AWS Shield & WAF

Proserve
김수종
2025/01/16

AWS WAF (Web Application Firewall)

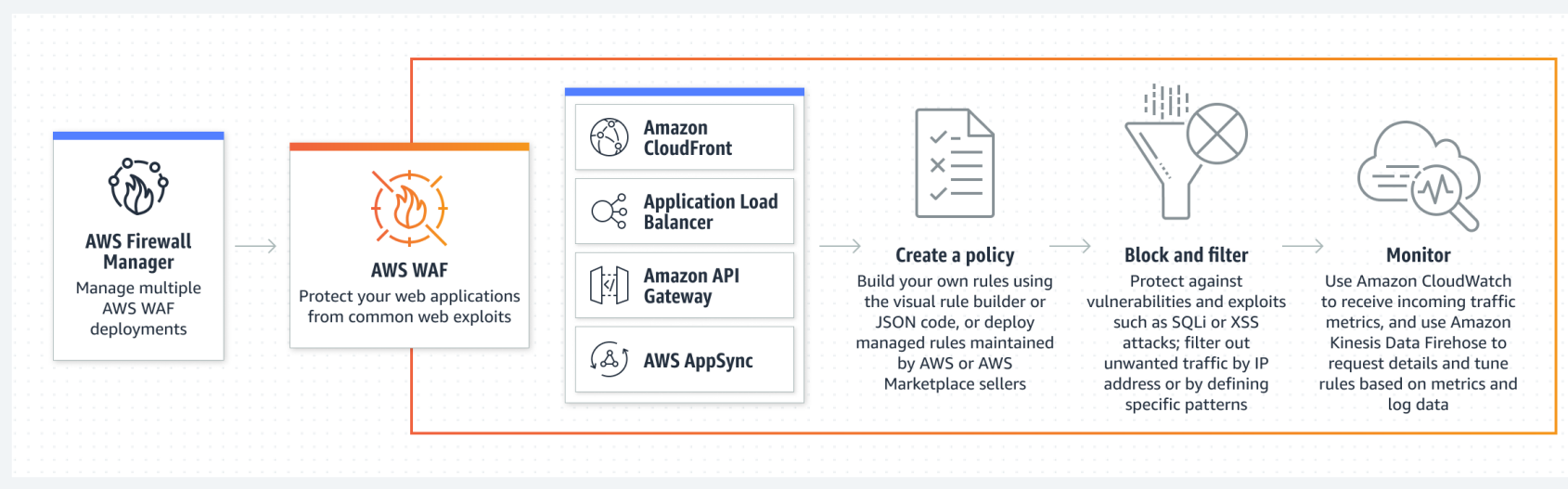
AWS WAF 개요

1. AWS WAF 란?

- 외부로 부터 유입되는 OWASP TOP 10 기반 웹해킹 공격에 대한 탐지 및 차단
- 적용가능 리소스

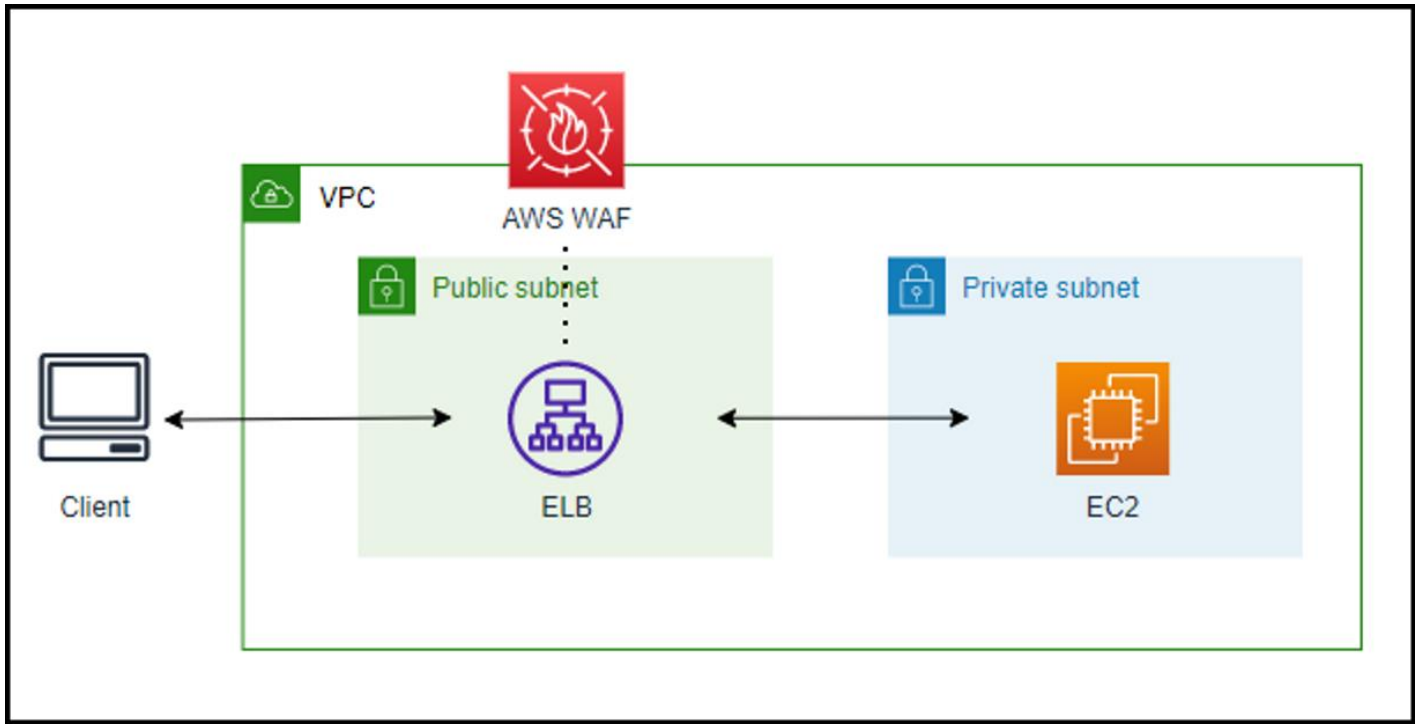
  Application Load Balancer, Cloud Front

  API Gateway, Cognito, AppSync, Apprunner



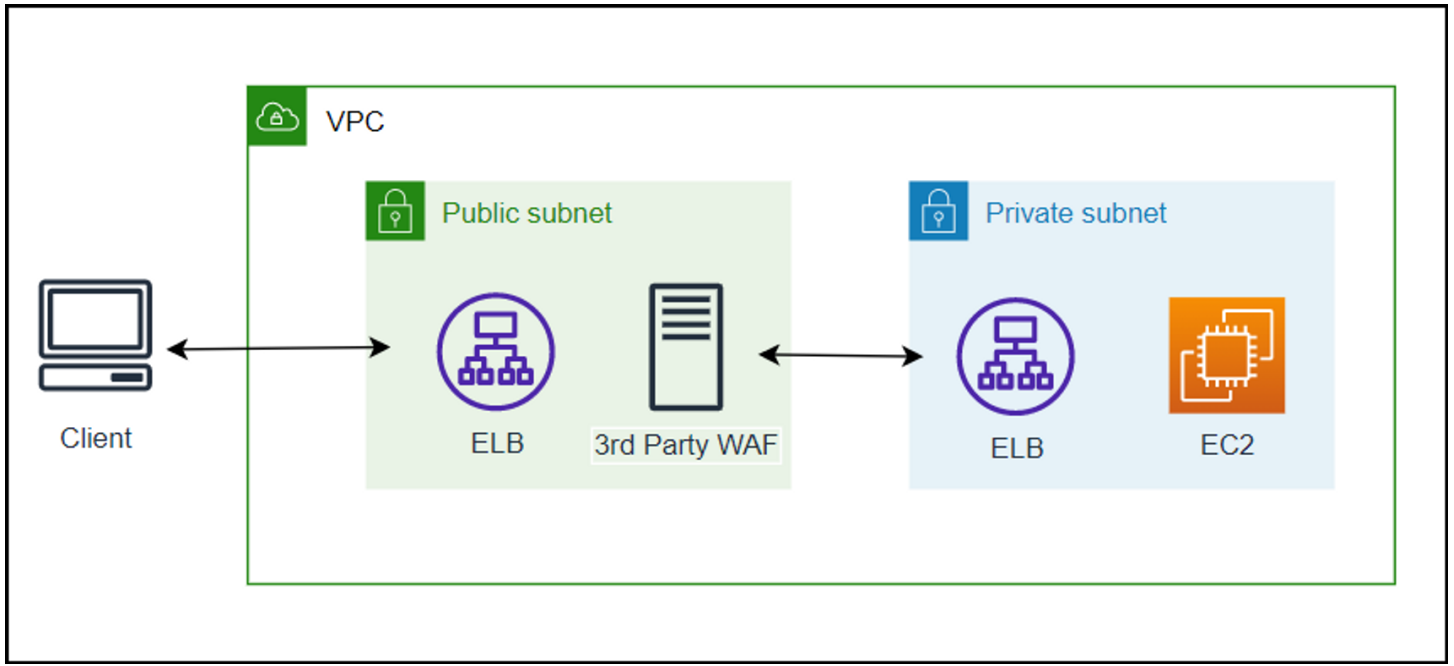
AWS WAF 개요

2. WAF 구성 소개 (AWS Native WAF)



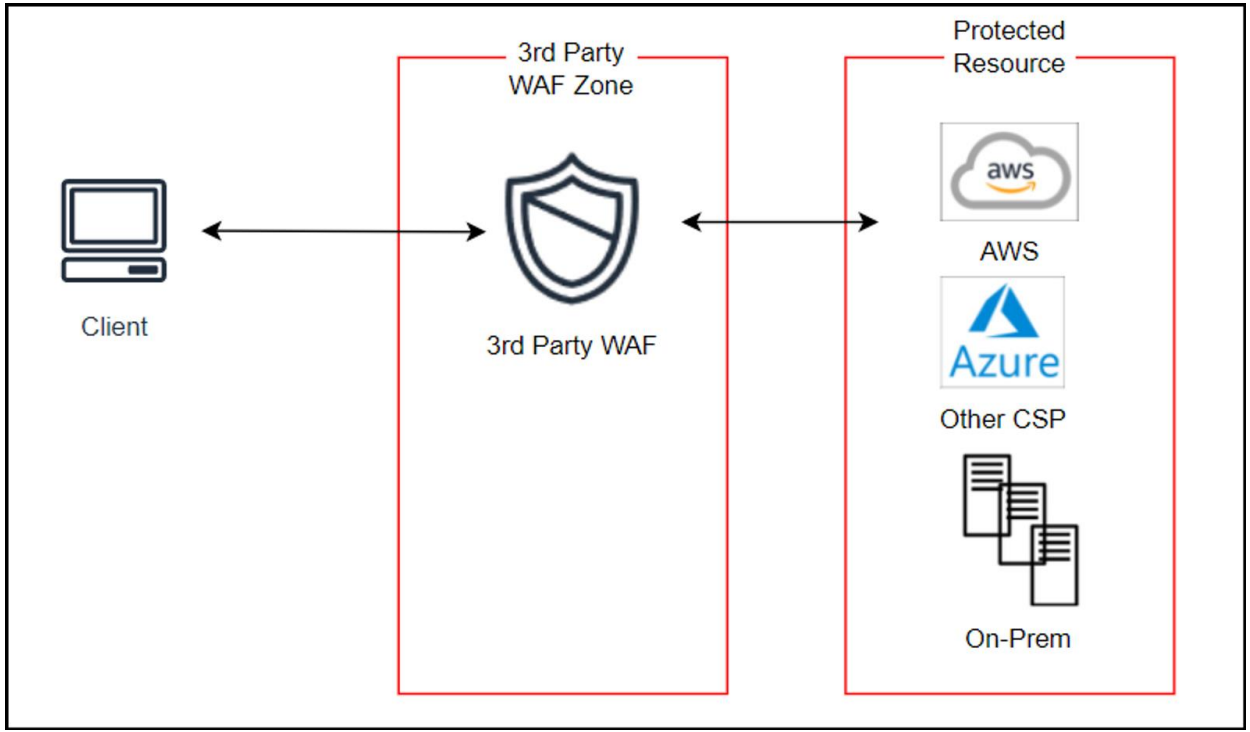
AWS WAF 개요

3. WAF 구성 소개 (샌드위치 형태 구조 3rd Party WAF)



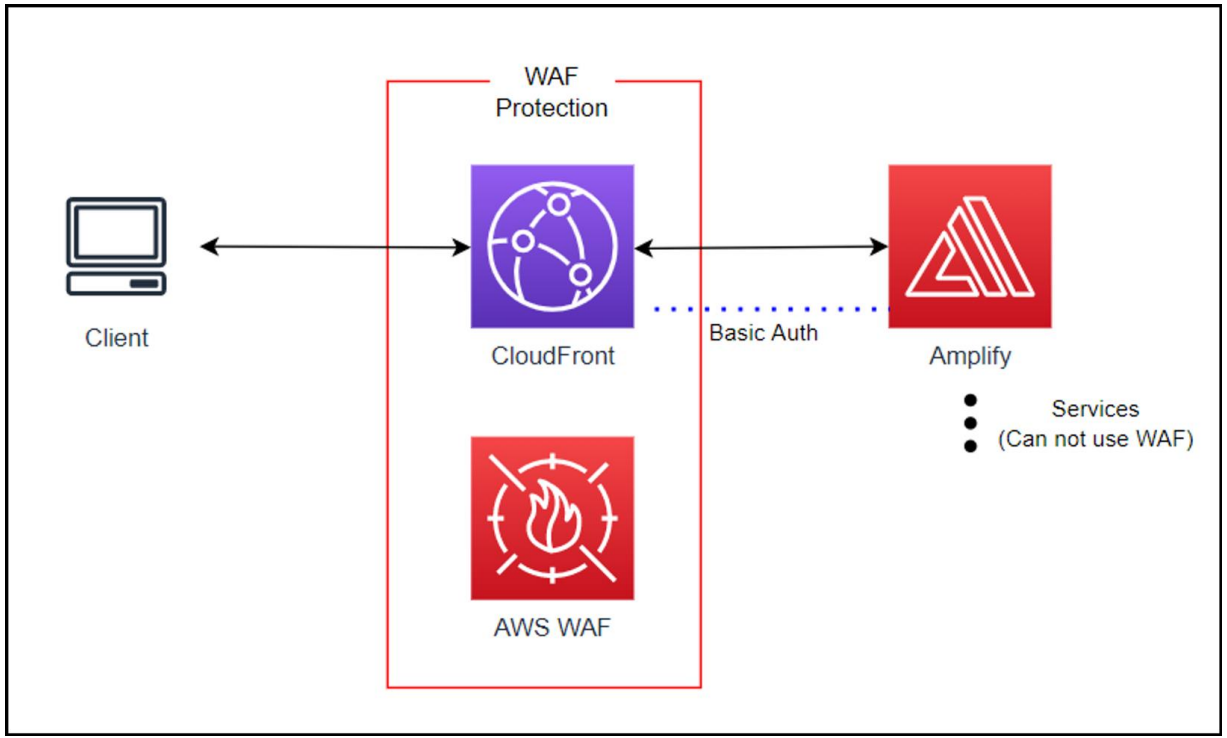
AWS WAF 개요

4. WAF 구성 소개 (SECaaS 형태 구조 3rd Party WAF)



AWS WAF 개요

4. WAF 구성 소개 (SECaaS 형태 구조 Native WAF)



AWS WAF 개요

4. WAF 특징

장점

- 3rd Party 대비 적용이 쉽고, 서비스 영향성이 적음
  - 3rd Party은 SECaaS 구성, 샌드위치 구성을 해야하여 구성이 크게 변경되며
  - DNS 변경 작업이 필요하고 순단이 발생할 수 있음
  - 반면 AWS WAF는 적용에 구성변경이 없고 운영 영향성이 없음
  - 서버 및 OS에 대한 관리 필요 없음
- 3rd Party 대비 가격이 저렴함
  - SECaaS의 경우 트래픽을 많이 처리해야 하기 때문에 라이선스비용이 매우 높음
  - 샌드위치 구성의 경우 WAF용 인스턴스,라이선스 비용에 대한 비용이 높음

단점

- 3rd Party 대비 탐지율이 낮고 오탐율이 높음
  - 룰 커스터마이징이 필수적임
- 사이즈가 큰 경우 탐지에 제약이 있음
  - HTTP Header, Body 각각 8KB (Cloud Front의 경우 최대 64KB)
  - Handling oversize web request components - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced
- 탐지 로그의 정보가 적음
  - HTTP/S Request Body 미표기, HTTP/S Response 미표기 (탐지도 불가
  - Can AWS WAF check the response message | AWS re:Post
- 탐지 정책 중앙관리를 위해 별도 구성이 필요함
  - Firewall Manager(Organization 필요) 혹은 별도의 Lambda모듈이 필요함
- WAF WCU 제한 (1500 > 5000)
- AWS WAF increases web ACL capacity units limits
- 탐지근거 적음
  - 일부 정책 (SQL, XSS 정책)만 탐지 근거 찾기 가능
  - AWS WAF, 일치하는 규칙과 관련된 컨텍스트에 대한 로깅 요청 개선

AWS WAF 개요

5. WAF 정책 설정 (웹사이트 신규, 변경)

1. 개발/품질환경에서 **Count모드** 설정하여 운영 (4~6주)
2. 수집된 로그를 Athena/CloudWatch/OpenSearch 등을 통해 분석
    - 많이 탐지되는 IP 중심으로 확인
3. 오탐 (정상인데 탐지 한 경우)이 있는지 개발팀과 검토
4. 오탐 정책 패턴 예외처리/정책제거
5. 개발/품질 환경에 **차단모드**로 적용하여 개발팀과 재확인
6. 운영 환경에서 1~5 반복

※ 운영 적용시 정상접속 차단을 인지할 방안 마련(custom response활용 권고)

AWS WAF의 주요 제공 기능

보호 대상으로서의 대응 리소스에 부착하여 이용

악의적인 요청의 차단

- SQL 인젝션
- 크로스 사이트 스크립트
- AWS 또는 파트너 제공의 매니지드 룰

커스텀 룰에 기반한 웹 트래픽의 필터

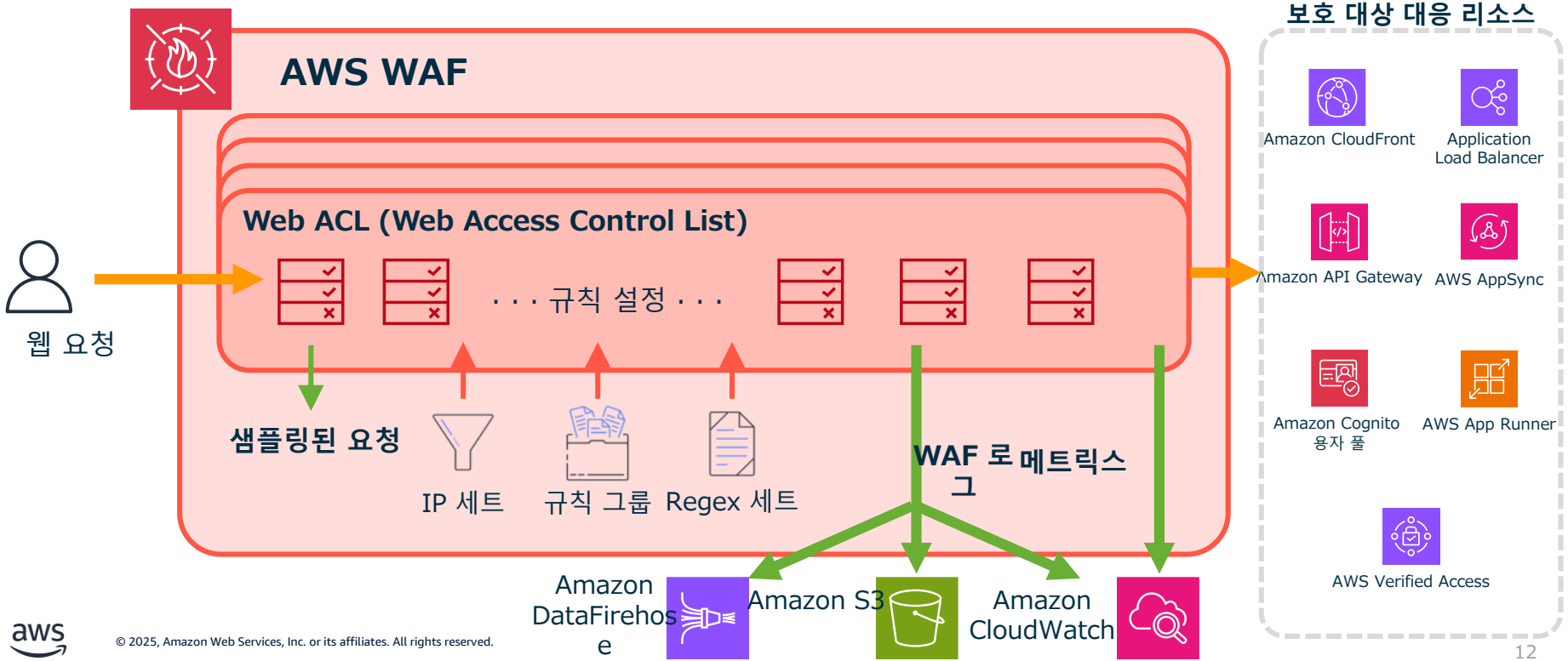
- Rate-based rules
- IP & Geo-IP filters
- 정규표현 패턴, 문자열
- 사이즈 제한
- 액션: 허용/거부

