7 Layers of the OSI Model

Layer	Description	Protocols / Examples
7. Application	End User layer	HTTP, FTP, IRC, SSH, DNS
6. Presentation	Syntax layer	SSL, SSH, IMAP, FTP, MPEG, JPEG
5. Session	Synch & send to port	API's, Sockets, WinSock
4. Transport	End-to-end connections	TCP, UDP
3. Network	Packets	IP, ICMP, IPSec, IGMP
2. Data Link	Frames	Ethernet, PPP, Switch, Bridge
1. Physical	Physical structure	Coax, Fiber, Wireless, Hubs, Repeaters

bmc

CROSS SİTE REQUEST FORGERY (CSRF)

Siteler Arası İstek Sahtekarlığı (Session Riding)

1. Victim logs into bank account.
2. Bank assigns victim a validation token.
3. Hacker sends forged request disguised as legitimate communication from the bank.
4. Victim unknowingly forwards request to bank.
5. Forged request is executed by the bank using previously assigned validation token.

VICTIM

BANK WEBSITE

HACKER

Cross Site Scripting (XSS)

① Attacker sends script-injected link to victim (e.g. email scam)

Attacker

② Victim clicks on link and requests legitimate website

Victim

④ Malicious script sends victim's private data to attacker

Website

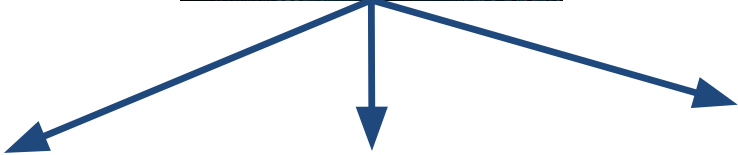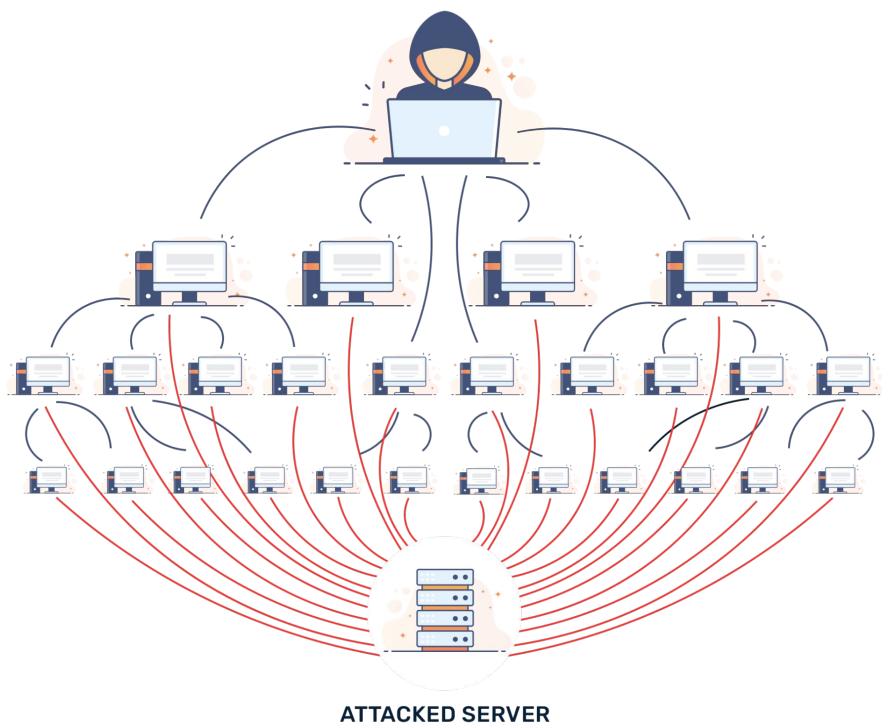③ Victim's browser loads legitimate site, but also executes malicious script

SSL

SQL INJECTION


```
"SELECT *
FROM users
WHERE login=$name
AND password = $pwd"
```

SELECT * FROM USERS WHERE username = 'osvaldo' and password = 'PI1234'

