Advanced Networking on Cloud
Web Application Firewall (WAF)

René Serral <rene.serral@upc.edu>

Agenda

- Introduction
- Proxies
- WAF
- AWS WAF
- Lab

Agenda

- **Introduction**
- Proxies
- WAF
- AWS WAF
- Lab

Introduction

- Security is always a problem
- We have plenty of security solutions
  - Firewalls
  - EDR/XDR
  - Antivirus
  - ...

What is a Firewall?

- Traffic filtering at Network Layer
  - Very efficient
  - Easy to configure
- Simple traffic filtering rules
  - Accept/Deny logic
- BUT!
  - No proper knowledge about Applications

Agenda

- Introduction
- **Proxies**
- WAF
- AWS WAF
- Lab

What is a Proxy?

- It’s an application layer tool to intercept application flows
- A proxy terminates a TCP flow
  - It interprets the payload
  - Forwards the query to the best responsible party

Things we can do with a proxy

- Balance load
- Analyze the payload
  - Make decisions depending on the values
- Modify the payload
  - Live patching
- Allow/Deny connections

Advantages of a proxy

- Can work in parallel
- Provides a natural load balancer
- Has knowledge about the application
  - Can make opinionated decisions
  - Provides intelligence to the whole pipeline
- It can convert between protocols
  - HTTP --> HTTPS

Disadvantages of a proxy

- Can add latency
- It can become slow depending on the workload
- Requires deep comprehension of the app it is proxying

Agenda

- Introduction
- Proxies
- **WAF**
- AWS WAF
- Lab

What is a WAF?

- A proxy devoted to filter Web queries
- It is used as an intelligent firewall
- Queries are analyzed and let go or not depending on a list of rules

What can we do with WAF

- Patch applications without redeploying
  - We can modify offending queries to avoid crashes or misconducts
  - Customize answers
  - This can be done live: no down times
- Avoid a plethora of typical attacks
  - SQL Injection
  - XSS
  - ...

Agenda

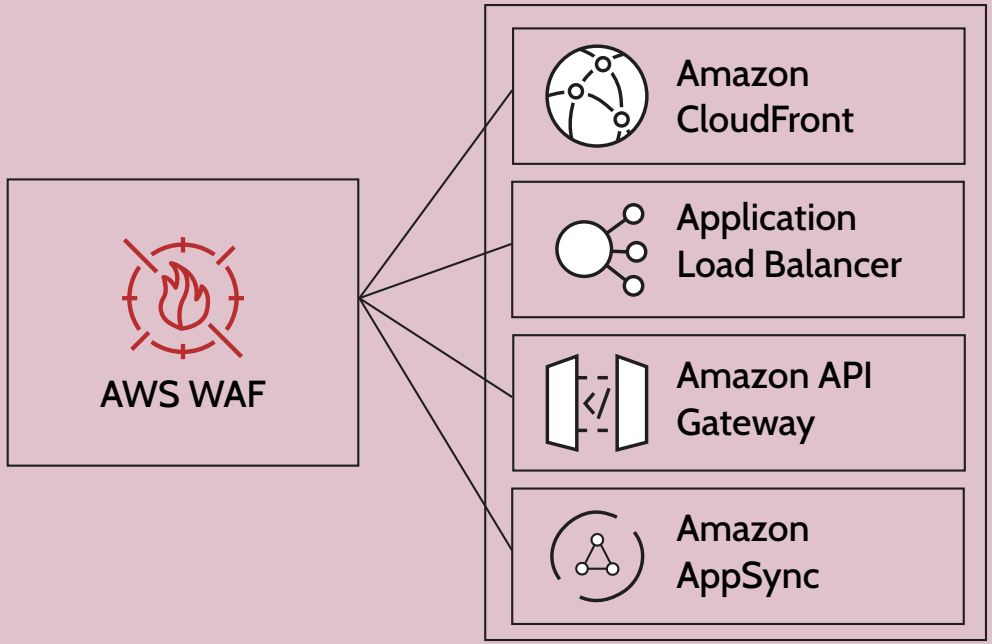
- Introduction
- Proxies
- WAF
- **AWS WAF**
- Lab

AWS WAF

- AWS integrates WAF seamlessly
- Autoscales with the infrastructure
- Can work together with the AWS Firewall Manager

AWS WAF Perks[1]

- Create policies
  - Visual and JSON
- Block and Filter
  - Versatile criteria
- Monitor
  - Integrated with CloudWatch



[1] https://aws.amazon.com/waf/

Rule generation

- Huge predefined set of rules
  - Ready to use in blocks
- SQLi
- XSS
- Linux attacks
- ...