모니터링과 튜닝

- Amazon CloudWatch 메트릭/알람
- WAF 로그 취득
- 카운트 모드(탐지 모드)

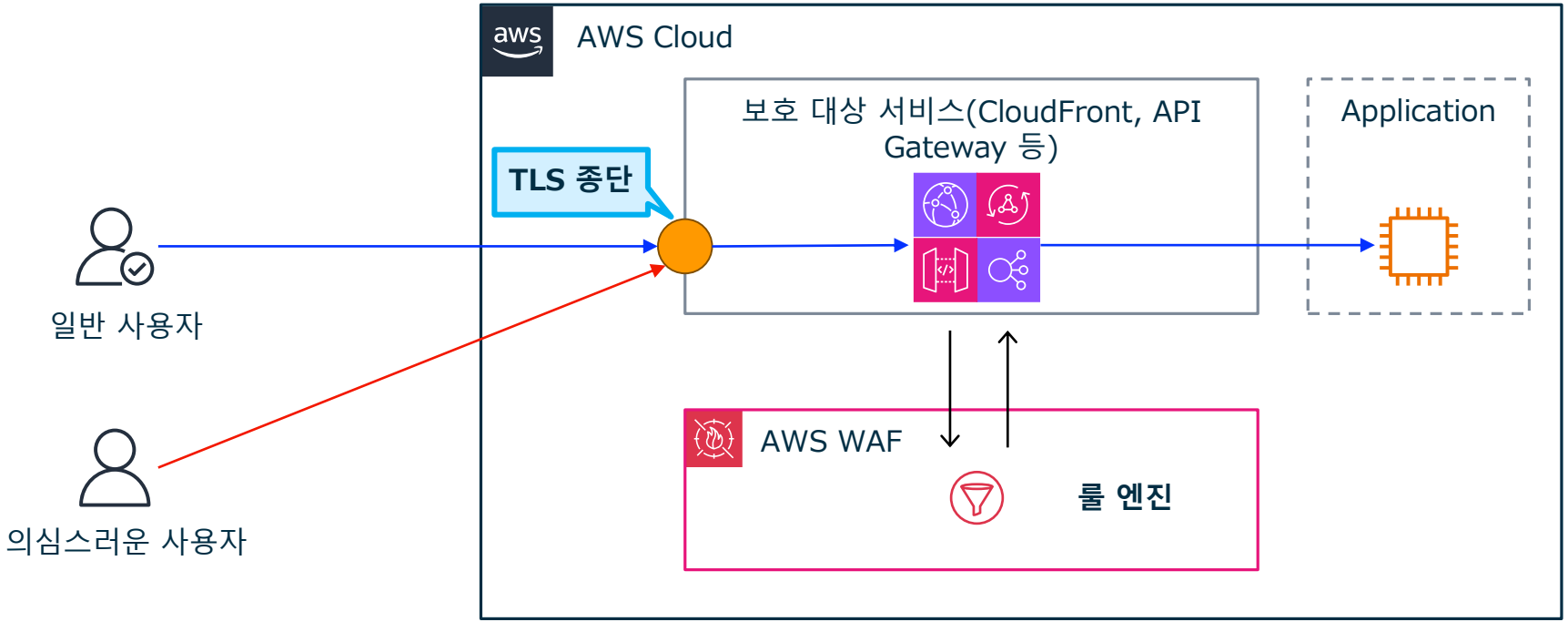
WAF - 전체 구성도

'규칙' 그룹을 설정한 Web ACL을 생성하고 보호 대상 리소스에 연결(규칙은 AWS 관리 규칙, 커스텀 규칙, 3rd Party 규칙(유료)을 이용 가능)



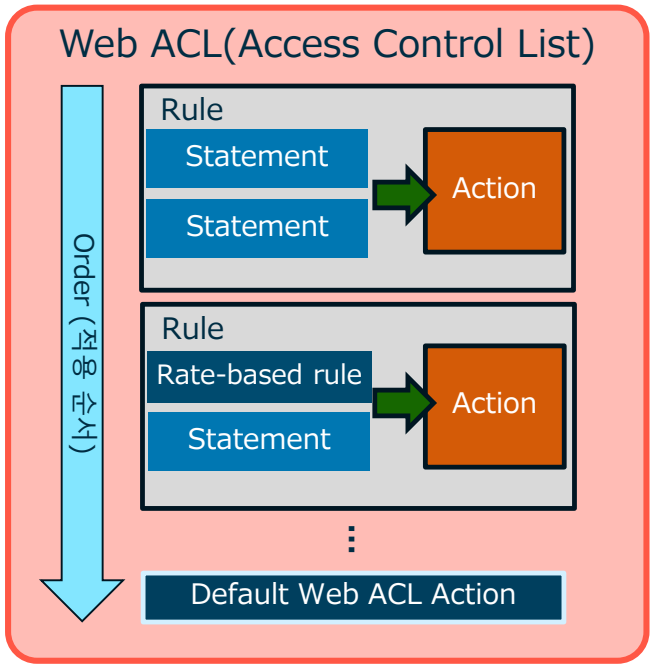
보충: WAF - 동작 아키텍처

WAF는 보호 대상 서비스와 협조하여, 보호 대상 서비스로부터 호출되는 형태로 WAF 룰 엔진이 동작함



WAF - Web ACL(Access Control List)

WAF의 기본이 되는 정의체
→ 대상 리소스에 연결하여 보호를 제공

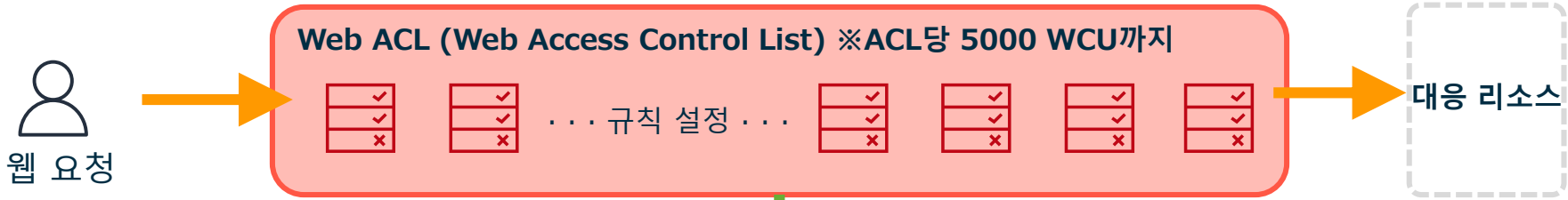


- Web ACL 내에는 여러 '규칙'을 순서와 함께 정의
  - 각 규칙에는 우선순위를 지정하여 적용 순서를 설정
  - 어떤 Rule에도 처리되지 않은 요청에 대한 '기본 액션'도 지정
- 하나의 '규칙' 내에는 여러 '스테이트먼트' 등을 정의할 수 있음
  - 요청을 검사하기 위한 조건이 정의되며, 액션을 통해 조건에 일치한 요청의 처리 방법이 지정됨
- 하나의 Web ACL 내에는 5,000 WCU(Web Capacity Unit)까지의 범위로 규칙을 추가 가능

※1,500WCU를 초과하는 요청 처리에 대해서는 500WCU마다 $0.20/100만 요청의 추가 요금이 발생

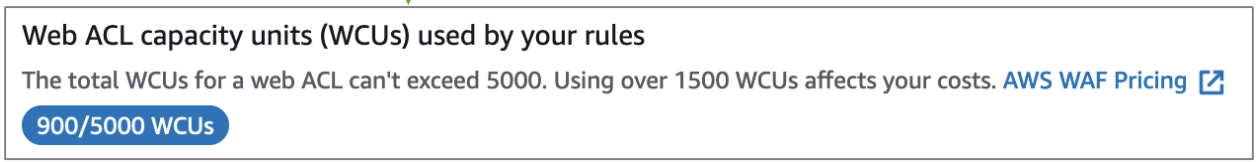
WAF - WCU(Web Capacity Unit)

WebACL 내 규칙 내용에 따라 정해진 "처리 비용"을 계산하며, 그 합계가 Capacity Unit (5,000)을 초과하지 않는 범위에서 규칙을 등록 가능



- Web ACL의 WCU 상한은 5000
- 매치 조건의 처리 내용에 따라 WCU 사용량이 다름
- 정규표현식 규칙 수의 상한은 10개까지 (Regex pattern sets)

각 규칙의 Capacity Unit 합계
(Web ACL 화면에 현재 총 WCU 값이 표시됨)



Layered protection at the edge with AWS WAF

L7 DDoS protection

Rate Based Rules

IP-based controls

IP Allow / Deny Lists

IP Reputation Lists

Rule-based controls

AWS Managed Rules

Customer Rules

Third Party Rules

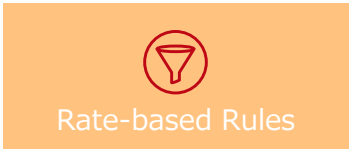
Intelligent Threat Mitigations

Bot Control

Fraud Control (ATP + ACFP)

애플리케이션 계층 DDoS 보호

HTTP 플러드 공격을 감지하고 요청을 억제



임계값에 도달하면 L7 DDoS 공격을 차단

임계값과 평가 기간 구성 가능

- 1/2/5(기본값)/10분의 평가 기간 동안 100 - 2천만 요청

집계를 위한 IP 또는 사용자 지정 키:

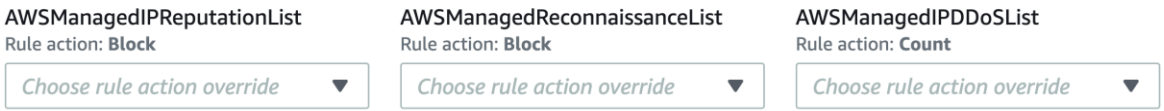
- IP 주소 또는 헤더, 쿼리 파라미터, 쿠키, HTTP 메서드, URI를 포함한 기타 요청 구성 요소를 집계에 사용할 수 있음

IP 기반 제어

악의적인 IP 주소로부터의 공격 방어

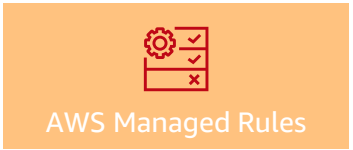
특정 IP 또는 IP 세트로부터의 요청을 차단하거나 허용

악의적인 활동에 적극적으로 관여하거나, 정찰을 수행하거나, DDoS 활동에 적극적으로 참여하는 Amazon Threat Intelligence 기반 IP



규칙 기반 제어

HTTP 요청 내에 숨겨진 악성 페이로드로부터의 보호



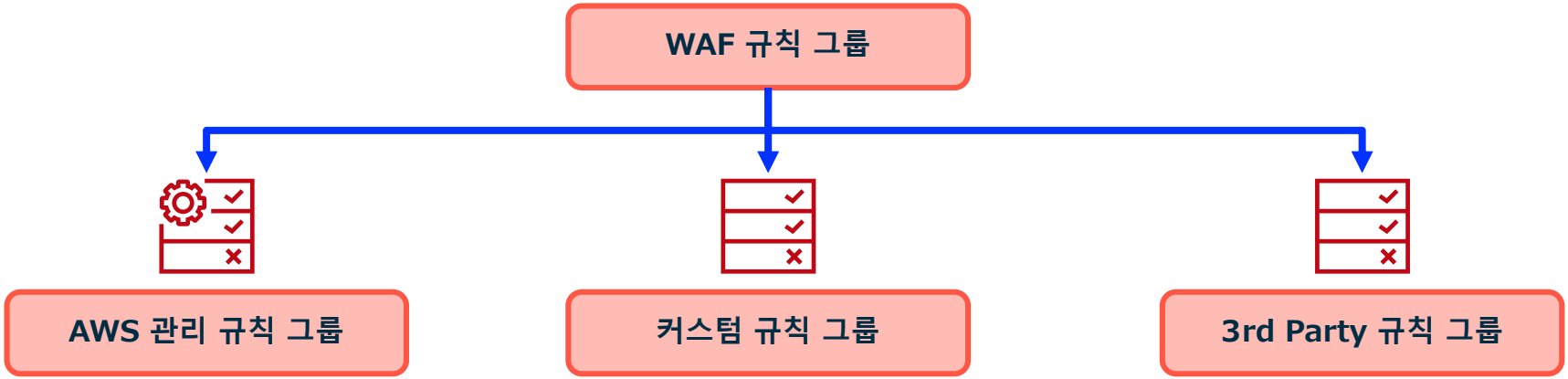
SQL 인젝션, 크로스 사이트 스크립팅 또는 명령어 인젝션과 같은 일반적인 공격 벡터에 대한 내장 규칙

애플리케이션의 특정 요구사항에 맞추고 새로운 취약점으로부터 보호하기 위한 자체 규칙 생성

외부 보안 공급업체의 추가 규칙 세트를 쉽게 배포하여 방어 태세 강화

WAF - 규칙 그룹

규칙은 여러 개를 묶어서 1개의 규칙 그룹으로 취급하는 것이 가능
→ 제공 출처에 따라 AWS 관리 / 커스텀 / 3rd Party의 3가지로 분류 가능



- AWS가 제공・내용을 관리
- 버전의 개념이 있음
- 내용 변경에 관한 알림 수신이 가능(SNS 토픽 이용)
- 이전 버전은 언젠가 만료되고, 새 버전이 항상 유효

- 사용자가 내용을 설정 & 관리

- 3rd Party가 제공・내용을 관리
- 사용자는 AWS Marketplace를 통해 구독함으로써 이용
- 원칙적으로 유료

WAF - AWS 관리 규칙 그룹 (1/2)

AWS Threat Research Team이 작성 및 유지보수를 실시하며 OWASP Top 10 등의 일반적인 위협부터 Bot 등의 고도화된 영역까지의 규칙을 제공

#	AWS 관리 규칙 그룹	WCU	설명
1	**Core Ruleset**	700	OWASP Top 10 및 많은 공통 취약점 식별자(CVE)에 기재된 대책 규칙
2	**Admin Protection**	100	공개된 일반적인 관리자용 페이지에 대한 외부 접근을 차단하기 위한 규칙
3	**SQL Database**	200	SQL 인젝션 공격 등 SQL 악용과 관련된 요청 패턴을 차단
4	**Linux OS**	200	Linux 고유의 취약점 악용과 관련된 요청 패턴을 차단하는 규칙
5	**Known Bad Inputs**	200	무효하고 취약점 악용 또는 발견과 관련된 요청 패턴을 차단하는 규칙
6	**PHP Application**	100	PHP 고유의 취약점에 대한 보호 규칙
7	**WordPress application**	100	WordPress 고유의 취약점에 대한 보호 규칙
8	**POSIX OS**	100	POSIX 기반 OS 고유의 취약점 악용과 관련된 요청 패턴을 차단하는 규칙
9	**Windows OS**	200	Windows 고유의 취약점 악용과 관련된 요청 패턴을 차단하는 규칙
10	**Amazon IP Reputation List**	25	봇 및 기타 위협과 관련된 IP 주소를 차단
11	**Anonymous IP list**	50	익명화를 허용하는 서비스(Tor, VPN, 프록시 등)로부터의 요청을 차단하기 위한 규칙

※상기 AWS 관리 규칙 그룹의 업데이트는 지정된 SNS 토픽 구독을 통해 감지 가능

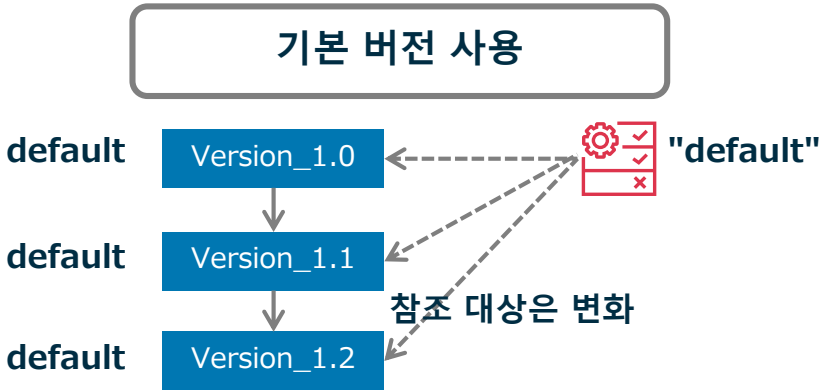
WAF - AWS 관리 규칙 그룹 (2/2)

AWS 위협 연구팀이 작성 및 유지보수를 실시하는 개별 유료 기능으로 제공되는 고급 규칙 그룹

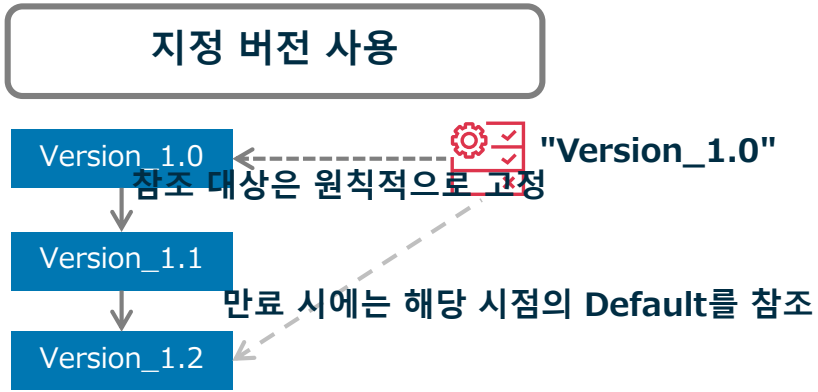
#	AWS 관리 규칙 그룹	WCU	설명
12	**AWS WAF Bot Control**	50	악의적인 봇(Bad Bot)을 감지하여 유해/불필요한 트래픽을 차단하는 규칙 (※추가요금)
13	**Account Takeover Prevention (ATP)**	50	웹(HTML) 기반 POST 요청을 통한 무차별 로그인 공격을 차단하는 규칙 (※추가요금)
14	**Account Creation Fraud Prevention (ACFP)**	50	웹(HTML) 기반 계정 생성 요청 공격을 차단하는 규칙 (※추가요금)

WAF - AWS관리 규칙 그룹 버전

AWS 관리 규칙 그룹은 '버전' 개념을 가지고 있으며, 사용자는 최신 버전으로 자동 추적 또는 일정 기간의 명시적 지정이 가능



- '기본 버전'을 항상 추적
- 기본 버전이 항상 최신 버전이 아닐 수 있음(권장 버전이 기본 설정)