SELECT * FROM USERS WHERE username = 'administrator' –' and password = ''
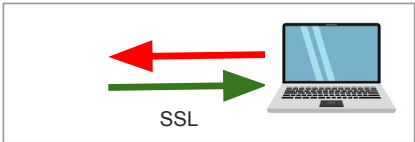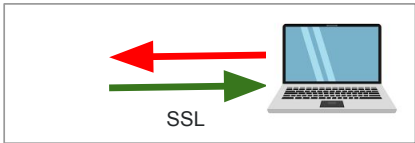
UNION SELECT username, password–

DDOS Attack

ATTACKED SERVER

Server Side Encryption (At Rest)

Encryption in Transition

Client Side Encryption
(Transition+At Rest)

SSL

SSL

aws

Customer managed keys → AWS CloudHSM

External

Custom key store (CloudHSM)

AWS CloudHSM

AWS managed keys → AWS KMS
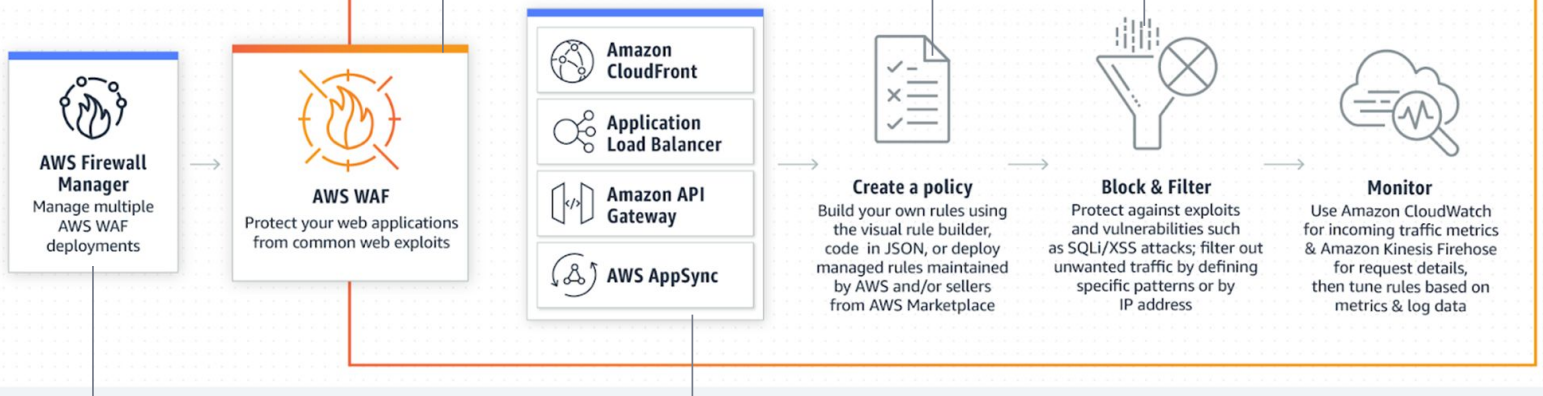

WAF → ALB → EC2 (WebServer)

