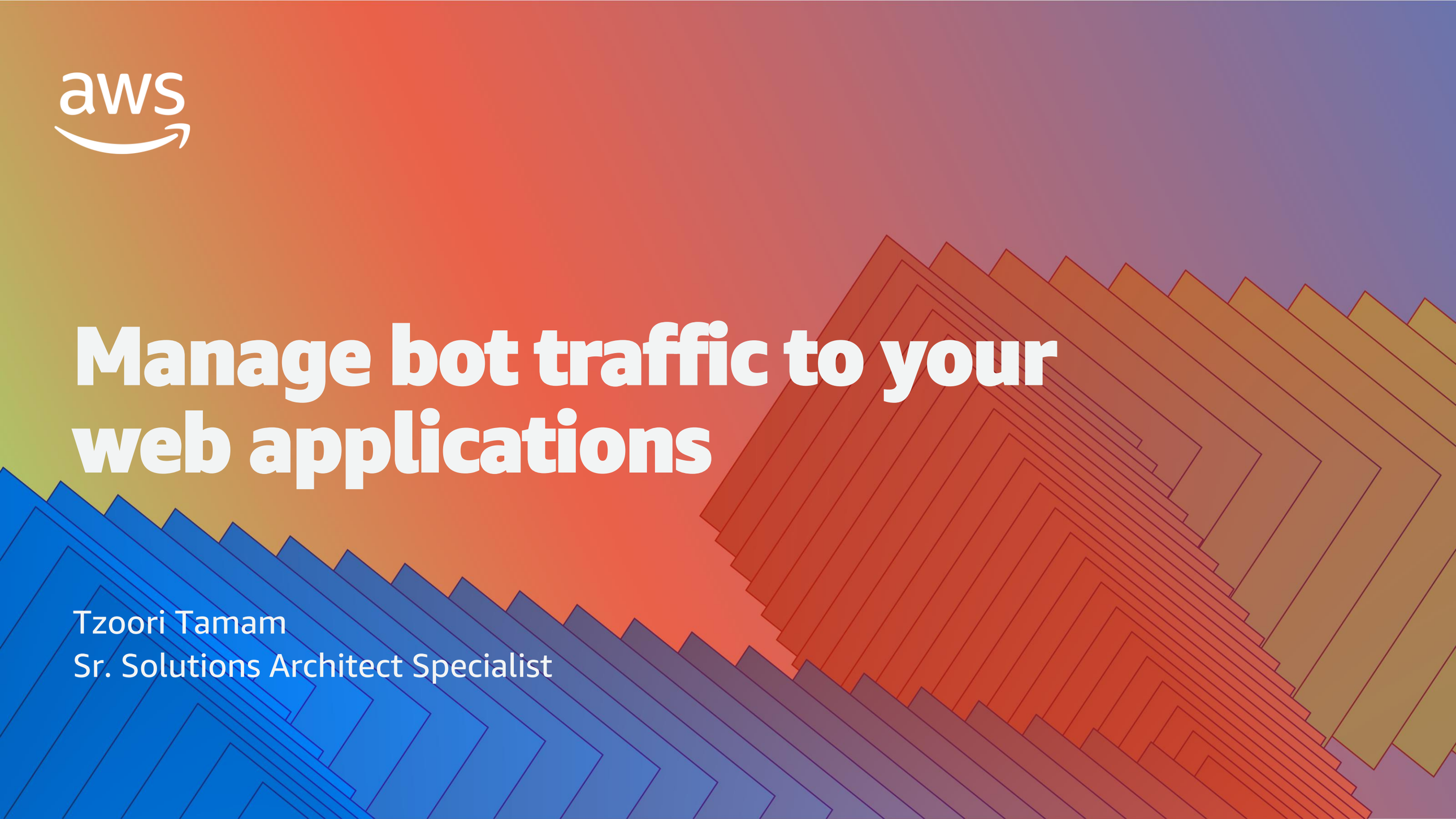


Manage bot traffic to your web applications

Tzoori Tamam
Sr. Solutions Architect Specialist

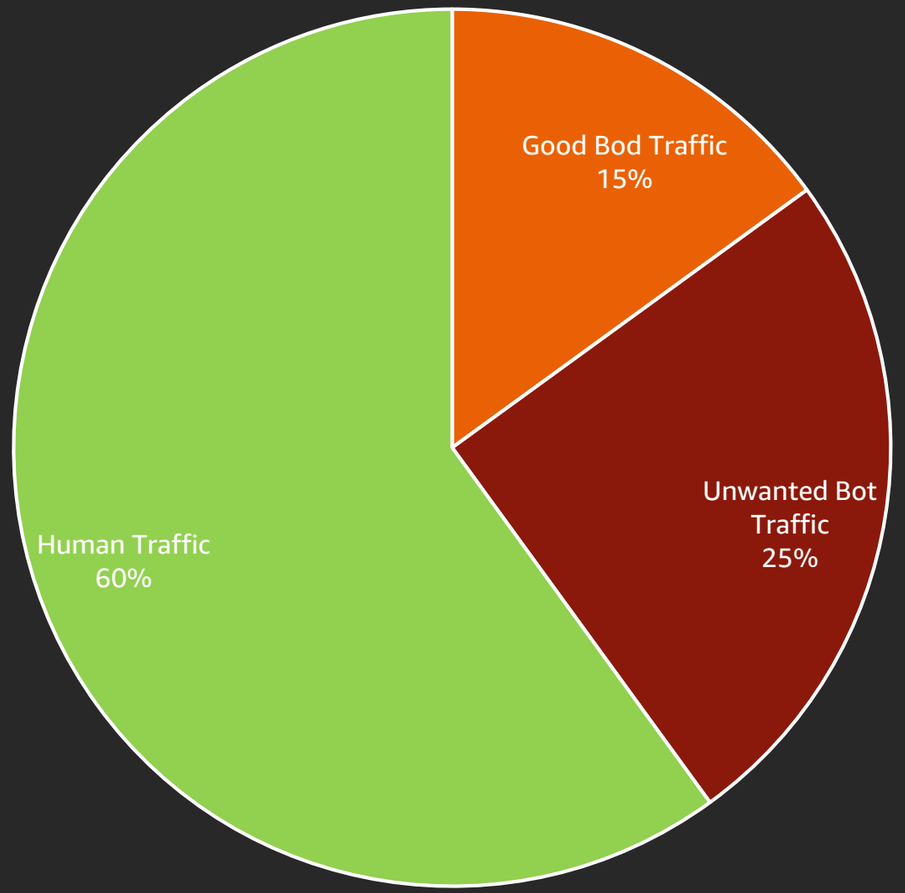
The World of Bots

Bots traffic is estimated at 40% of an average website's overall traffic

Bot traffic introduces

- Infrastructure Load
- Operational Overhead
- Additional Costs

At least 25% of traffic hitting an average website is unwanted/dangerous



Unwanted Bots

Have both security and business concerns associated with them

Security

- Vulnerability scanners
- L3/L4 denial of service
- L7 denial of service

Business

- Account takeover
- Fraudulent transactions
- Denial of inventory

Controlling Bots with AWS

AWS WAF

Frictionless setup: deploy without changing your existing architecture, and no need to configure TLS/SSL or DNS

Low operation overhead: managed rules from AWS and AWS Marketplace, ready to use CloudFormation templates, and built-in SQLi/XSS detection

Customizable security: highly flexible rule engine that can inspect any part of incoming request under single-millisecond latency

Simply pull in third party rules: Within the WAF console, you can pivot to our Marketplace to select Industry Leading Security vendor rules to pull into AWS WAF

AWS Managed Rules

AWS Managed Rules for AWS WAF

- Amazon IP reputation list
- Anonymous IPs
  - Data Centers
  - VPNs, Tor exit nodes

AWS managed rule groups

Paid rule groups

Name	Capacity	Action
Bot Control AWS WAF Bot Control offers you protection against automated bots that can consume excess resources, skew business metrics, cause downtime, or perform malicious activities. Bot Control provides additional visibility through Amazon CloudWatch and generates labels that you can use to control bot traffic to your applications.	50	Add to web ACL Edit

