

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

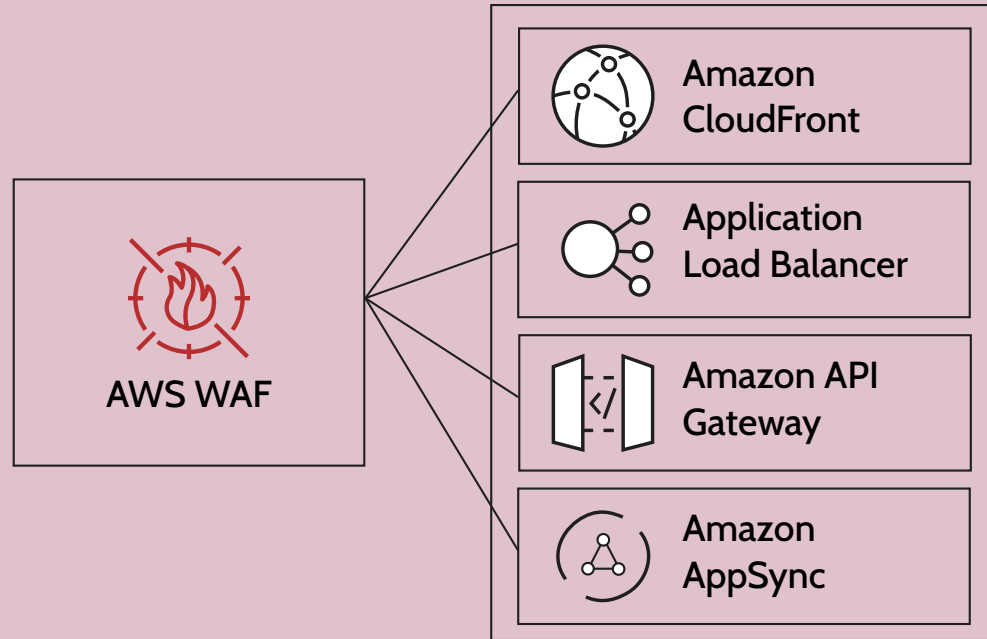
- ▷ Introduction
- ▷ Proxies
- ▷ WAF
- ▷ **AWS WAF**
- ▷ Lab

AWS WAF

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

AWS WAF Perks¹

- ▷ 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

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

Create web ACL

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

- ☐ Amazon CloudFront distributions
- ☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region

Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

US East (N. Virginia) ▼

Name

Test WAF

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

The description can have 1-256 characters.

Steps to create a WAF

groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0)

[Edit](#)[Delete](#)[Add rules ▼](#)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
--	------	----------	--------

No rules.

You don't have any rules added.

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#)

0/5000 WCUs

are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. [Learn More](#)

Linux operating system

Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. [Learn More](#)

200

☐ Add to web ACL

PHP application

Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. [Learn More](#)

100

☐ Add to web ACL

POSIX operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not be allowed. [Learn More](#)

100

☐ Add to web ACL

SQL database

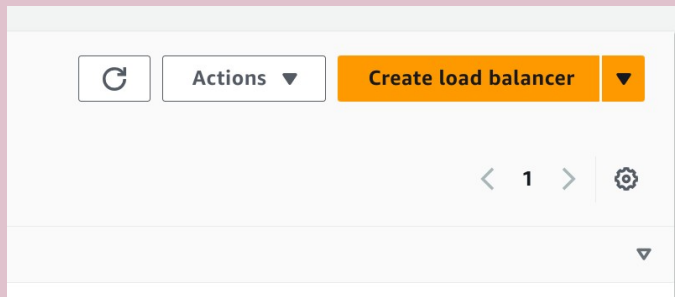
Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. [Learn More](#)

200

☐ Add to web ACL

Windows operating system

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 instances on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which target is 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.

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

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection when the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-
vpc-0b4ab230bf82a375d
IPv4: 172.31.0.0/16

Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not associated with the VPC or the VPC are not available for selection.

☒ us-east-1a (use1-az1)

Subnet

subnet-0cbd8a87cc65e5fe0

IPv4 address

Assigned by AWS

☒ us-east-1b (use1-az2)

Subnet

subnet-04cd435e8423955af

IPv4 address

Assigned by AWS

☐ us-east-1c (use1-az4)

☐ us-east-1d (use1-az6)