Security Group
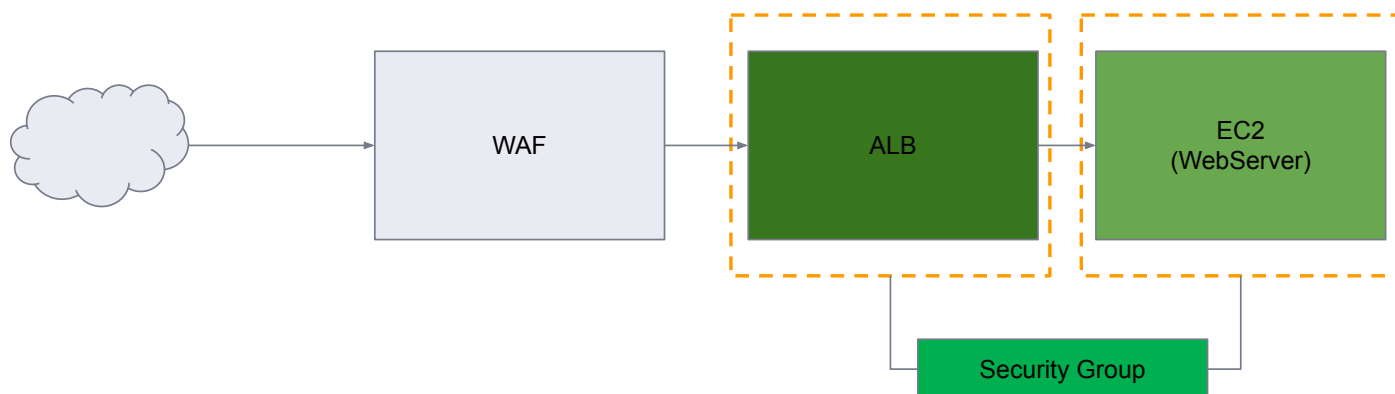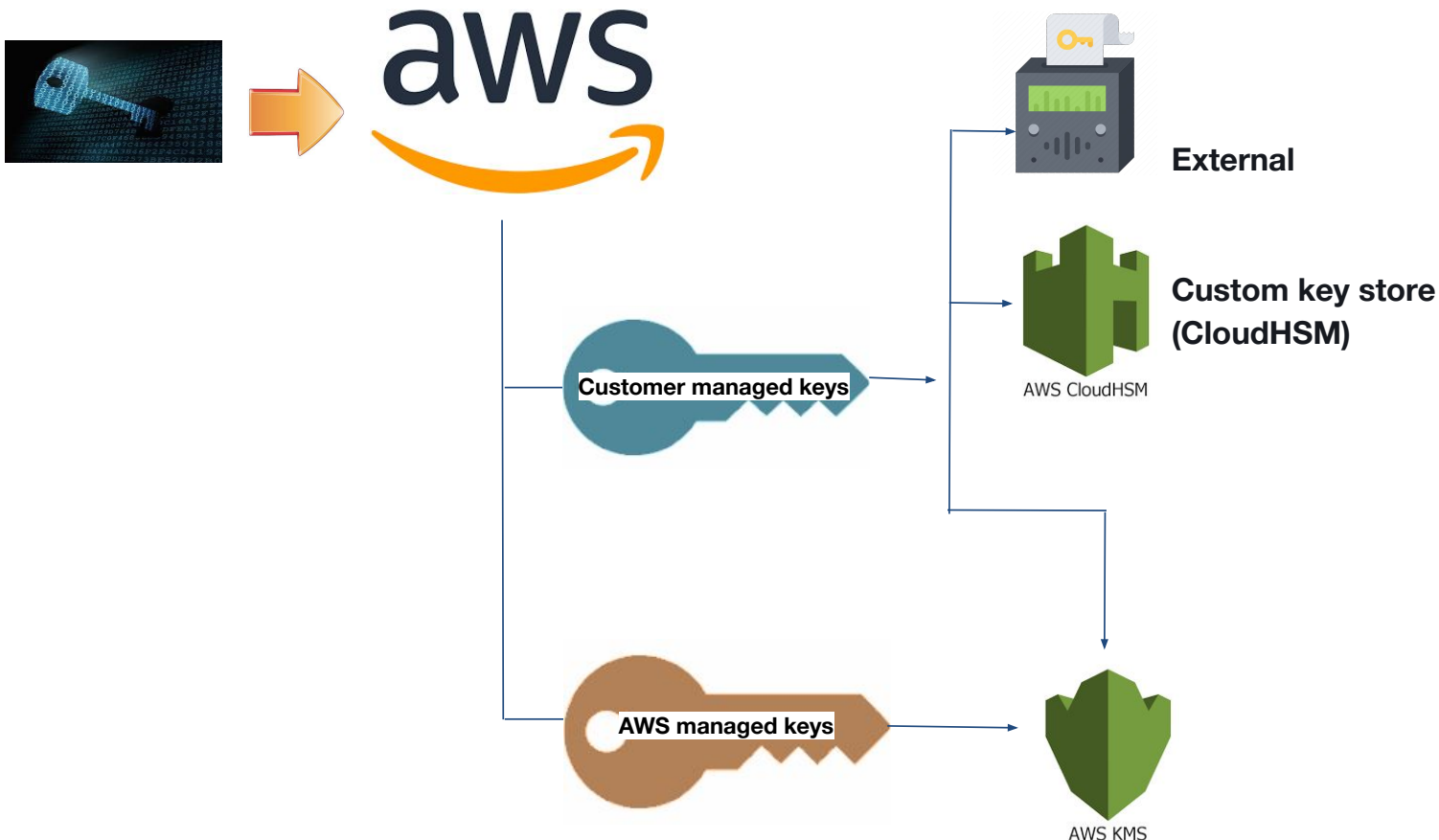
AWS WAF

