NREL
Transforming ENERGY

AWS Web Application Firewall

Darren Weiner
Cloud Architect/Engineer

Colorado CSA Fall Summit 2018
November 8, 2018
Denver, Colorado

NREL/PR-6A20-72666

My journey

20 years in IT
8 years in the cloud

Rode the .com wave

- Web Admin
- DBA
- IT Director
- Cloud Consulting

Today's Journey

Adoption of cloud technologies

Security ecosystem

AWS Web Application Firewall

- Feature overview
- Process of adoption

Live Demo

Credits: https://design.tutsplus.com/tutorials/use-filter-forge-and-adobe-photoshop-to-create-a-yellow-brick-road--cms-25029

National Renewable Energy Laboratory Mission Statement

Advance the science and engineering of energy efficiency, sustainable transportation, and renewable power technologies and provide the knowledge to integrate and optimize energy systems.

Cloud Team Mission Statement

Provide cloud services and expertise as an enterprise NREL-solution for enabling mission-driven data science, computing, application development, data management, and analysis innovation at the laboratory.

Cloud First/Cloud Native

Why?

- Fast/Agile
- Purpose built
- Innovation
- Continuum of service offerings
- Scalable, resilient
- Can reduce management complexity
- It's shiny, new and fun

When?

- Is the business ready? (Federal Risk and Authorization Management Program)
- Is it best of breed? Does it need to be?
- Who are the stakeholders and the decision makers?
- Are your people ready? Training, comfort level.
- Will the code/platform adapt easily?

Before talking about the Web Application Firewall…

Let's talk about the WAF
Well Architected Framework

In the cloud it's easy to do things fast. It's another thing entirely to do them well