Free rule groups

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	Add to web ACL Edit
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	Add to web ACL Edit
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application.	50	Add to web ACL Edit
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.	700	Add to web ACL Edit
Known bad inputs Contains rules that allow you to block request patterns that are known to	200	Add to web ACL

WAF > Web ACL

WAF Automation Solution

https://amzn.to/3kU4WHR

AWS WAF

Lambda

Amazon Kinesis

Amazon S3

API Gateway

Amazon CloudWatch

- Allowlist
- Blocklist
- SQL Injection
- XSS
- HTTP Flood
- Scanners & Probes
- IP Reputation Lists
- Bad Bots

AWS Marketplace Managed Rules for AWS WAF

TREND MICRO™

GEOGUARD

FORTINET®

imperva

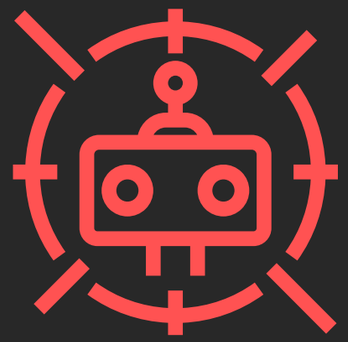
CSC
CYBER SECURITY CLOUD

Trustwave®

Bot Mitigation Integration Vendors

Bot Control for AWS WAF

- ABC is a managed rule group
- ABC rules are based on category and signals
- Protects traffic from Verified bots
- Generates labels for customization and visibility
- Free visibility report for all WAF customers

