TREND MICRO

Security
TRENDS 2018

aws

DDoS 대응을 위한 AWS 모범 사례

Amazon Web Services
이경수 솔루션즈 아키텍트

- DDoS 대응을 위한 AWS Best Practices
- AWS Shield 서비스 소개

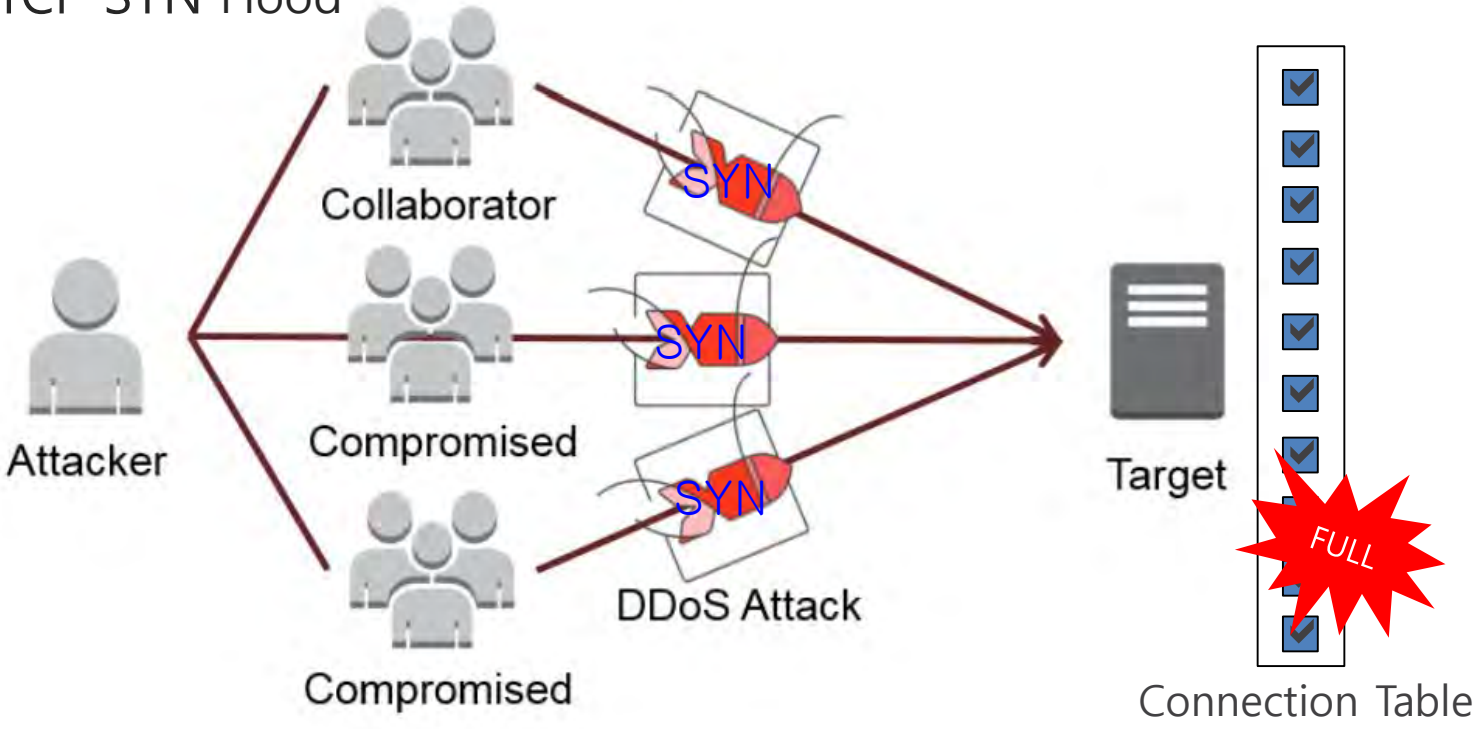
DDoS 트랜드

TREND MICRO | Security TRENDS 2018

- 인프라 레벨 공격 (Layer 3 / 4)
  - 평균 공격 규모 900Mbps (50%는 500Mbps 이하)
  - 전체 공격중 78% 는 인프라레벨에서 발생(공격의 용이성)
- 어플리케이션 레벨 공격 (Layer 7)
  - 나머지 22% 는 포트 80 & 443 에 대한 공격(보다 복잡함)
- 멀티 팩터 – 동시에 다른 형태의 공격 조합
- 증폭 공격(NTP, SSDP, DNS, Chargen, SNMP)
- Hit and run DDoS (91% < 1 시간), 연막 공격 비중(16-18%)