Operational Excellence


Security

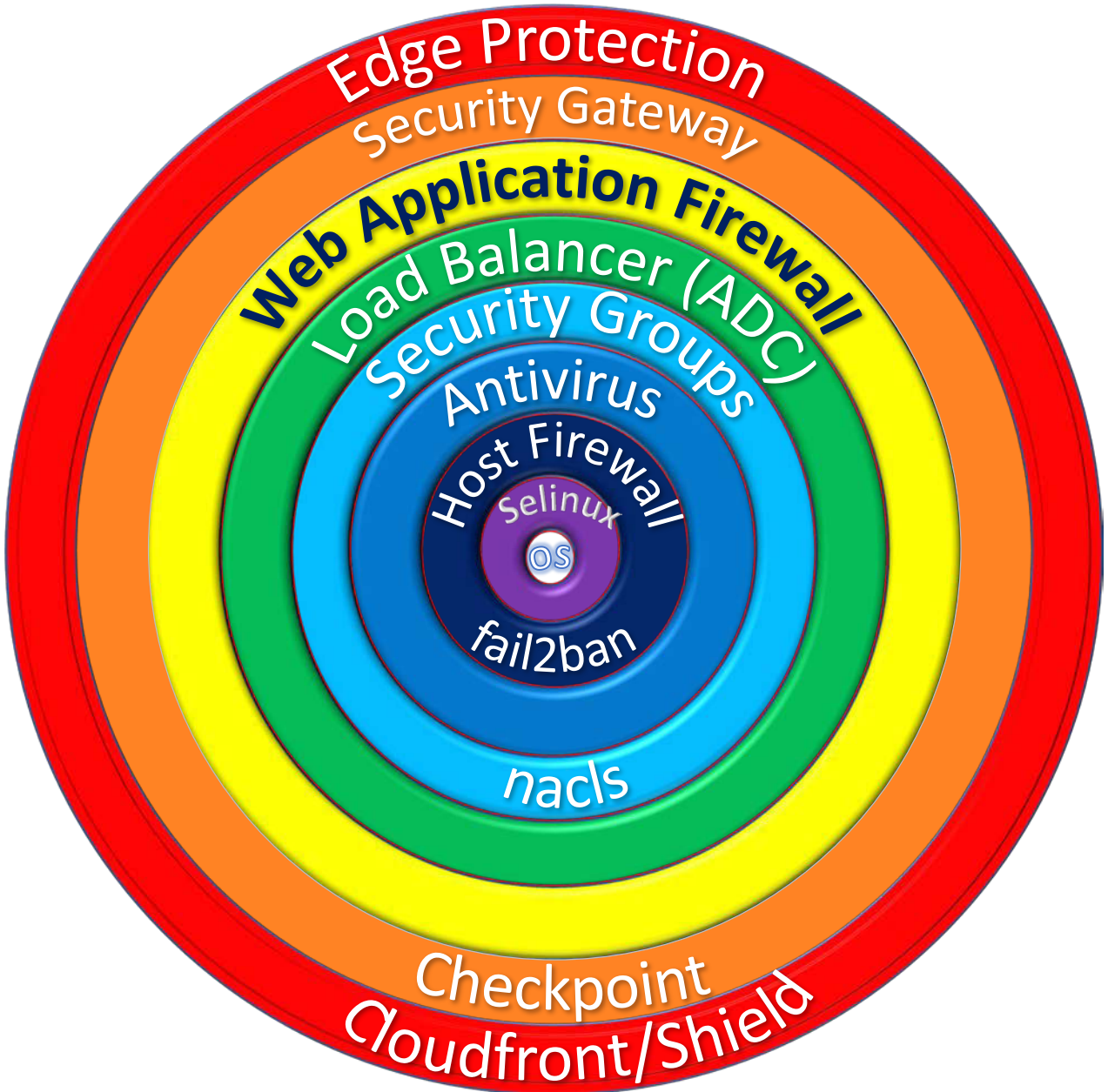

Reliability


Performance Efficiency

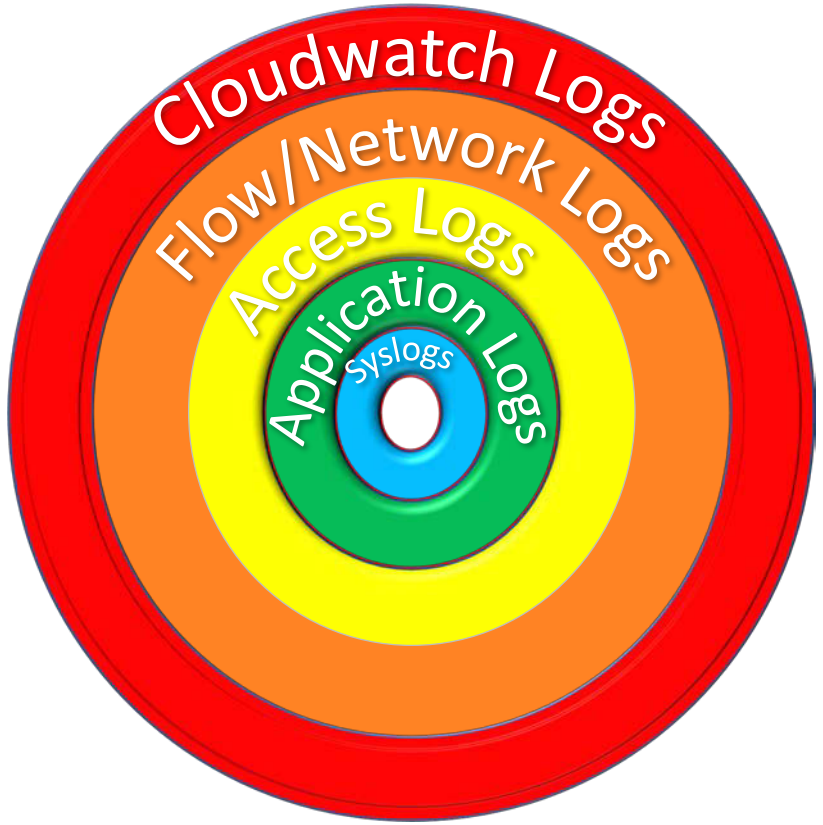

Cost

Pillar by Bohdan Burmich from the Noun Project

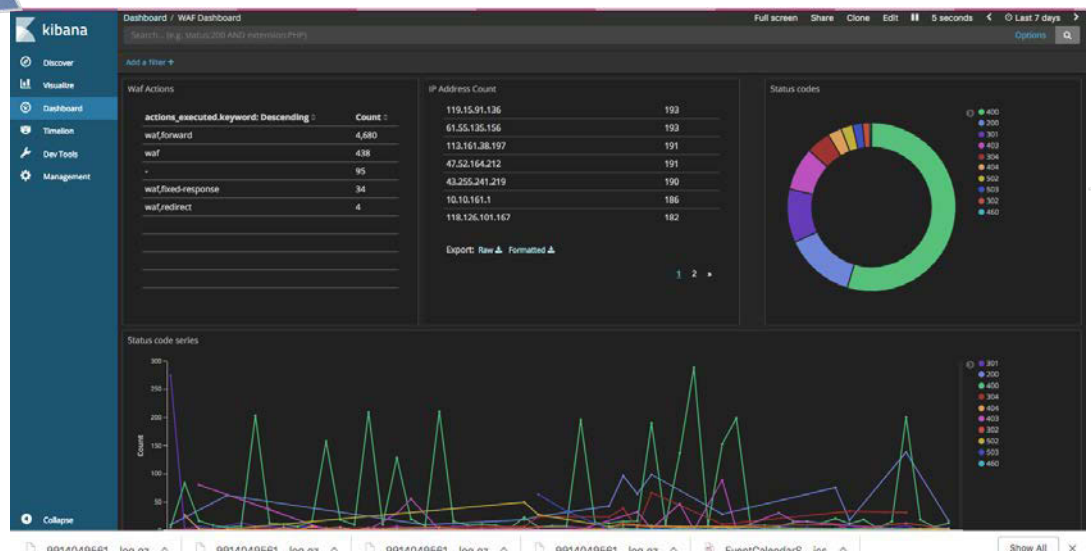
Security tools



Data Capture



Ability to respond



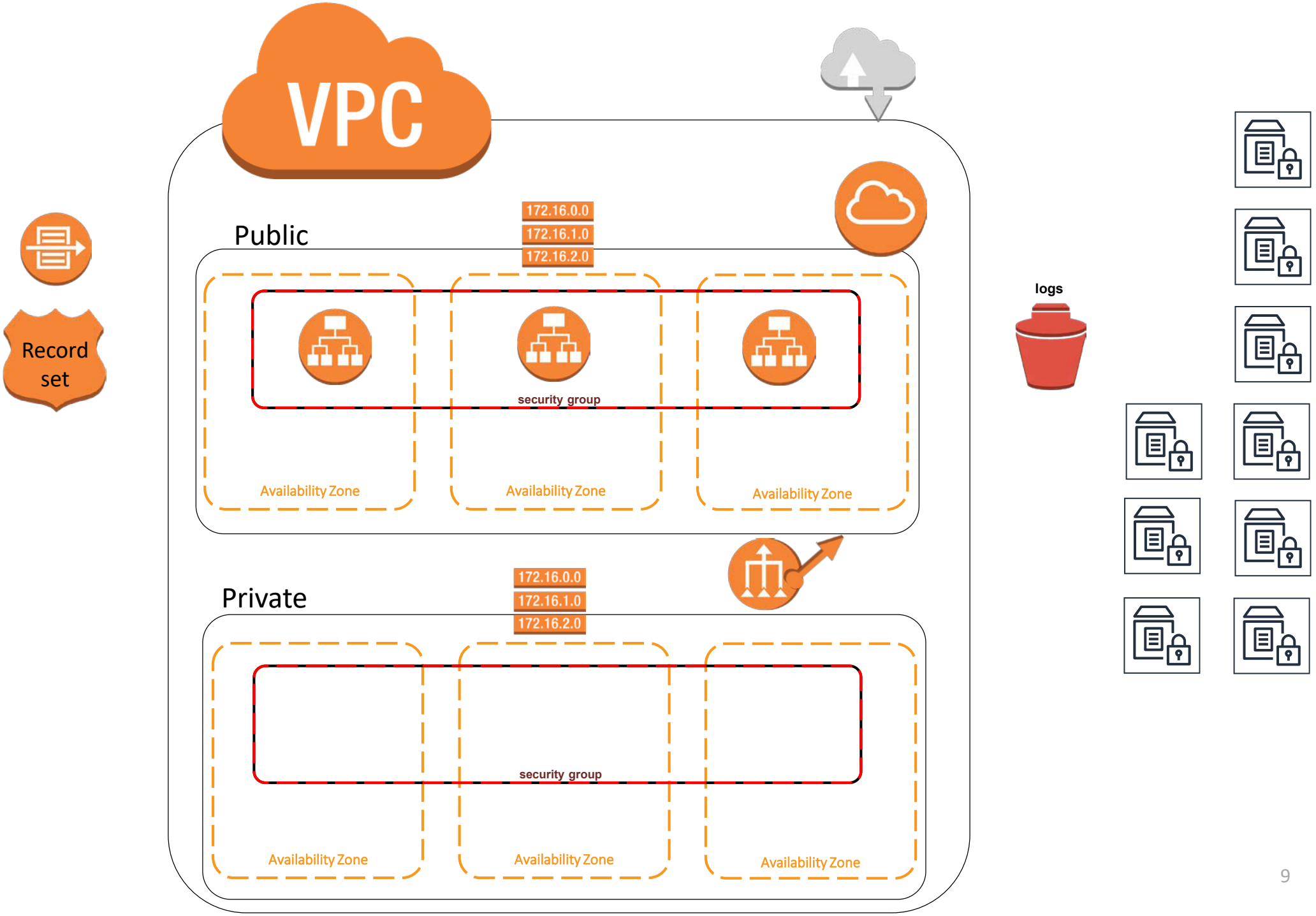
Application Testing
Vulnerability Scans
Network Pen Testing
Load Testing