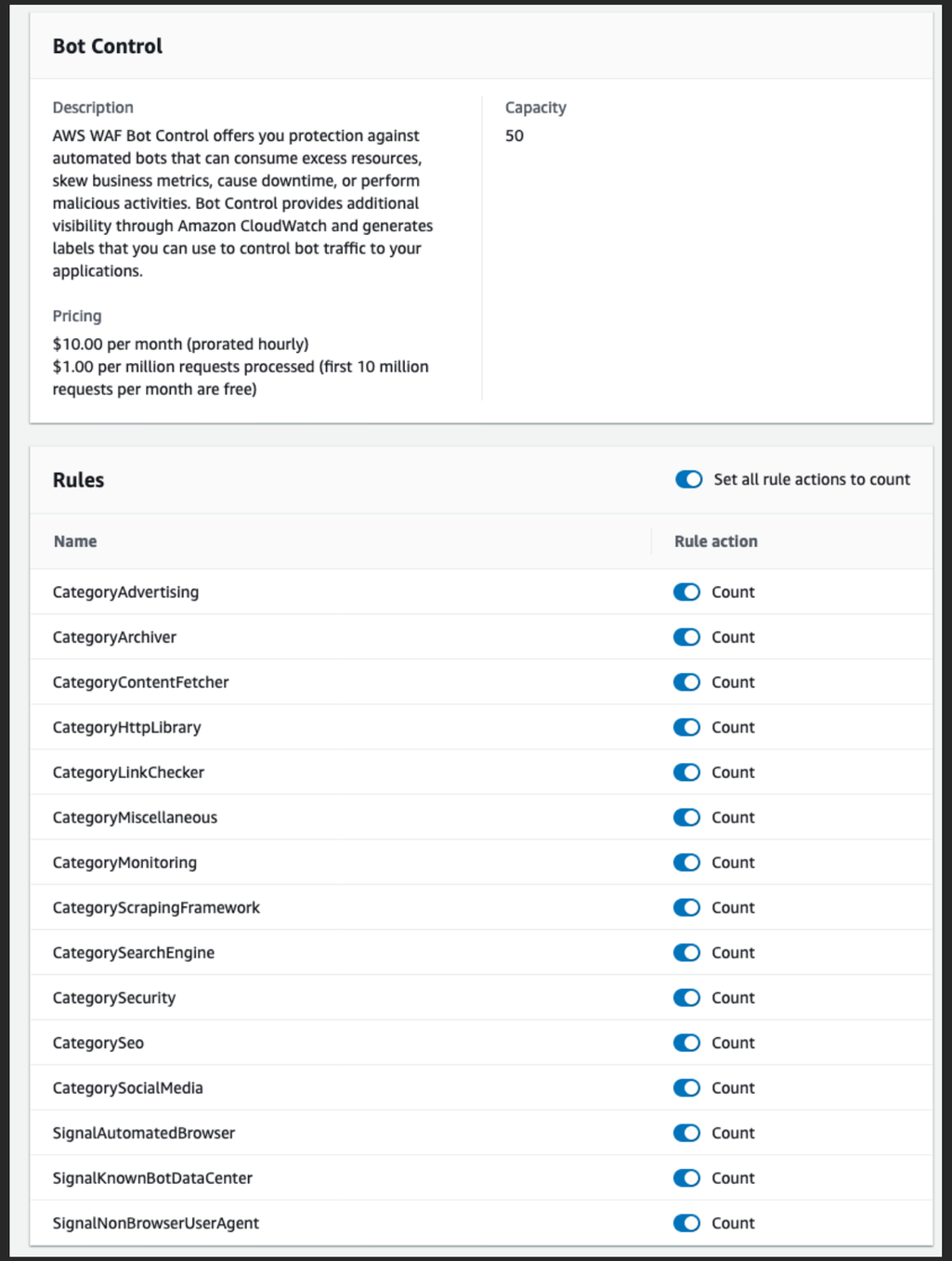


Flexible and Configurable

- Edit managed rule to configure filters that meet your needs
- Adjust coverage with scope down statements
- Utilize labels to customize which what to block or rate limit

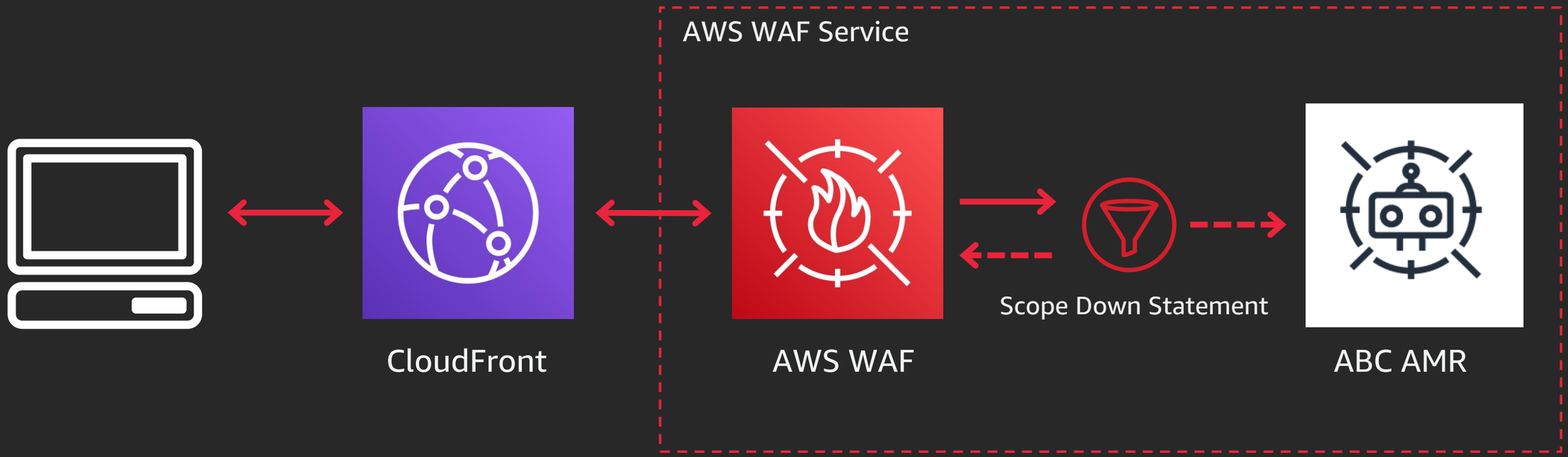
Edit Managed Rule

- Customize the action taken for different rule categories
- Combine results with other WAF logic to customize rules

