AWS WAF

Victoria Almazova

@texnokot

AGENDA

- What is WAF
- What is Amazon WAF
- WAF security automation
- WAF Managed rules
- Firewall Manager
- Summary

WEB APPLICATION FIREWALL

WHAT IS WAF?

- Web application firewall
- Monitors HTTP/S requests and protects web applications from malicious activities
- Layer 7 inspection and mitigation tool

WHAT IS AWS WAF

Malicious request blocking

- SQLi
- XSS

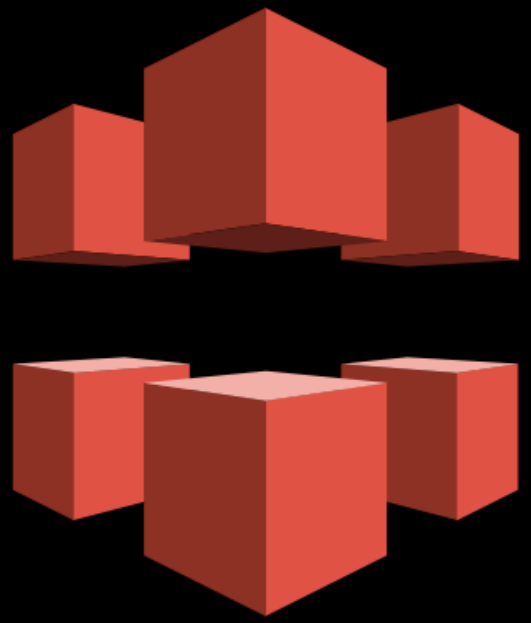
Web traffic filtering with custom rules

- Rate based rules
- IP Match & Geo IP filters
- Regex & String Match
- Size constraints
- Action: Allow/Block

Active monitoring & tuning

- CloudWatch Metrics and Alarms
- Sampled Logs
- Count Action mode

AWS WAF AVAILABLE ON



SET UP AWS WAF

Create a web ACL

- BLOCK requests
- BLOCK requests
- BLOCK requests
- **COUNT** requests

DEFAULT: **ALLOW**

Add a Rule

- Originating from…
- That have….

  AND are….
- That are

  and NOT from…

That have

Add Match conditions

- Blacklisted IPs
- SQLi in query String

  Login Requests
- Admin requests

  Office IPs

SQLi in query String

https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html

PRICING

- $5 per WebACL $1 per Rule per month
  - Reuse across with no additional charge
  - Use more rule for more visibility
- $0.60 per million web requests

AWS WAF LIMITS

Per account and changeable

- Web ACLs: 50
- Rules: 100
- Rate-based rules: 5
- Conditions: 100 per type, 10 regex match (cannot be increased)
- Request per second: 10000 per web ACL (Load Balancer)

