Accelerate DDoS event response with DDoS Fire Extinguisher

September 30th, 2021

Ian Olson
Senior Technical Account Manager

Agenda

- What customer challenge does this solution solve
- DDoS protection best practices
- Initial deployment and overview
- Gaining insights using Amazon Athena queries/reports
- Tuning deployment based on insights
- Next steps

What customer challenge does this solutions solve

- Relieve DDoS impact even when not prepared
- Get started with AWS Shield Advanced and AWS WAF quickly

DDoS protection best practices – Overview

- Be proactive
- Block requests at or close to the edge
- Protect with the right tool/mechanism
- Architect for DDoS resiliency

DDoS protection best practices – AWS services

AWS Shield Advanced

- L3/L7 protection
  - UDP reflection
  - SYN flood, etc.
  - L7 anomaly detection

AWS WAF

- L7 web protection
  - HTTP floods/cache-busting attacks
  - Bot management

Amazon Route 53 health checks

- Enable proactive engagement
- Measure application health

Initial deployment and overview

Primary steps

- Subscribe to AWS Shield Advanced
- Add resources to protect
- Configure layer 7 DDoS mitigation

Optional

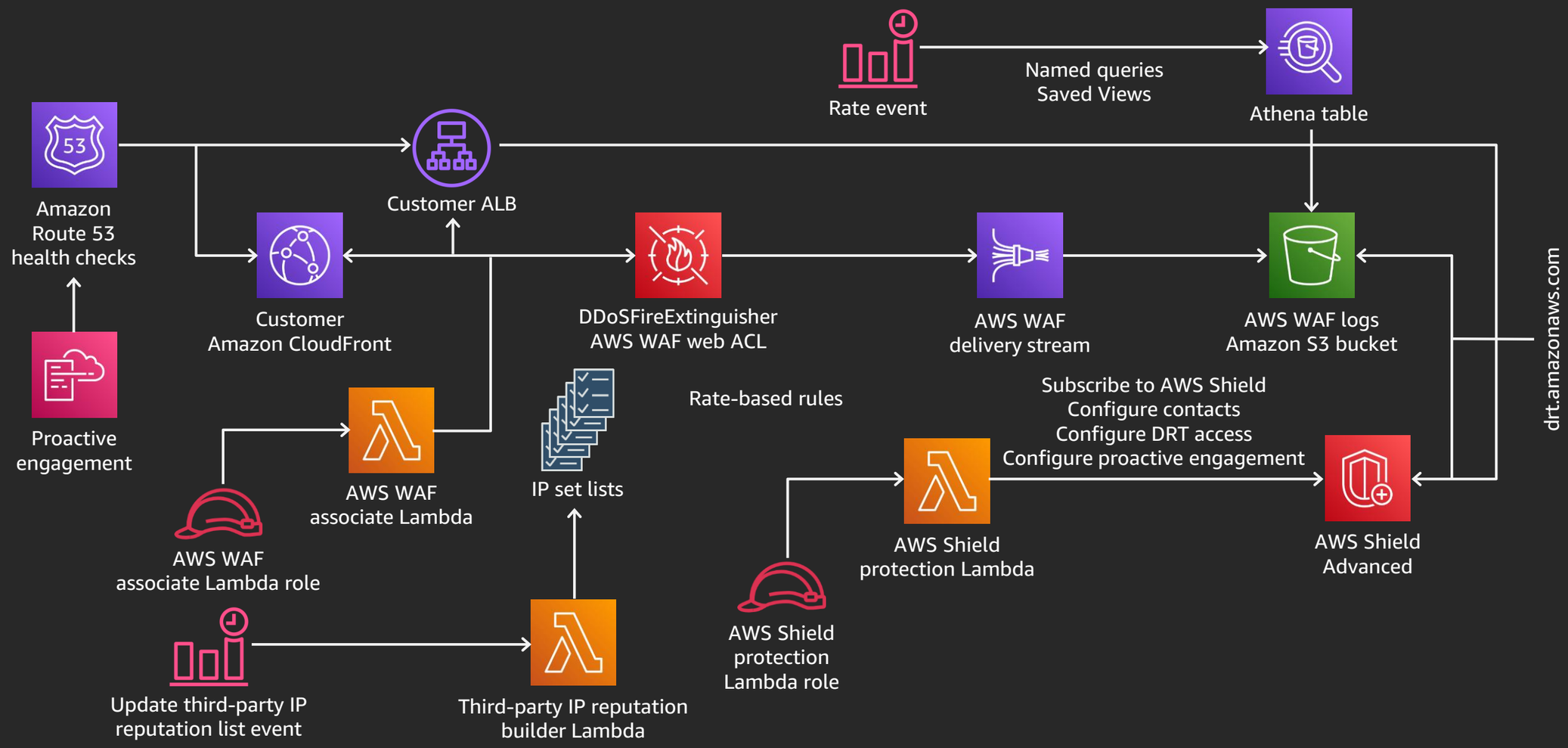
- Configure SRT access
- Endpoint health checks
- Proactive engagement