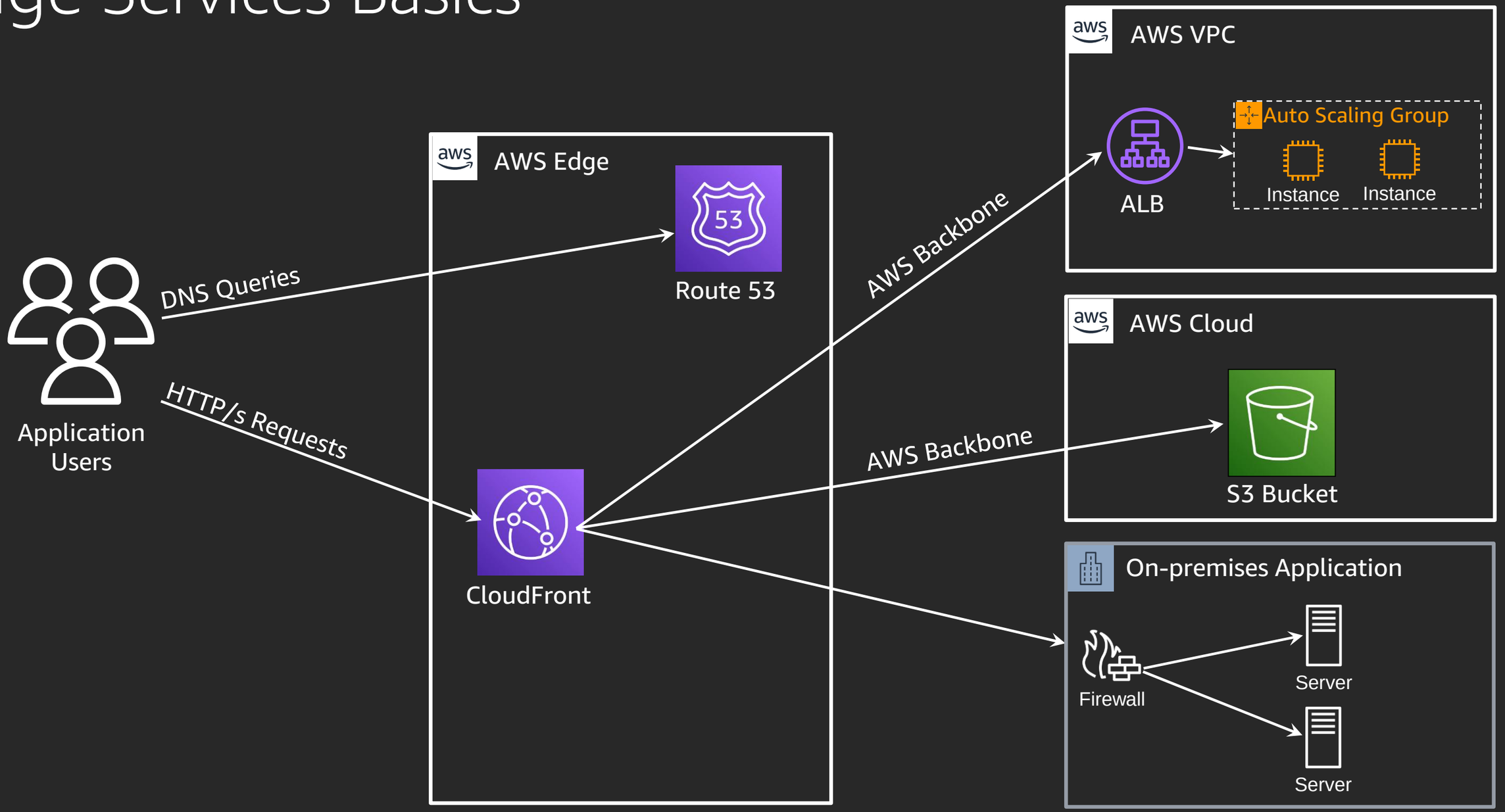


Scope Down Statements – Example AWS WAF Bot Control

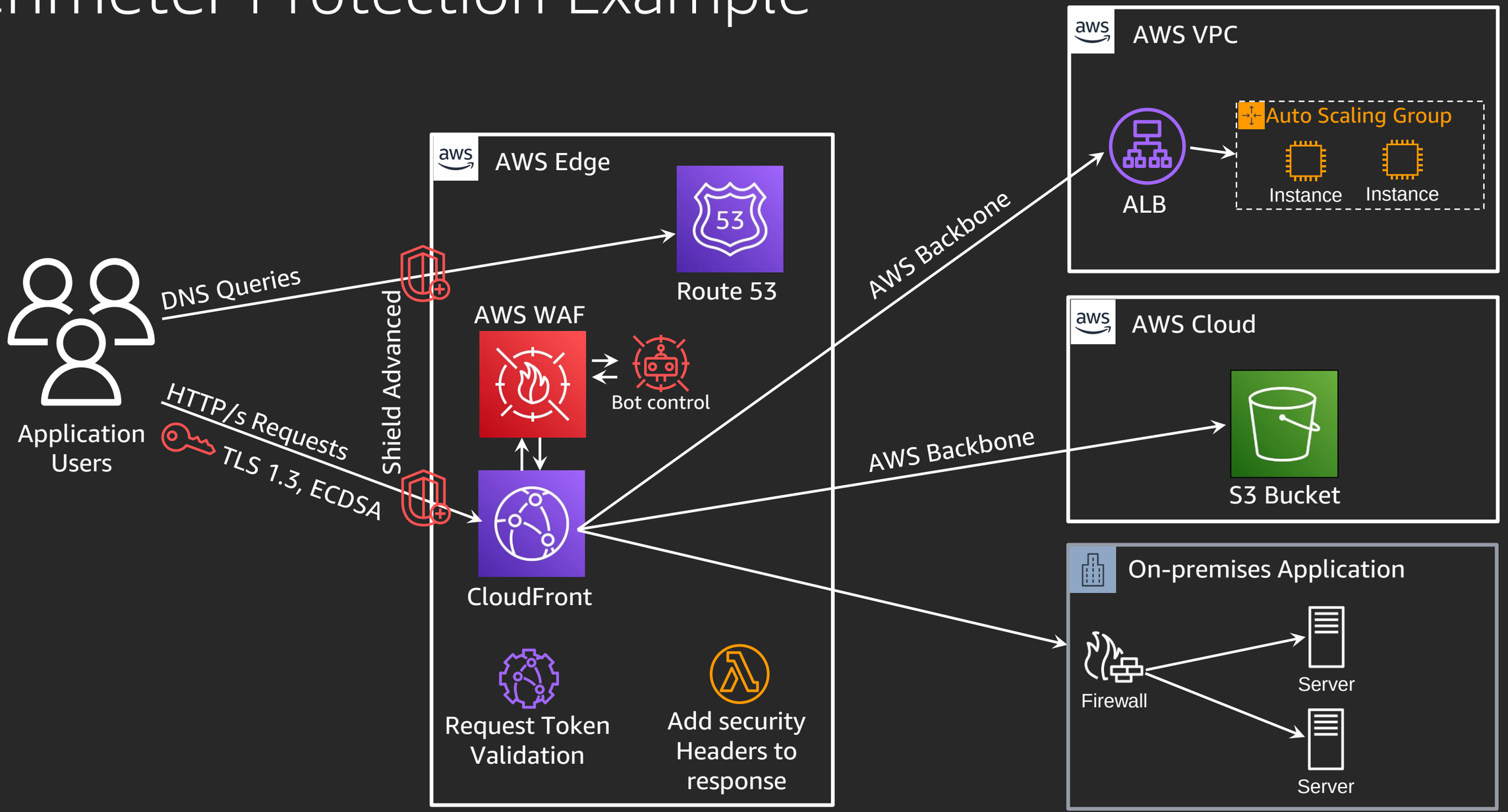
- Use WAF rules to determine which requests are evaluated by ABC
- Bypass ABC for traffic not effected by bots (eg, images)
- Managed ABC usage based costs



