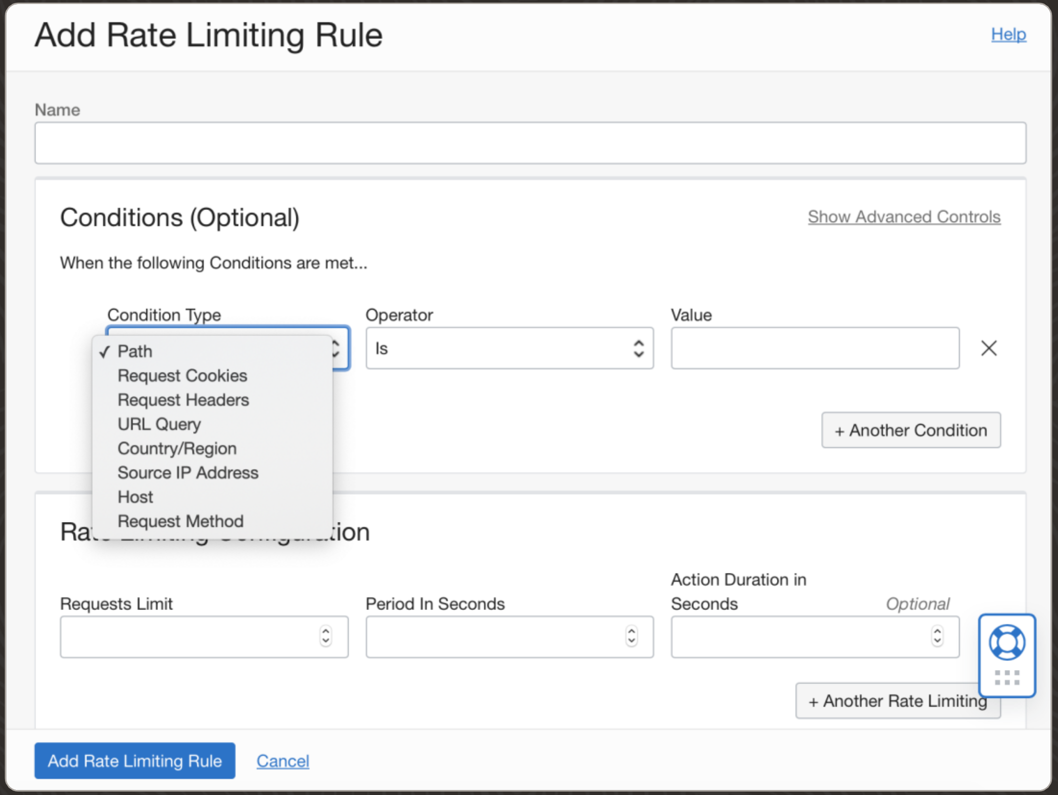
Reset All Filters

□	Key	Name	Description	Collaborative	Tags
□	944300	Java attack Attempt:Interesting keywords for possibly RCE on vulnerable classess and methods base64 encoded	Java attack Attempt: Interesting keywords for possibly RCE on vulnerable classess and methods base64 encoded	No	OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A1, A1-2017, Java
□	944250	Java attack Attempt:SAP CRM Java vulnerability CVE-2018-2380	Java attack Attempt: SAP CRM Java vulnerability CVE-2018-2380	No	OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A1, A1-2017, Java
□	944240	Java attack Attempt:Remote Command Execution: Java serialization	Java attack Attempt: Remote Command Execution: Java serialization	No	OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A1, A1-2017, Java

Rate limit rules

Rate limiting rules based on URL request parameters and client IP to protect against layer 7 DDOS attacks.

- Allows inspection of HTTP request properties and limits the frequency of requests for each unique client IP address



Add Rate Limiting Rule

Name

Conditions (Optional)

When the following Conditions are met...

Condition Type: ✓ Path

Operator: Is

Value

Rate Limiting Configuration

Requests Limit

Period In Seconds

Action Duration in Seconds *Optional*

Bot management

Entity attributes and behavioral detection

Human interaction

Oracle WAF identifies normal usage patterns based on legitimate user behavior to the site.
The WAF will challenge with CAPTCHA
or block requests when it detects abnormalities or traffic exceeds defined interaction thresholds.

Device fingerprinting

Oracle WAF collects unique various characteristics about a device entity, generating a hashed signature. This hashed signature is then compared to other requests to determine the same signature is being leverages across different contexts.

Shared responsibility model for OCI WAF

Responsibility	Oracle	Customer
Onboard/configure the WAF policy for the web application	No	Yes
Configure WAF onboarding dependencies (DNS, ingress rules, network)	No	Yes
Provide high availability (HA) for the WAF	Yes	No
Monitor for distributed denial of service (DDoS) attacks	Yes	No
Keep WAF infrastructure patched and up-to-date	Yes	No
Monitor data-plane logs for abnormal, undesired behavior	Yes	Yes
Construct new rules based on new vulnerabilities and mitigations	Yes	No
Review and accept new recommended rules	No	Yes
Tune the WAF's access rules and bot management strategies for your traffic	No	Yes

What's New in OCI WAF

- Include `${http.request.id}` in custom responses for faster troubleshooting and correlation (Release Notes).
- Additional in-region protection rule sets and threat-intel feeds; easier tuning.
- HTTP Request Body Inspection—buffers and scans request bodies.

*All features supported on both Edge and Flexible Load Balancers.

Simplified Pricing – 2025

- First WAF instance + first 10 million requests/month are FREE for OCI commercial customers.
- After free tier: charged per WAF instance/month and per 1 million incoming requests.
- Pricing identical for Edge and In-region WAF; pay-as-you-go or commit models.

Thank you

ORACLE