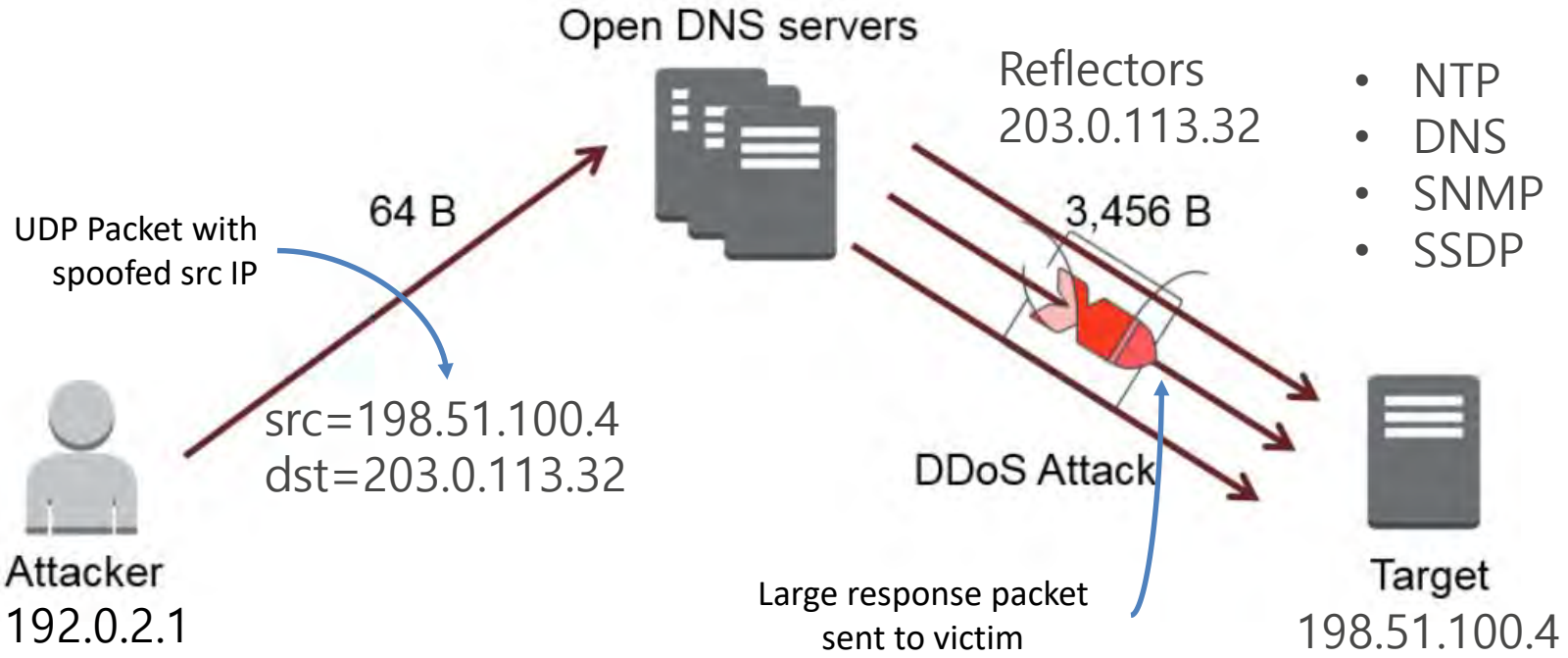
전형적인 인프라 레벨의 공격 – L3/4

- TCP SYN Flood

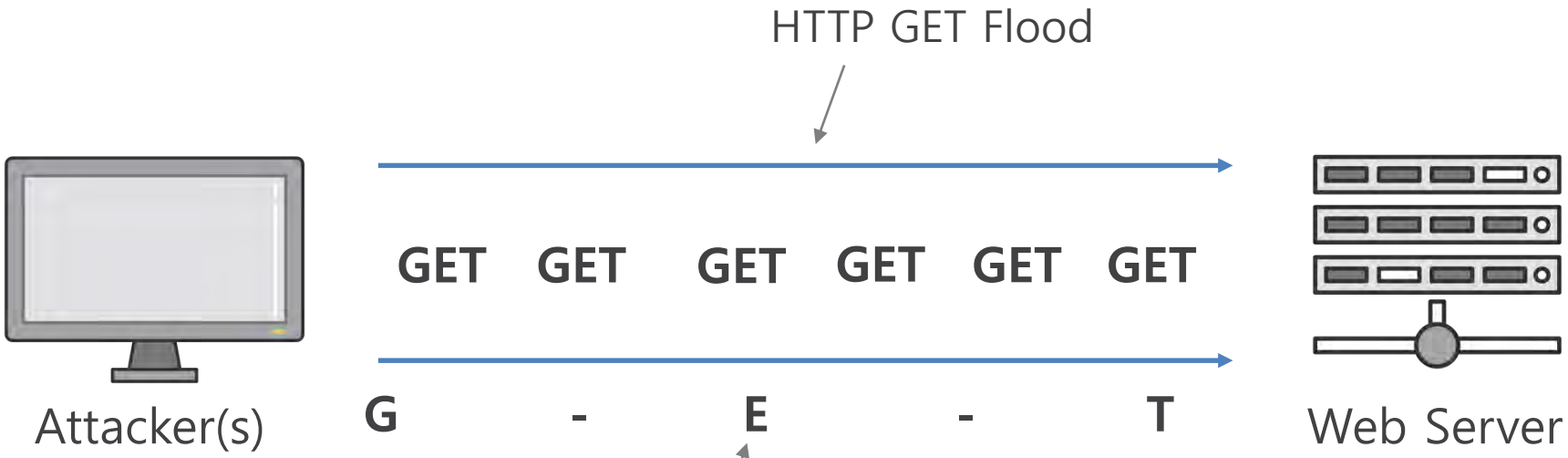


반사/증폭 공격 – Layer 3/4

- UDP (DNS) Amplification Flood



전형적인 어플리케이션 레벨의 공격 - L7



그외, cache-busting attack, WordPress XML-RPC flood 등

OSI 모델 계층별 대표 공격유형

TREND MICRO Security TRENDS 2018

각 계층에서 발생하는 공격의 유형이 상이하고 대응 방식도 완전히 다르기 때문에, 이와 같은 구분을 이해하는 것이 굉장히 중요

#	계층	유닛	설명	대표적인 공격 벡터
7	응용(Application)	데이터	어플리케이션에 대한 네트웍 프로세스	HTTP floods, DNS query floods
6	표현(Presentation)	데이터	데이터 표현과 암호화	SSL abuse
5	*세션(Session)*	*데이터*	*호스트 간 통신*	*N/A*
4	전송(Transport)	세그먼트	종단 간 연결 및 신뢰성	SYN floods
3	네트웍(Network)	패킷	경로 결정과 논리적인 어드레싱	UDP reflection attacks
2	*데이터 링크(Data Link)*	*프레임*	*물리적인 어드레싱*	*N/A*
1	*물리(Physical)*	*비트*	*미디어, 시그널,바이너리 전송*	*N/A*

6가지 효과적인 대응 방안

TREND MICRO | Security TRENDS 2018

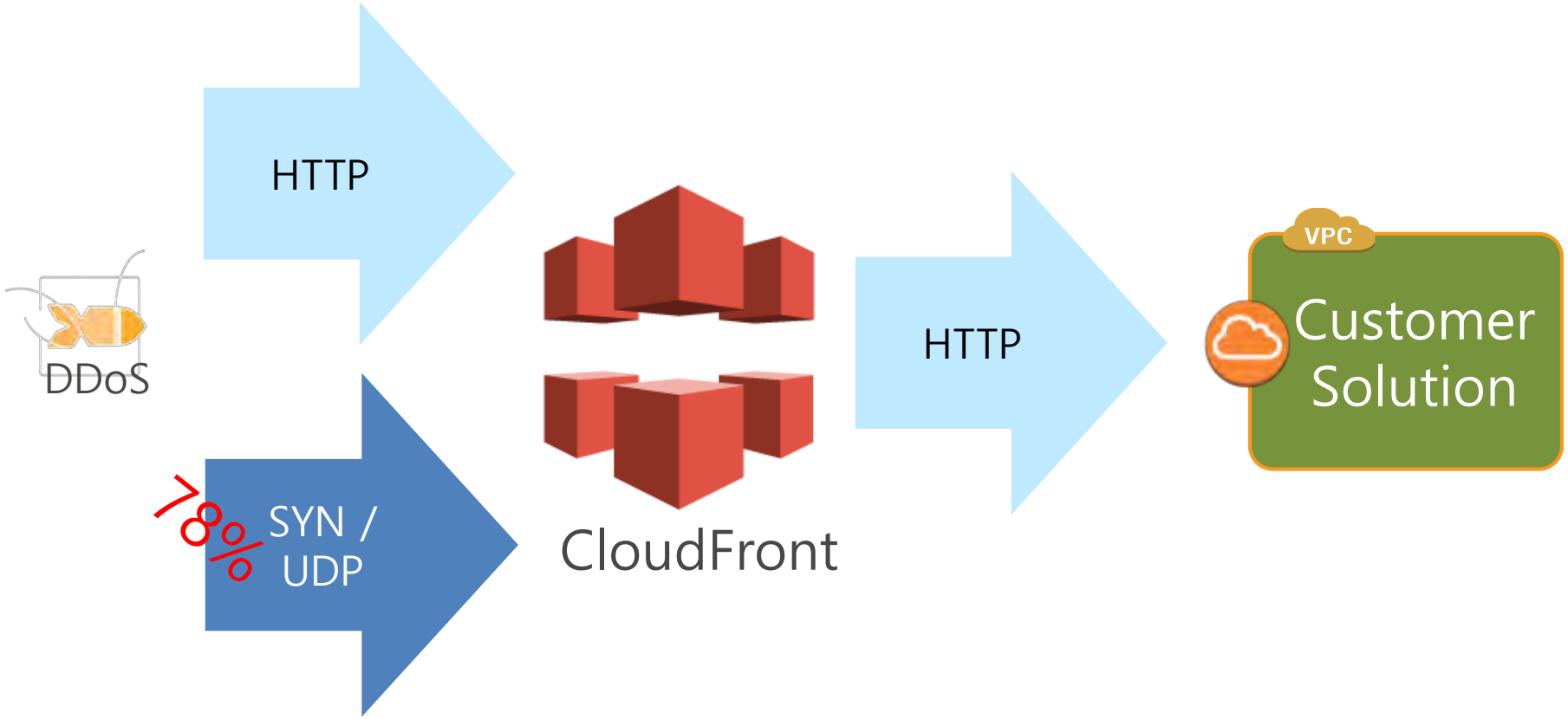
1. AWS 서비스들을 앞단에 배치하세요.
2. 공격지점을 최소화 시키세요.
3. 노출된 리소스에 대한 대책을 세우세요.
4. 공격을 흡수할 수 있는 확장성을 구현하세요.
5. 정상 상태에 대한 기준을 확립하세요.
6. 공격에 대응하기 위한 계획을 수립하세요.