- Functionality is same as a standard web application firewall
  - protect against web exploits
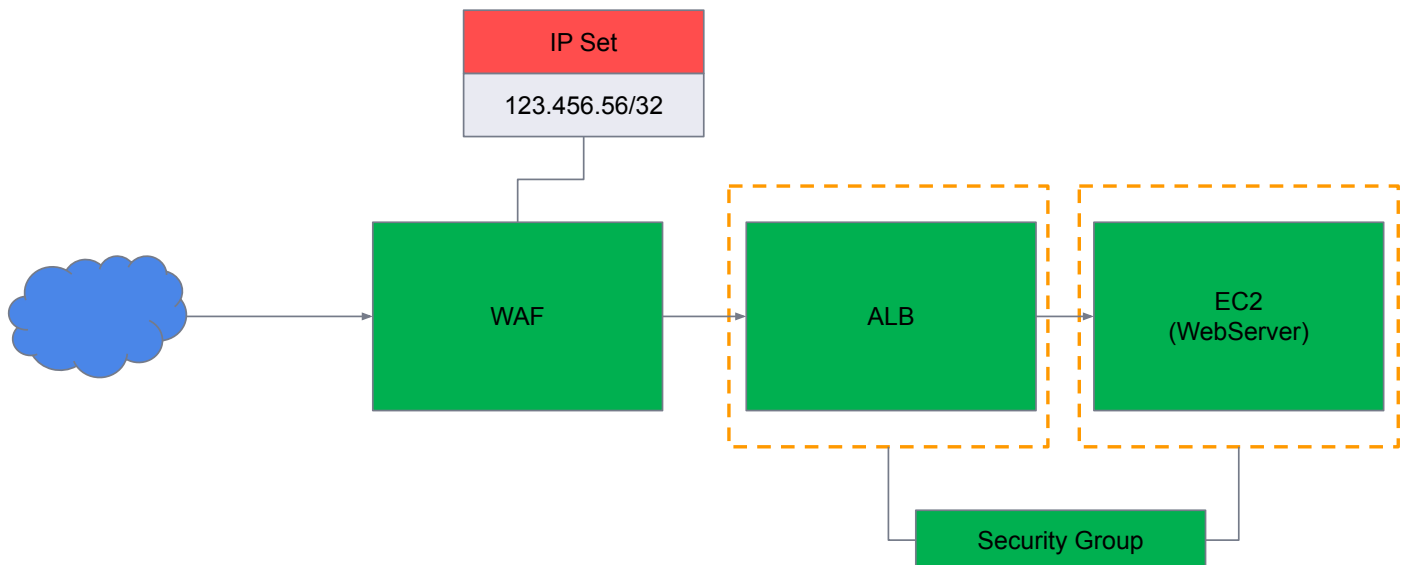 - SQL injection, cross-site scripting, etc…