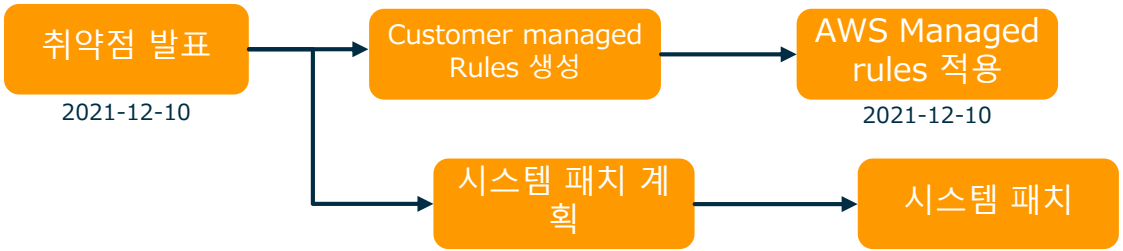


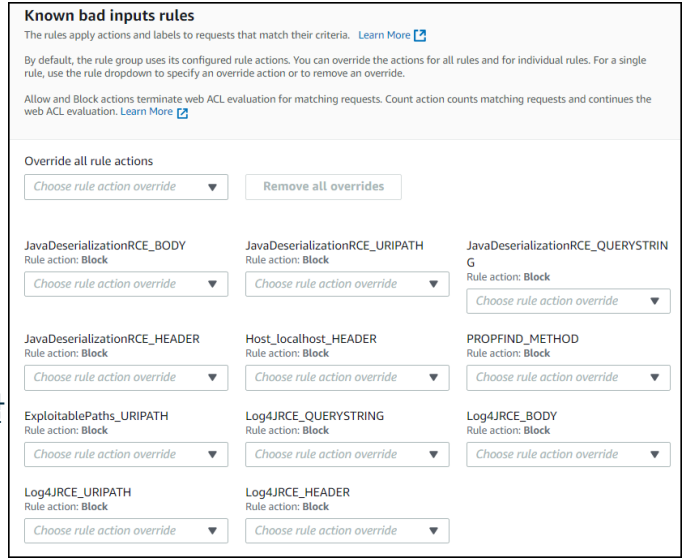
- '지정한 버전'을 고정 사용
- 특정 버전은 언젠가는 만료되며, 더 새로운 버전의 사용이 필요하게 됨 (만료 후에는 default를 자동 참조 → 유효 버전의 사용을 권장)

※AWS 관리 규칙 그룹의 업데이트는 지정된 SNS 토픽의 구독을 통해 감지 가능
※AWS 관리 규칙 그룹의 종류에 따라서는 버전이 제공되지 않는 경우가 있음

사례 연구: 새로운 취약점으로부터의 보호

- **Log4Shell (CVE-2021-44228)은 널리 사용되는 Java 로깅 프레임워크인 Log4j의 제로데이 취약점으로, 임의의 원격 코드 실행(RCE)을 가능하게 했습니다**



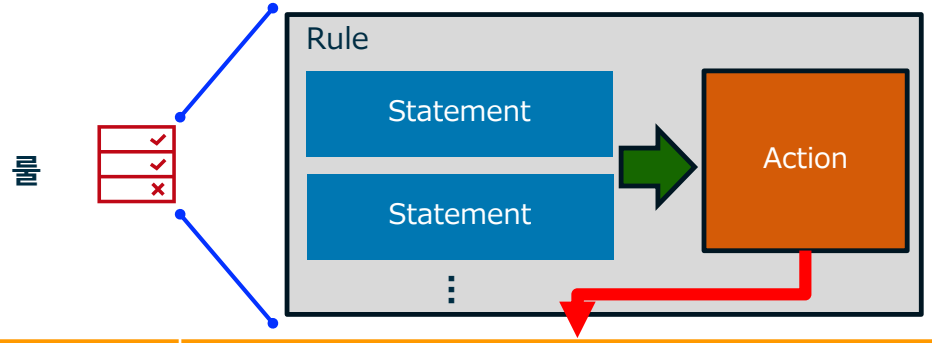


AWS WAF는 24시간 이내에 Log4Shell에 대한 규칙을 출시했습니다. 고객들은 시스템 패치 작업을 하는 동안 AWS Managed Rules를 사용하여 시스템을 보호할 수 있습니다.

https://aws.amazon.com/blogs/security/using-aws-security-services-to-protect-against-detect-and-respond-to-the-log4j-vulnerability/

WAF - 룰 액션

룰에 해당한다고 판정된 경우의 액션으로 4(+1)개 중에서 선택 가능



#	동작	설명
1	**Allow**	• 일치한 요청을 허용(후속 규칙은 평가하지 않고, 보호 대상 리소스로 요청을 통과)
2	**Block**	• 일치한 요청을 거부
3	**Count**	• 요청을 허용하거나 거부하지 않고, 카운트만 함. WebACL의 나머지 규칙을 평가함 • 단, 사용자 정의 헤더 추가나 다른 규칙에서 평가하기 위한 "라벨" 추가는 가능
4	**CAPTCHA**	• CAPTCHA 토큰(실제로는 Cookie)이 요청에 없거나 기간 만료된 경우로, 요청의 Accept 헤더에 값 "text/html"이 포함되어 있는 경우, HTML을 통한 CAPTCHA 입력 페이지를 표시
5	**Challenge**	• AWS WAF용 클라이언트 JavaScript 라이브러리와 연동하여 aws-waf-token의 생성을 강제

WAF - 규칙 액션(CAPTCHA)

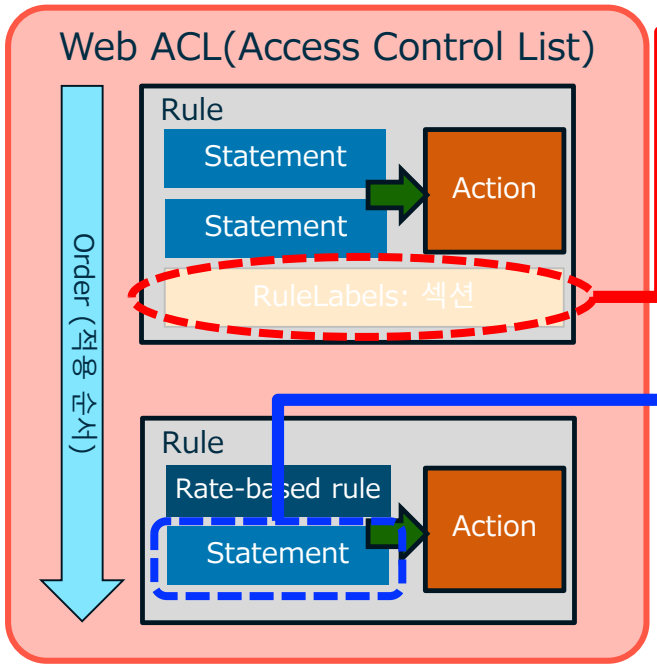
CAPTCHA는 실행 횟수당 종량제 요금 발생
정답 후 토큰(Cookie) 발행(기본 300초, 60초~3일간 설정 가능)

Action [CAPTCHA] ※아래 4가지 중 사용자가 선택

※CAPTCHA는 GET 요청에 대해 유효하게 작동(POST 요청 등은 지원되지 않음)

WAF - 요청 라벨

하나의 요청에 메타데이터로서 라벨 부여 가능
→ 판정 로직의 재사용과 규칙 간 판정에 활용



RuleLabels 섹션:
이 Rule에 매치된 요청에 "라벨" 부여

- 라벨은 "네임스페이스"에 기반하여 스코프가 분리됨
(AWS 관리 규칙도 독자적인 네임스페이스로 라벨을 부여)
- 하나의 규칙에서 복수의 라벨 부여 가능

LabelMatch 스테이트먼트:
지정된 "라벨" 유무를 판정 → 이에 기반한 액션 가능

- 라벨의 유무에 기반하여 액션을 제어 가능
- 커스텀 응답과 조합하여 응답 헤더 추가도 가능

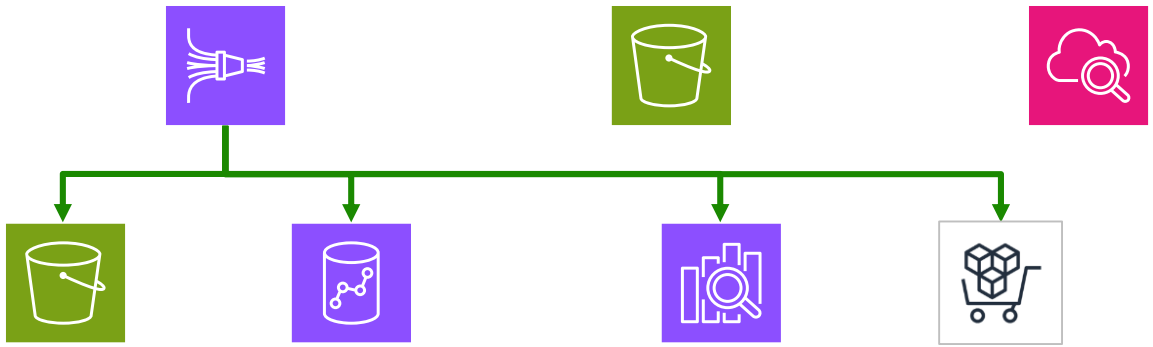
※규칙 내에서의 라벨 부여는 1WCU 소비로 라벨을 최대 5개까지 설정 가능
※이후의 라벨 유무 판정도 1WCU를 소비

WAF - 로그 출력(3가지 서비스 중 하나)

Web ACL별로 Data Firehose / CloudWatch Logs / S3 버킷 중 하나에 Web ACL 로그를 출력 가능(라벨로 필터링)

- 모든 요청 기록에는 일치한 요청 헤더와 Rule ID가 포함됨
- 쿠키나 인증 헤더 등 민감한 정보를 로그에서 제외 가능
- 요청의 어디에서(헤더/쿼리/Body) 어떤 값이 규칙에 일치하여 차단되었는지 확인 가능


```
"terminatingRuleId": "STMTest_SQLi_XSS",
"terminatingRuleType": "REGULAR",
"action": "BLOCK",
"terminatingRuleMatchDetails": [
{
"conditionType": "SQL_INJECTION",
"location": "HEADER",
"matchedData": [
"10",
"AND",
"1"
]
}
```

보충: WAF - 로그 분석

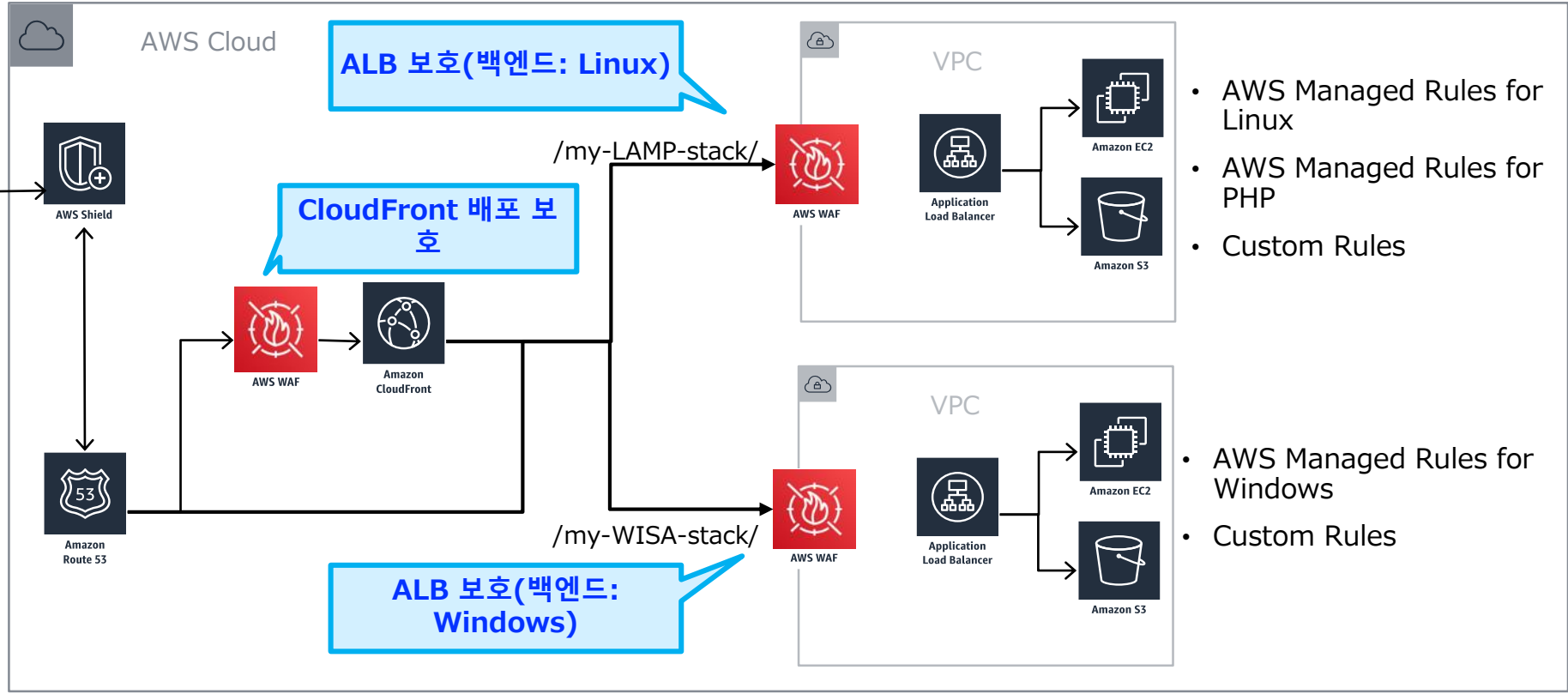
action의 값 "ALLOW | BLOCK | EXCLUDED_AS_COUNT"
하나의 로그 레코드 구조의 상세는 일부 다름

```
{
"formatVersion": 1,
"action": "ALLOW | BLOCK | EXCLUDED_AS_COUNT",
"timestamp": <epochnumber>,
"webaclId" :  "<web-acl-arn>",
"terminatingRuleId" : "<id>"
"terminatingRuleType": "REGULAR | …",
"httpSourceName": "ALB | CF | APIGW",
"httpSourceId":  "<request_soruce_id>",
"ruleGroupList": [],
"ruleBasedRuleList" [],
"nonTerminatingMatchingRules": [],
"terminatingRuleMatchDetails: [],
"httpRequest": {
"clientIp":
"country": "JP",
"headers": []
"uri": "<uri>",
"args": "key=value",
"httpVersion": "HTTP/1.1 | …",
"httpMethod: "GET | POST | …",
"requestId": "<id>
}
}
```

AWS 관리 규칙 그룹에서 COUNT로 설정한 경우에는 "Action":"COUNT"라는 값은 없음. "EXCLUDED_AS_COUNT"를 포함한 로그 엔트리를 추출할 필요가 있음

AWS 관리 규칙 그룹에서의 COUNT인지, 커스텀 규칙에서의 COUNT인지에 따라 출력 구조가 다름

보충: AWS 관리 규칙을 이용한 다단계 방어



- AWS Managed Rules for Linux
- AWS Managed Rules for PHP
- Custom Rules

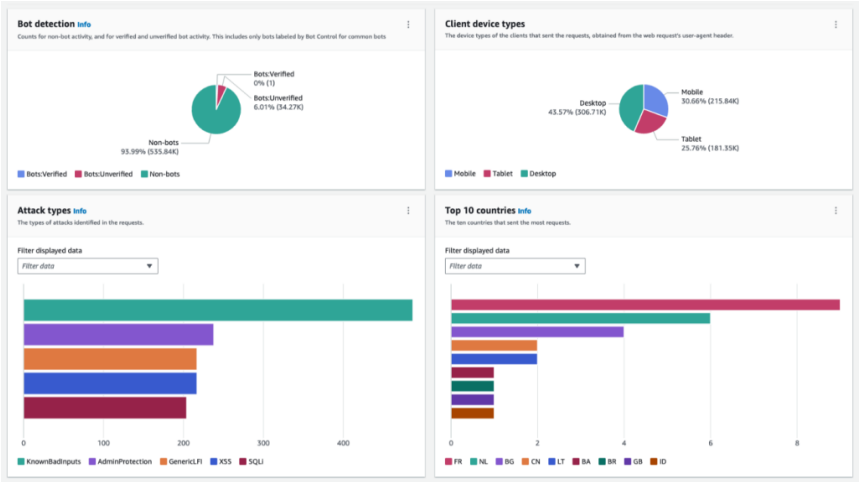
- AWS Managed Rules for Windows
- Custom Rules