1. AWS 서비스들을 앞단에 배치

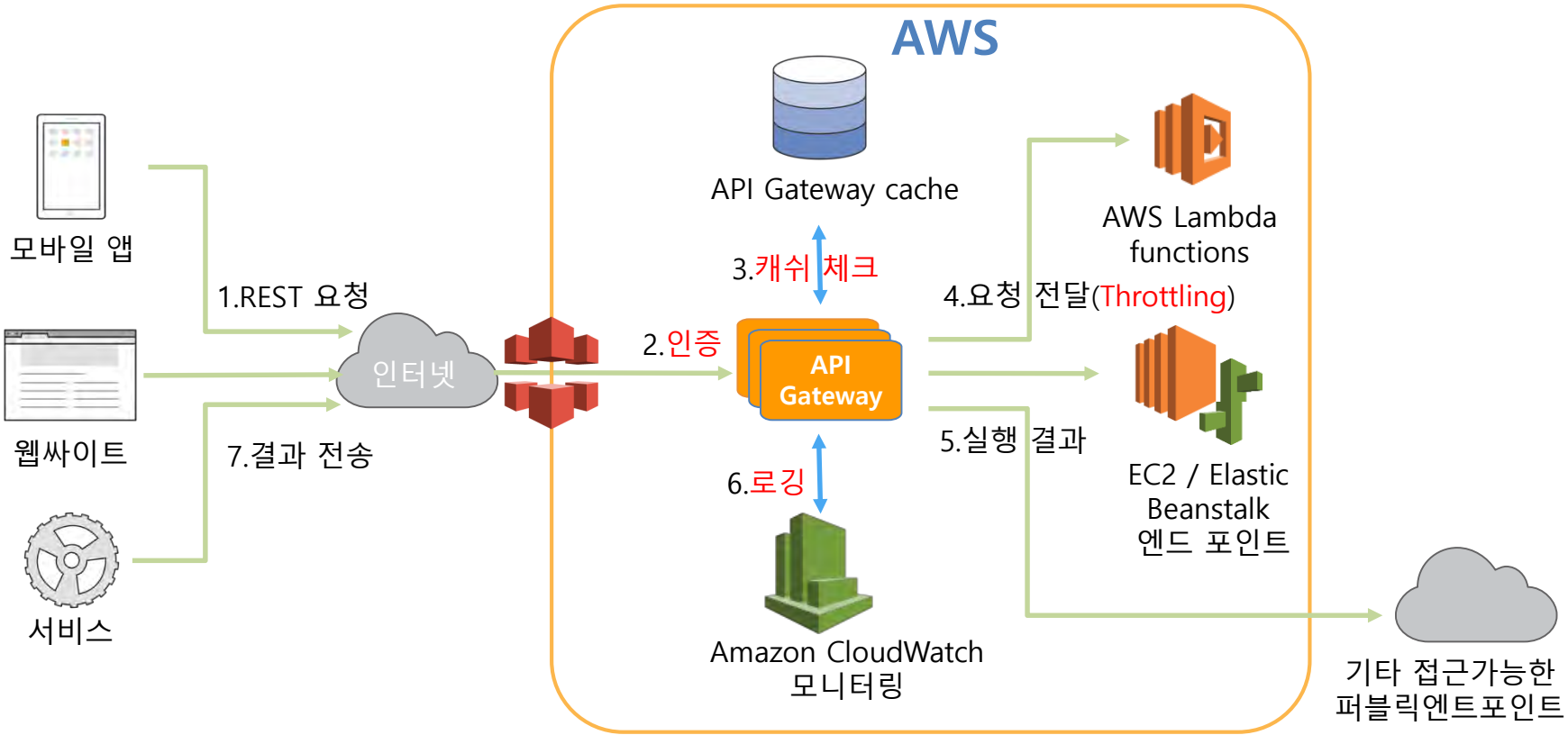
TREND MICRO | Security TRENDS 2018

- 레이어 3/4 공격을 방어하기 위해 Amazon API Gateway 나 Amazon CloudFront와 같은 AWS서비스들을 어플리케이션 앞단에 배치 ➔ 캐싱기능을 통해 성능 및 보안성 향상
- Amazon API Gateway가 제공하는 기능:
    - User authentication.
    - Request throttling.
    - Response caching.
    - Requests logging.

VPC가 Layer 7 트래픽만 받도록 구성



Amazon API Gateway의 요청 플로우



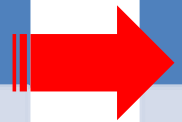
AWS 플랫폼 서비스 보안기능을 이용하여 워크로드 줄이기

손상되기 쉬운 백엔드 컴포넌트 보호

2. 공격지점을 최소화

공격 지점을 최소화할 수 있는 아키텍쳐

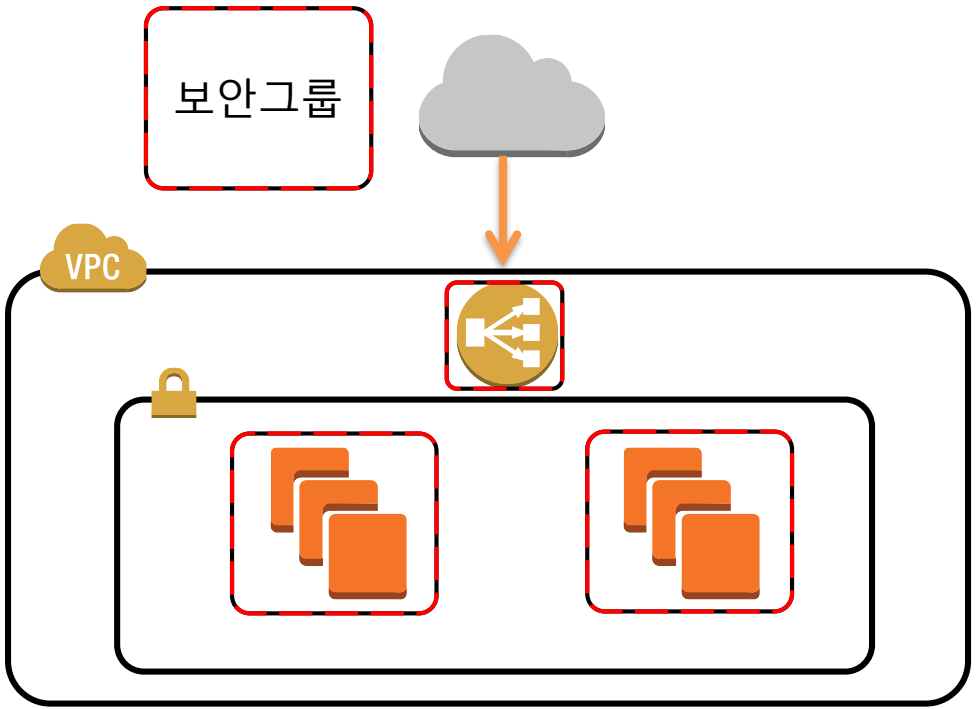
- 인터넷 연결지점 최소화
- 사용자와 관리자 트래픽 분리
- 적법한 사용자와 트래픽만 허용



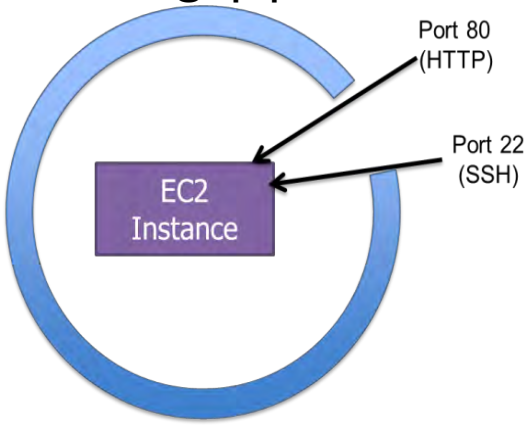
VPC를 이용하여 공격지점 최소화

- VPC와 Internet Gateway 구성
- 보안그룹 구성
- Network ACL 구성
- VPC 상에서 인스턴스 기동

AWS 방화벽 – Security Group



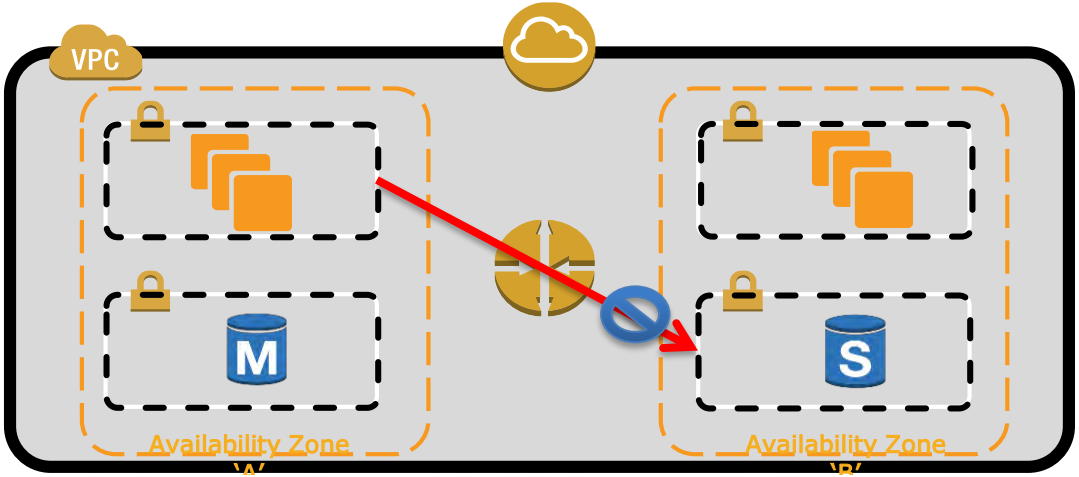
- **보안그룹 규칙**
  - **적용포인트 : 인바운드/아웃 바운**
  - **Protocol : 모든 인터넷 프로토콜 지원**
  - **IP/Port 에 대한 접속 허용/차단**
  - **Stateful 방화벽**



