

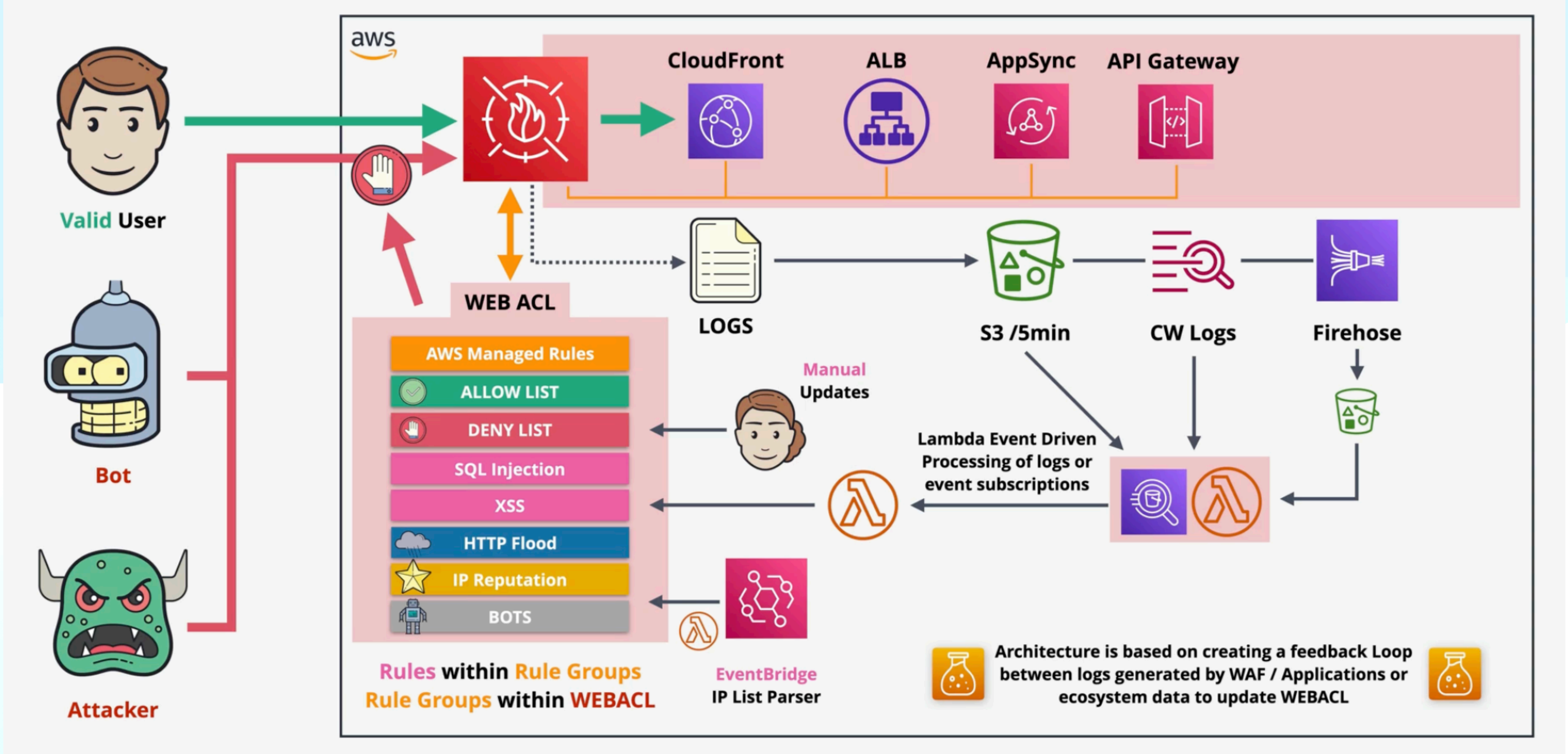
# WAF and Shield

# Today's Agenda

- What is WAF
- WAF Features
- WAF on the Load-balancer
- What is Shield
- Shield Features



# Web Application Firewall





# WEB ACLS

- WEB Access Control lists
- Default action is either to Allow or Block
- Can be associated to Regional Resource and Global resource such as Cloudfront
- Web ACLS can have Rules or Rule Groups which will be processed in order

# Rules

- Rules has Type, Statement, Action
- Type: Regular or Rate-Based
- Statement:
  - WHAT to match, Count ALL, What & Count
- Can mention origin country, IP, Label, header, cookies, query parameter, URI path, query string, body, HTTP method
- Single rule, can have AND, OR, NOT rules
- Action: Allow, Block, Count, Captcha
- Allow and Block Stops the processing of WAF rule, Count and Captcha continues



# AWS Shield

- AWS Shield Standard and Advanced - DDoS Protection
- Standard is free, Advanced has cost associated
- What kind of attacks it can protect
  - Network Volumetric Attacks (L3)
  - Network Protocol Attacks (L4) - TCP SYNC Flood
  - These will leave connection open, prevent new ones to connect
  - Application Layer - Web Request Floods

# AWS Shield - Standard

- Free for AWS Customers
- At regional level or VPC level protection
- Can prevent L3 or L4 layer attacks
- Can use along with Route 53 and CloudFront



# AWS Shield - Advanced

- 3000\$ per month for all accounts in your organisation
- Protects CF, R53, EIPs, ALBs and NLBs
- Cost protection for attacks which are not prevented
- Proactive Engagement and Shield Response Team
- WAF integration
- Layer 7 - DDOS Attacks protection
- Real time visibility of DDOS events and attacks



**QUIZ TIME**

# Q & A