Development practices:
OWASP
Peer reviews

AWS Web Application Firewall

Web Application firewall that **natively** integrates with key AWS services
(Load balancers, CloudFront, more to come)

- Pushbutton deployment includes out-of-the gate solutions that address rate and rule-based vectors.
- Centralized WAF management
- Ideal solution for serverless architectures
- There are no infrastructure or appliances to manage.
- Ability to deploy new rules in a dev/test/prod paradigm
- Granular user access control to read/modification of ACLs.
- Reduces architectural footprint
- Provide ability to respond rapidly to user requests: Can automate Application Delivery Control features
- Fits nicely with CI/CD frameworks
- Alerts/notification and deep reporting capabilities
- Consumption based pricing model

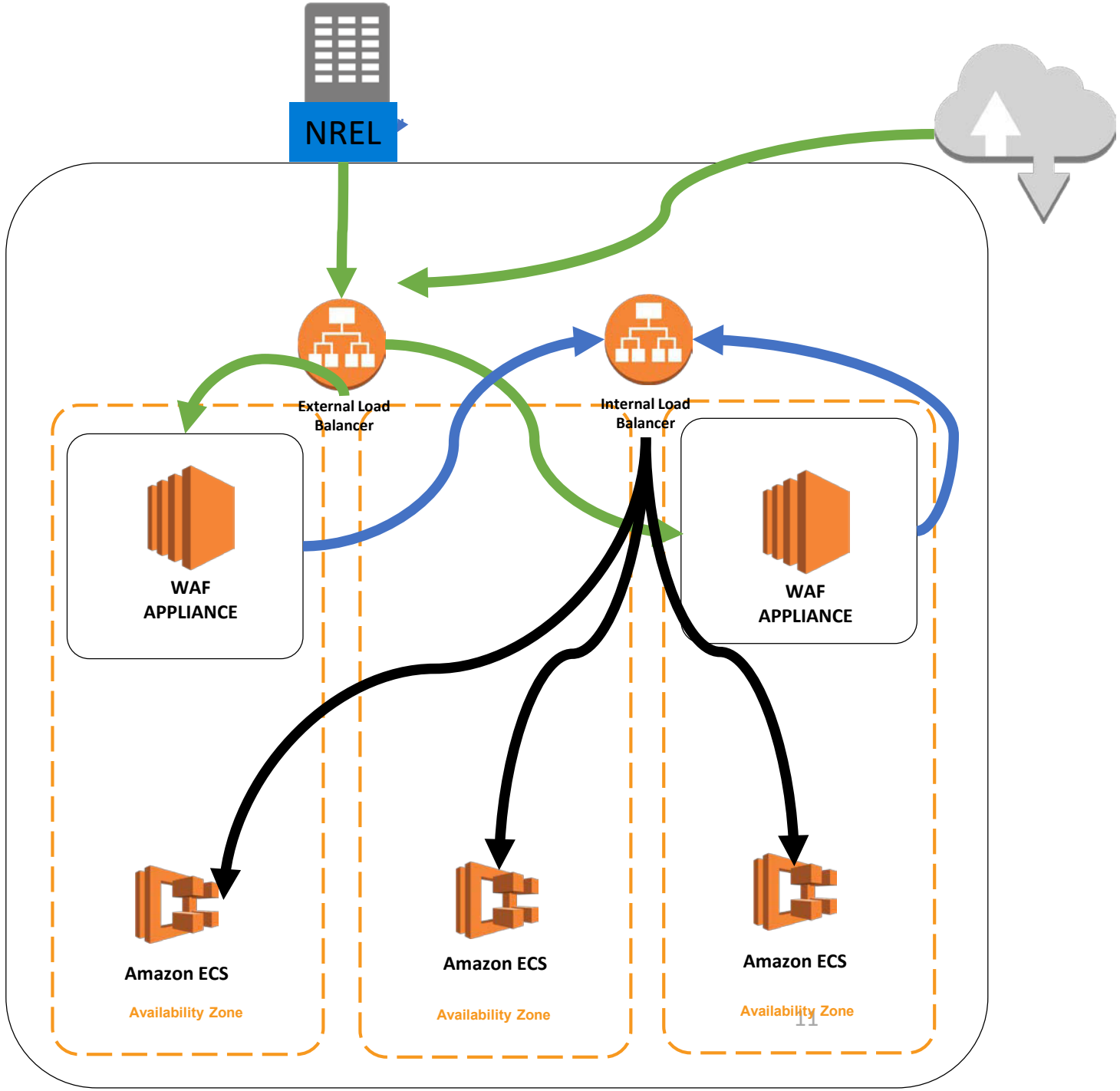

VPC
Public
172.16.0.0
172.16.1.0
172.16.2.0
security group
Availability Zone
Availability Zone
Availability Zone
Private
172.16.0.0
172.16.1.0
172.16.2.0
security group
Availability Zone
Availability Zone
Availability Zone
Record set
logs