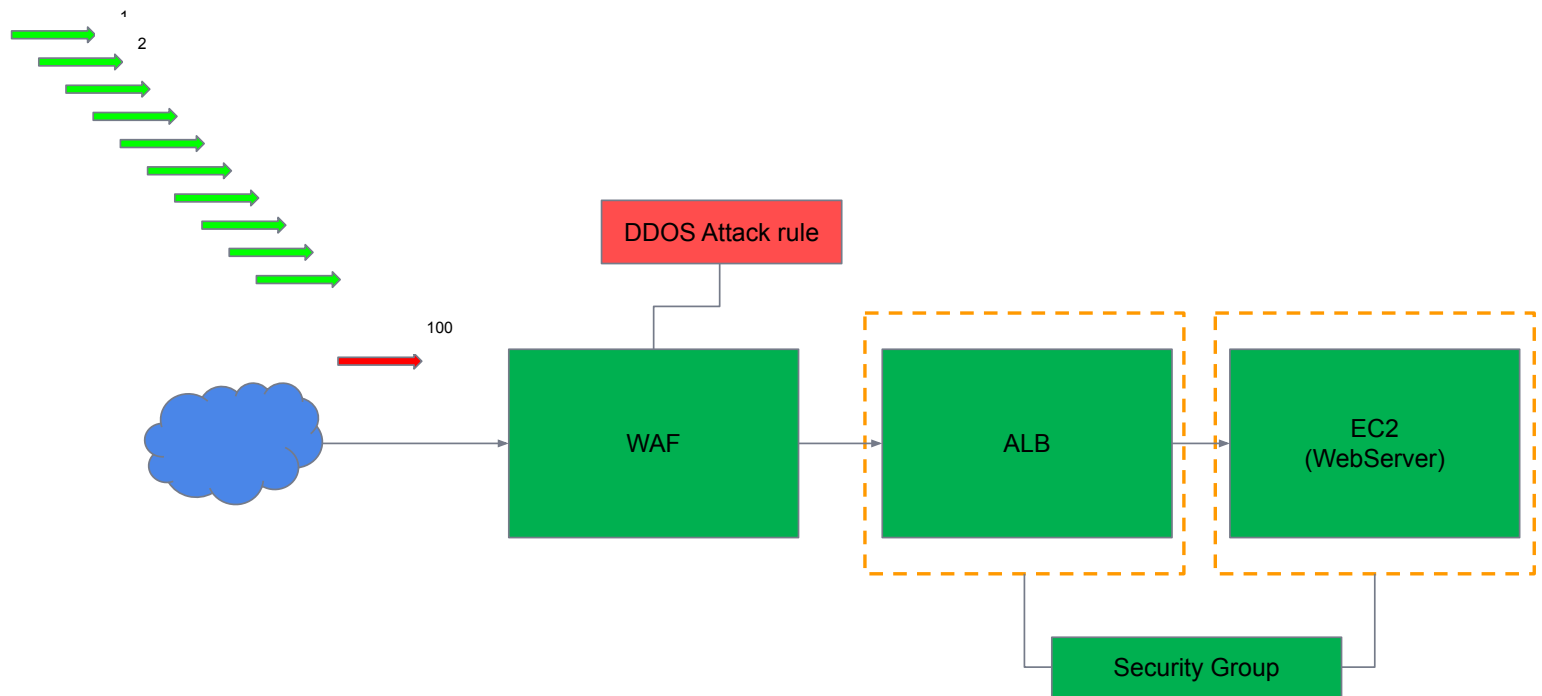- Has available "rule packages"
  - AWS Managed
  - 3rd Party Vendors

- Can run in detective or preventative mode

AWS Firewall Manager
Manage multiple AWS WAF deployments

AWS WAF
Protect your web applications from common web exploits

Amazon CloudFront

Application Load Balancer

Amazon API Gateway

AWS AppSync

Create a policy
Build your own rules using the visual rule builder, code in JSON, or deploy managed rules maintained by AWS and/or sellers from AWS Marketplace

Block & Filter
Protect against exploits and vulnerabilities such as SQLi/XSS attacks; filter out unwanted traffic by defining specific patterns or by IP address

Monitor
Use Amazon CloudWatch for incoming traffic metrics & Amazon Kinesis Firehose for request details, then tune rules based on metrics & log data

- Can manage rules centrally and apply to all endpoints in an organization

- Works with AWS endpoints

CLARUSWAY
WAY TO REINVENT YOURSELF

9

IP Set

123.456.56/32

WAF

ALB

EC2
(WebServer)

Security Group

CLARUSWAY
WAY TO REINVENT YOURSELF

10

1
2
100

DDOS Attack rule

WAF

ALB

EC2
(WebServer)

Security Group

CLARUSWAY
WAY TO REINVENT YOURSELF

DDoS attacks cost business between US$20,000 and US$40,000 per hour
(Source: Cox BLUE)

32% of serious DDoS coincided with a network intrusion
(Source: Cox BLUE)

Q1 2020 reported a 542% increase in DDoS activity compared to Q4 2019
(Source: Nexus Guard)

CLARUSWAY
WAY TO REINVENT YOURSELF