AWS 보안 서비스 - Network ACL

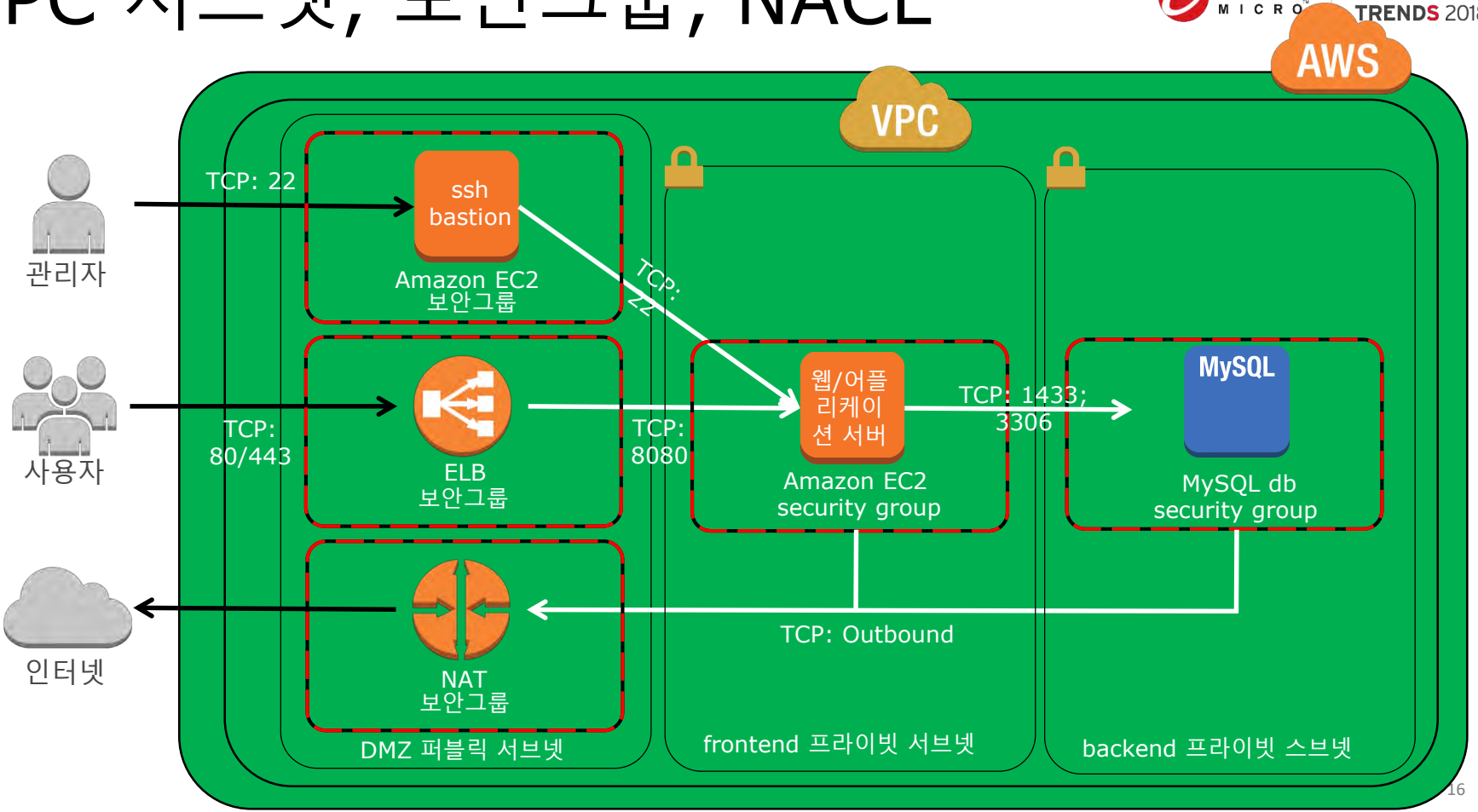
TREND MICRO Security TRENDS 2018

Subnet ACL 예시



Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	HTTP (80)	TCP (6)	80	10.1.0.0/16	ALLOW
101	HTTPS (443)	TCP (6)	443	10.1.0.0/16	ALLOW
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	DENY
201	HTTPS (443)	TCP (6)	443	0.0.0.0/0	DENY
1000	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

VPC 서브넷, 보안그룹, NACL



3. 노출된 리소스에 대한 대책

- CloudFront 리소스에 대한 제한된 접근
  - 불필요한 지역 blocking, Origin Access Identity(S3)

- Route 53을 통해 DNS 노출 정보 최소화
  - Create hosted zone: www.example.com
  - Create A record set
  - Create alias to CNAME
  - Point alias to CloudFront URL
  - Point CloudFront origin to ELB

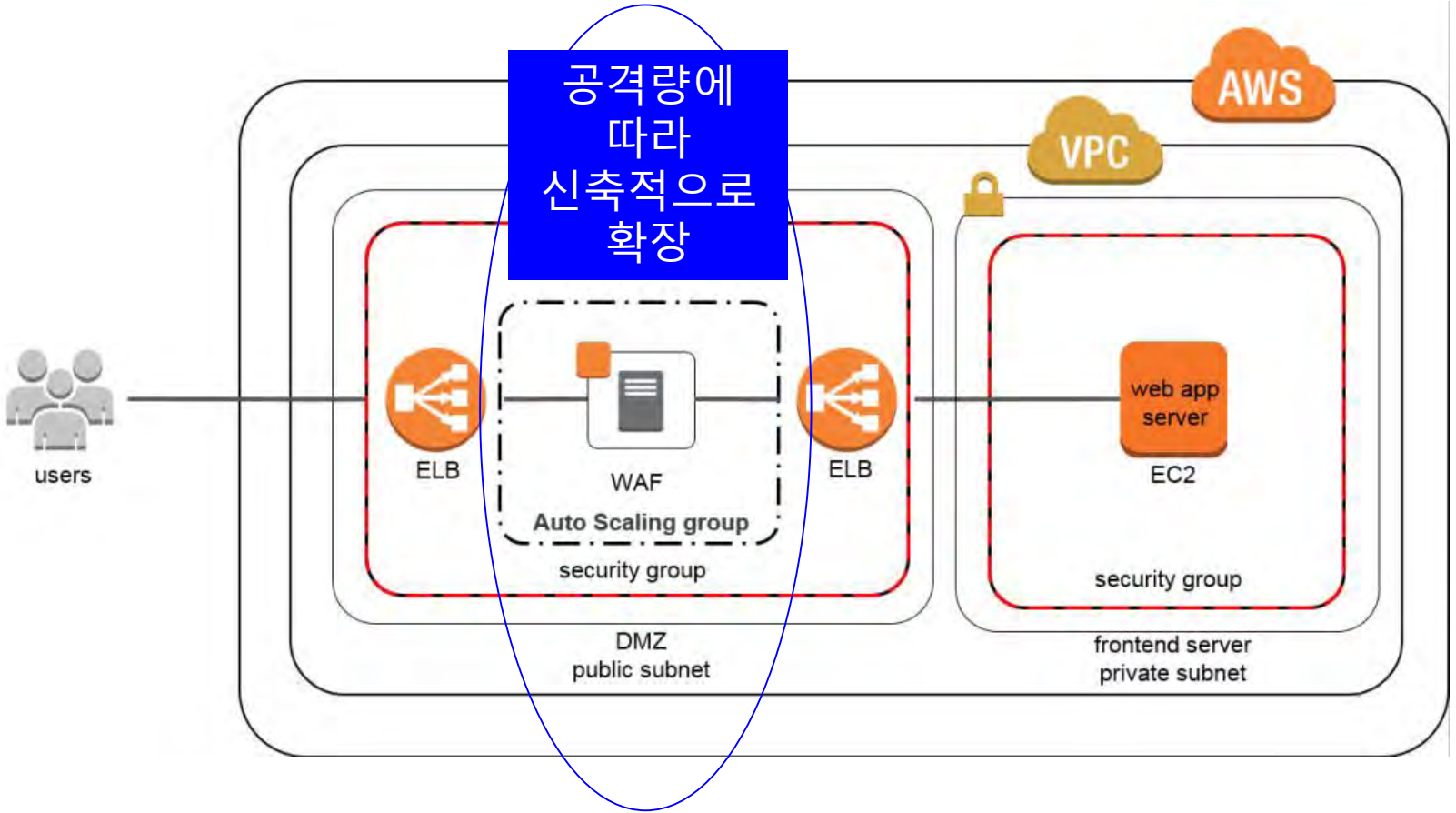
- 3rd party WAF를 통해 어플리케이션 보호
  - Request rate limits
  - 특정 유형의 요청 블락

비싼 리소스에 대한 보호조치 – WAF

TREND MICRO | Security TRENDS 2018

- 확장이 쉽지 않은 백엔드 리소스에 대한 보호
- WAF : 어플리케이션 레이어의 트래픽들을 조사하고 필터링 – HTTP & HTTPS
  - OWASP Top 10
  - Rate Limiting
  - Whitelist / Blacklist (Customizable Rules)
  - Native Auto Scaling with WAF Sandwich
  - Learning Engine
- Benefits
  - ACLs 을 보완해줌(누가 공격하고 있는지 정확히 파악할 필요성 경감)
  - 적법한 사용자에게 가용성 제공