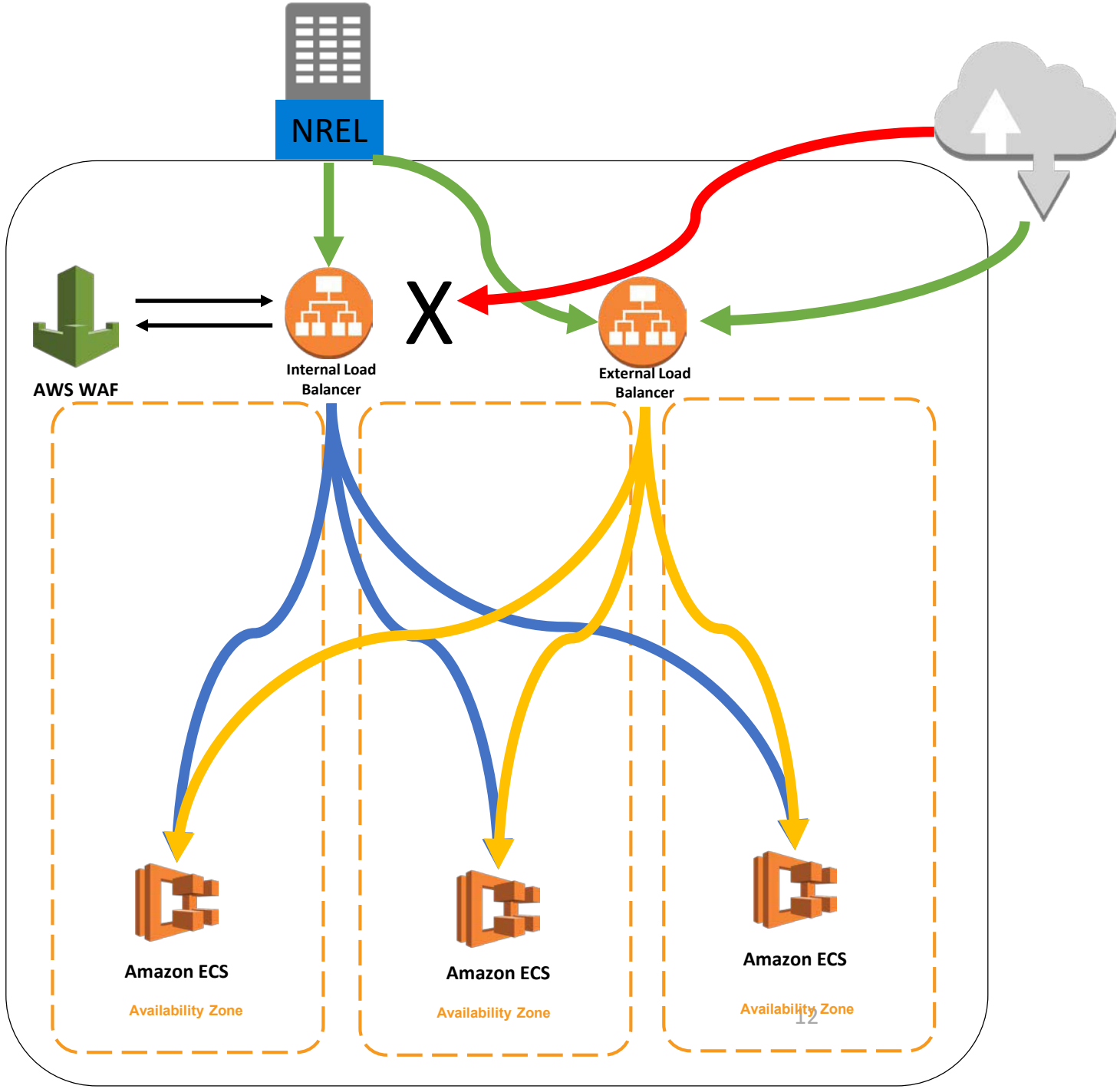
Templatized deployment

- Rate/scan blocks:
  - ❖ Http floods
  - ❖ Scanner and probe
- Global blocks:
  - ❖ Global IP Reputation lists (11,1324 blocks, Updated hourly
  - ❖ Blacklist
- Application protection:
  - ❖ SQL Injection
  - ❖ XSS
- Whitelist
- Bad bot blacklisting

Additional Options:

