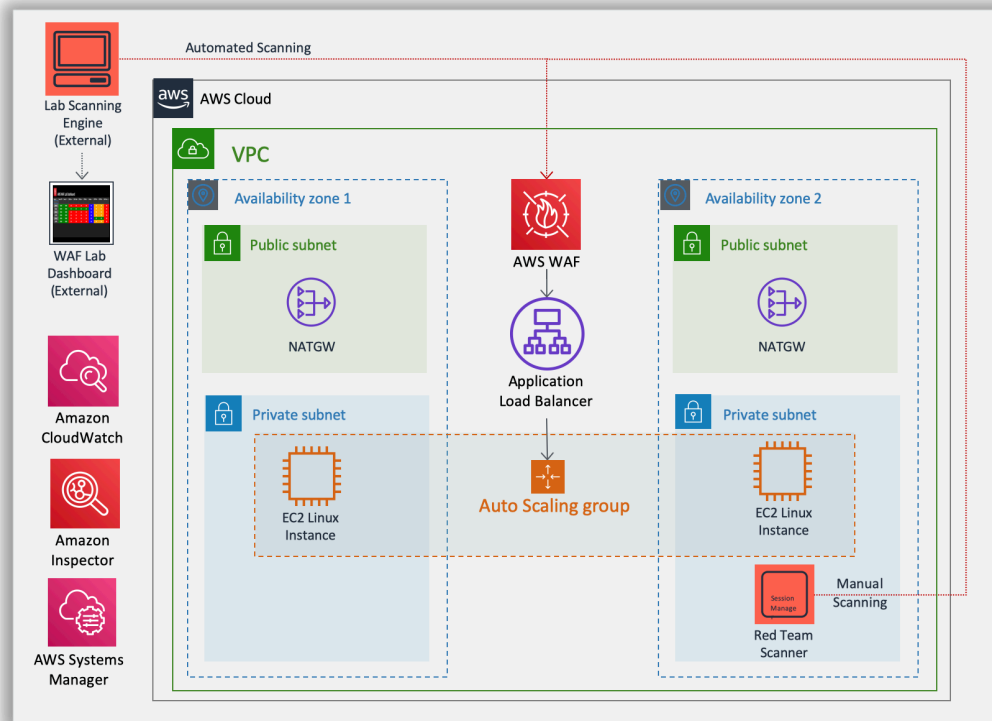


Protecting Workloads on AWS from the Instance to the Edge Companion Guide

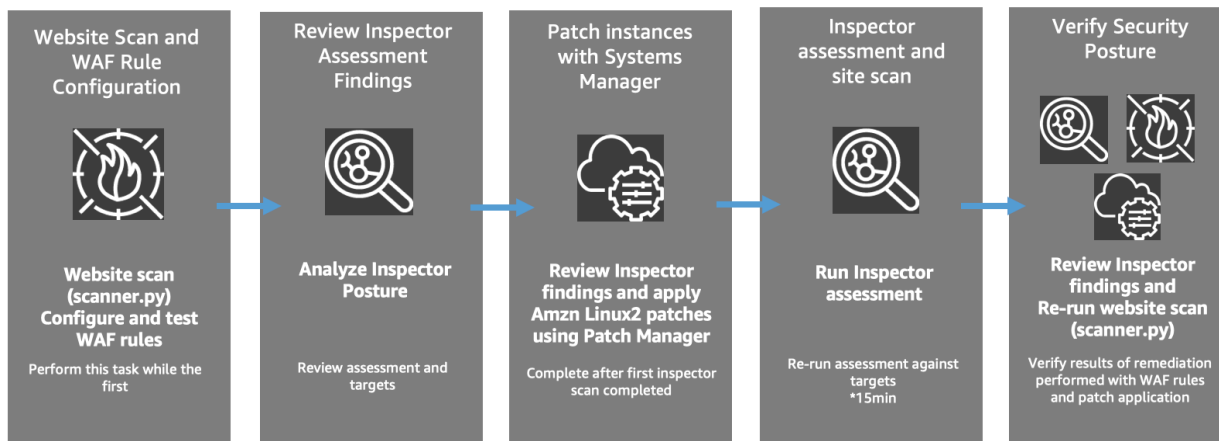
Getting Started

- Hand on Guide: <https://bit.ly/2uhcClw> or <http://protecting-workloads.awssecworkshops.com/>
- Event Engine: <https://dashboard.eventengine.run/login>

Architecture



Hands on Workflow



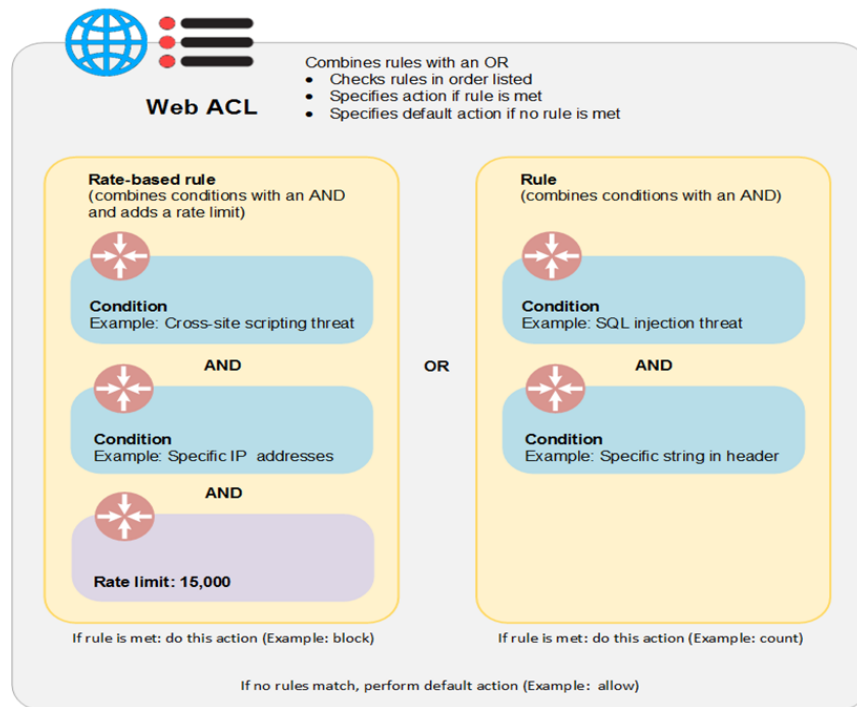
How AWS WAF Works

You use AWS WAF to control how API Gateway, Amazon CloudFront or an Application Load Balancer responds to web requests. You start by creating conditions, rules, and web access control lists (web

Protecting Workloads on AWS from the Instance to the Edge

Companion Guide

ACLs). You define your conditions, combine your conditions into rules, and combine the rules into a web ACL.



Amazon Inspector Rules Packages

3 kinds of rules packages and Severity Levels for Rules: High, Medium, Low, Informational



References

How AWS WAF Works: <https://amzn.to/2Xayoib>

Amazon Inspector Findings: <https://amzn.to/2XxrDq2>

CVE Website - <https://cve.mitre.org/>

AWS Systems Manager Patch Manager:

<https://amzn.to/2J96f11>

AWS WAF OWASP Whitepaper: <https://bit.ly/2t503Su>