Not changeable

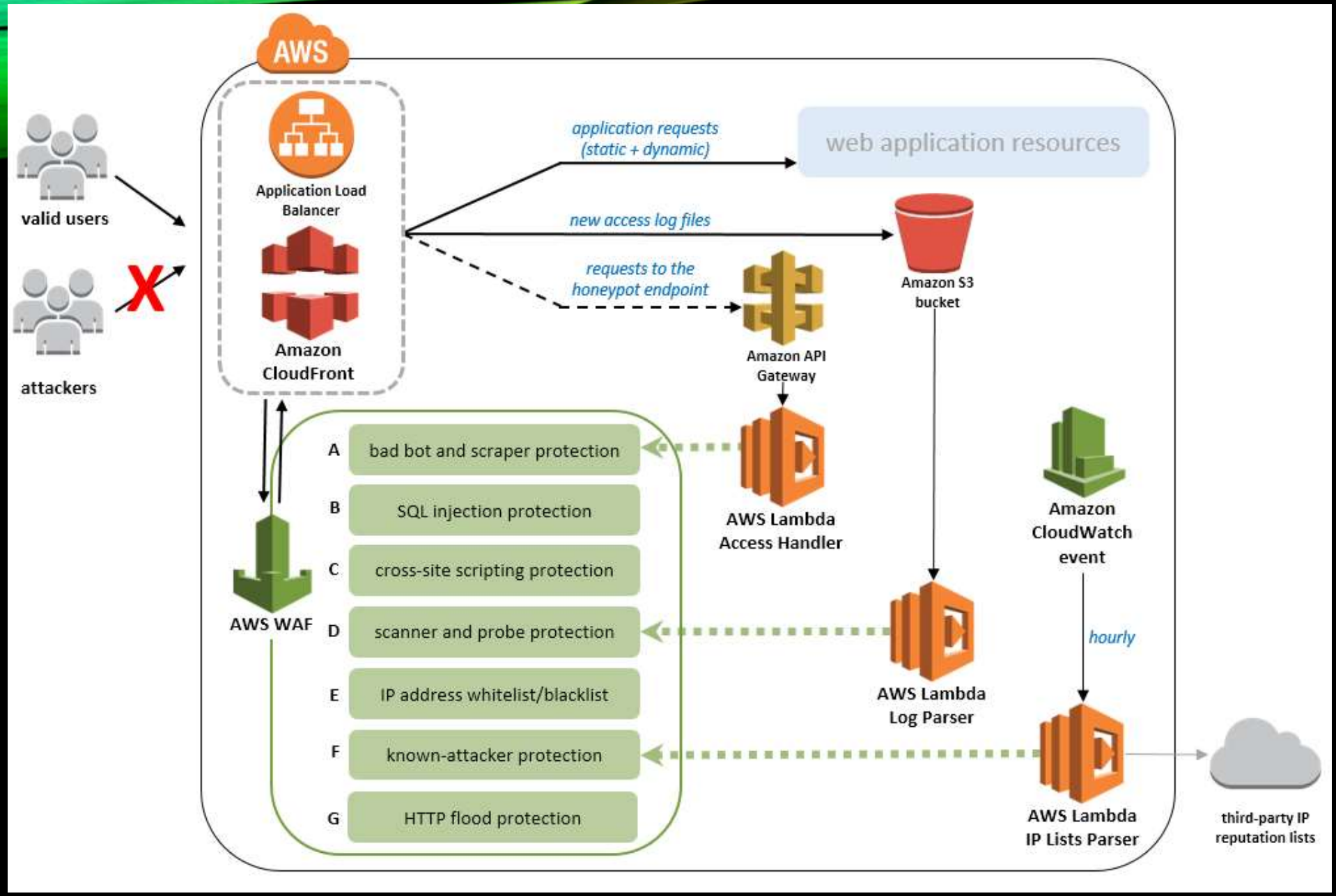
- Rule groups per web ACL: 1 customer, 1 Marketplace rule group
- Rules per web ACL: 10
- Conditions per rule: 10
- Filters (per css, size, SQLi, string match): 10
- And others…