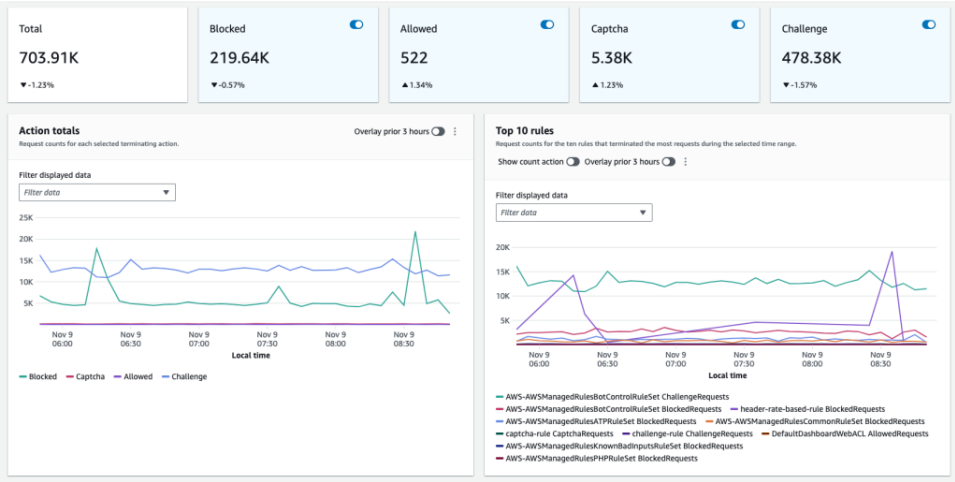
보충: AWS 관리 콘솔 대시보드

Bot을 포함한 탐지된 공격 유형, 보안 관련 메트릭을 개괄적으로 보여주는 트래픽 대시보드 제공

트래픽 대시보드

액션 대시보드





탐지된 공격 유형

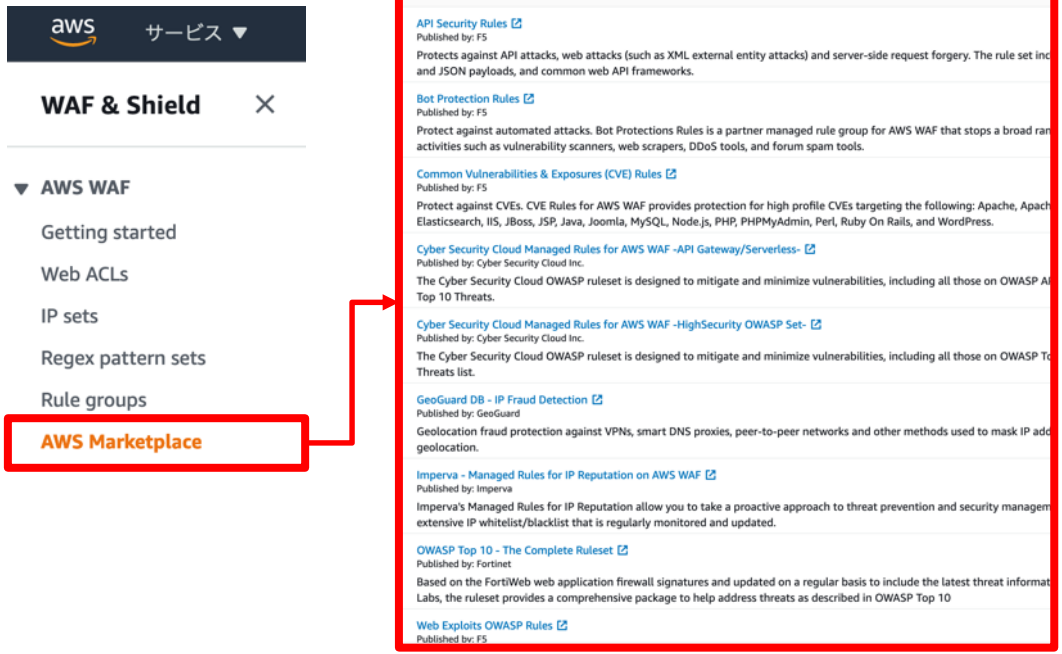
요청 출처 유형

필터 데이터 수

처리 규칙 상위

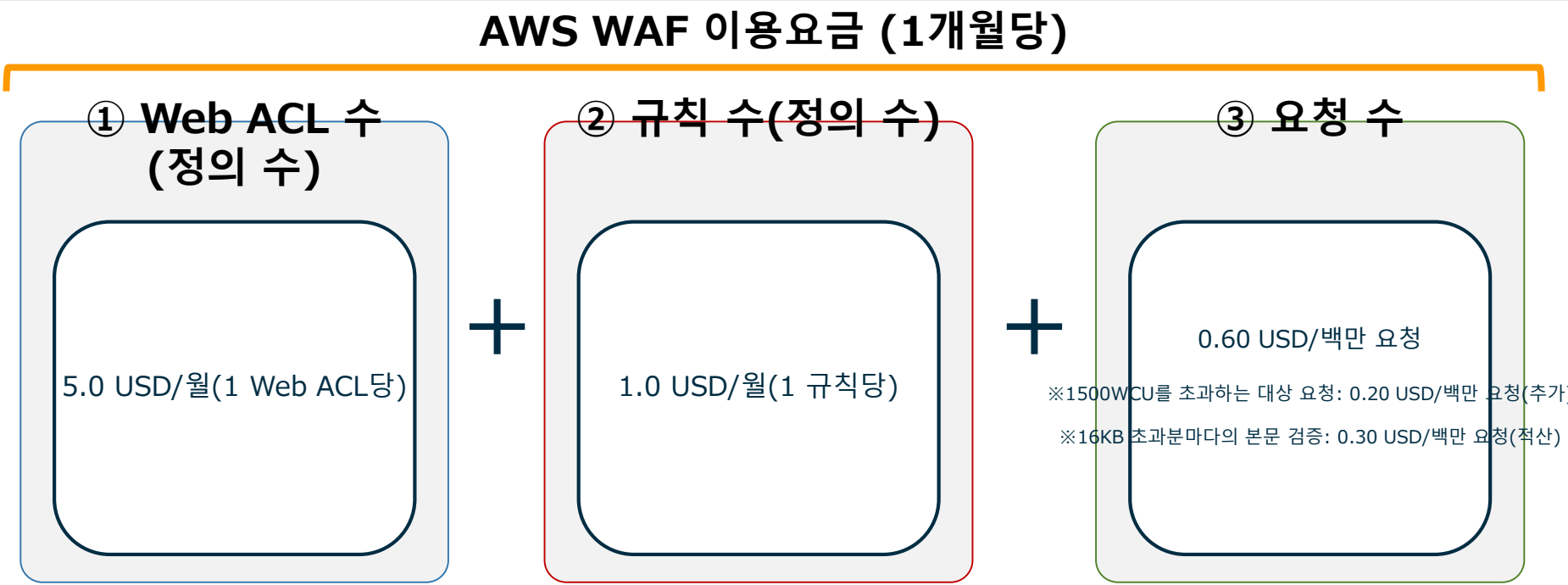
AWS WAF 3rd Party 매니지드 룰 참고 정보

3rd Party가 제공하는 AWS WAF 매니지드 룰
→ AWS Marketplace에서 구독(이용 계약)이 가능



WAF - 이용요금

"①Web ACL 수" "②규칙 수" "③처리된 요청 수" "④CAPTCHA 실행 횟수"에 기반한 종량제 과금 (모든 리전에서 동일 요금)

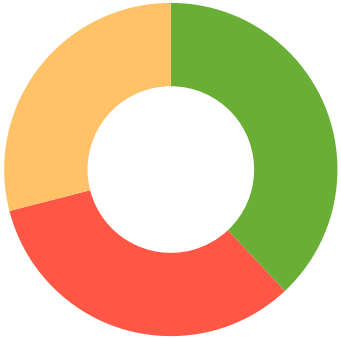


※Bot Control(후술), CAPTCHA, ATP 이용 시에는 위 요금에 추가로 각각의 이용요금이 발생

AWS WAF BotControl

Bad Bot 대책의 필요성

일반적인 웹 애플리케이션 트래픽의 최대 51%는 기계에서 실행되는 스크립트(이른바 봇)에서 발생한다



Good Bot

크롤러
모니터링 외

사람

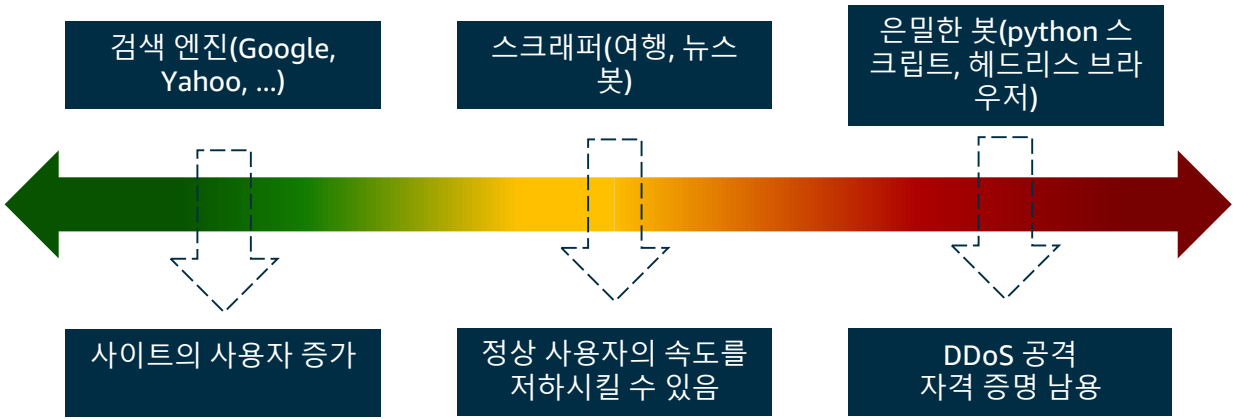
Bad Bot

Layer7 DDoS
취약점 스캔
웹 스크래핑
클릭 / 다운로드 외

원하는 봇과 원하지 않는 봇

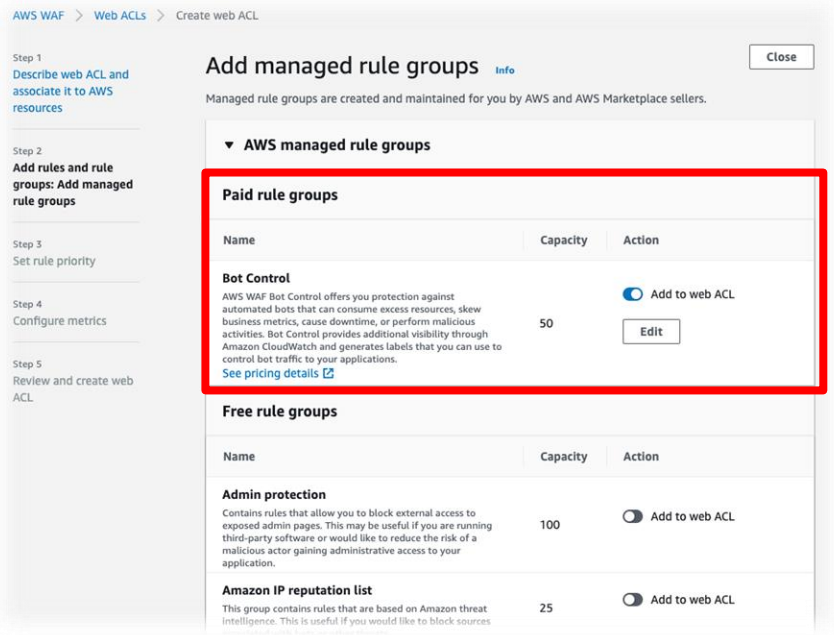
웹 트래픽의 상당 부분이 봇이지만, 모든 봇이 나쁜 것은 아님

각 봇 카테고리에 대해 적절한 조치를 취함



AWS WAF Bot Control - 더 고도화된 봇 대책

AWS가 관리하는 룰에 기반하여 "Bad Bot"으로부터의 접근을 제어 → 요청을 차단 또는 카운트하여 통과



- 'AWS 관리 룰 그룹' 중 하나로 Web ACL에 추가하여 사용
- Web Capacity Unit (WCU)는 50을 소비
- 시간 과금으로 이용 가능

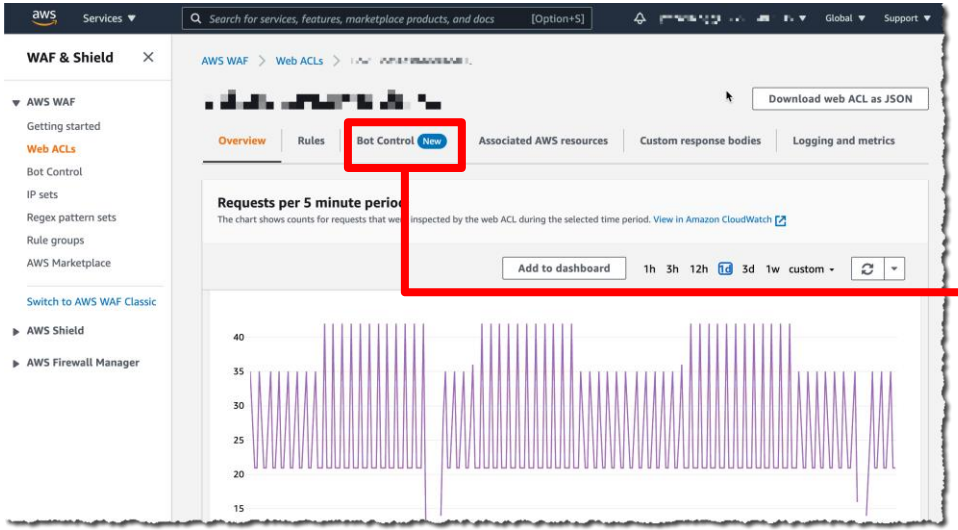
AWS WAF Bot Control - 봇 대시보드

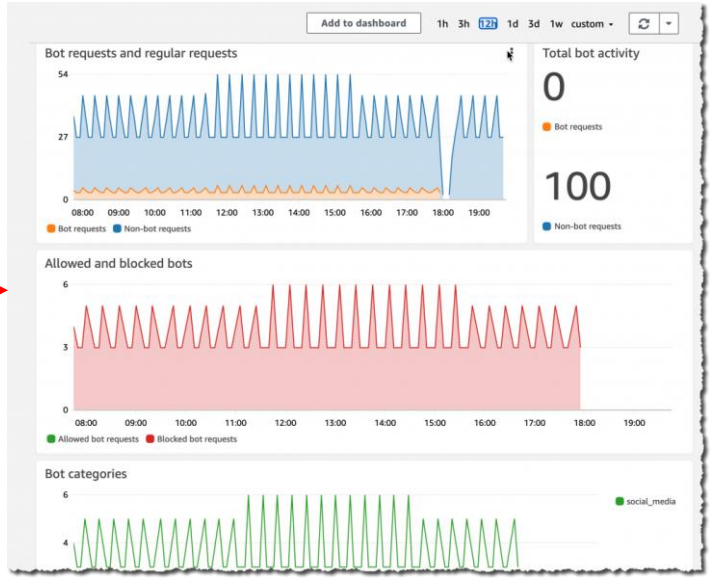
적용 전에, 현재 WAF 적용 대상 리소스 전체에서 어느 정도의 비율로
봇(악성 또는 비악성)으로부터의 접근이 이루어지고 있는지 확인 가능 (무료 기능)

- AWS WAF를 이용하는 고객은 Bot Control을 이용하지 않더라도, 대시보드에서 봇 트래픽의 요약 정보를 확인할 수 있습니다

AWS WAF Bot Control - 봇 대시보드

실제로 Bot Control 규칙을 적용한 후에는 동일한 Web ACL 단위의 상세 대시보드를 참조할 수 있습니다





AWS WAF Bot Control - 컨트롤 리스트

AWS 위협 연구팀이 작성 및 유지보수를 실시하며 OWASP Top 10 등의 일반적인 위협부터 봇 등의 고도화된 영역까지의 규칙을 제공

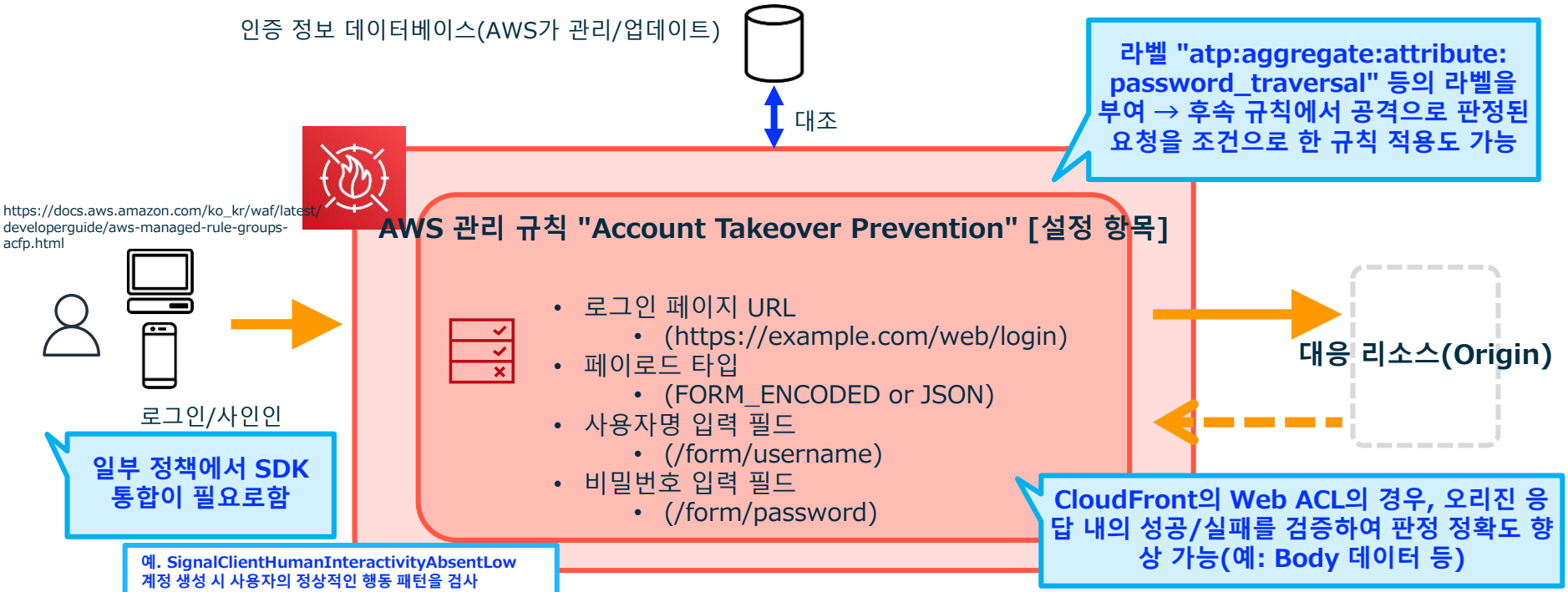
#	Bot Control 목록	설명
1	CategoryAdvertising	서드파티 광고 서비스
2	CategoryArchiver	웹 아카이브 수집 서비스
3	CategoryContentFetcher	RSS 피드 등의 정보 수집
4	CategoryEmailClient	이메일 내 URL 접근 체크
5	CategoryHttpLibrary	개발 언어의 HTTP 라이브러리 접근
6	CategoryLinkChecker	링크 체커(링크 생존 확인)
7	CategoryMiscellaneous	기타 봇
8	CategoryMonitoring	웹사이트 가동・생존 감시 봇
9	CategoryScrapingFramework	스크래핑 프레임워크
10	CategorySearchEngine	검색 엔진의 웹 크롤링
11	CategorySecurity	보안 체크 툴
12	CategorySeo	SEO 툴(랭킹 제어)
13	CategorySocialMedia	소셜 미디어
14	CategoryAI	AI 봇(뉴스 수집 등의 학습 용도)

#	Bot Control リスト	목록
15	SignalAutomatedBrowser	자동 조작 하의 브라우저(테스트 등)
16	SignalKnownBotDataCenter	봇이 사용하는 DC로부터의 접근
17	SignalNonBrowserUserAgent	웹 브라우저가 아닌 UA 헤더
18	TGT_VolumetricIpTokenAbsent	최근 5분간 부정 토큰의 접근
19	TGT_VolumetricSession	최근 5분간 비정상적인 양의 접근
20	TGT_SignalAutomatedBrowser	표적형 봇: 자동 조작 대상 브라우저
21	TGT_SignalBrowserInconsistency	표적형 봇: 브라우저 일관성 없음
22	TGT_TokenReuseIp	5개 이상의 IP에서 부정 토큰 재사용
23	TGT_ML_CoordinatedActivityMedium	비정상적인 행동을 하는 분산된 표적형 봇
24	TGT_ML_CoordinatedActivityHigh	비정상적인 행동을 하는 분산된 표적형 봇

https://docs.aws.amazon.com/ko_kr/waf/latest/developerguide/aws-managed-rule-groups-bot.html

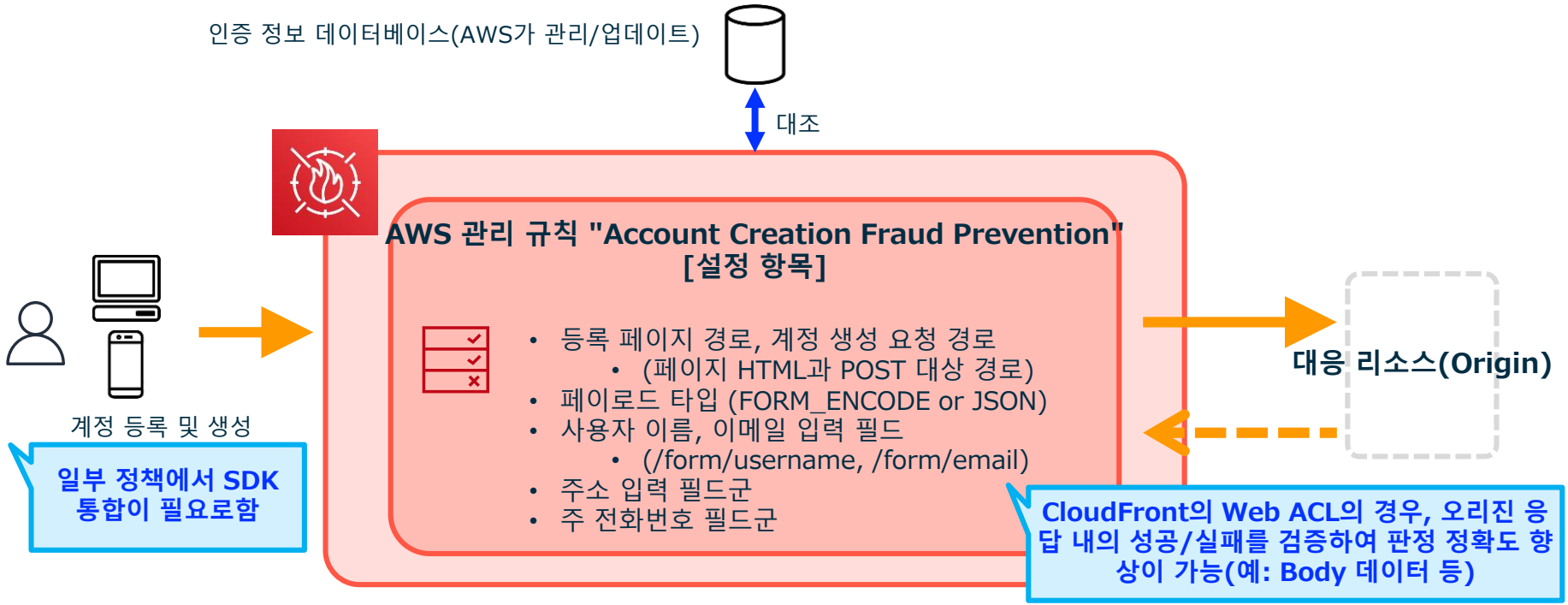
보충: ATP (Account Takeover Prevention)

로그인(HTML 기반)에 특화된 보호를 위한 AWS 관리 규칙 그룹
→ POST 요청에서의 브루트포스 공격(로그인 공격)을 방지



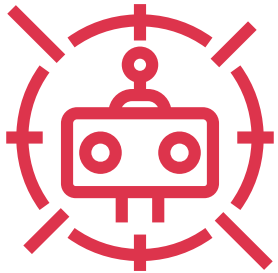
Account Creation Fraud Prevention (ACFP)