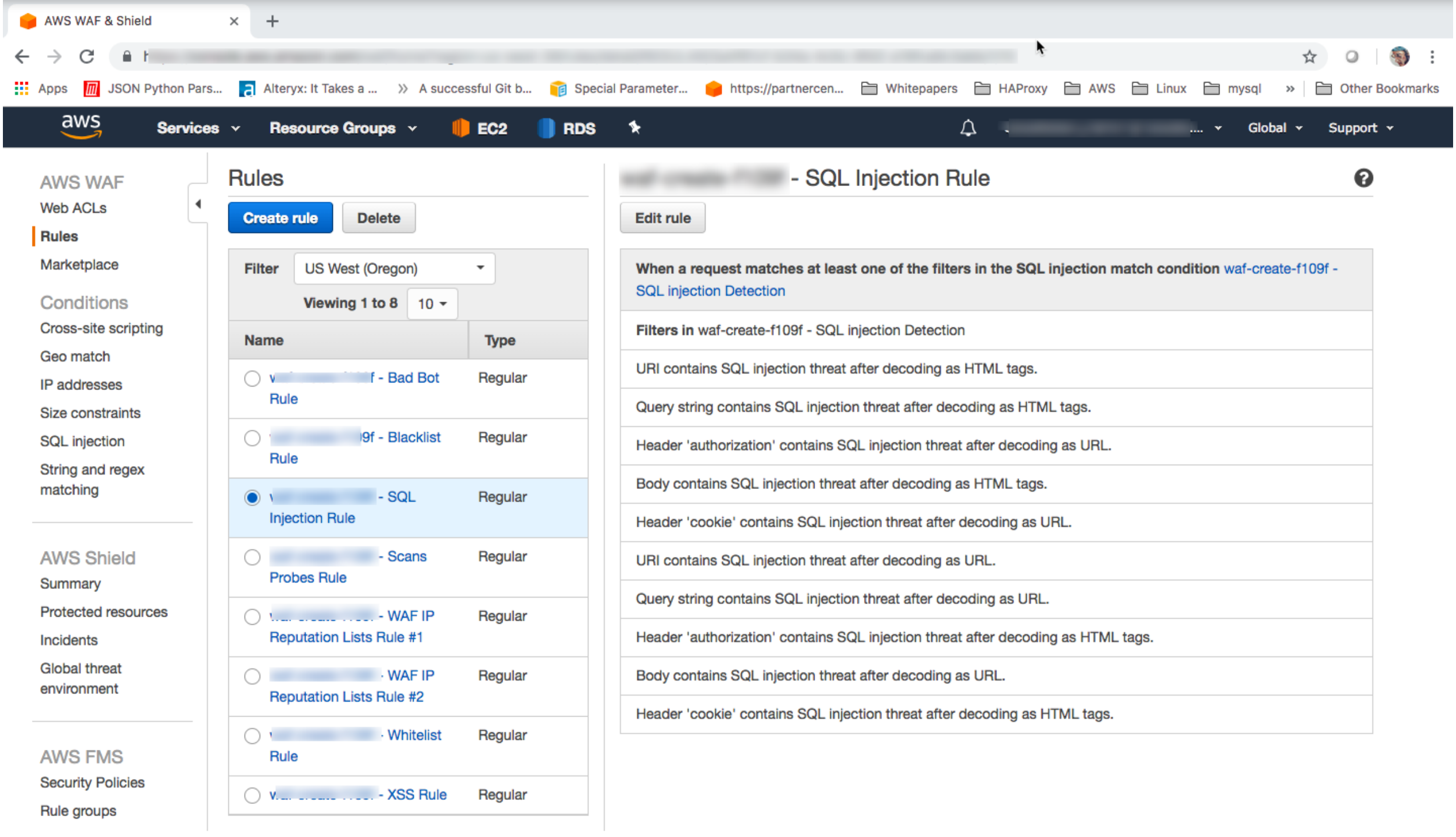
size-constrained rules	third party rulesets*
Customized regex-based rules	Any rate-based function (via lambda)


NREL
External Load Balancer
Internal Load Balancer
WAF APPLIANCE
WAF APPLIANCE
Amazon ECS
Availability Zone
Amazon ECS
Availability Zone
Amazon ECS
Availability Zone


NREL
AWS WAF
Internal Load Balancer
X
External Load Balancer
Amazon ECS
Availability Zone
Amazon ECS
Availability Zone
Amazon ECS
Availability Zone

The Big Sell

- Requirements
- Finding stakeholders, then peddling wares.
  - Cyber, Operations, Networking
  - Top down, bottom up
- Proof-of-concept
- Powerpoint
- Ensuring exceptions are handled with appropriate change management.
- Forcing ourselves to move slow
- Limits to cloud knowledge


AWS WAF & Shield
Apps
JSON Python Pars...
Alteryx: It Takes a ...
A successful Git b...
Special Parameter...
https://partnercen...
Whitepapers
HAProxy
AWS
Linux
mysql
Other Bookmarks
aws
Services
Resource Groups
EC2
RDS
Global
Support
AWS WAF
Web ACLs
Rules
Marketplace
Conditions
Cross-site scripting
Geo match
IP addresses
Size constraints
SQL injection
String and regex matching
AWS Shield
Summary
Protected resources
Incidents
Global threat environment
AWS FMS
Security Policies
Rule groups
Rules
Create rule
Delete
Filter
US West (Oregon)
Viewing 1 to 8
10
Name
Type
- Bad Bot Rule
Regular
- Blacklist Rule
Regular
- SQL Injection Rule
Regular
- Scans Probes Rule
Regular
- WAF IP Reputation Lists Rule #1
Regular
- WAF IP Reputation Lists Rule #2
Regular
- Whitelist Rule
Regular
- XSS Rule
Regular
- SQL Injection Rule
Edit rule
When a request matches at least one of the filters in the SQL injection match condition waf-create-f109f - SQL injection Detection
Filters in waf-create-f109f - SQL injection Detection
URI contains SQL injection threat after decoding as HTML tags.
Query string contains SQL injection threat after decoding as HTML tags.
Header 'authorization' contains SQL injection threat after decoding as URL.
Body contains SQL injection threat after decoding as HTML tags.
Header 'cookie' contains SQL injection threat after decoding as URL.
URI contains SQL injection threat after decoding as URL.
Query string contains SQL injection threat after decoding as URL.
Header 'authorization' contains SQL injection threat after decoding as HTML tags.
Body contains SQL injection threat after decoding as URL.
Header 'cookie' contains SQL injection threat after decoding as HTML tags.

Cross-site scripting
Geo match
IP addresses
Size constraints
SQL injection
String and regex matching

