DDOS Attack

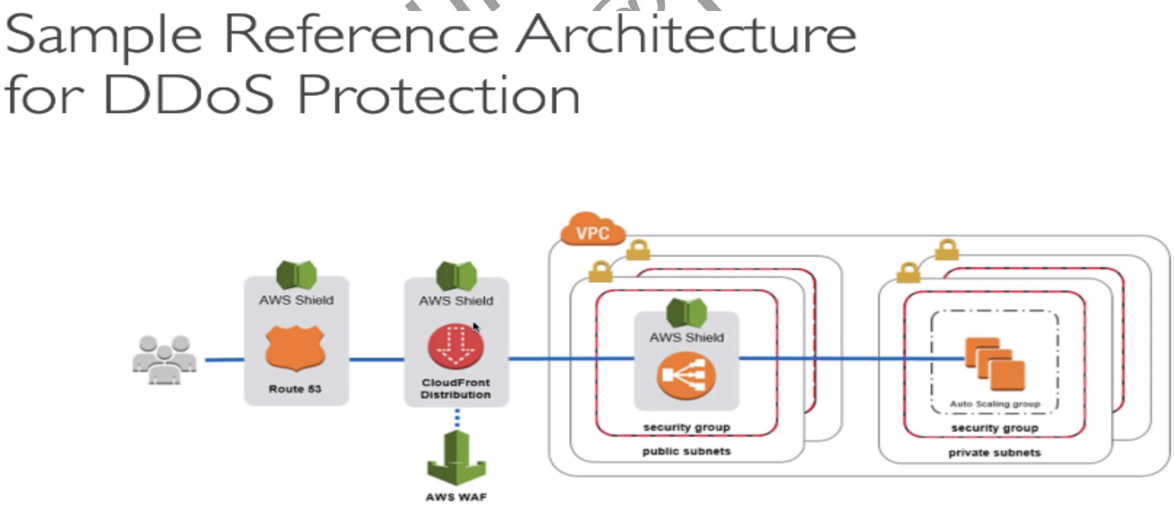
***AWS Shield Standard:**

- Protects against DDOS attack for your website and applications, for all customers at no additional costs
- AWS Shield Advanced: 24/7 Premium DDoS protection
- AWS WAF: Filter Specific requests based on rules

CloudFront and Route 53:

- Availability protection using global edge network
- Combined with AWS Shield, Provides attack migration at the edge

Be Ready to Scale – Leverage AWS Auto Scaling



Sample Reference Architecture for DDoS Protection

AWS Shield Standard:

- Free service that is activated for every AWS customer
- Provides protection from Attacks such as SYN / UDP Floods, Reflection Attacks and other layer 3/ Layer 4 attacks

AWS Shield Advanced:

- Optional DDoS mitigation service ($3000 per month per organization)
- Protect against more sophisticated attack on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
- 24/7 access to AWS DDoS response team (DRP)
- Protect against higher fees during usage spikes due to DDoS

AWS WAF – Web Application Firewall

- Protects your web applications from common web exploits (Layer 7)
- Layer 7 is HTTP (VS Layer 4 is TCP)
- Deploy on Application Load Balancer, API Gateway, CloudFront

Define Web ACL (WEB Access Control List):

- Rules can include IP addresses, HTTP headers, HTTP body, or URI Strings
- Protects from common attack – SQL injection and Cross-Site Scripting (XSS)
- Size Constraints, geo-match (Block Countries)
- Rate-based Rules (to Count occurrences of events) -for DDoS protection

Penetration Testing on AWS Cloud

- AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 Services:
  1. Amazon EC2 Instances, Nat Gateway, Elastic Load Balancers
  2. RDS
  3. CloudFront
  4. Aurora
  5. API Gateway
  6. Lambda and Lambda edge functions
  7. Lightsail resources
  8. Elastic Beanstalk Environments

Penetration Testing on your AWS Cloud

Restricted Activities:

- DNS Zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
- Port Flooding
- Protocol Flooding
- Request flooding (login request flooding, API request flooding)