웹사이트의 계정 등록 페이지(이름/이메일/주소/전화번호 입력)에 대한 대량 요청 공격에 특화된 보호를 위한 AWS 관리 규칙 그룹



※ACFP 이용에는 별도 요금이 발생 (10.0 USD/월 + 1.0 USD/1,000요청)

Bot Control Rules 상세 내용

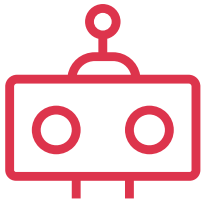


일반적인 봇

자체 식별이 가능한 단순 봇

시그니처 기반 탐지:

- IP 평판 목록
- request headers
- reverse DNS lookup



Targeted 봇

은밀하고 회피적인 봇

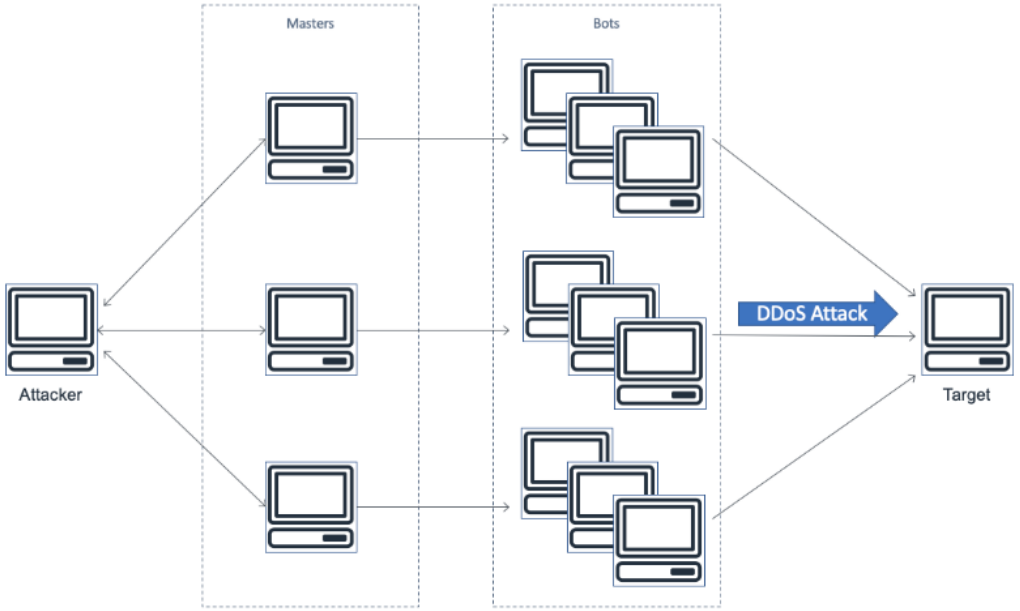
행동 기반 탐지:

- browser fingerprinting
- 환경 조사
- 작업 증명
- 머신 러닝을 통한 조직화된 활동 탐지

AWS Shield

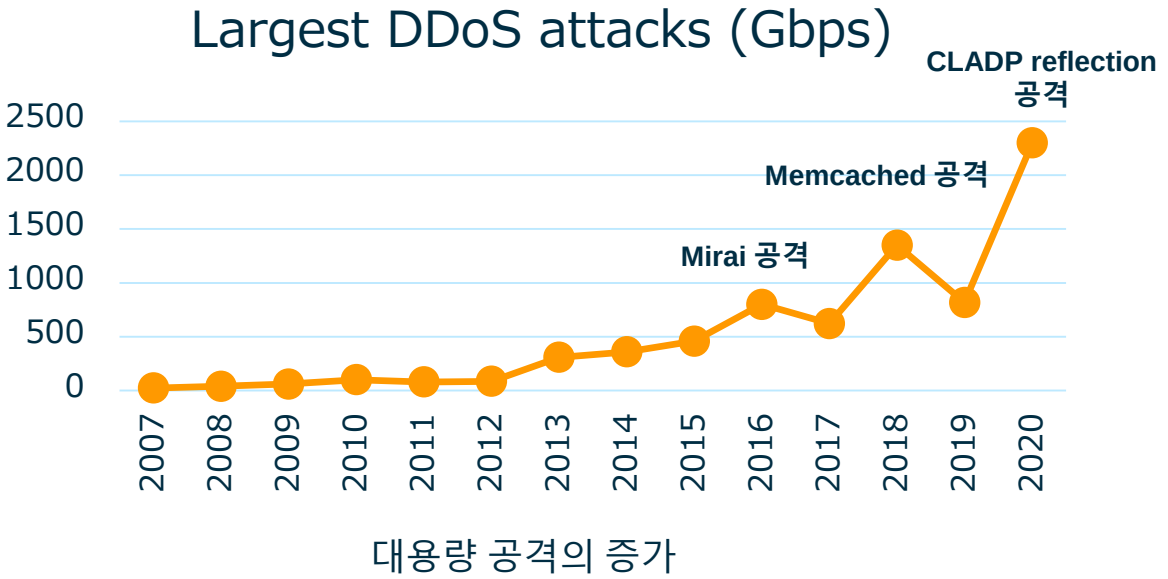
DDoS 정의

- 정당한 사용자/고객이 서비스에 접근하는 것을 거부(DoS)
- 효과를 높이기 위해 다수의 출처로부터 공격(분산)
- 공격은 일반적으로 감염된 기기들(IoT 기기, 서버 및 개인용 컴퓨터 등)의 봇넷으로부터 발생



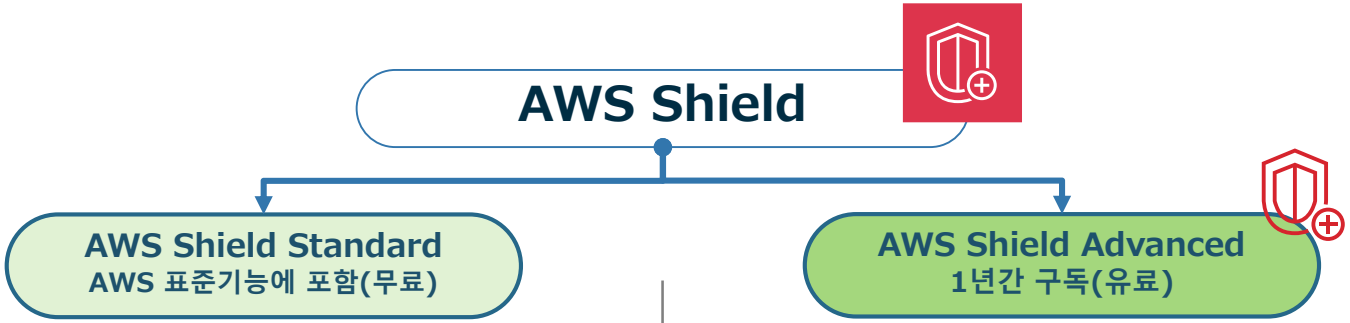
DDoS 공격 동기

- Extortion
- Competition
- Hacktivism
- Boredom
- Cyber warfare



AWS Shield

AWS 인프라가 제공하는 DDoS 보호 서비스 (무료 Standard와 유료 Advanced 2종류)



- AWS 서비스에 포함되며 무료(항상 유효=비활성화 불가)
- 인터넷 경계의 모든 곳에 항상 적용
- 일반적인 L3/4 DDoS에 대한 방어 제공

- 더 대규모/정교한 공격에 대처
- Shield Response Team(SRT)의 지원/상담
  - 자동 L7 방어(AWS WAF 규칙 설정)
- 보호 대상에 대한 AWS WAF 무료 이용 가능

※SRT 연락은 Business 또는 Enterprise 지원 레벨이 전제조건(지원 요청은 AWS 지원 케이스 티켓을 통해 실시)

DDoS 공격 유형

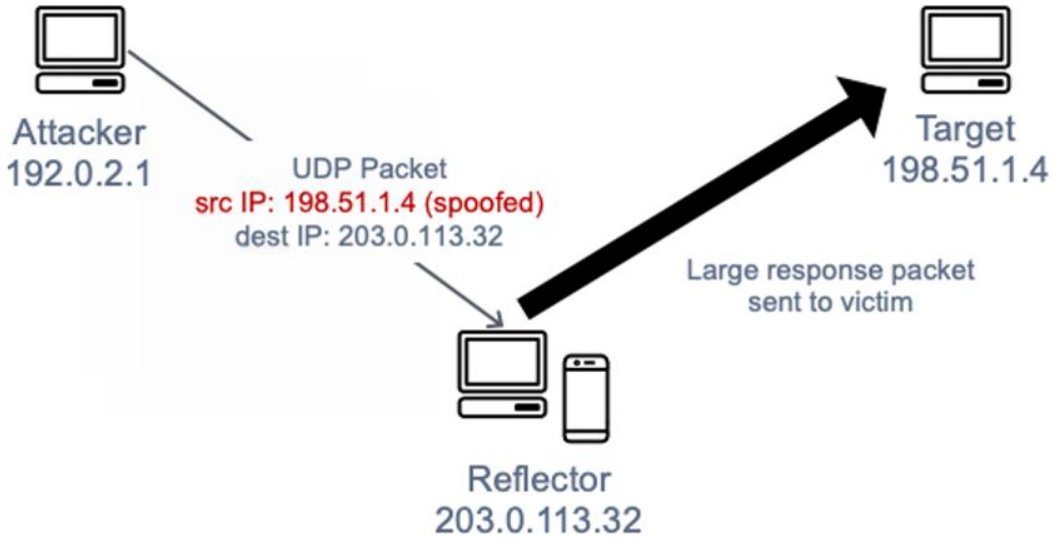
	계층	단위	설명	구분
7	Application	Data	Network process to application	App Content (ex. HTTP Header, URL)
6	Presentation	Data	Data representation and encryption	
5	Session	Data	Interhost communication	
4	Transport	Segments	End-to-end connections and reliability	IP Address, PORT, Flag(Syn, Ack, Fin ..)
3	Network	Packets	Path determination and logical addressing	IP Address
2	Data Link	Frames	Physical addressing	MAC Address
1	Physical	Bits	Media, signal, and binary transmission	-

L3 물량기반 디도스 공격

	계층	단위	설명	구분
7	Application	Data	Network process to application	App Content (ex. HTTP Header, URL)
6	Presentation	Data	Data representation and encryption	
5	Session	Data	Interhost communication	
4	Transport	Segments	End-to-end connections and reliability	IP Address + PORT
3	Network	Packets	Path determination and logical addressing	IP Address
2	Data Link	Frames	Physical addressing	MAC Address
1	Physical	Bits	Media, signal, and binary transmission	-

L3 물량기반 디도스 공격
정상적으로 처리할 수 있는 수준을 상회하는 트래픽을 전송하여 네트워크 기능을 마비시킴
(e.g., UDP reflection attacks)

L3 물량기반 디도스 공격 - 예시



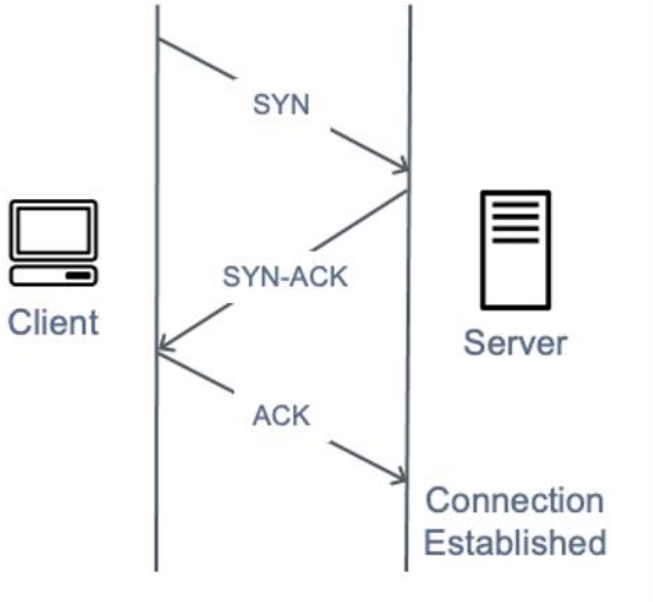
UDP reflection

L4 상태 소진 형 디도스 공격

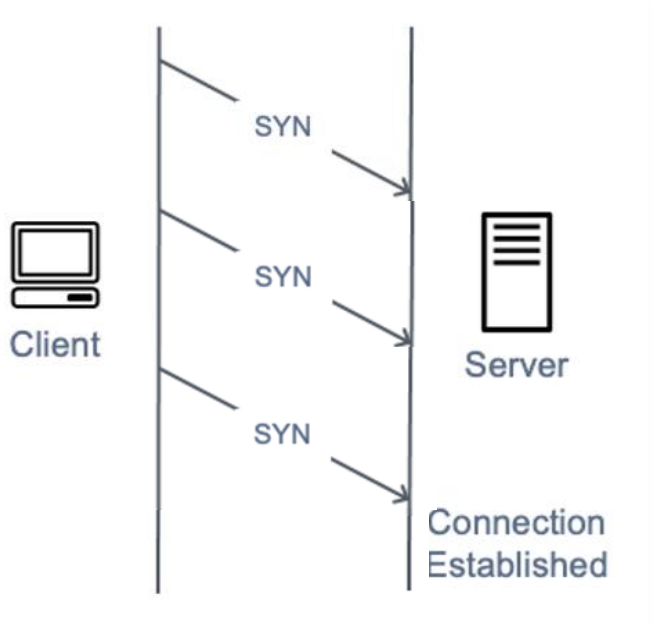
	계층	단위	설명	구분
7	Application	Data	Network process to application	App Content (ex. HTTP Header, URL)
6	Presentation	Data	Data representation and encryption	
5	Session	Data	Interhost communication	
4	Transport	Segments	End-to-end connections and reliability	IP Address + PORT
3	Network	Packets	Path determination and logical addressing	IP Address
2	Data Link	Frames	Physical addressing	MAC Address
1	Physical	Bits	Media, signal, and binary transmission	-

L4 상태 소진 형 디도스 공격
프로토콜 특성을 악용하여 방화벽, IPS, 로드밸런서 같은 시스템을 무력화
(e.g., TCP SYN flood)

L4 상태 소진 형 디도스 공격 - 예시



3-way Handshake



SYN Flood

L7 어플리케이션 레이어 기반 디도스 공격

	계층	단위	설명	구분
7	Application	Data	Network process to application	App Content (ex. HTTP Header, URL)
6	Presentation	Data	Data representation and encryption	
5	Session	Data	Interhost communication	
4	Transport	Segments	End-to-end connections and reliability	IP Address + PORT
3	Network	Packets	Path determination and logical addressing	IP Address
2	Data Link	Frames	Physical addressing	MAC Address
1	Physical	Bits	Media, signal, and binary transmission	-

L7 어플리케이션 레이어 기반 디도스 공격
정상 요청으로 가장하지만, 방어수단을 우회하고 어플리케이션 리소스를 소진하기 위한 악의적인 요청을 통한 공격
(e.g., HTTP GET, Slowloris)

일반적인 DDoS 완화 기술

L3 물량기반

- BPS와 PPS 속도 제한
- Network ACL
- 대규모 대역폭
- 트래픽 엔지니어링

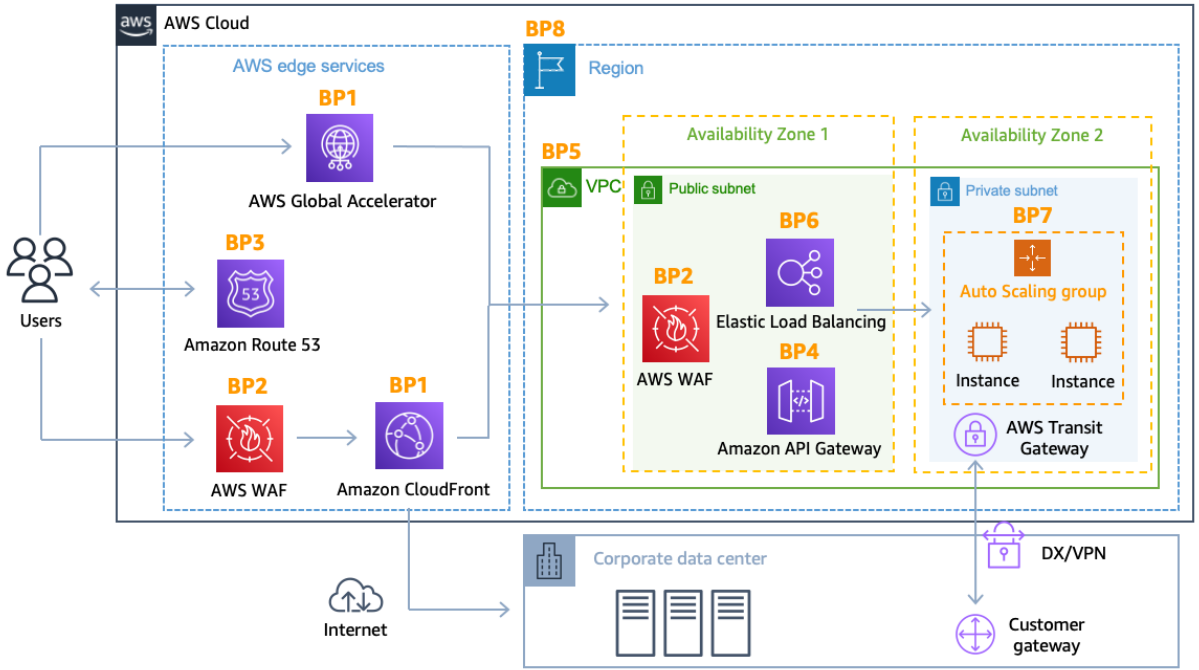
L4 상태 소진형

- 프로토콜 검증
- 프로토콜별 PPS 속도 제한
- 프로토콜별 기술(SYN Cookies, 불량 DNS 리졸버 등)
- 서비스 규모 확장/분산

L7 어플리케이션 레이어 기반

- 애플리케이션 수준 속도 제한(예: HTTP 속도 제한)
- 원하지 않는 동작을 차단하기 위한 Web Application Firewall 또는 Network Firewall(IPS)
- 경계에서 소스 인증(서명된 쿠키, 토큰, 봇 제어)
- 애플리케이션 규모 확장/분산

AWS DDoS 완화 모범사례



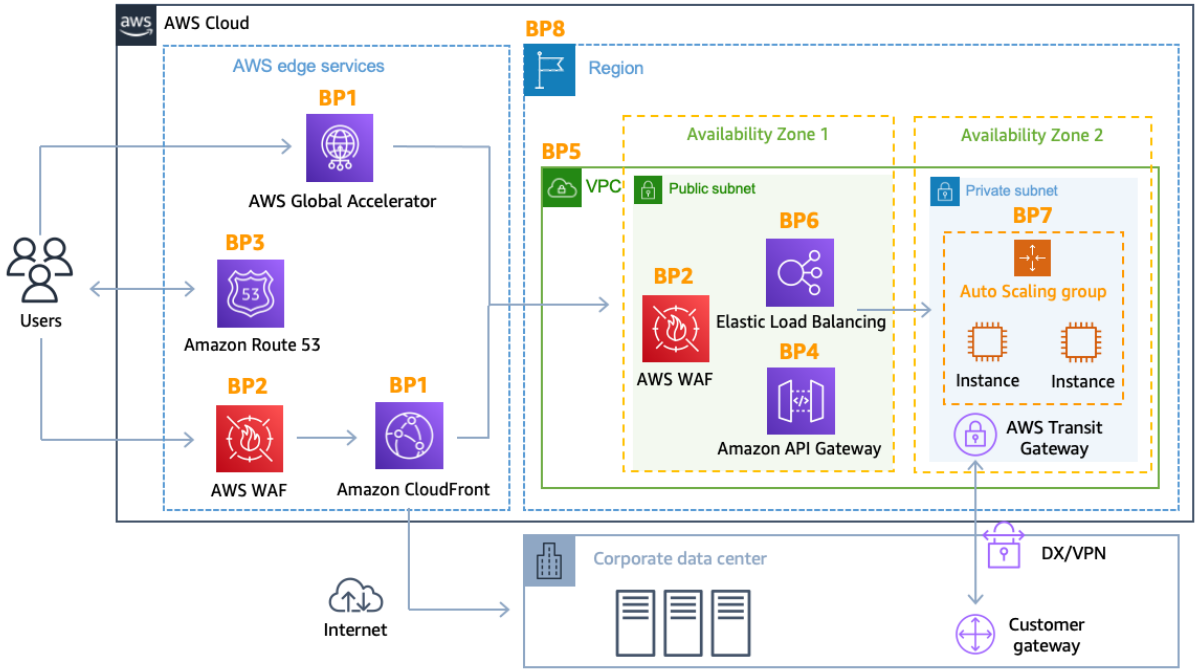
1. 확장가능하고, 고가용성 구조 준비

Amazon EC2 with Auto Scaling (BP7)
규모 확장 운영을 통한 대응
로드밸런서로 여러 EC2 인스턴스에 트래픽 분산
자동확장 구성으로 급증 트래픽 대응
CloudWatch 경보로 Auto Scaling 자동화
CPU/RAM/네트워크 I/O 등 사용자 정의 메트릭 기반 확장