AWS Shield
Summary
Protected resources
Incidents
Global threat environment

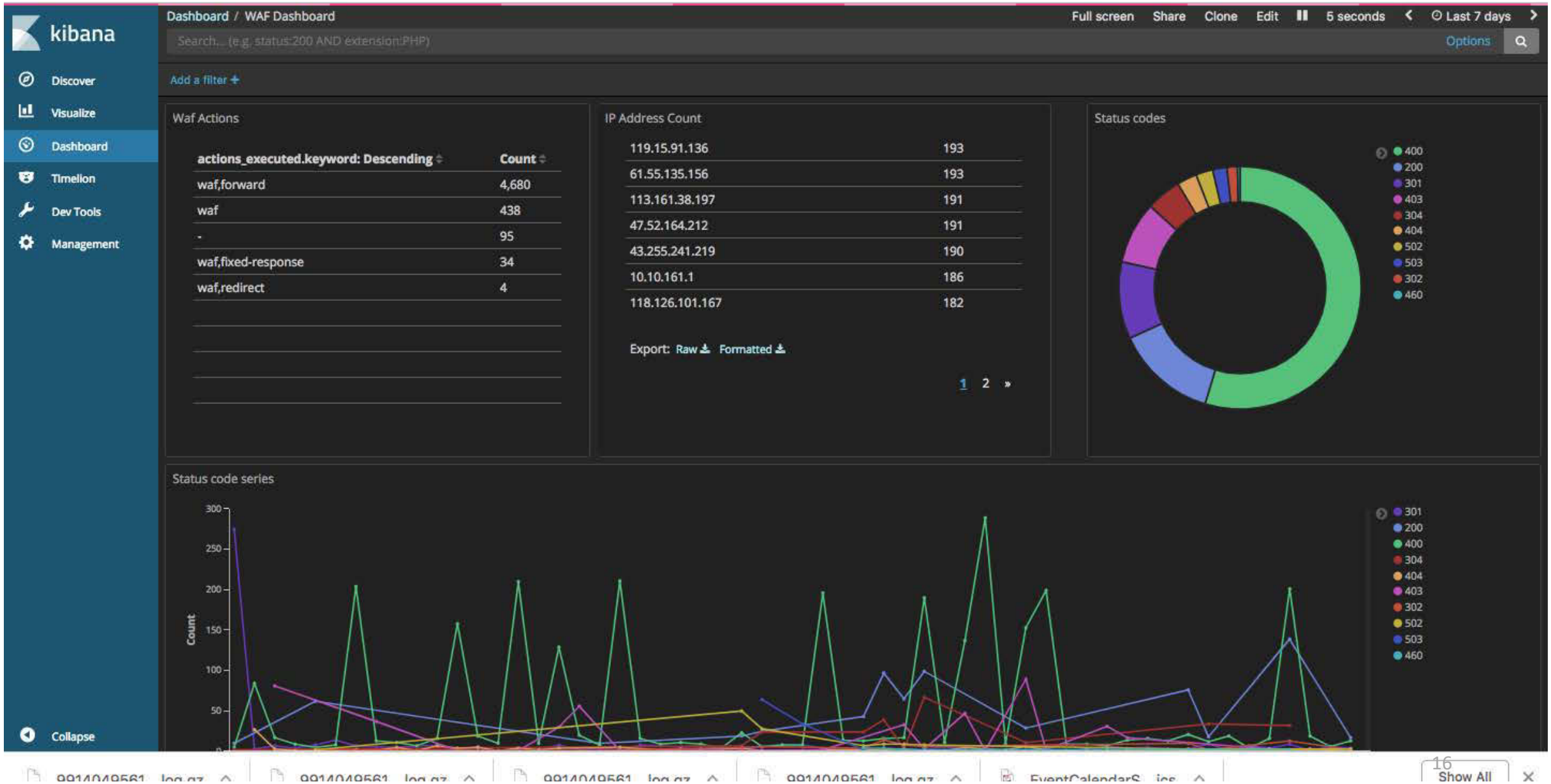
AWS FMS
Security Policies
Rule groups
Settings

Available marketplace products

Search by product name or publisher name

Name	Published by	Details
c Managed Rules for AWS WAF - OWASP Top 10 for WordPress	Alert Logic	**Description:** OWASP Top 10 Virtual Patches for WordPress protect against the last six months of exploitable WordPress core and WordPress plugin attacks. The rule group protects against 250 variations of known WordPress core and plugin vulnerabilities discovered by the Threat Intelligence team. Use this managed rule group to help you achieve compliance against standards that use the OWASP Top 10 as a reference. Visit our Getting Started resource in the AWS Marketplace for a full detailed description of what is covered in this rule group.
Bot Detection Signatures For AWS WAF	F5	**Description** Bot detection signatures will allow you to filter unwanted bot activity traffic that includes vulnerability scanners, scrapers, email correctors, network scanners, SPAM bots, spywares, web spiders, web server stress tools.
Web Application CVE Signatures For AWS WAF	F5	**Description:** Web Application CVE Signatures For AWS WAF will allow you to filter collection of the high profile CVE(Common Vulnerabilities and Exposures), for web applications and infrastructure, among the protected platform are: Struts, Java, Apache, windows, Linux, PHP, MySQL, Shellshock, Elastic Search, CMS
AWS WAF - Web Exploits Rules	F5	**Description:** Protect against web exploits. Web Exploits Rules for AWS WAF, provides protection against web attacks that are part of the OWASP Top 10, such as: SQLi, XSS, command injection, No-SQLi injection, path traversal, and predictable resource. Protect your applications and services with F5, the trusted leader in web application security.
: Managed Rules for AWS WAF - Malicious Bots	Fortinet	**Description:** Fortinets WAF rulesets are based on the FortiWeb web application firewall security service signatures, and are updated on a regular basis to include the latest threat information from The Malicious Bots Ruleset analyzes requests and blocks known content scrapers, spiders looking for vulnerabilities, and other unwanted

Full visibility with drill-down capability



Timely alerting of rule threshold breach

ALARM: "nrel-waf-XSS" in US West (Oregon)

AN

AWS Notifications <no-reply@sns.amazonaws.com>

[redacted]

Saturday, September 22, 2018 at 9:15 PM

Show Details

View this alarm in the AWS Management Console:

[redacted]

Alarm Details:
- Name: nrel-waf-XSS
- Description: XSS Breach Alarm
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [2.4285714285714284 (23/09/18 03:10:00)] was greater than or equal to the threshold (2.0).
- Timestamp: Sunday 23 September, 2018 03:15:48 UTC
- AWS Account: [redacted]

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 2.0 for 300 seconds.