WAF 샌드위치 아키텍쳐

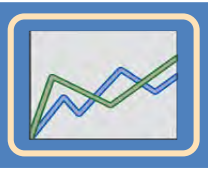


4. 공격을 흡수할 수 있는 확장성

TREND MICRO | Security TRENDS 2018

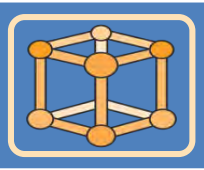
- AWS 를 통한 수직적 / 수평적 확장성 구현

공격을 넓은 지역으로 소산시켜줌



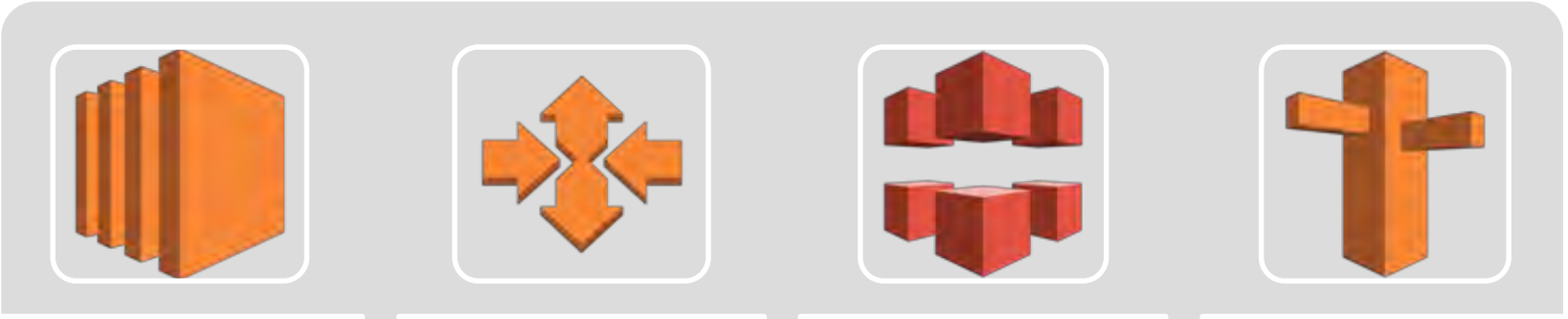
공격자가 공격규모를 늘리는데 많은 리소스가 필요하게 해줌

DDoS공격을 분석하고 대응하기 위한 시간을 벌어줌



덤으로 장애 시나리오에 대비한 아키텍쳐

AWS 환경을 통한 수직적 / 수평적 확장

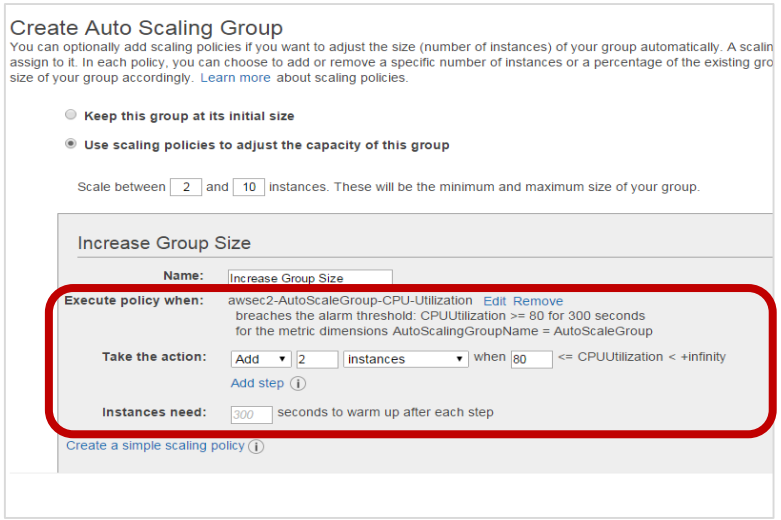


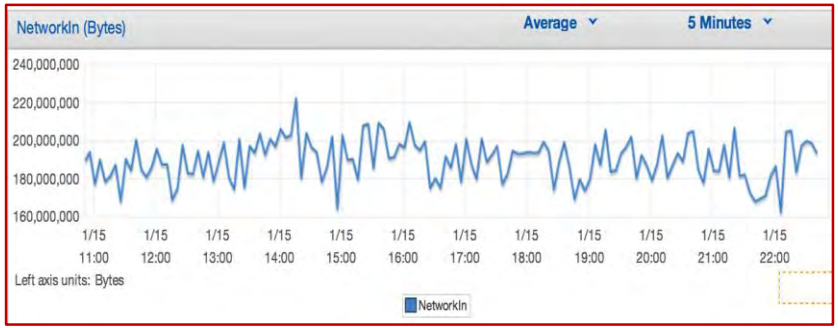
EC2 Enhanced Networking 활성화	Elastic Load Balancing & Auto Scaling 설정	Amazon CloudFront를 통해 지역별로 분산	Amazon Route 53의 Shuffle Sharding, Anycast Routing을 통한 가용성 향상

- 공격자가 더많은 노력을 쏟아야...
- 인스턴스, 네트웍에 대한 유연성
- 생각하고 대응할 시간을 제공

5. 정상 상태에 대한 기준을 확립

- CloudWatch를 통해 정상 사용 수준에 대한 이해와 측정
- 비정상 수준 또는 공격 패턴을 판별하는 명확한 기준으로 활용
- 공격 과정에 대한 모니터링 및 기록
- 오토스케일링 정책의 조건으로서 CloudWatch 알람 이용



