Advanced Techniques for DDoS Mitigation and Web Application Defense

Dr. Andrew Kane, Solutions Architect
Giorgio Bonfiglio, Technical Account Manager

June 28th, 2017
What to expect from this session

- Types of Threats
- AWS Shield
- AWS WAF
- AWS VPC
What to expect from this session

Types of Threats

AWS Shield

AWS WAF

AWS VPC
Types of Threats

**DDoS**
- HTTP floods

**Application Attacks**
- SQL injection
- Social engineering
- Application exploits
- Sensitive data exposure

**Bad Bots**
- Crawlers
- Content scrapers
- Scanners & probes

**Application Layer**
- HTTP floods
- SQL injection
- Social engineering
- Application exploits
- Sensitive data exposure

**Network / Transport Layer**
- Reflection
- SSL abuse
- Amplification
- Slowloris
- Layer 4 floods
DDoS Threats

Network / Transport Layer DDoS
DDoS Threats

Application DDoS

- Good users
- Bad guys
- Web server
- Database
Application Threats

Good users  

Bad guys  

Exploit code  

Web server  

Database  

XSS  

SQL injection
Bad Bot Threats

Good users

Bad guys

Web server

Database

Steal premium content
What to expect from this session

Types of Threats

AWS Shield

AWS WAF

AWS VPC
Types of Threats

Application Layer
- HTTP floods

Network / Transport Layer
- Reflection
- SSL abuse
- Amplification
- Slowloris
- Layer 4 floods

Application Attacks
- SQL injection
- Sensitive data exposure
- Social engineering
- Application exploits

Bad Bots
- Crawlers
- Content scrapers
- Scanners & probes

DDoS
- Reflection
- Layer 4 floods

AWS Shield
AWS Shield

Standard Protection

Available to ALL AWS customers at No Additional Cost

Advanced Protection

Paid service that provides additional protections, features and benefits.
Benefits of AWS Shield

**AWS Integration**
DDoS protection without infrastructure changes

**Always-On Detection and Mitigation**
Minimize impact on application latency

**Affordable**
Don’t force unnecessary trade-offs between cost and availability

**Flexible**
Customize protections for your applications
AWS Shield Standard

**Layer 3/4 protection**
- Automatic detection & mitigation
- Protection from most common attacks (SYN/UDP Floods, Reflection Attacks, etc.)
- Built into AWS services

**Layer 7 protection**
- AWS WAF for Layer 7 DDoS attack mitigation
- Self-service & pay-as-you-go

*Automatic Protection against 96% of Layer 3/4 attacks*

Available globally on all internet-facing AWS services
AWS Shield Advanced

- Additional Detection & Monitoring
- Protection Against Large DDoS Attacks
- Visibility Into Attack Detection & Mitigation
- AWS WAF at No Additional Cost
- 24x7 DDoS Response Team
- Cost Protection (Absorb DDoS Scaling Cost)
AWS Shield Advanced

Multi-Layered Mitigation

Effective Against:
- Large-Scale Attack
**AWS Shield Advanced**

**Multi-Layered Mitigation**

**Effective Against:**
- SYN Floods
- Reflection Attacks
- Suspicious Sources

**Internet-Layer Mitigations**

**Border Network**

**Network Layer Mitigations**

**AWS Services**

**Web Layer Mitigations**

**Customer Infrastructure**

**DDoS Detection**

**DDoS Response Team**
AWS Shield Advanced

Multi-Layered Mitigation

Effective Against:
• SSL Attacks
• Slowloris
• Malformed HTTP
AWS Shield Advanced

Multi-Layered Mitigation

Effective Against:
• HTTP Floods
• Bad Bots
• Suspicious IPs
AWS Shield Advanced

Multi-Layered Mitigation

Effective Against:
• Sophisticated Layer 7 attacks
Shield Demo
AWS Shield Advanced

Available on ...

Application Load Balancer  Classic Load Balancer  Amazon CloudFront  Amazon Route 53

In the following regions ...

- Northern Virginia (us-east-1)
- Oregon (us-west-2)
- Ireland (eu-west-1)
- Tokyo (ap-northeast-1)
What to expect from this session

Types of Threats

AWS Shield

AWS WAF

AWS VPC
Types of Threats

Application Layer
- HTTP floods
- SQL injection
- Social engineering
- Application exploits

Network / Transport Layer
- Reflection
- SSL abuse
- Amplification
- Slowloris
- Layer 4 floods

Bad Bots
- Crawlers
- Content scrapers
- Scanners & probes

DDoS
AWS WAF
Application Attacks
Challenges of Web Application Firewalls

- Setup is complex and slow
- Too many false positives
- Limited APIs for automation
- Expensive to implement and maintain
AWS WAF

A web application firewall designed to help you defend against common web application exploits

Fast Incident Response  Flexible Rule Language  APIs for Automation  Preconfigured Protection
What is AWS WAF

- Web traffic filtering with custom rules
- Malicious request blocking
- Active monitoring and tuning
How Does AWS WAF Protect You?

- Security Automations
- Preconfigured Protections
- Highly Flexible Rule Language
Highly Flexible Rule Language

- Quick Incident Response
- Mitigations in < ~1 Min
- Inspect Any Part of the Request
Preconfigured Protections

You can get started quickly with built-in rules based on common use-cases.
Preconfigured Protections Demo
Virtual Patching Demo
Security Automations

Automated anomaly detection that you can take action on using Lambda functions.

✓ Dynamic Rules Based on Anomaly
✓ Using Lambda & Service Logs
Security Automations

Traditional incident response

Diagram showing good users, bad guys, AWS WAF, Server, Logs, Threat analysis, Notification, Security engineer, Preconfigured Protections, and Highly Flexible Rules Engine.
Security Automations

Next-generation incident response

Diagram showing the flow of good users and bad guys through a system involving AWS WAF, logs, threat analysis, notification, and the highly flexible rules engine.
What to expect from this session

Types of Threats
AWS Shield
AWS WAF
AWS VPC
What customers asked for…

✓ Private IP space in AWS
✓ Familiar networking model
✓ Customer-defined networking logic
✓ Strong security controls
✓ Private connectivity to their data centers
Key Features of VPC

Choosing an address range

Setting up subnets in Availability Zones

Creating a route to the Internet

Authorizing traffic to/from the VPC
VPC Controls

Private Subnet (Web Tier)
- SG-Web
- 10.0.2.0/24

Private Subnet (App Tier)
- SG-App
- 10.0.3.0/24

Public Subnet
- SG-ALB
- 10.0.1.0/24
Simple Approach

- Public Subnet
  - 10.0.1.0/24
  - SG-ALB
  - Allow all traffic
  - Allow 10.0.1.0/24

- Private Subnet (Web Tier)
  - 10.0.2.0/24
  - SG-Web
  - Allow 10.0.2.0/24

- Private Subnet (App Tier)
  - 10.0.3.0/24
  - SG-App
  - Allow 10.0.3.0/24
Secure Approach

- VPC
- Private Subnet (Web Tier)
  - SG-Web
  - SG-Web
  - SG-Web
- Private Subnet (App Tier)
  - SG-App
  - SG-App
  - SG-App
- Public Subnet
  - SG-ALB
  - Allow CloudFront IP Ranges only
  - 10.0.1.0/24
  - 10.0.2.0/24
  - 10.0.3.0/24
- SG-Web only
- SG-App only
- SG-ALB only

Allow SG-ALB only
Allow SG-Web only
Security Groups + CloudFront IP ranges

Blog Post here -> http://amzn.to/2fj4Q8e
Thank you!