Monitored Metric:
- MetricNamespace: WAF
- MetricName: BlockedRequests
- Dimensions: [Region = us-west-2] [WebACL = SecurityAutomationsMaliciousRequesters] [Rule = SecurityAutomationsXssRule]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: NonBreaching

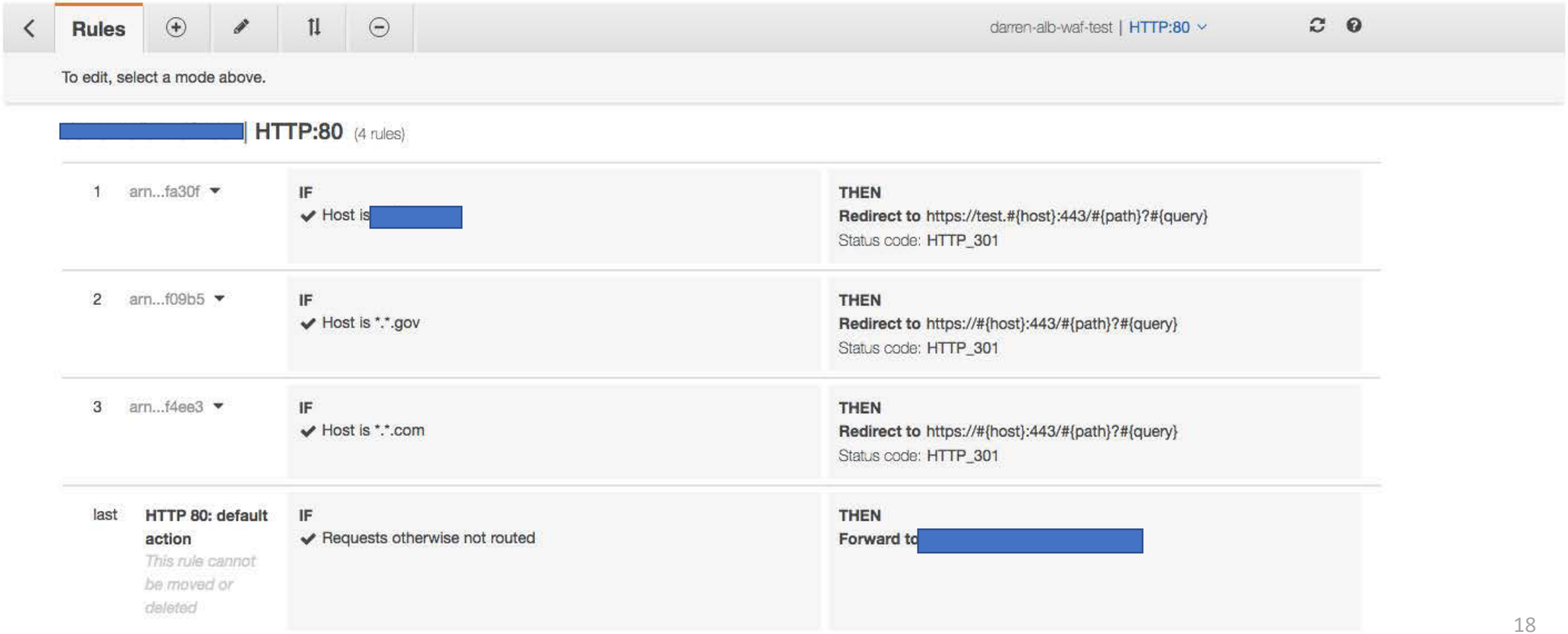
State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-west-2[redacted]]
- INSUFFICIENT_DATA:

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

[redacted]

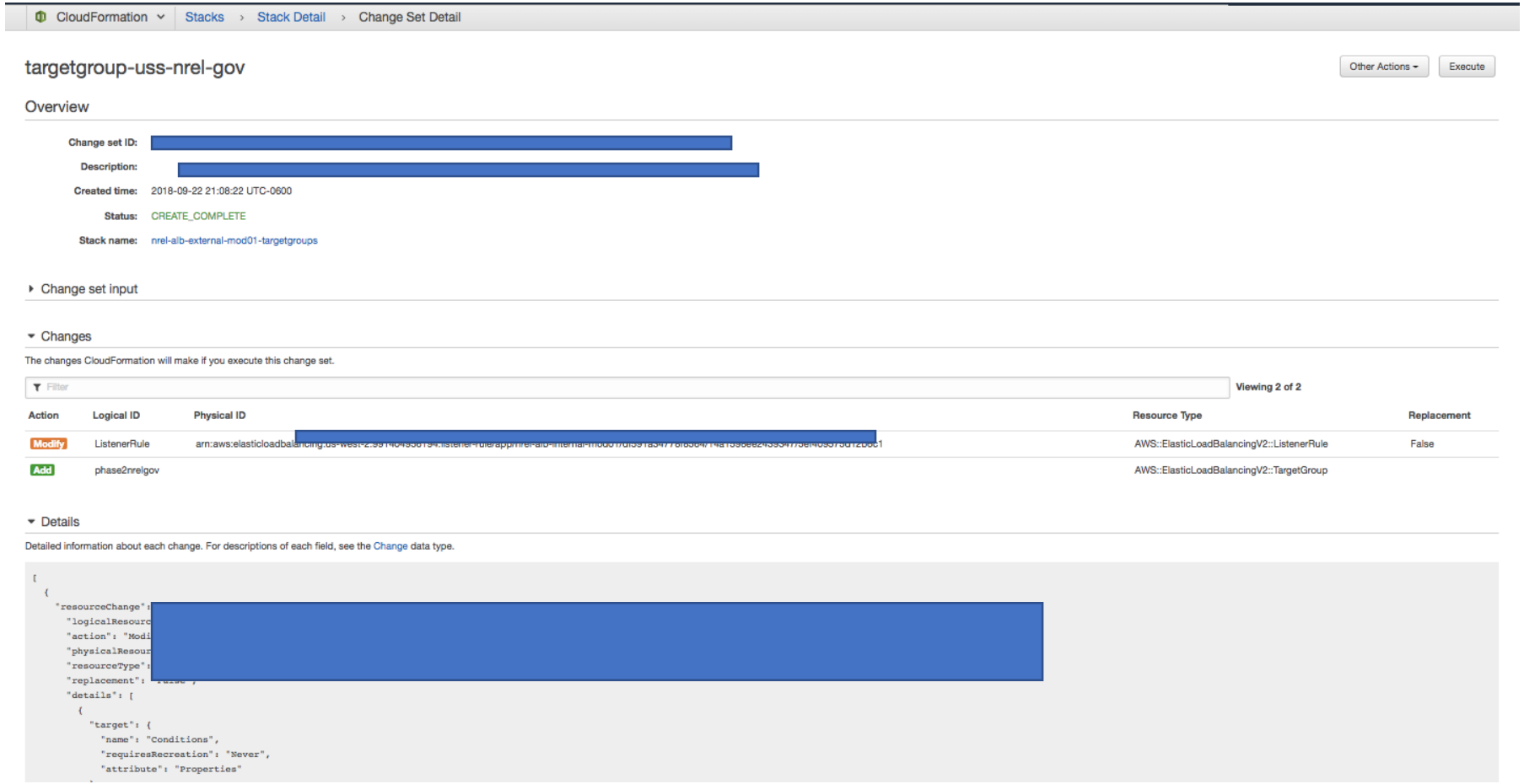
Application Delivery Control (Redirect/rewrite/internal/external access)

- Managed a bit differently - via load balancers



Change management process to be defined

- Can build a pipeline that integrates with service now process for tracking changes that impact external-facing systems.
- Cloud Team could stage changes, Networking team approves.