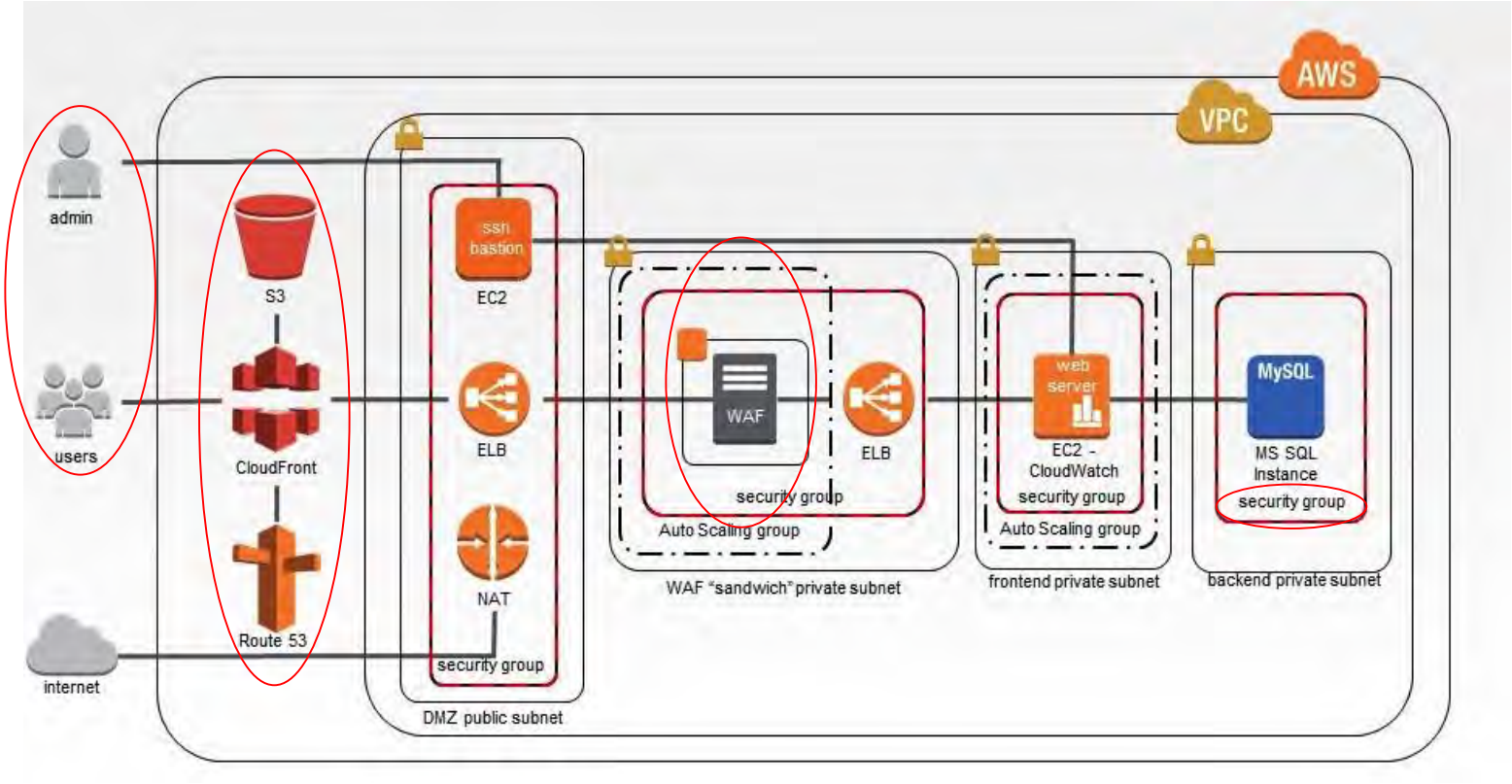


6. 공격에 대응하기 위한 계획 수립

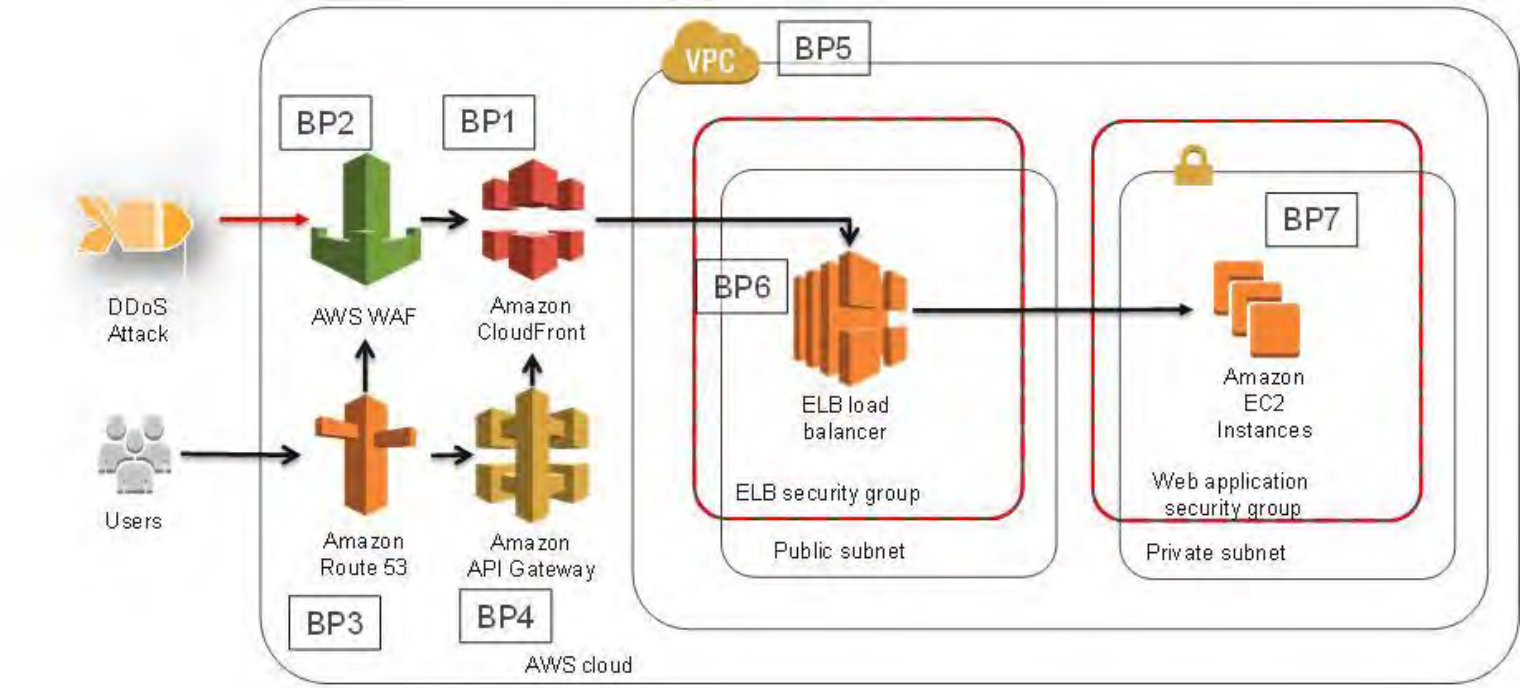
TREND MICRO | Security TRENDS 2018

- 공격을 대비하여 다음을 확인:
  - 복원력있는 아키텍쳐인지 ➔ 수립한 아키텍쳐에 대한 검증 및 사전 기능 테스트 (AWS에 사전 공지)
  - 공격 수용시 서비스 확장의 규모 및 비용에 대한 부분 고려
  - 공격 받을 경우 비상 연락망

권장 아키텍쳐 1

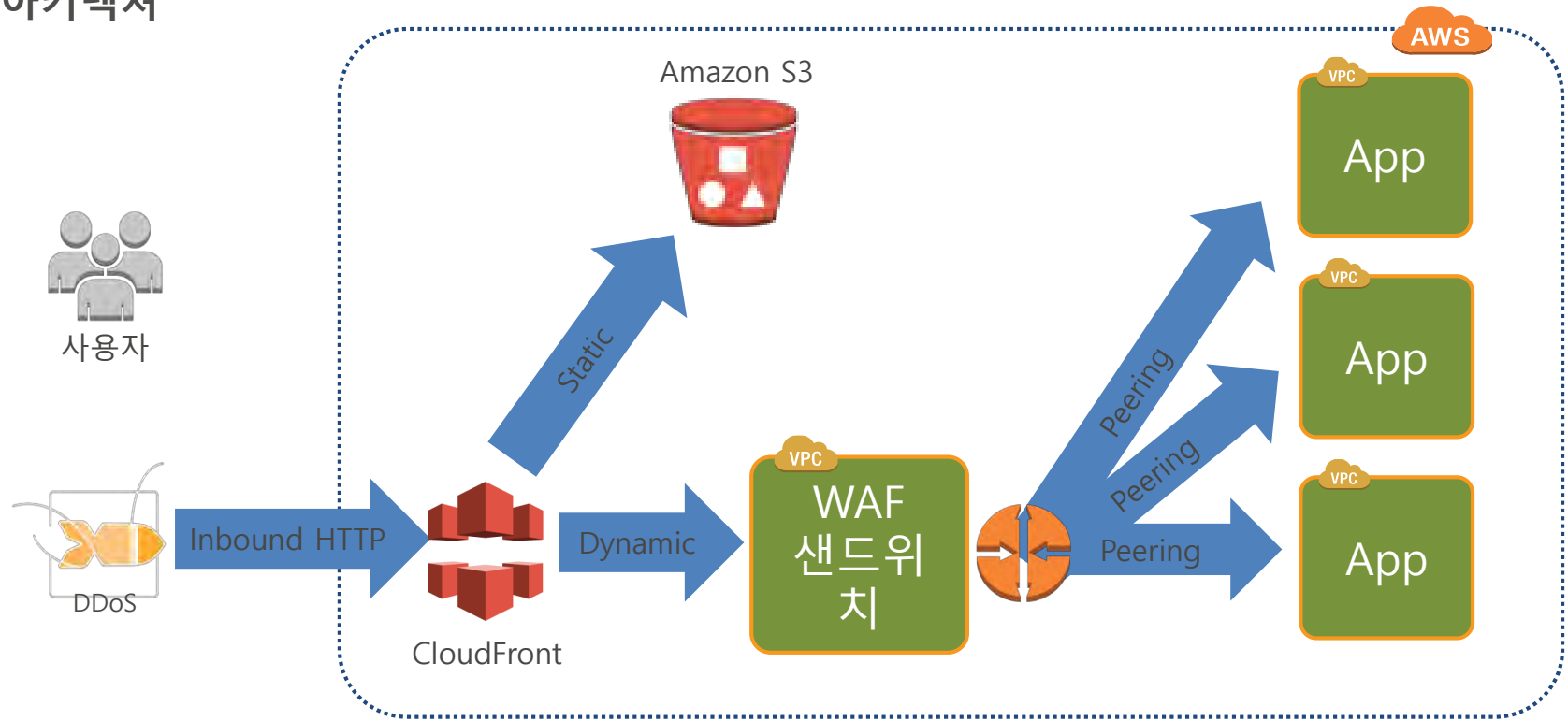

AWS
VPC
admin
users
internet
S3
CloudFront
Route 53
ssh bastion
EC2
ELB
NAT
security group
DMZ public subnet
WAF
ELB
security group
Auto Scaling group
WAF "sandwich" private subnet
web server
EC2 - CloudWatch
security group
Auto Scaling group
frontend private subnet
MySQL
MS SQL Instance
security group
backend private subnet

권장 아키텍쳐 2


VPC
BP5
BP2
BP1
BP6
BP7
DDoS Attack
AWS WAF
Amazon CloudFront
ELB load balancer
Amazon EC2 Instances
ELB security group
Web application security group
Users
Amazon Route 53
Amazon API Gateway
Public subnet
Private subnet
BP3
BP4
AWS cloud

권장 아키텍쳐 – 인바운드 제어

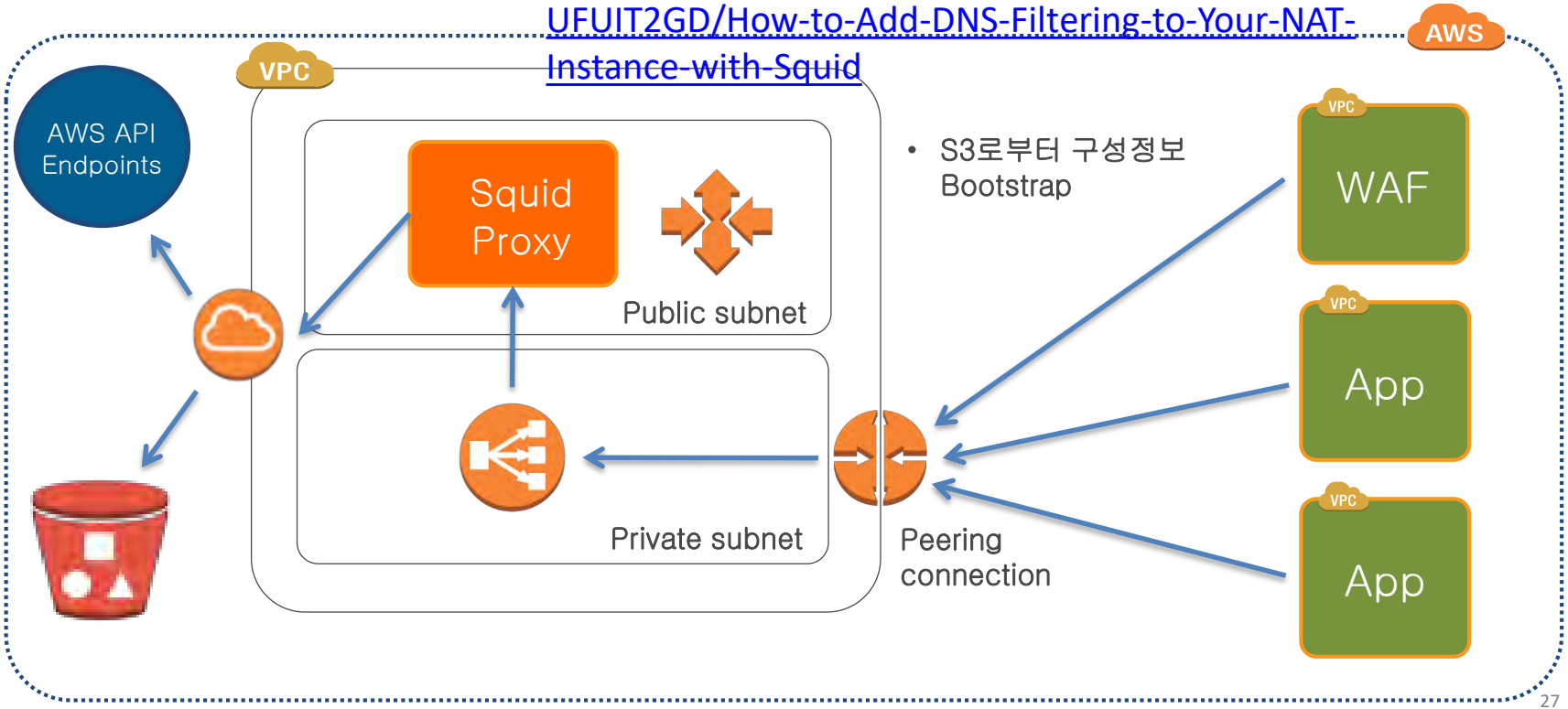
VPC peering기능을 이용하여 다수의 어플리케이션을 지원할 수 있는 확장성 있는 아키텍쳐



