AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET324

Web security: 2021 updates and implementations

Diana Alvarado
Senior Technical Account Manager
AWS

Justin Kurpius
Edge GTM Specialist
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

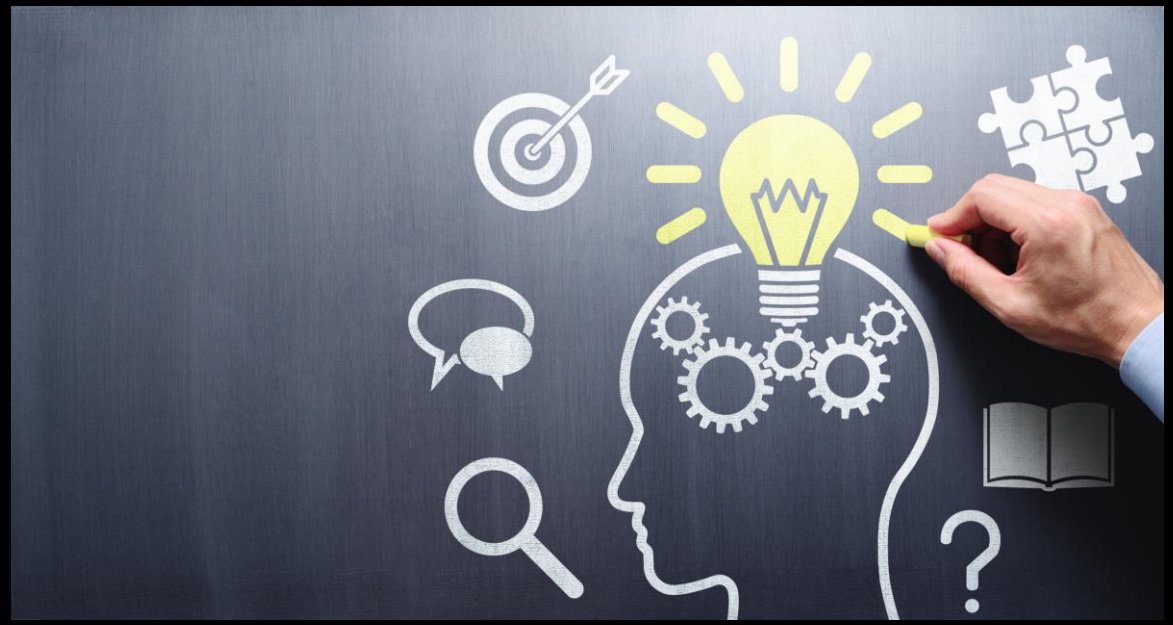
Agenda

- New AWS WAF features
- Common edge architectures
- Demo: implementing new features
- Key takeaways