Possible Rule Actions

- **Allow:** permits the traffic matching the rule
- **Block:** denies the request
- **Count:** counter for statistics
- **CAPTCHA & Challenge:** to avoid abuse

Monitor

- Integration with CloudWatch
- Statistics about traffic
  - Blocked connections
  - Intercepted queries
  - General counters
-

Cost

- Has two dimensions:
  - WCUs
    - Cost per weight
- Computational and BW costs
- More info at:
  - https://aws.amazon.com/waf/pricing/

Agenda

- Introduction
- Proxies
- WAF
- AWS WAF
- **Lab**

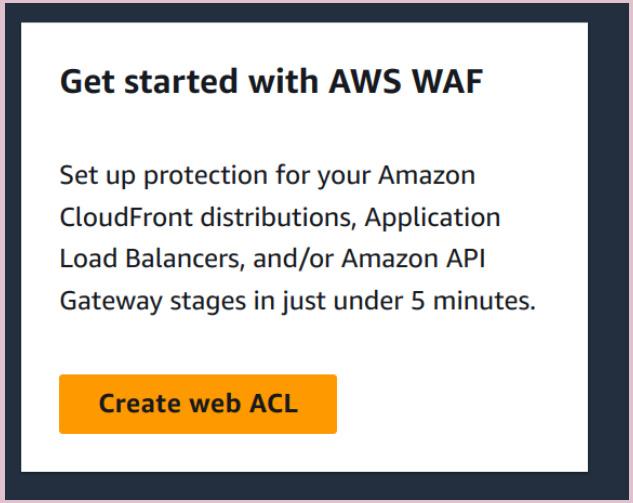
Lab 3

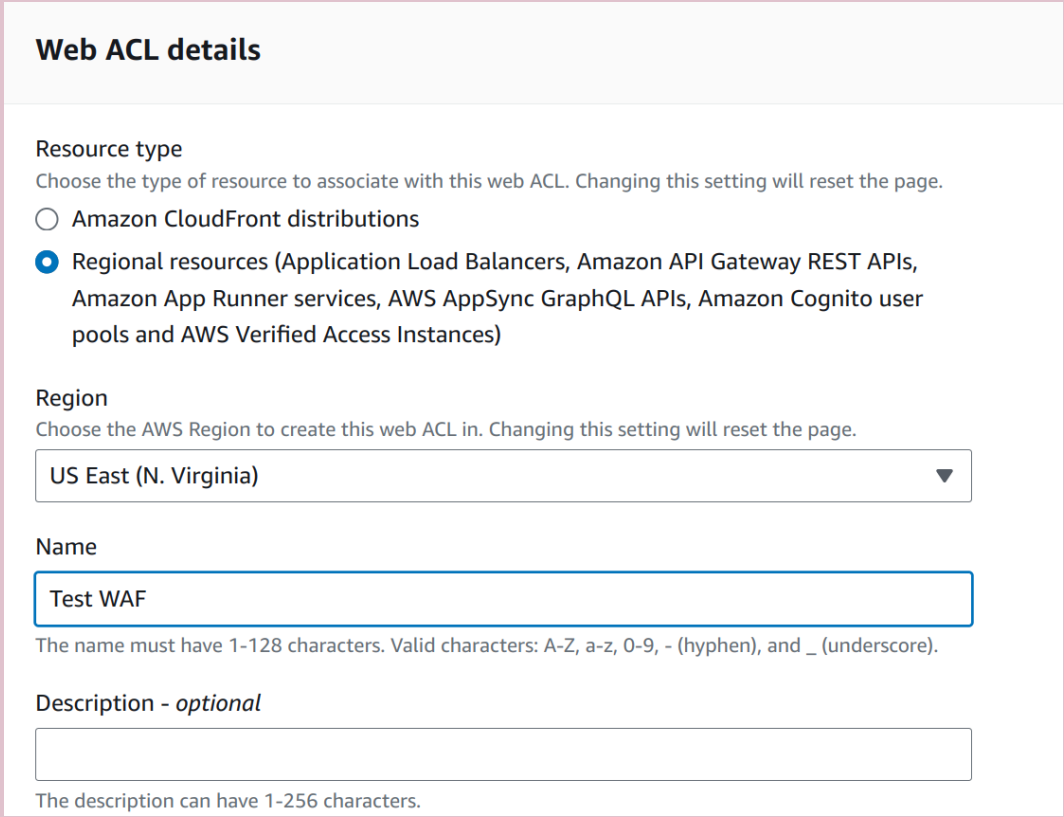
- Create a EC2 Instance and run:

```
docker run --restart=always -d -p 80:3000 --name juice-shop -e "NODE_ENV=ctf" bkimminich/juice-shop
```