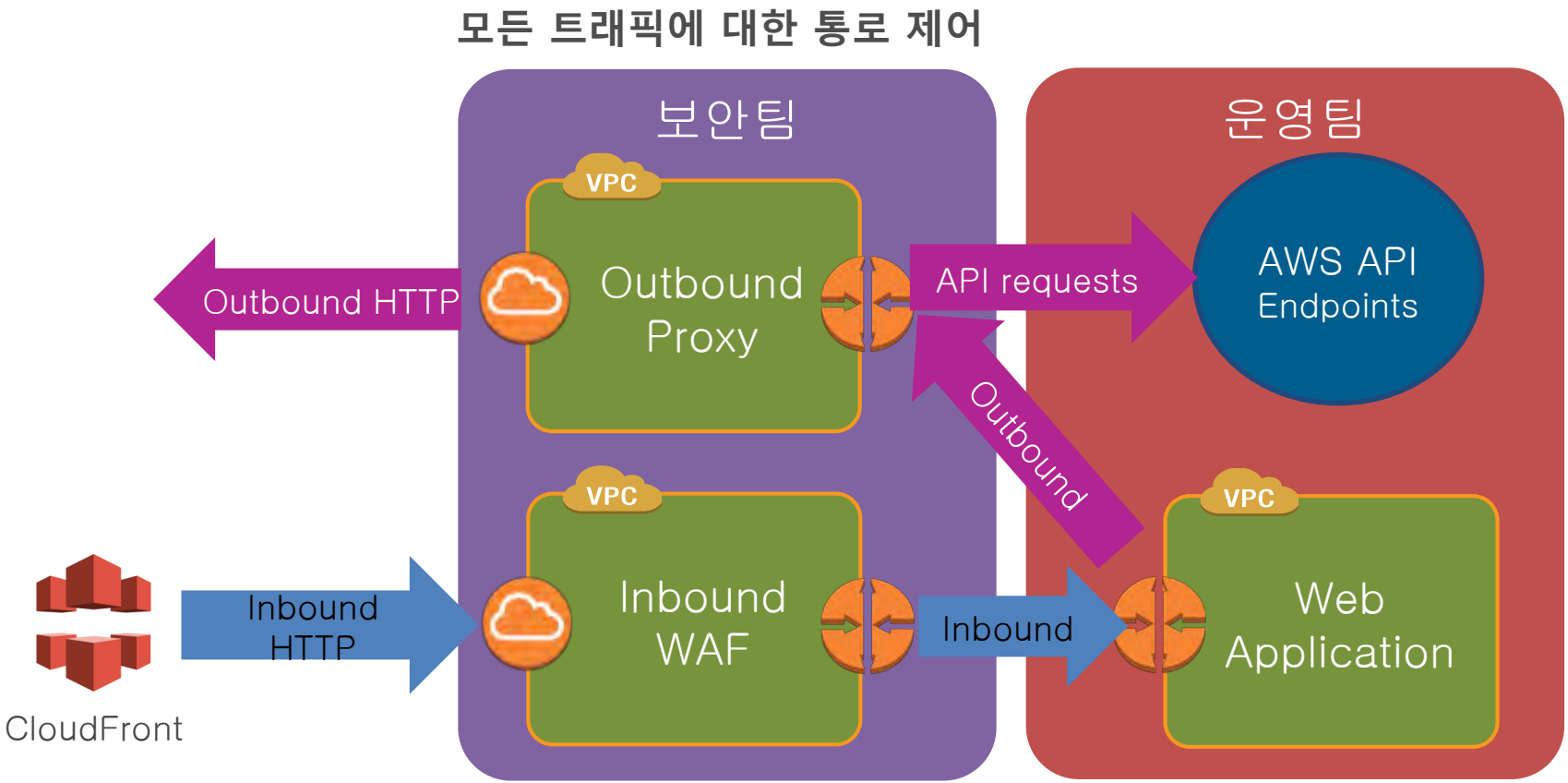
권장 아키텍쳐 – 아웃 바운드 제어

모든 HTTP 및 API 접근에 대한 아웃 바운드 트래픽을 프록시를 통하도록 구성 – 중요 데이터 유출 검사

https://blogs.aws.amazon.com/security/post/TxFRX7UFUIT2GD/How-to-Add-DNS-Filtering-to-Your-NAT-Instance-with-Squid



권장 아키텍쳐


모든 트래픽에 대한 통로 제어
보안팀
운영팀
VPC
Outbound HTTP
Outbound Proxy
API requests
AWS API Endpoints
Outbound
VPC
VPC
Inbound HTTP
Inbound WAF
Inbound
Web Application
CloudFront

얼마나 빨리 대응할 수 있는가에 대한 문제

- 보안은 빅데이터
  - 공격의 징후를 정확히 판정하기 위해 로그를 남기고 취합.
  - 어떻게 AWS서비스들을 활용하여 도움을 받을 수 있을지.
- 지능적이고 즉각적인 대응
  - Cloudwatch alarm 기능을 활용하여 WAF 규칙을 자동으로 업데이트 하는 워크플로를 구성 – AWS lambda를 이용하여 의심되는 Source IP를 WAF Rule 조건에 포함
  - 실시간 WAF 규칙 업데이트 – 예: 특정 IP로부터 5분간 5번이상 공격을 받은 경우, 그 IP로부터의 접근을 30분동안 막음.

AWS Shield

관리형 DDoS 보호 서비스

Standard Protection

별도 비용 없이 모든 AWS 고객들이 이미 사용 중!

Advanced Protection

대규모 혹은 복잡한 공격으로부터 서비스를 보호하는 유료 서비스

AWS Shield Standard

레이어 3/4 보호

- ✓ 자동 탐지 및 대응
- ✓ 가장 흔한 공격유형에 대한 방어 (SYN/UDP Floods, Reflection Attacks, 등)
- ✓ AWS 서비스에 밀결합