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

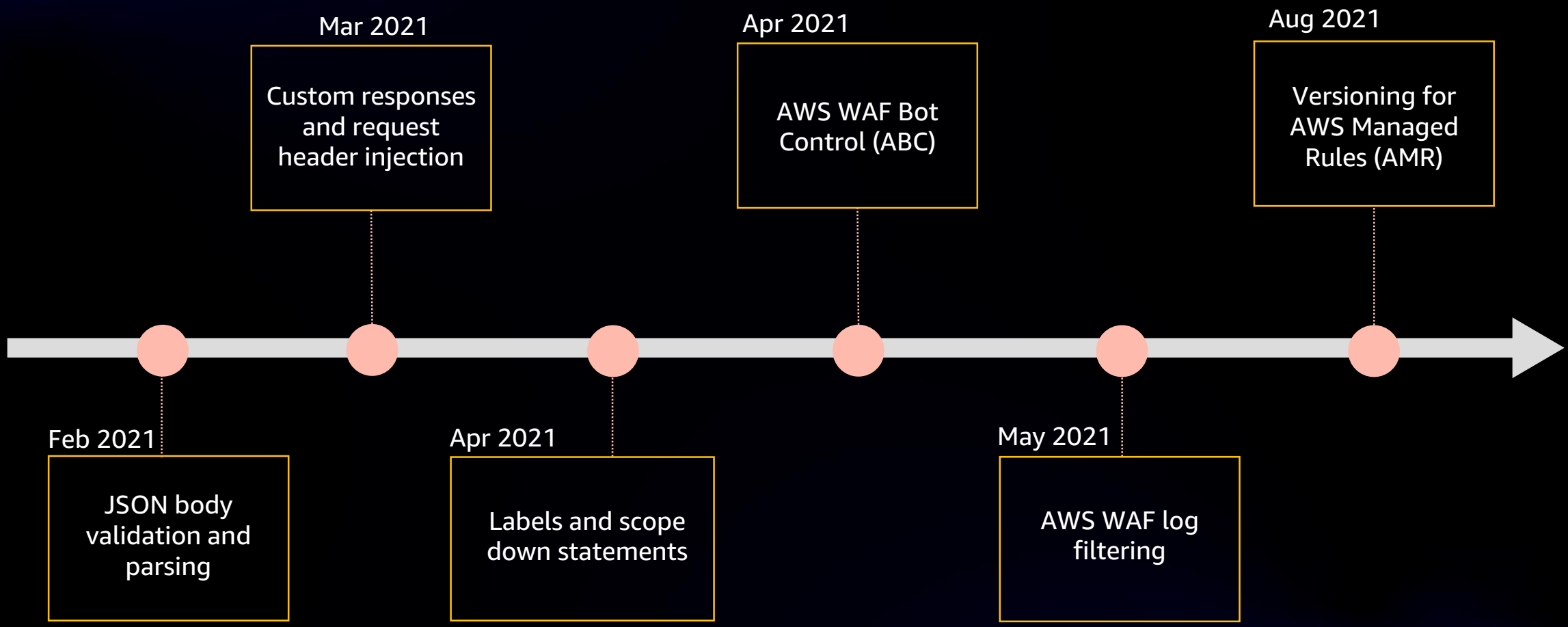
Advanced session

- **Not** a review of services
- Assumed familiarity with:
  - AWS services
  - Perimeter security



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New 2021 AWS WAF features covered



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature: JSON body validation/parsing

- Natively parses JSON request body
- Checks for valid JSON structure
- Protects APIs
- Uses JSON Pointer syntax for keys/values

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature: Custom response

- It’s an action associated with a rule
- Overrides default AWS WAF response
- Provides customization of response code and response body
- Used to provide information on a block action

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature: Header insertion

- Can be used to:
  - Customize a count/allow action
  - Validate information on requests
  - Signal downstream processing
- Included in the AWS WAF logs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature: AWS WAF Bot Control

- ABC targets common and pervasive bots, such as:
  - Scrapers
  - Crawlers
  - Spammers
- Managed by AWS
- Provides logging and monitoring