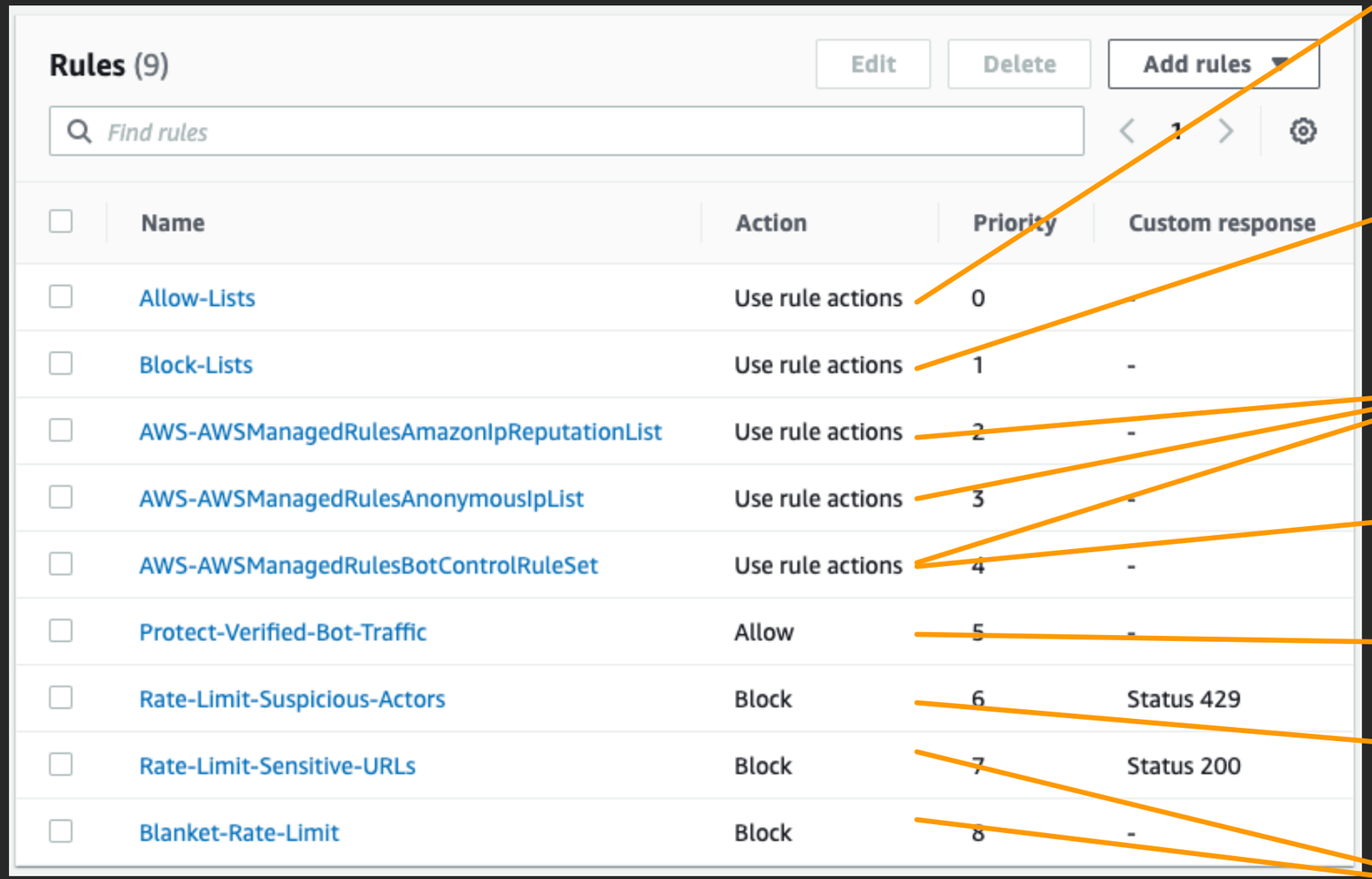
Edge Services Basics



Perimeter Protection Example



AWS WAF WebACL Example



Reusable rule group. Contains IP CIDR blocks – corporate IPs, partner IPs, etc. Set to “Allow”

Reusable rule group. Contains IP CIDR blocks and countries - can be automatically populated through automations. Uses XFF as well. Set to “Block”

Set to “Count” (if you wish)