Elastic Load Balancing (BP6)
다수의 백엔드 인스턴스로 트래픽 분산
자동 확장 기능으로 급증 트래픽 대응

- ALB(Application Load Balancer)
웹 애플리케이션용
콘텐츠 기반 트래픽 라우팅
SYN 플러드, UDP 리플렉션 공격 등 자동 차단
공격 감지 시 자동 확장
- NLB(Network Load Balancer)
비 HTTP/HTTPS 애플리케이션용
초저지연 트래픽 라우팅
TCP SYN/UDP 트래픽은 타겟으로 직접 전달
Global Accelerator로 SYN 플러드 보호 권장
Shield Advanced로 EIP 보호 가능

AWS DDoS 완화 모범사례

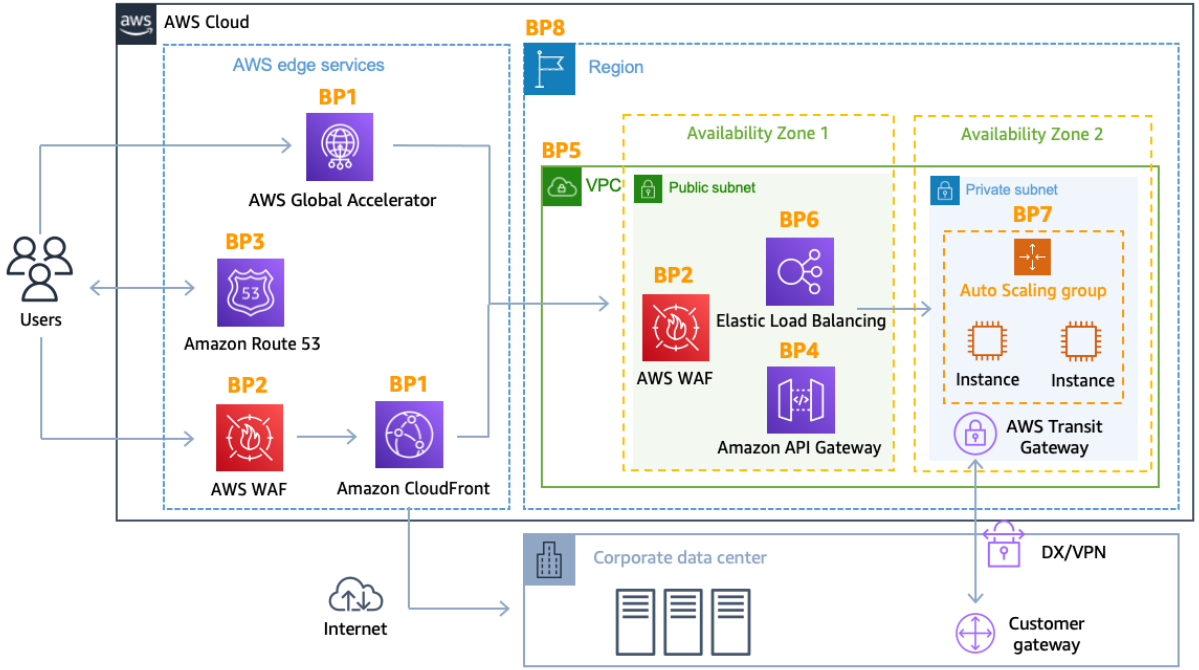


1. 확장가능하고, 고가용성 구조 준비

Using Route 53 for DNS availability (BP3)

Route 53은 AWS의 고가용성 DNS 서비스로 100% 데이터 플레인 가용성 SLA를 제공
셔플 샤딩과 애니캐스트 스트라이핑 기술을 통해 DDoS 공격에도 서비스 유지 가능
고급 기능들을 통해 웹 애플리케이션 성능 향상 및 중단 방지
최적의 위치에서 DNS 요청을 처리하여 지연 시간 최소화
DNS 쿼리 이상 감지 및 신뢰할 수 있는 사용자 요청 우선 처리 기능 제공

AWS DDoS 완화 모범사례



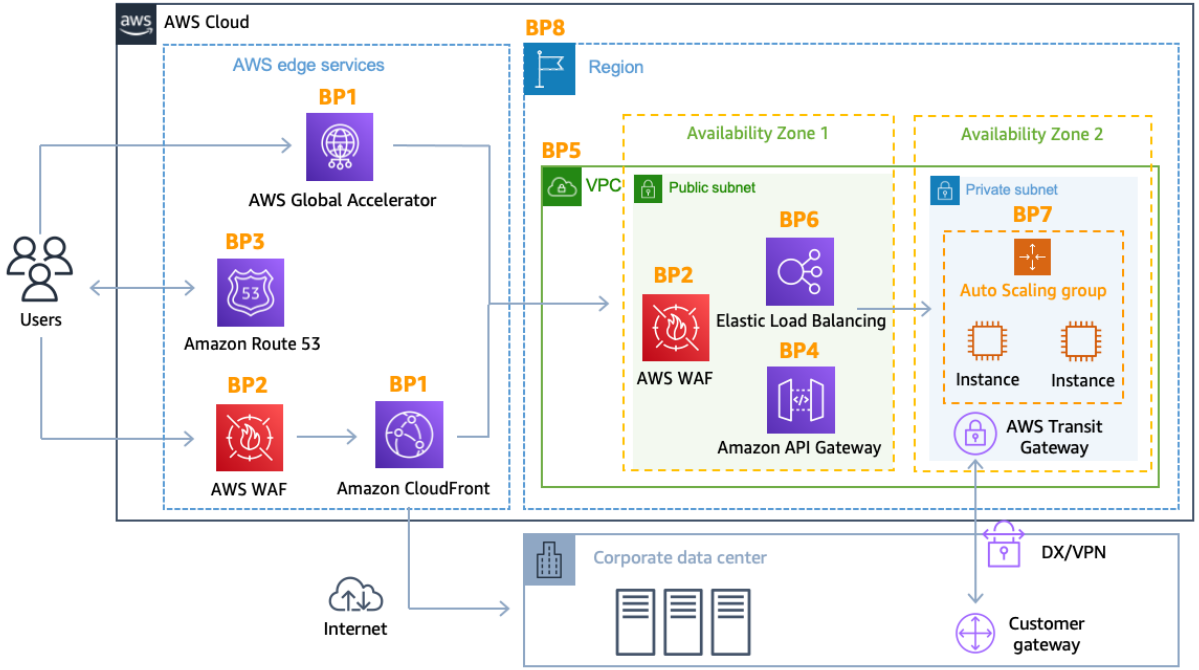
2. 공개적으로 노출되는 엔드포인트 최소화

Web application delivery at the edge - Cloud Front (BP1)
정적/동적/스트리밍/인터랙티브 콘텐츠 전체 제공
지속적 연결과 가변 TTL 설정으로 원본 트래픽 부하 감소
Protect network traffic further from your origin using AWS Global Accelerator (BP1)
사용자 트래픽의 가용성/성능 60% 향상
가장 가까운 엣지 로케이션에서 트래픽 수신
AWS 글로벌 네트워크 인프라를 통한 라우팅
TCP/UDP 트래픽의 최적 엔드포인트 라우팅
장애 시 30초 이내 페일오버 제공

SecurityGroup
불필요한 외부 Open정책 삭제

Elastic Load Balancing (BP6)
EC2, EKS 등 워크로드 자원에 ALB 적용

AWS DDoS 완화 모범사례



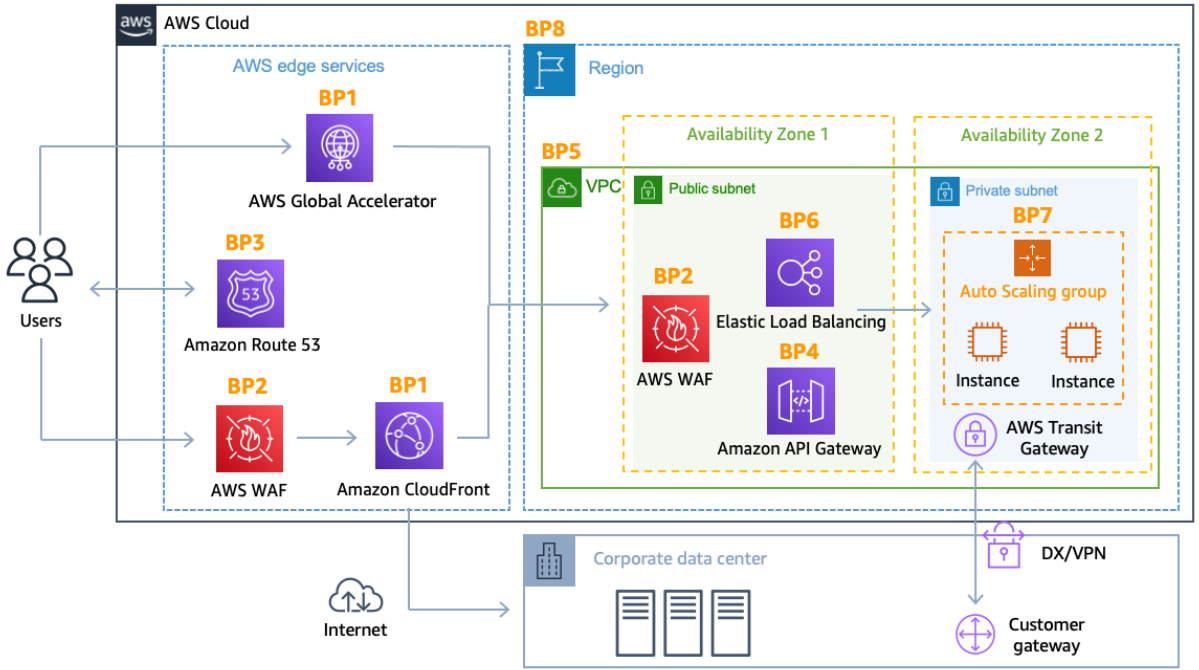
3. 웹방화벽 사용
Using AWS WAF (BP2)

AWS WAF의 속도 기반 규칙:
5분 동안의 요청 수를 기준으로 IP 주소 자동 차단
일반적인 속도 제한 규칙과 특정 URI에 대한 더 엄격한 규칙을 계층적으로 설정 권장
기본 500회/5분 제한과 특정 경로에 대해 100회/5분까지 더 엄격한 제한 설정 가능

IP 평판 기반 보호:
Amazon의 내부 위협 정보 기반 규칙 그룹 제공
익명 IP 목록으로 VPN, 프록시, Tor 노드 등 차단
서드파티 IP 평판 목록 활용 가능

지능형 위협 완화:
Bot Control 관리형 규칙 그룹으로 봇넷 공격 방지
계정 탈취 방지(ATP) 규칙으로 로그인 페이지 보호
계정 생성 사기 방지(ACFP) 기능으로 가짜 계정 생성 시도 통제

AWS DDoS 완화 모범사례



4. Shield Advanced 사용
Using Shield-Advanced

AWS Shield Advanced 구독자를 위한 기능:
자동으로 AWS WAF 규칙을 생성, 평가, 배포
레이어 7 DDoS 공격 자동 완화

작동 방식:
보호된 리소스마다 트래픽 기준선 설정
기준선에서 크게 벗어난 트래픽을 잠재적 DDoS 공격으로 식별
공격 서명을 식별하고 해당 트래픽을 차단하는 WAF 규칙 생성

규칙 관리:
과거 기준선과 비교하여 안전성 평가
Shield 관리 규칙 그룹에 추가
카운트 또는 차단 모드 선택 가능
위협이 사라지면 자동으로 규칙 제거

AWS Shield Standard

AWS Shield Standard

L3/4 DDoS 공격에 대한 표준 방어 제공
설정/운용이 불필요(자동 감지・자동 완화)・L7 보호는 AWS WAF로 대응 필요

AWS Shield Standard의 범위

Layer 3/4 protection

- 일반적인 공격으로부터 방어
- 자동 감지 & 자동 완화
- AWS 서비스에 기본 내장

Layer 7 protection

- Layer 7 DDoS 공격에 대한 완화는 AWS WAF 이용
  - 셀프 서비스
  - 사용한 만큼만 지불

AWS Shield Standard - Activity detected

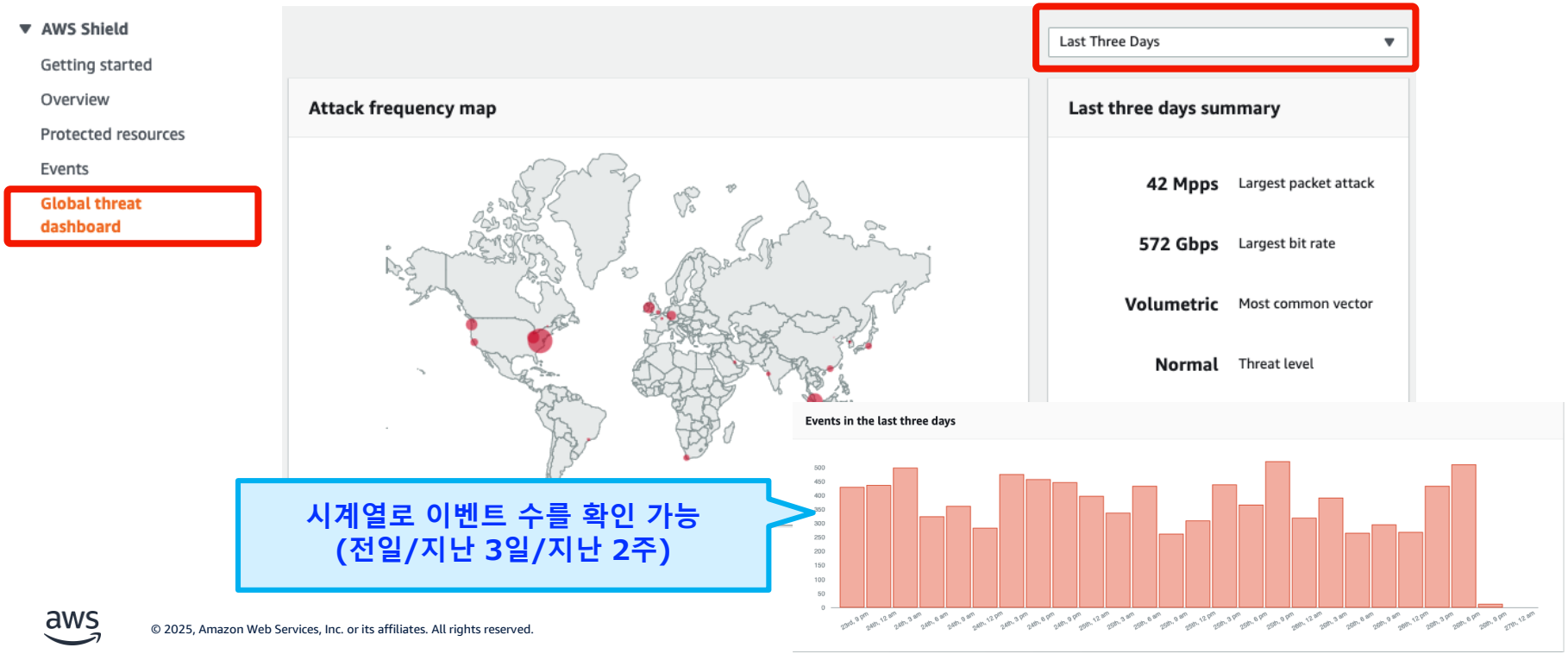
AWS Shield가 감지한 지난 2주간의 요약 정보 확인 가능

- 최대 패킷 레이트
- 최대 비트 레이트
- 가장 많은 공격 수법
- 위협 레벨
- 총 공격 수

자신의 계정에서 지난 1년간 받은 DDoS 이벤트의 수와 규모를 확인 가능 (Standard 이용만으로도 우측만 표시 가능, 상세 표시는 Advance만 가능)

AWS Shield Standard - Global threat dashboard

AWS Shield가 감지한 전일/지난 3일/지난 2주간의 정보를 표시 가능



AWS Shield Advanced

AWS Shield Standard VS Advanced

AWS Shield **Standard**

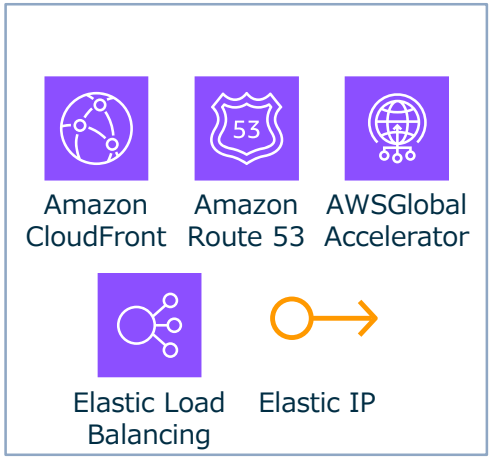
- 일반적인 레이어 3/4 공격으로부터 보호 (SYN/ UDP Floods, Reflection Attacks, 등등)
- 자동으로 감지 및 완화
- AWS 서비스에 빌트인
- 모든 사용자에게 무료로 제공

AWS Shield **Advanced**

- 상시 모니터링 및 감지
- 추가적인 레이어 3/4/7 공격으로부터 보호
- 공격 지표, 경보 및 리포트
- 24X7로 DDoS Response Team (DRT) 지원
- 추가 비용 없이 AWS WAF 사용
- DDoS 대응에 사용된 추가 자원 비용 보존
- 1년 약정 방식

AWS Shield Advanced (Standard에 대한 추가 기능)

Shield Advanced는 Shield Standard에 더해 DDoS 이벤트에 관한 더 많은 기능을 제공



Standard

- 내장된 DDoS 보호 & 일반적인 DDoS 공격 완화
- 글로벌 위협 대시보드
- 선제적 대응
- 애플리케이션 레이어(L7)의 공격 자동 완화
- CloudWatch를 통한 메트릭과 이벤트 알림
- Shield Response Team (SRT)에 24시간 액세스
- 헬스 기반 공격 탐지
- 적응형 L3/L4 방어
- AWS WAF L7 이상 탐지
- AWS WAF 무료 이용 가능(지정 보호 리소스)
- AWS Firewall Manager 무료 이용 가능
- 비용 보호(DDoS 기인 비용 흡수)

AWS Shield를 통한 L3-L4 DDoS 보호

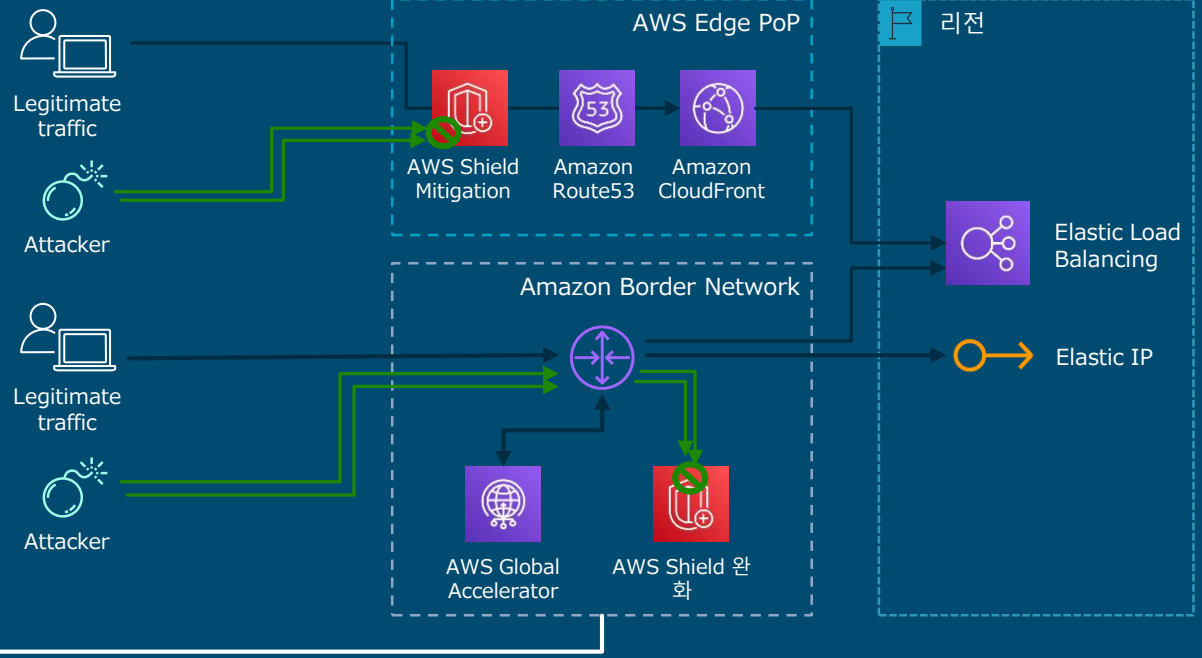
AWS Shield DDoS 완화 시스템은 AWS 네트워크 경계와 AWS 엣지 로케이션에 존재합니다.