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature: Labels

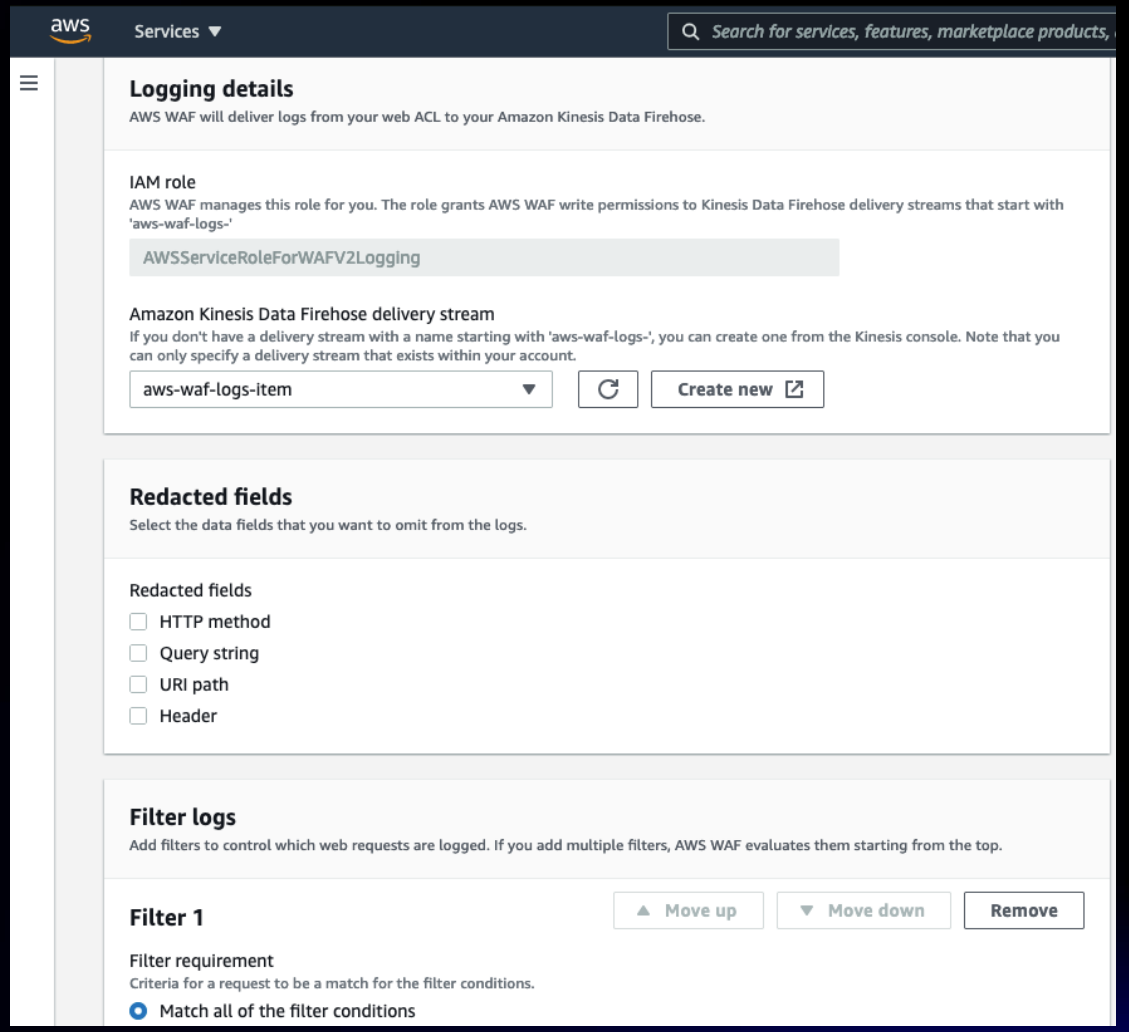
- Available for AWS WAF Bot Control, AWS Managed Rules, IP lists
- Labels work as tags for requests
- Added with a rule match
- Can be reused and are available across subsequent rules