Initial deployment and overview

AWS CloudFormation template

- High value/lower risk options default to block or rate limit
- Other helpful options default to count(log) mode
- Maximize visibility with added context
- 8 parameters to get started
- Prebuild framework for source IP and country block and rate-based rules
- Automatic reports of common AWS WAF log queries
- Easy tuning and customization

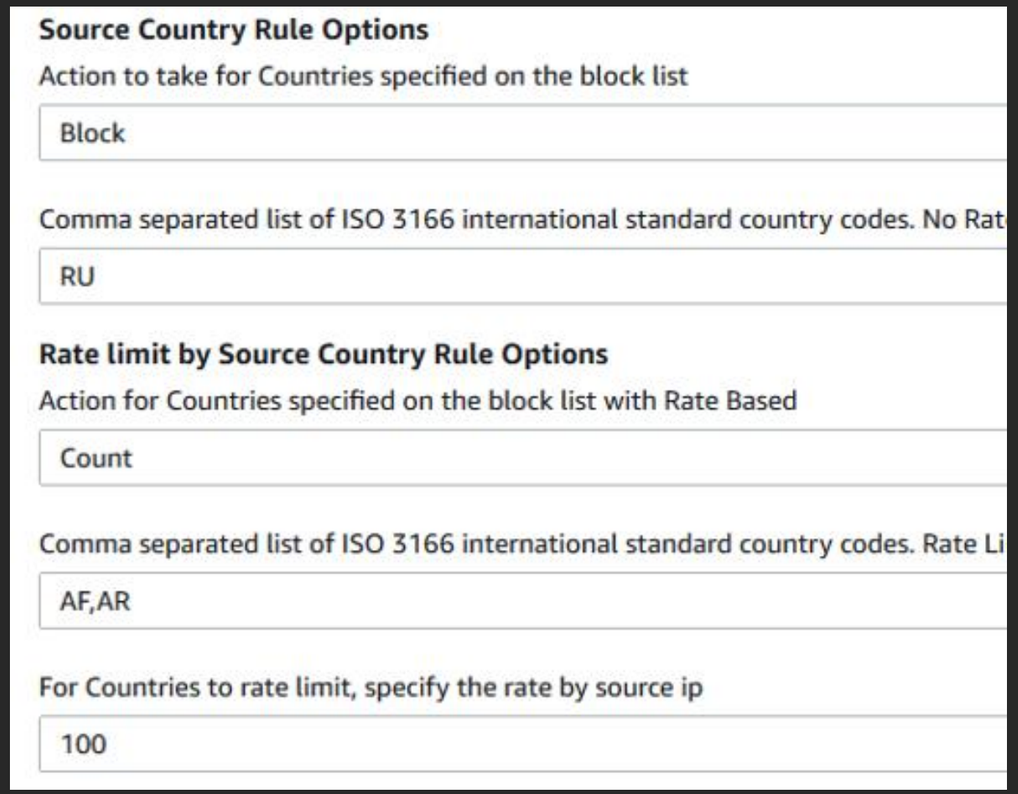
Initial deployment and overview

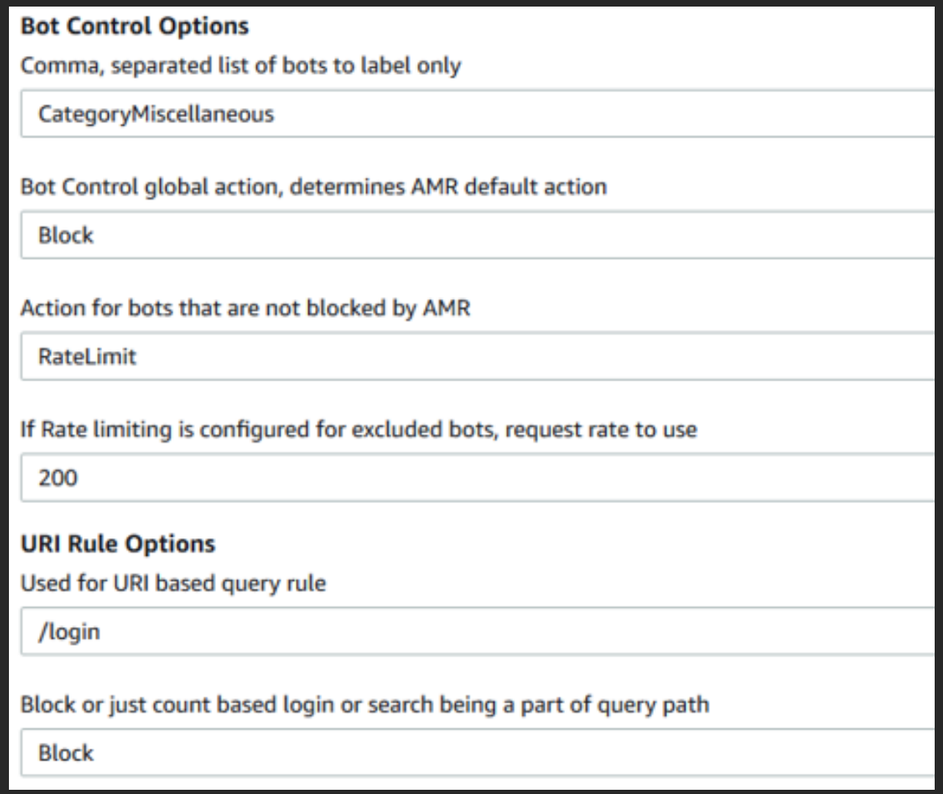


Insights using Amazon Athena

Top talkers	IP identity or reputation
Source IP or IP header	Geolocation
URI Path by source IP	Reputation (AWS, third party, customer managed)
Restricted or expensive URI paths	Anonymous or hidden IP owner (ToR/VPN, proxy) Cloud Hosting providers (AWS, GCP, Azure, Digital Ocean, etc.)
	Bot categories or names

Tuning deployment based on insights





Demo

Next steps

Further refinements

Customize health checks

Architect for DDoS resiliency

AWS SRT – engagement and assistance

Alternative wider-scope approaches to DDoS protection

Resources

GitHub – AWS DDOS Fire Extinguisher

- https://github.com/aws-samples/aws-ddos-fire-extinguisher

The three most important AWS WAF rate-based rules

- AWS Security Blog – https://amzn.to/2VrGvXq

AWS Best Practices for DDoS Resiliency

- AWS Whitepaper - https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.pdf

Thank you!

Ian Olson

olsonian@amazon.com

Please complete the session survey in the mobile app.