AWS Shield @Edge

- SYN Proxy
- Continuous inspection (inline)
- Packet validation
- Distributed scrubbing capacity
- Automated routing policies to absorb large attacks

AWS Shield @경계

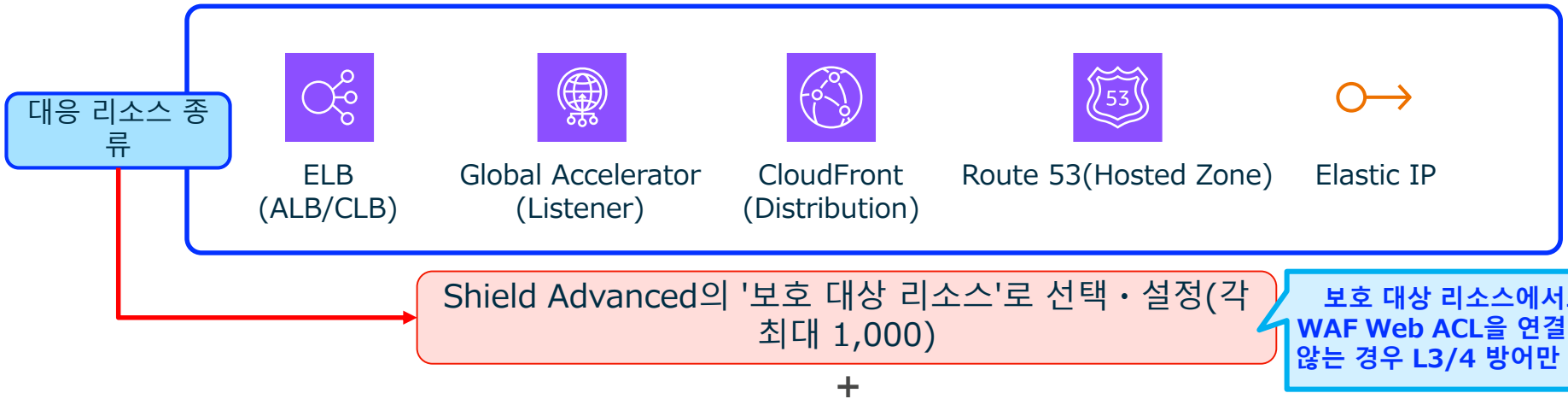
- Traffic filtering (Network ACL and Geo blocking)
- Resource-level detection & mitigation (based on resource capacity)
- Health-based detection improves accuracy



AWS Shield를 통한 L3-L4 DDoS 보호

Advanced는 개별적으로 활성화 + 보호 대상을 명시적으로 지정하여 이용 + AWS WAF를 셀프 서비스로 설정 (Advanced 적용 시 무상 이용 가능*)

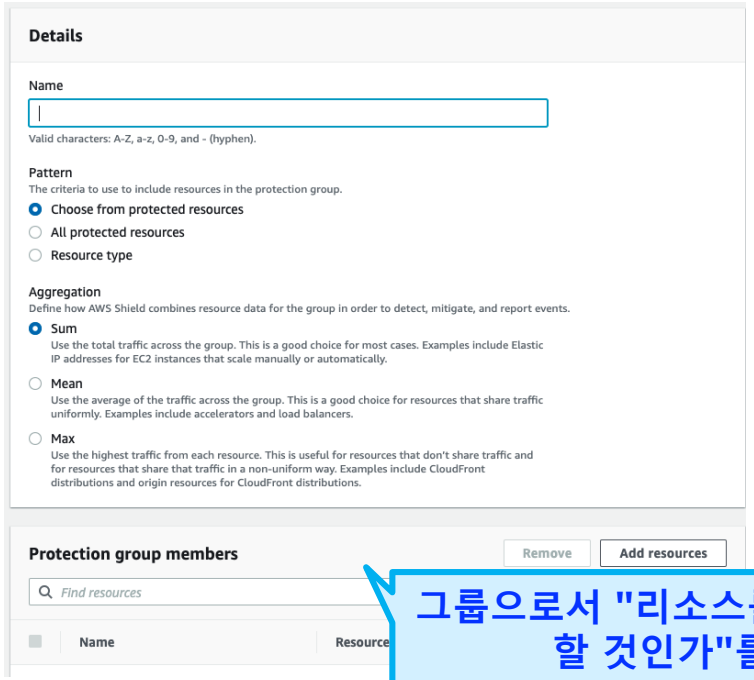
(*) AWS Marketplace에서 구매한 3rd Party AWS WAF 규칙은 유료



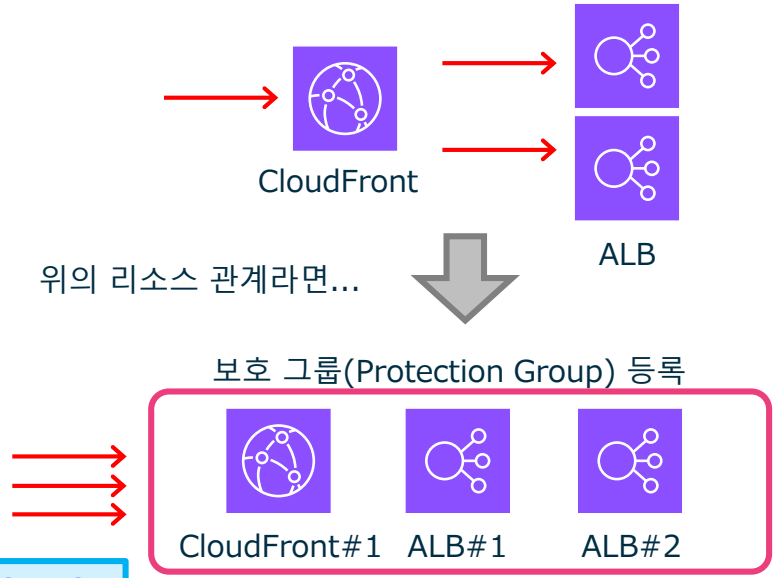
- 보다 정교한 L3/L4 공격의 탐지와 완화
- 서포트 케이스를 통한 SRT(Shield Response Team)의 공격 전/중/후 지원(24h x 7)
- DDoS 공격 이력의 이벤트 정보・CloudWatch 메트릭스를 통한 실시간에 가까운 상황 파악
- DDoS 공격으로 인해 발생한 일부 AWS 이용 요금에 대한 서비스 크레딧 제공

AWS Shield Advanced - L7 보호 리소스 그룹

보호 대상 리소스를 그룹화함으로써 여러 리소스를 하나의 그룹으로 취급하고, DDoS 탐지의 정확도를 향상



그룹으로서 "리소스를 어떻게 조합할 것인가"를 정의



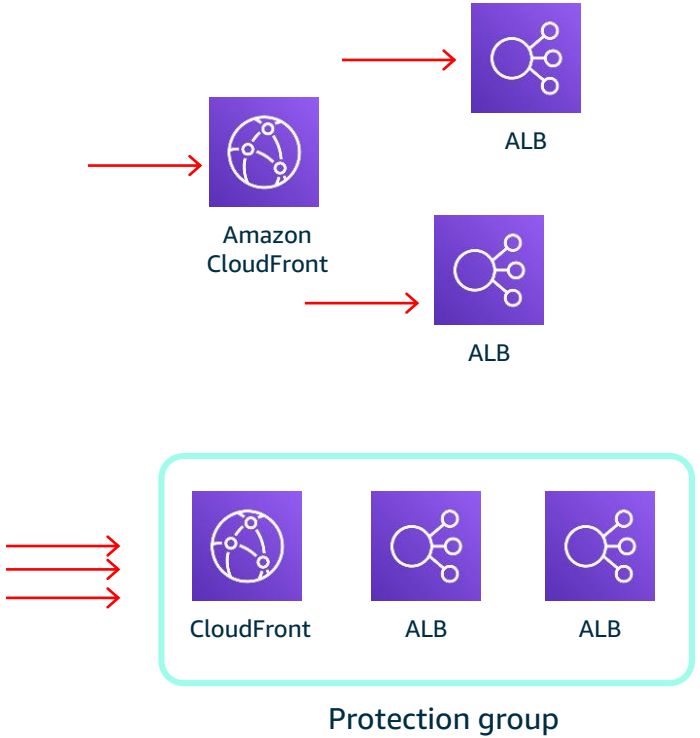
AWS Shield Advanced - L7 보호 리소스 그룹

탐지 및 완화를 위해 여러 리소스를 단일 단위로 처리

- 탐지 정확도 향상 (그룹이 동일한 기준선 공유)
- 그룹 수준 보고
- 경보 감소
- 그룹화된 리소스에 대한 자동 선제적 완화

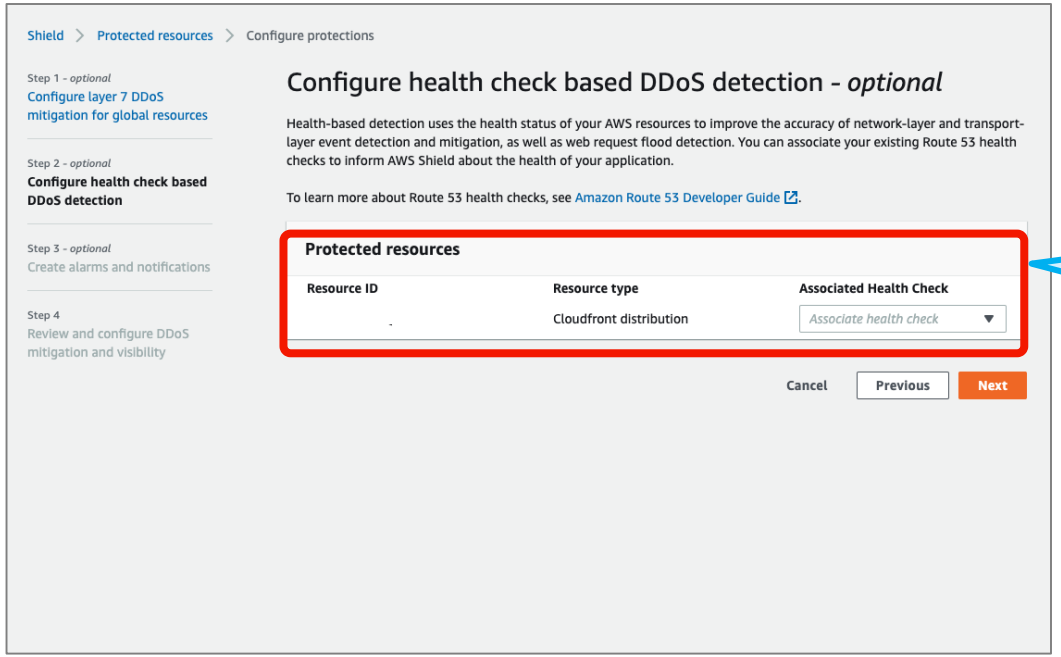
유용한 경우

- 개별적으로는 적은 트래픽을 가진 많은 리소스들이지만, 총계로는 큰 볼륨을 차지하는 경우
- 보호된 리소스 간에 트래픽이 전환되는 블루-그린 배포의 경우 애플리케이션 기준선 보존
- 공격 발생 시 완화 속도를 높이기 위해. Protection group의 한 리소스가 공격 대상이 되면, 다른 모든 리소스에 대해서도 기준이 확립됨



AWS Shield Advanced - L7 헬스 기반 탐지

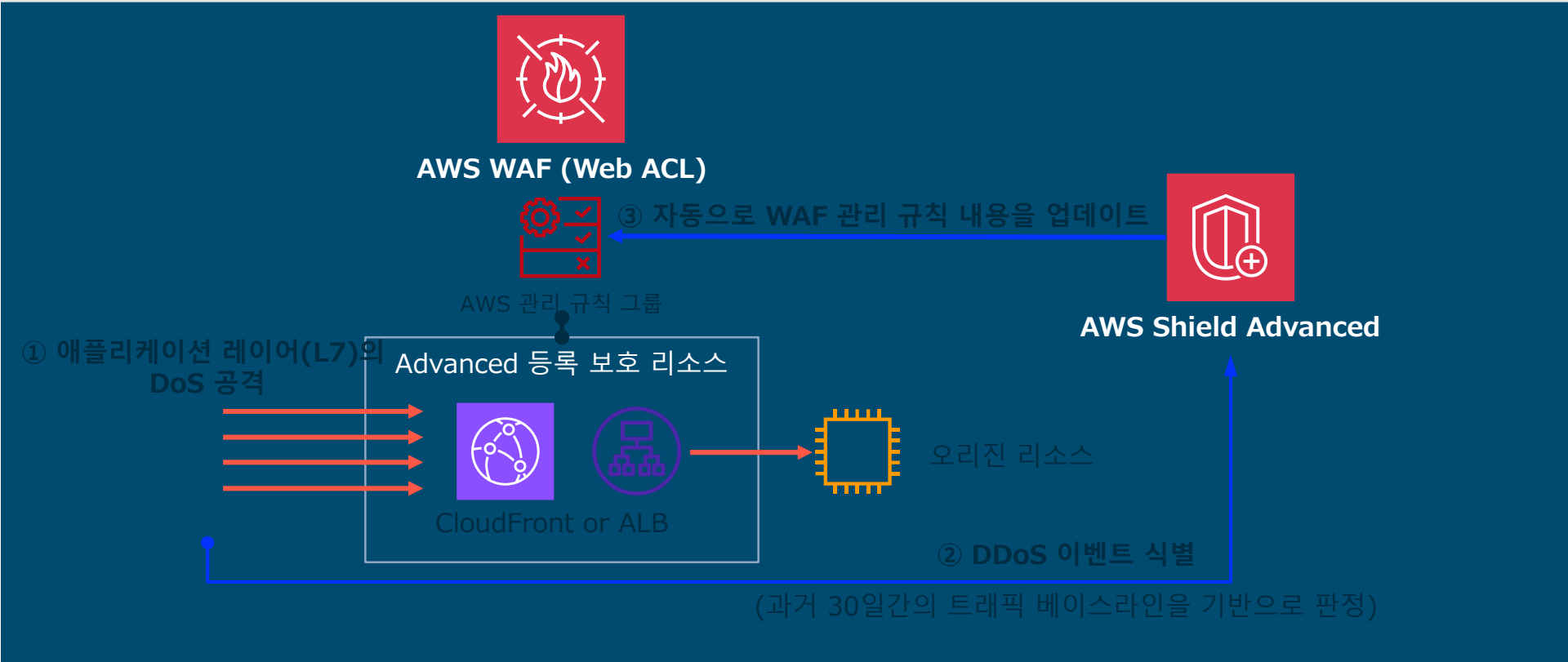
보호 대상 리소스 등록 시, Route 53 헬스 체크 설정을 연결 가능
→ L7 방어에서 DDoS 탐지 정확도 향상을 실현



리소스 연결에 대한 옵션 설정
(나중에 변경 가능)

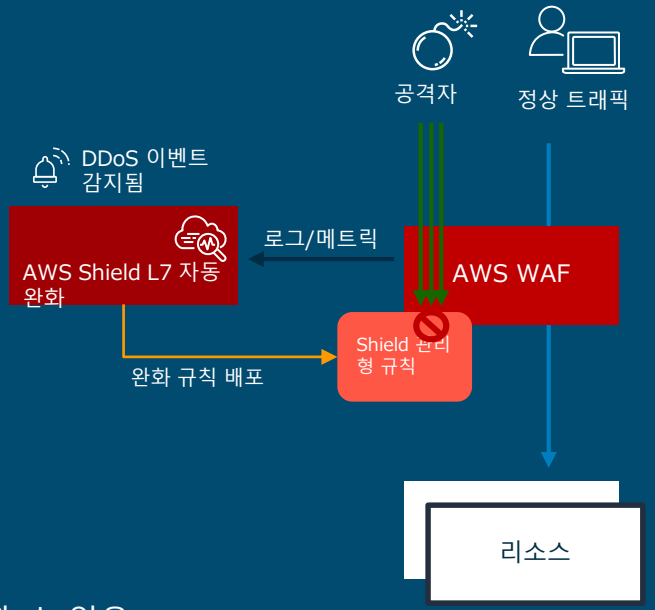
AWS Shield Advanced - 자동 L7 DDoS 완화

애플리케이션의 가용성을 위협하는 이벤트에 즉시 대응
→ 완화 조치까지의 시간 단축



AWS Shield Advanced - 자동 L7 DDoS 완화

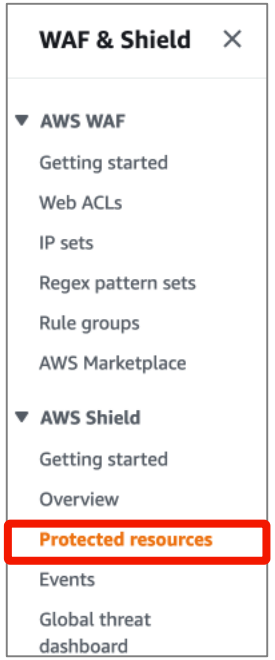
- 완화 시간을 단축하고 애플리케이션 가용성 위협에 즉시 대응
  - 감지된 DDoS 이벤트를 완화하기 위해 AWS WAF 규칙이 자동으로 생성됨
  - 오탐을 최소화하기 위해 AWS WAF 규칙이 정상 트래픽에 대해 테스트됨
  - 차단 모드로 배포하기 전에 효과를 관찰하기 위해 AWS WAF 규칙을 Count 모드로 생성할 수 있음
  - 이벤트가 종료되면 AWS WAF 규칙이 자동으로 제거됨
  - 수동 개입 불필요



Shield Advanced만이 Shield 관리형 규칙 그룹 내에 규칙을 생성할 수 있음

AWS Shield Advanced - 자동 L7 DDoS 완화

WAF 규칙 세트 내의 규칙 그룹을 플레이스홀더로 설정하고, 내부 규칙의 자동 구성을 통해 L7 계층의 DDoS 대책을 일부 자동화



대응 리소스 종류(2개) CloudFront 디스트리뷰션 또는 ALB

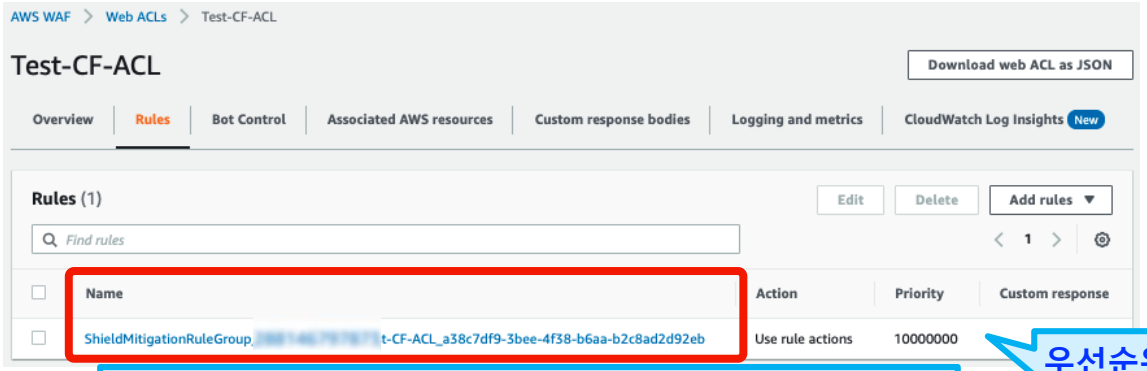
Shield Advanced의 보호 리소스로 Web ACL을 지정하고, "Automatic application layer DDoS mitigation"을 설정