Use ”Scope Down” to control costs and reduce logging noise

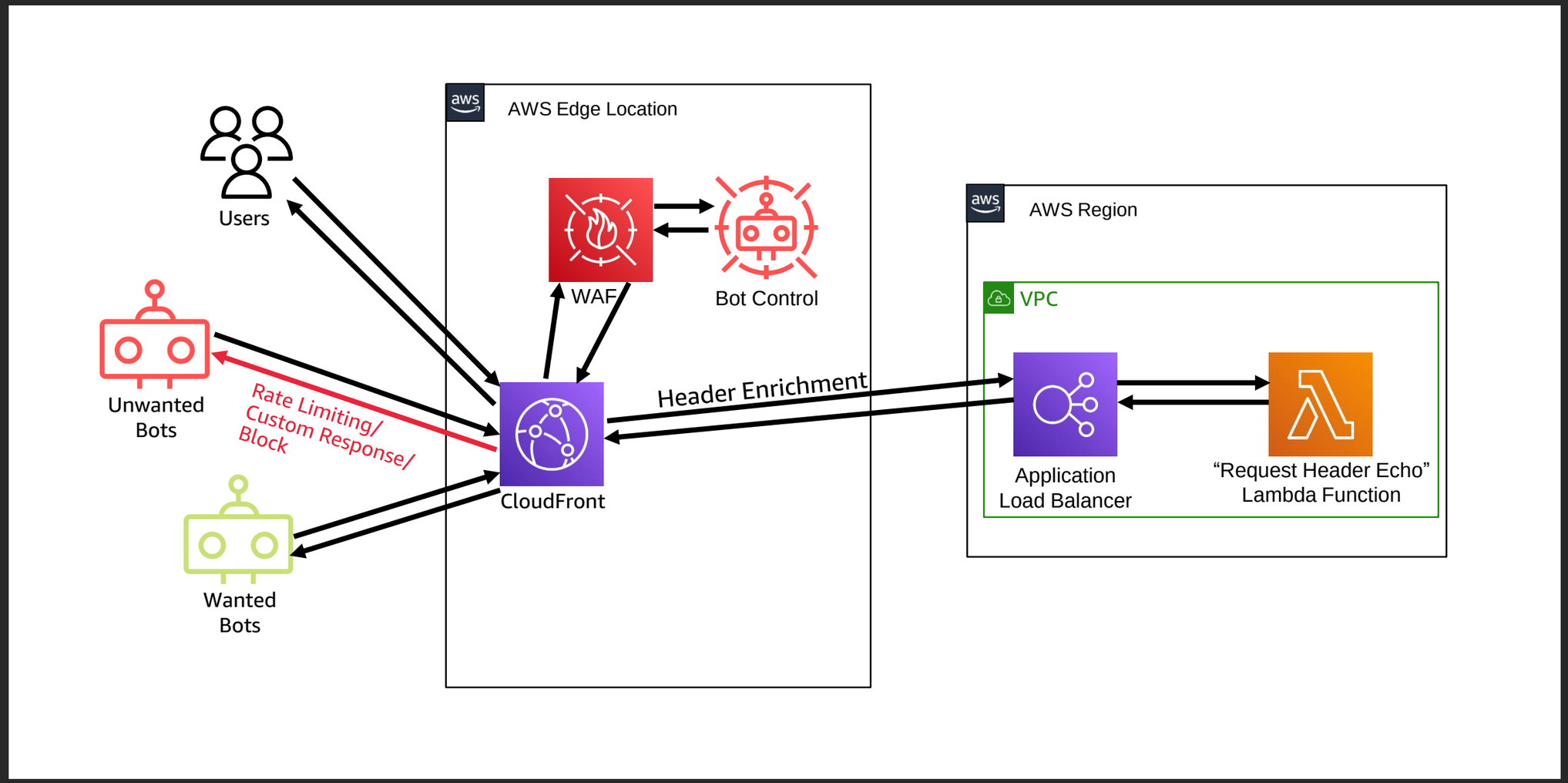
Matches label: “bot:verified”

Aggressive limit

Limit set based on application capabilities

Demo

Demo Setup



In Summary

Bots take a heavy toll on your applications

Understanding bot traffic pattern is easy through AWS WAF and Bot Control

Create custom mitigations and control policies through WAF, Bot Control, and the AWS platform

Thank you!

Tzoori Tamam

tzoorit@amazon.com