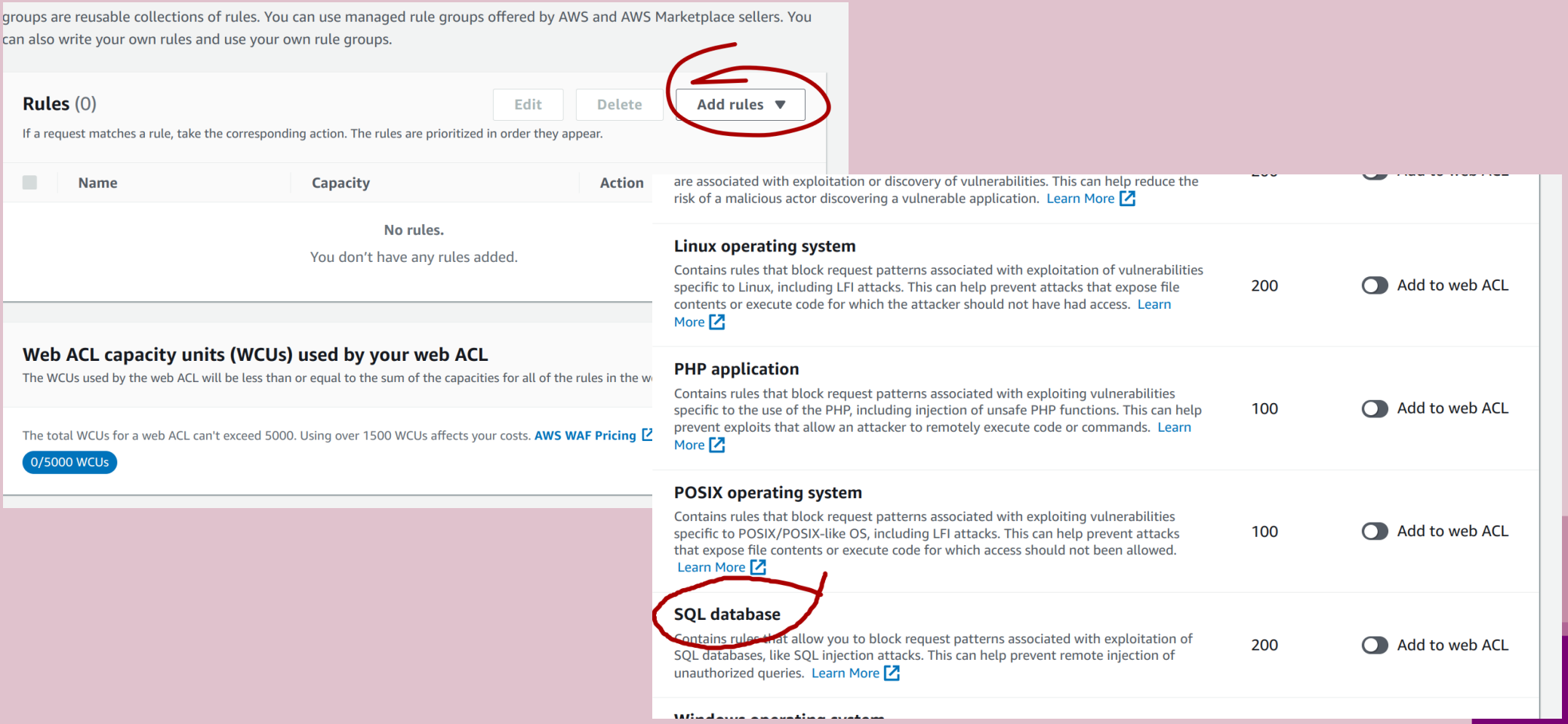
- Create a ALB
  - Associate the Instance to the ALB
- Create a WAF
  - Associate to the ALB

Steps to create a WAF

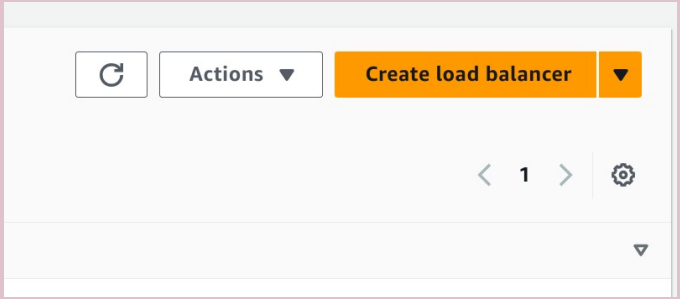




Steps to create a WAF



Steps to create a WAF



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instanc
on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to de
applicable, it selects a target from the target group for the rule action.

▶ **How Application Load Balancers work**

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

JShopBalancer

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info

Scheme can't be changed after the load balancer is created.

- (•) Internet-facing
  An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more
- ( ) Internal
  An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type Info

Select the type of IP addresses that your subnets use.

- (•) IPv4
  Recommended for internal load balancers.
- ( ) Dualstack
  Includes IPv4 and IPv6 addresses.

Steps to create a WAF