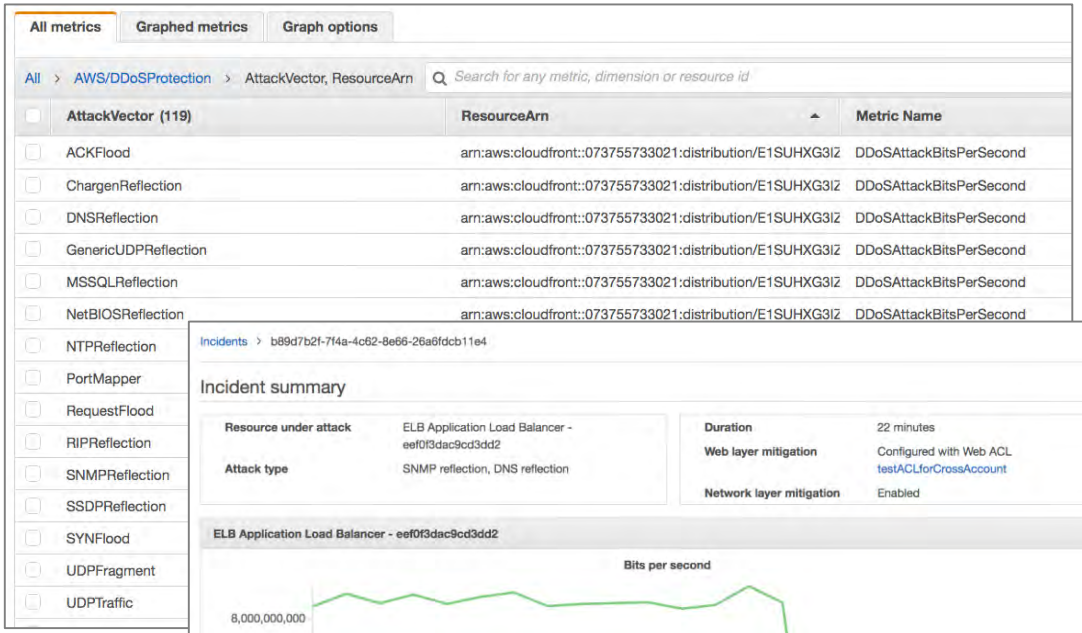
레이어 7 보호

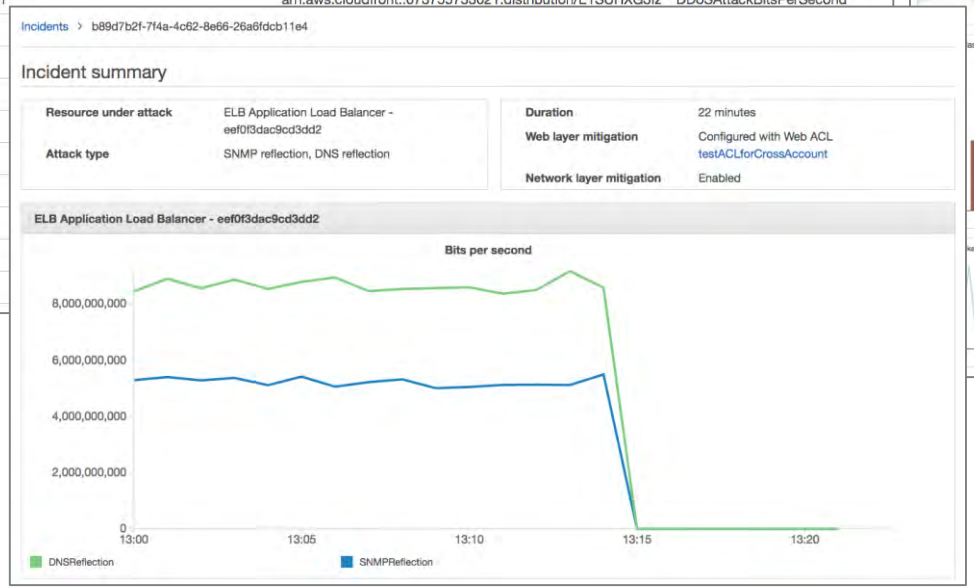
- ✓ 레이어 7 디도스 공격 대응을 위해 AWS WAF 활용
- ✓ 셀프서비스 및 사용량 과금

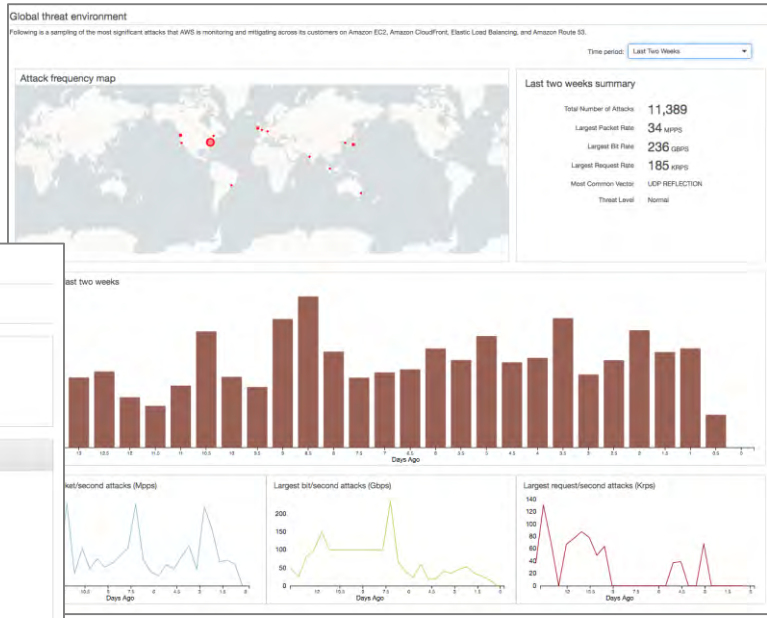
AWS Shield Advanced

- 관리형 Anti-DDoS 서비스
- 네트워크 에지 단에서 분산형 보호
- AWS 리전내의 ALB/ELB 단에서 보호
- AWS WAF 기본제공
- DDoS Response Team (DRT) 지원
- 공격 수용에 따른 AWS자원 사용비용 경감

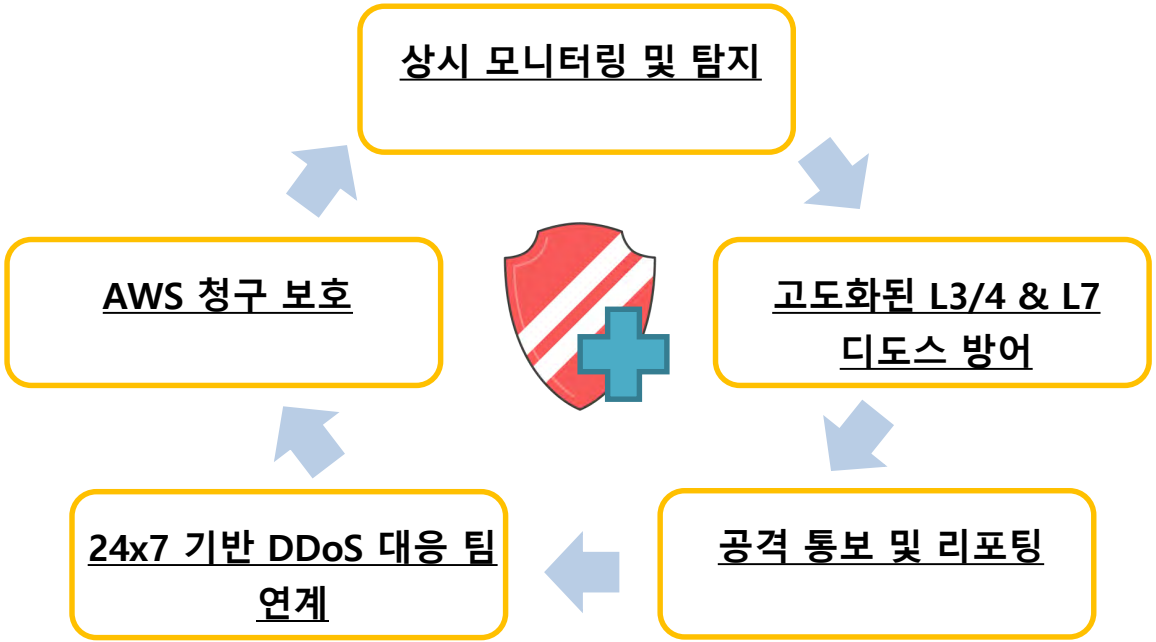
AWS Shield Advanced 콘솔







AWS Shield Advanced

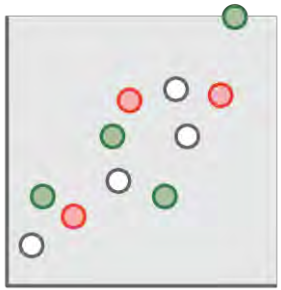


상시 모니터링 및 탐지

시그니쳐 기반 탐지

휴리스틱 기반
비정상 상태 탐지

- 소스 IP
- Traffic levels
- 검증된 소스



기본 패턴 비교

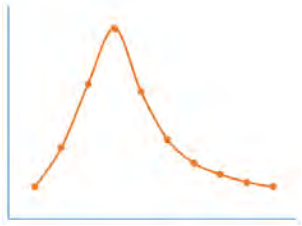
- 초당 HTTP 요청 수
- 소스 IP 주소
- URLs
- User-Agents

레이어 3/4 인프라 방어

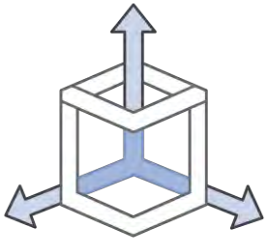
고도화된 방어 기법들

필터링 규칙

- IP checksum
- TCP valid flags
- UDP payload length
- DNS request validation



점수 기반 트래픽 처리 순위화

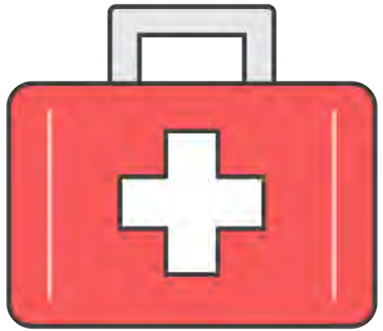


고도화된 라우팅 정책

24x7 기반 DDoS 대응 팀 연계

- 중대하고 급박한 우선순위의 케이스에 대해 신속하게 답변이 제공될 수 있도록 디도스 전문가와 직접 연결됨

- 복잡한 케이스를 AWS 및 아마존을 비롯한 기타 서비스들을 보호하고 있는 경험많은 AWS 디도스 대응팀(DRT)으로 바로 요청할 수 있음.



TREND MICRO

Security
TRENDS 2018

THANK YOU

Amazon Web Services
이경수 솔루션즈 아키텍트