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature: Log filtering

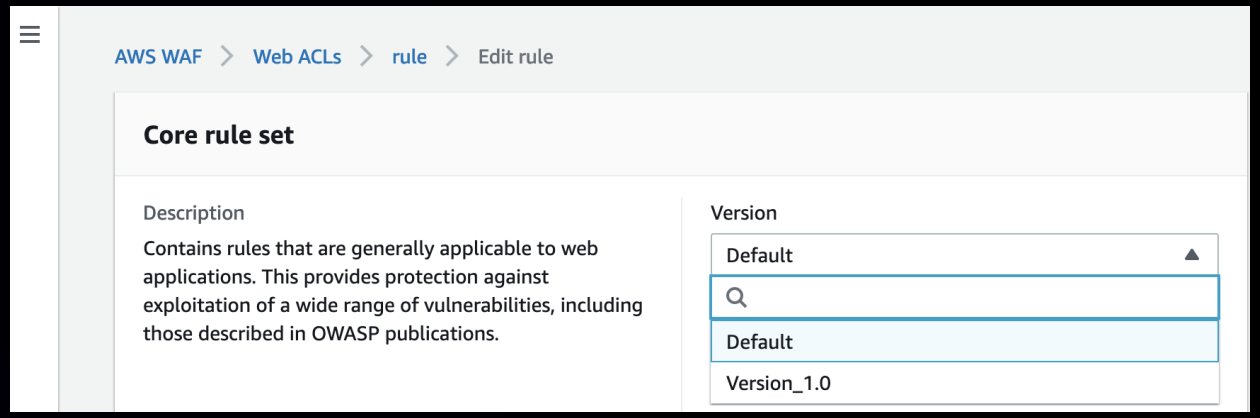
- Keep only what you need
- Redact fields
- Save on costs



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

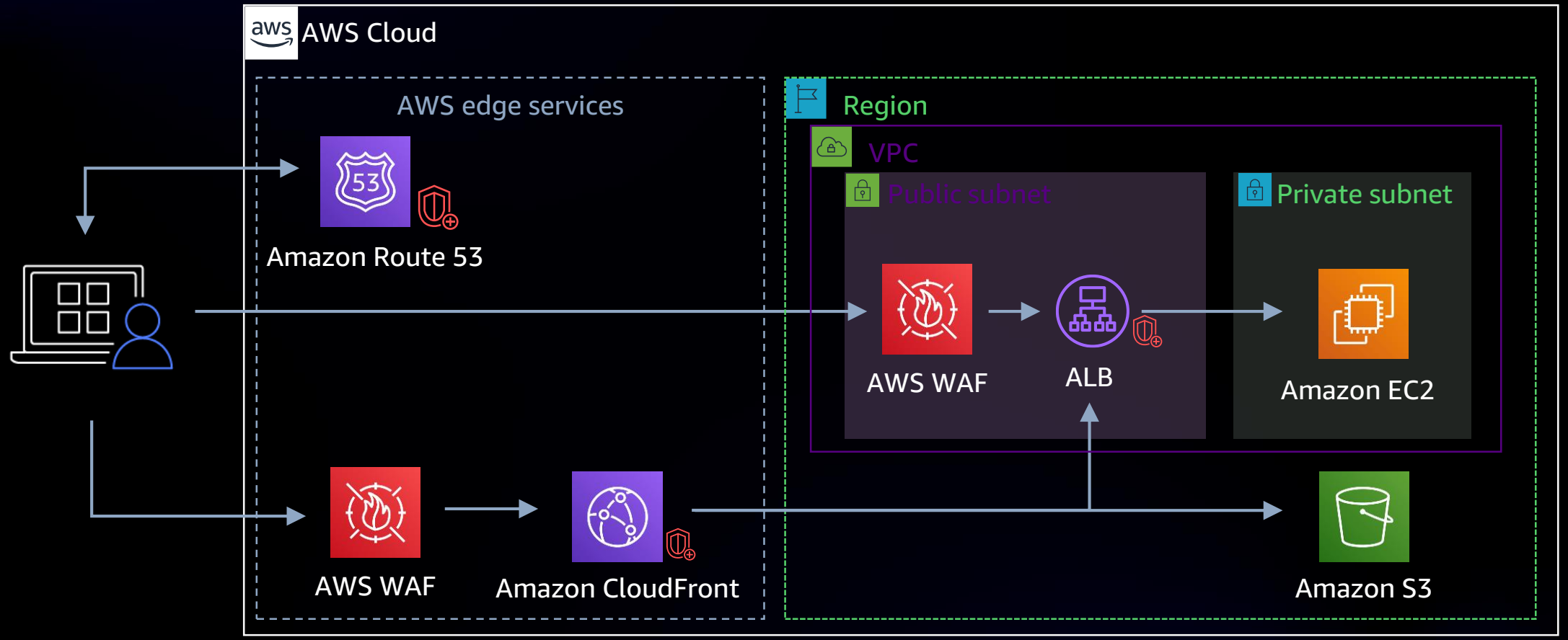
New feature: Versioning for AWS Managed Rules