Pricing

Pricing is largely consumption based.

Fixed cost (per Ruleset): ~$20/month*

Per 1 million requests: $1.20

$1.20

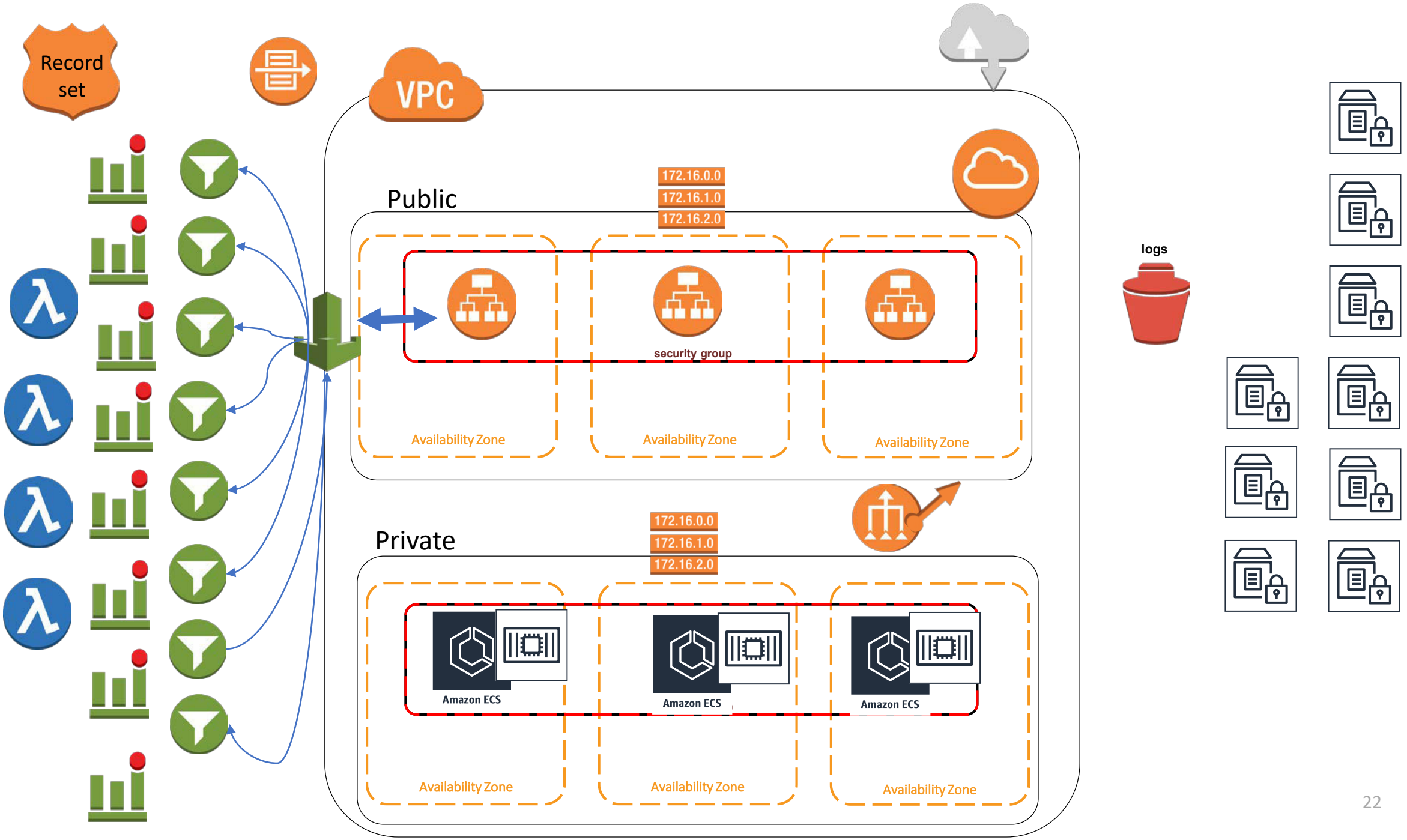
*Price is for using a 3rd party ruleset. Using native AWS rulesets is roughly ½ the cost

Reasons to NOT deploy

- Don’t have a single management plane across the enterprise
- Not best of breed?
  - Some latency on rate-based rules
  - Body inspection size limit
- Vendor lock
- Lack of expertise/training

Current Status

- Currently implemented for internal websites and one small externally-facing site
- Enhanced with third party rulesets
- Working out centralizing logs on the cyber logging platform
- Training ops team on WAF and Load balancers


Record set
VPC
Public
172.16.0.0
172.16.1.0
172.16.2.0
security group
Availability Zone
Availability Zone
Availability Zone
Private
172.16.0.0
172.16.1.0
172.16.2.0
Amazon ECS
Amazon ECS
Amazon ECS
Availability Zone
Availability Zone
Availability Zone
logs

All journeys must come to an end

AWS Web Application Firewall is a mature integrated product

Organizations and individuals need to keep up with the pace of cloud innovation

Evaluate maturity of cloud services to determine when is the right time

Work towards compliance and security – most organizations can and should do both

Well architect your systems, don’t just do it fast

Remember…developers rule the world

Resources:
https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/
https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf
https://docs.aws.amazon.com/solutions/latest/aws-waf-security-automations/template.html

NREL
Transforming ENERGY

Thank you!

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.