https://docs.aws.amazon.com/waf/latest/developerguide/limits.html

DEMO

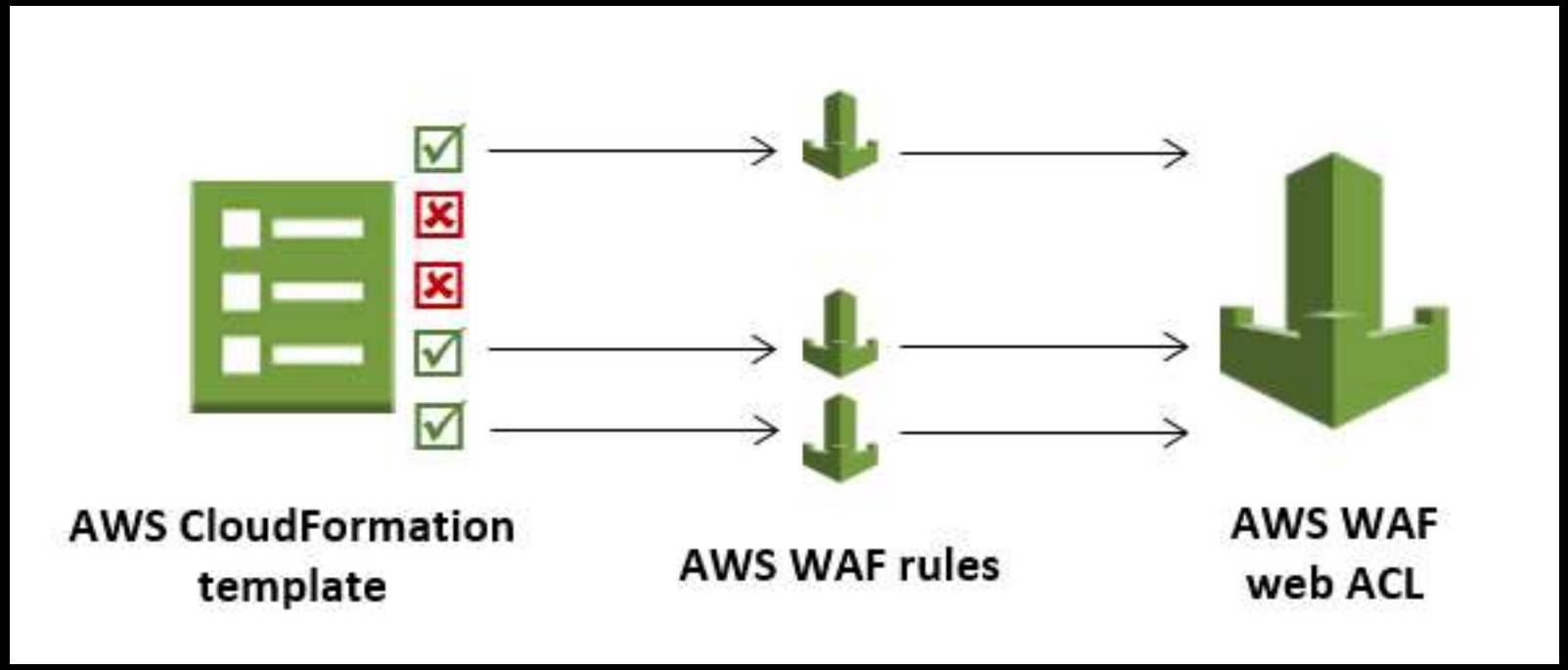
WAF basic setup

AWS WAF SECURITY AUTOMATION



https://docs.aws.amazon.com/solutions/latest/aws-waf-security-automations/architecture.html

CLOUDFORMATION DEPLOYMENT



DEMO

WAF security automation

AWS WAF MANAGED RULES

SELLER MANAGED RULES

- A set of WAF rules written and managed by trusted security vendors
- Available on AWS Marketplace and the WAF Console
- Deployed on AWS WAF
- Pay-As-You-Go pricing
- Auto Updates, no extra costs

F5 RULES FOR AWS

Web exploits (OWASP)

- SQLi,
- XSS,
- command injection,
- No-SQLi,
- path traversal,
- and predictable resource

CVE vulnerabilities

Apache, Apache Struts, Bash, Elasticsearch, IIS, Jboss, JSP, Java, Joomla, MySQL, Node.js, PHP, PHPMyAdmin, Perl, Ruby on Rails WordPress

Bot protection

Vulnerability scanners, web scrapers, DDoS tools, and forum spam tools

PRICING

- Two pricing dimensions:

  Rule Group monthly fee ($/month)

  Request fee per Million Requests ($/Million Request)

- Sellers set their own prices in AWS Marketplace

- Seller prices are in addition to normal AWS WAF charges

https://aws.amazon.com/mp/security/WAFManagedRules/

DEMO

WAF managed rules

AWS FIREWALL MANAGER

FIREWALL MANAGER

- makes it easier to configure AWS WAF rules across all aws accounts within an organization
- security administrators can write company-wide rules from one place, enforce them across applications protected by AWS WAF
- gets the central visibility of attacks against Application Load Balancers and Amazon CloudFront infrastructure.
- lets you use your own custom rules, or purchase managed rules from AWS Marketplace
- automatically adds protection to resources that are added to your account
- hierarchical application of rules
- visual dashboard
- compliance notifications

Pricing: https://aws.amazon.com/firewall-manager/pricing/

DEMO

AWS Firewall Manager

SUMMARIZING

WHEN TO CHOOSE WHAT?

WAF SECURITY AUTOMATION

WAF MANAGED RULES

FIREWALL MANAGER

WAF BEST PRACTICES

REMEMBER WAF IS JUST A TOOL

COUNT BEFORE ACT

FOCUS ON MONITORING

LONG TERM INVESTMENT PAYS OFF

Q&A

Thanks!