- Choose version to use
- Evaluate changes
- Subscribe to notifications
- Keep up to date



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

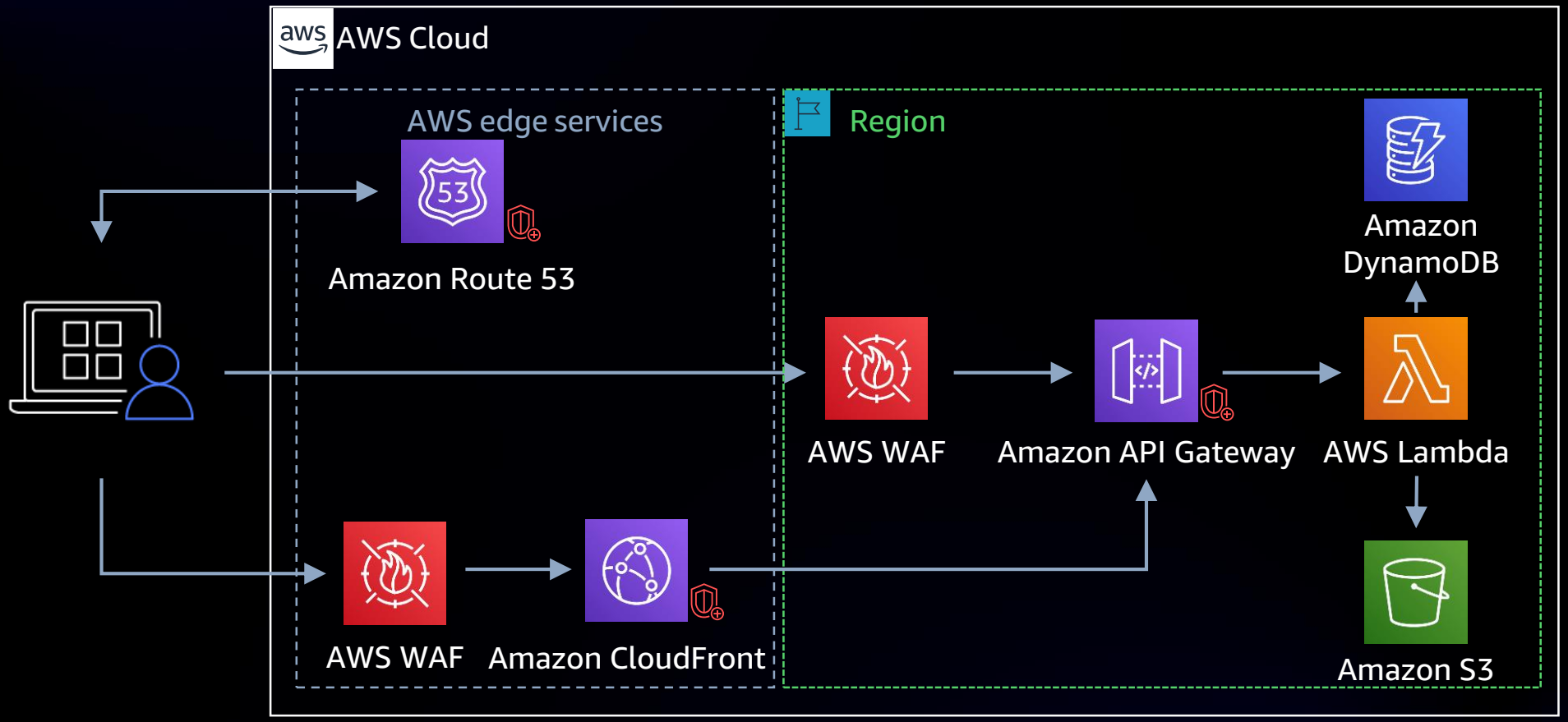
Common architecture: Web application



AWS Shield Advanced protected resource

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common architecture: API

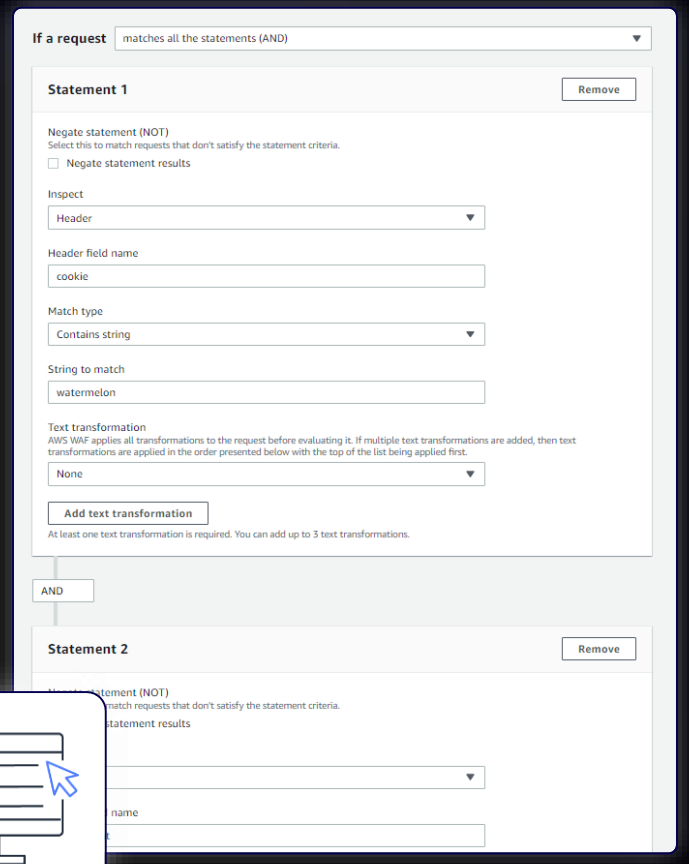


AWS Shield Advanced protected resource

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Writing rules in AWS WAF

Visual rule builder



Code (JSON)



Online Tech Talk – Using AWS WAF Rules
https://www.youtube.com/watch?v=ll-uvVgQ3Jg

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

- Analyze your traffic; evaluate possible solutions
- Review what you have and consider an update
- New, already integrated features can simplify management

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

- AWS Best Practices for DDoS Resiliency
  https://go.aws/3jSrkjI
- Guidelines for Implementing AWS WAF
  https://d1.awsstatic.com/whitepapers/guidelines-implementing-aws-waf.pdf
- Secure Content Delivery with Amazon CloudFront
  https://go.aws/3GFEURd
- AWS WAF Security Automations
  https://aws.amazon.com/solutions/implementations/aws-waf-security-automations/
- The three most important AWS WAF rate-based rules
  https://aws.amazon.com/blogs/security/three-most-important-aws-waf-rate-based-rules/
- How to improve visibility into AWS WAF with anomaly detection
  https://aws.amazon.com/blogs/security/how-to-improve-visibility-into-aws-waf-with-anomaly-detection/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Relevant sessions

ARC322 – Building DDoS-resilient perimeters with response automation

NET320 – Observability with Amazon CloudFront and AWS WAF

SEC313-R1 – Protecting against automated bots with AWS WAF Bot Control

NET308-R1 – Protect your web applications across multiple AWS accounts

LAB006 – Filtering and blocking web security events with AWS WAF

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.