자동 규칙의 동작으로 "Block" 또는 "Count" 모드 선택 (※초기에는 Count 권장)

※AWS Firewall Manager를 사용하여 Organizations 내 멤버 계정에 일원화된 적용도 가능

AWS Shield Advanced - 자동 L7 DDoS 완화

지정한 Web ACL에 150 WCU를 소비하는 규칙이 추가됨
(이 규칙은 우선순위: 10,000,000 = 즉 "우선순위: 최저"로 고정)



Web ACL에 Shield Advanced가 내용을 자동 조정하는 규칙 그룹이 추가됨(내용은 동일 서비스만이 변경 가능)

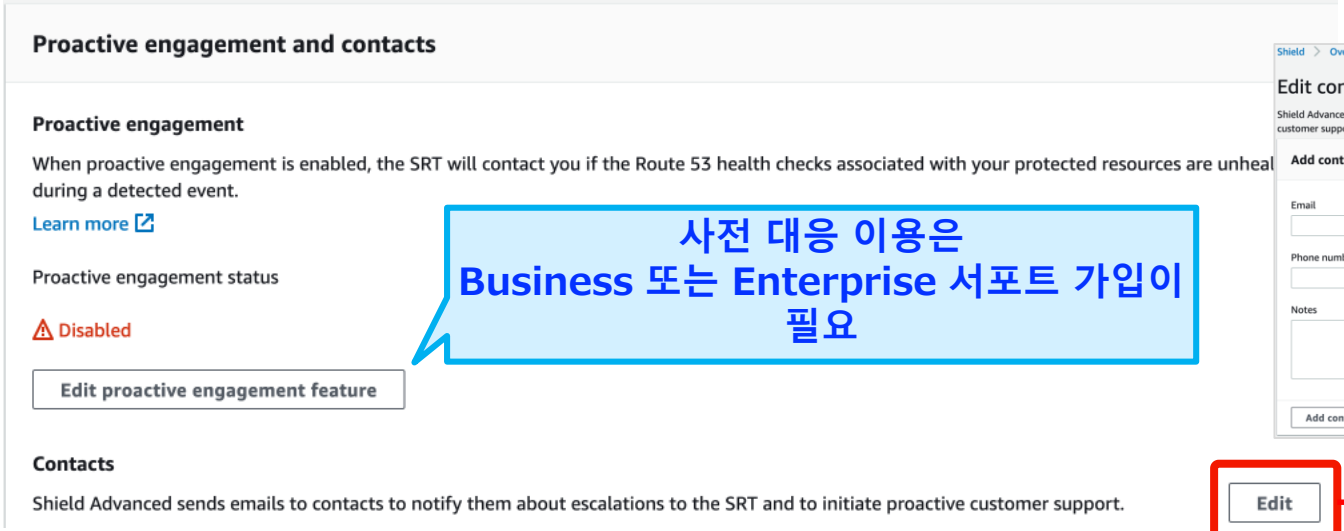
우선순위가 최저이므로 사용자 설정 규칙이 항상 우선됨

- "지난 30일간의 트래픽 상황"을 기준선으로 하여, 이를 기반으로 자동 이상 감지
- 기준선에서 유의미한 편차가 있는 경우 DDoS 이벤트로 보고
- Route 53 헬스체크 상태도 DDoS 이벤트 판정 시 참고 자료로 사용됨
- 각 L7 DDoS 이벤트마다 공격 시그니처가 판정되며, "공격이다"라고 높은 확률로 판단된 경우 자동 규칙으로 Web ACL의 해당 규칙 그룹에 추가됨(공격 종료 판정 후 자동 삭제)

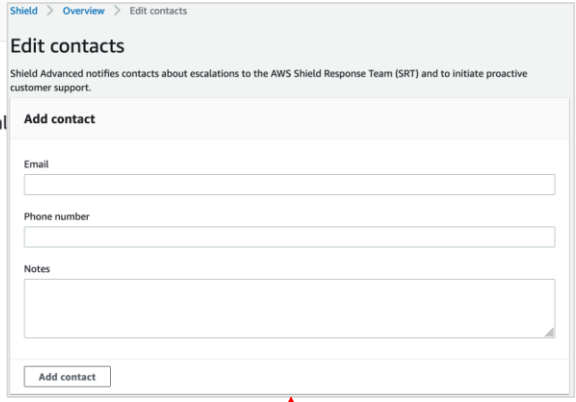
※필수는 아니지만, Web ACL에 레이트 기반 보호 규칙 설정을 동시에 수행하는 것을 권장

AWS Shield Advanced - 사전 대응

Route 53 헬스체크의 활성화 및 보호 리소스에 대한 설정을 전제로, 공격 이벤트로 인한 Unhealthy 상태 시 SRT에서 등록된 연락처로 연락



사전 대응 이용은 Business 또는 Enterprise 서포트 가입이 필요



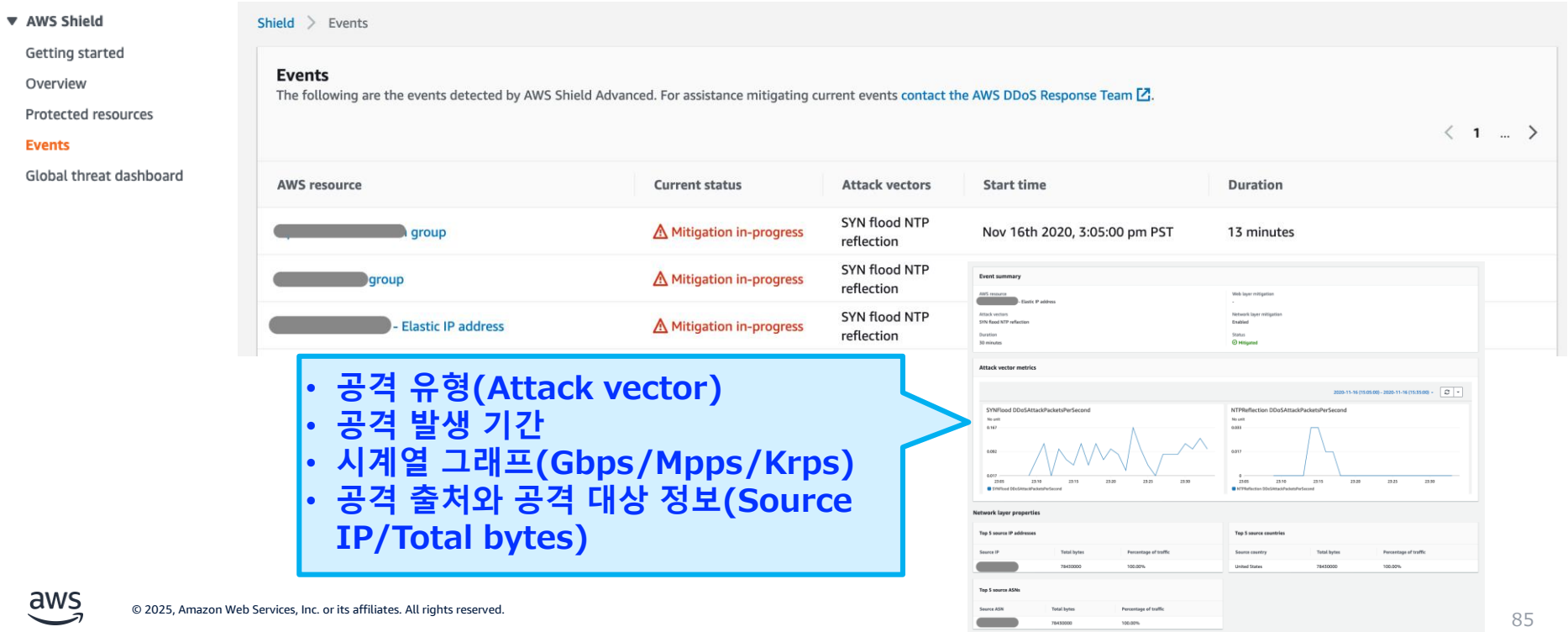
Edit

※서포트 레벨의 전제 조건에 더해,
보호 리소스에 대한 "정상성 기반 체크(헬스 기반 체크)" 설정이 필수

계정당 최대 10개까지의 연락처 등록 가능 (이메일, 전화번호)

AWS Shield를 통한 DDoS 가시성 확보

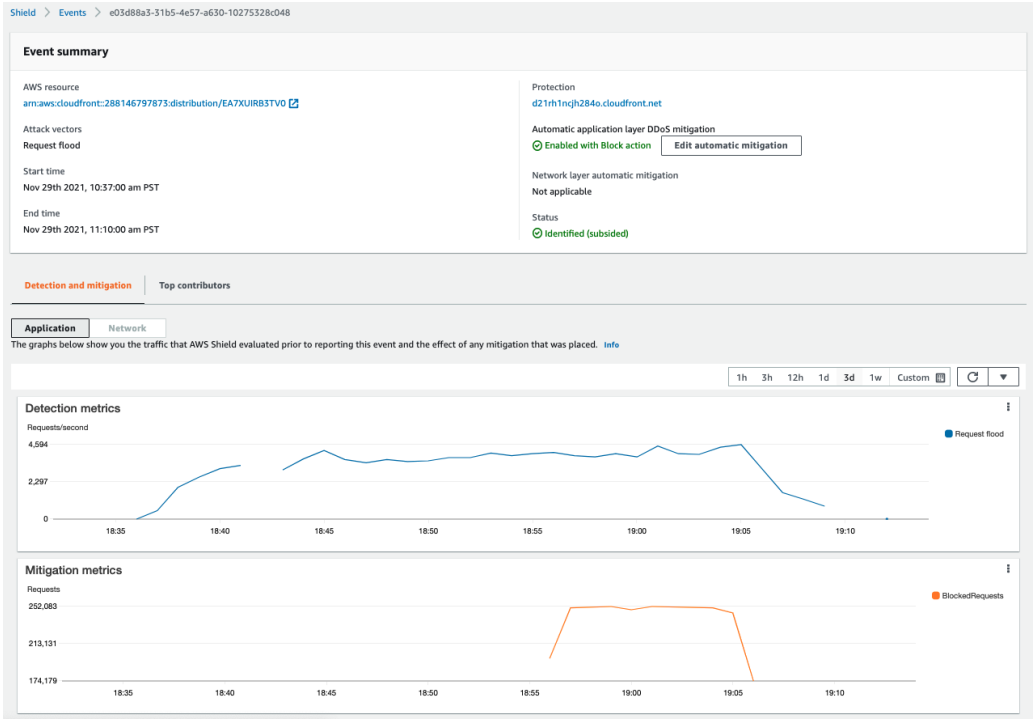
현재 진행중인 것을 포함하여, 지난 13개월 동안의 자신의 계정에 대한 DDoS 공격 이력 확인 가능



- **공격 유형(Attack vector)**
- **공격 발생 기간**
- **시계열 그래프(Gbps/Mpps/Krps)**
- **공격 출처와 공격 대상 정보(Source IP/Total bytes)**

AWS Shield를 통한 DDoS 가시성 확보

'보호 대상 리소스'에 관한 개별 DDoS 이벤트를 인식하고, 요약하여 대시보드에 시각화



- 검출된 '이벤트' 마다 다음 항목이 표시
  - 리소스에 대한 요청량
  - 차단된 요청량
  - 이벤트 고유의 타임라인
  - 13개월간 보관
- 상위 Contributor(각 상위 5개)
  - 출발지/목적지 IP 주소
  - 국가
  - URL
  - 사용자 에이전트
  - 리퍼러
- CloudWatch 메트릭스

AWS Shield를 통한 DDoS 가시성 확보

Shield Advanced는 아래 표의 CloudWatch 메트릭을 발행

https://docs.aws.amazon.com/waf/latest/developerguide/shield-metrics.html

네임스페이스	메트릭스명	설명
AWS/DDoSProtection	DDoSDetected	특정 리소스의 DDoS 공격 상태(공격 중일 때 1, 그 외의 경우 0)
	DDoSAttackBitsPerSecond	특정 리소스의 DDoS 이벤트 중 감지된 비트 수 ※평상시에는 1일 1회 0.0이 기록되며, 공격 중에는 0이 아닌 값
	DDoSAttackPacketsPerSecond	특정 리소스의 DDoS 이벤트 중 감지된 패킷 수 ※평상시에는 1일 1회 0.0이 기록되며, 공격 중에는 0이 아닌 값
	DDoSAttackRequestsPerSecond	특정 리소스의 DDoS 이벤트 중 감지된 요청 수 ※평상시에는 1일 1회 0.0이 기록되며, 공격 중에는 0이 아닌 값

※ DDoS 공격 감지 중에는 1분에 1회, 그리고 완화 시에 1회 메트릭이 발행됨
※ DDoS 공격 감지 외에는 1일에 1회 메트릭이 발행됨
※ 글로벌 서비스(CloudFront 배포, Route 53)는 us-east-1 리전에 메트릭이 기록됨

AWS Shield를 통한 DDoS 가시성 확보

Shield Advanced 고유 기능: 관리 콘솔 내 메뉴와 CloudWatch 메트릭스 (거의 실시간으로 알림 → 이벤트 알림 설정 가능)

AWS Shield Advanced - 서비스 요금

① 월 3,000 USD의 1년 구독 계약 (Organizations 단위) + ② 아래 표의 데이터 전송(아웃바운드) 요금 (각 계정 단위)

※①은 Organizations의 관리 계정에 대해 발생 (비용 청구는 Organizations 단위로 1개. 이용을 위한 '활성화' 설정은 계정 단위)
※보호 그룹 리소스에 대해 설정한 AWS WAF 요금(Web ACL, 규칙, 요청에 대한 요금)은 발생하지 않음

	데이터 전송량 ($ per GB)				
	Amazon CloudFront	**ELB**	**Elastic IP**	**AWS Global Accelerator**	**Amazon Route 53**
처음 100 TB	$0.025	$0.050	$0.050	$0.050	추가 요금 없음
다음 400 TB	$0.020	$0.040	$0.040	$0.040	추가 요금 없음
다음 500 TB	$0.015	$0.030	$0.030	$0.030	추가 요금 없음
다음 4 PB	$0.010	문의하기	문의하기	문의하기	추가 요금 없음
5 PB 초과	문의하기	문의하기	문의하기	문의하기	추가 요금 없음

https://aws.amazon.com/ko/shield/pricing/

※②표의 데이터 전송 요금은 보호 대상 리소스에서 인터넷으로의 아웃바운드에 대해 발생
(→ VPC 및 기타 서비스의 '데이터 전송(아웃바운드) 요금'과는 별도로 발생)

가격 책정에 대해 기억해야 할 몇 가지 사항 (1/2)

- 가격은 1년 약정으로 월 3천 달러의 구독료와 각 보호 리소스에서 발생하는 데이터 전송 사용 요금(GB당)을 기준으로 책정됩니다
- 월 3천 달러의 구독료는 전체 AWS 조직에 적용됩니다
- 귀사에 여러 AWS Organization이 있는 경우, AWS에 연락하여 결제를 통합하고 전체 회사에 대해 하나의 구독료만 지불할 수 있습니다
- AWS Organization의 모든 연결된 계정에서 Shield Advanced를 구독할 수 있습니다. 결제는 Payer 계정 수준에서 이루어집니다

가격책정에 대해 기억해야 할 몇 가지 사항 (2/2)

- Shield Advanced로 보호되는 각 리소스에 설정된 WAF 사용량은 요금이 부과되지 않습니다.
- 보호되는 리소스와 관련되지 않은 다른 WAF 기능들은 여전히 요금이 부과됩니다. 예: AWS WAF Bot Control, Shield Advanced로 보호되지 않는 리소스에 대한 WAF 요금 등
- AWS Shield Advanced 고객의 경우, AWS Firewall Manager 보호 정책이 추가 비용 없이 포함됩니다. Shield Advanced 고객은 리소스 구성 변경을 모니터링하기 위해 생성된 AWS Config 규칙에 대해서만 요금이 부과됩니다.

비용 보호: 크레딧이 적용 가능한 요금 유형

- Amazon CloudFront HTTP/HTTPS 요청
- CloudFront 데이터 전송 출력
- Amazon Route 53 쿼리
- **AWS Global Accelerator 표준 액셀러레이터 데이터 전송**
- **Application Load Balancer의 로드 밸런서 용량 단위**
- 보호된 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스의 사용량 급증

비용 보호: 크레딧을 받기 위한 자격 조건

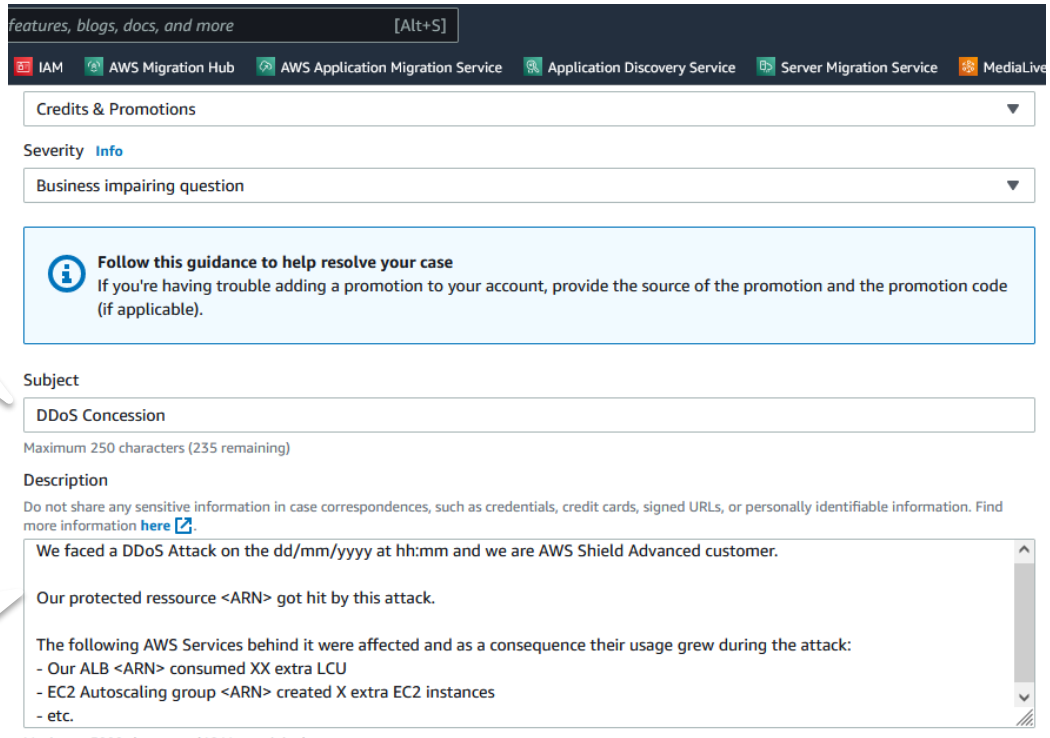
- DDoS 복원력을 위한 AWS 모범 사례를 구현해야 함
- 공격이 시작되기 전에 리소스가 보호되어 있어야 함
- CloudFront Distribution과 ALB로 보호된 리소스의 경우, AWS WAF web ACL을 연결하고 해당 web ACL에 요율 기반 규칙을 구현해야 함

https://docs.aws.amazon.com/waf/latest/developerguide/request-refund.html

AWS Shield Advanced 크레딧 신청 방법

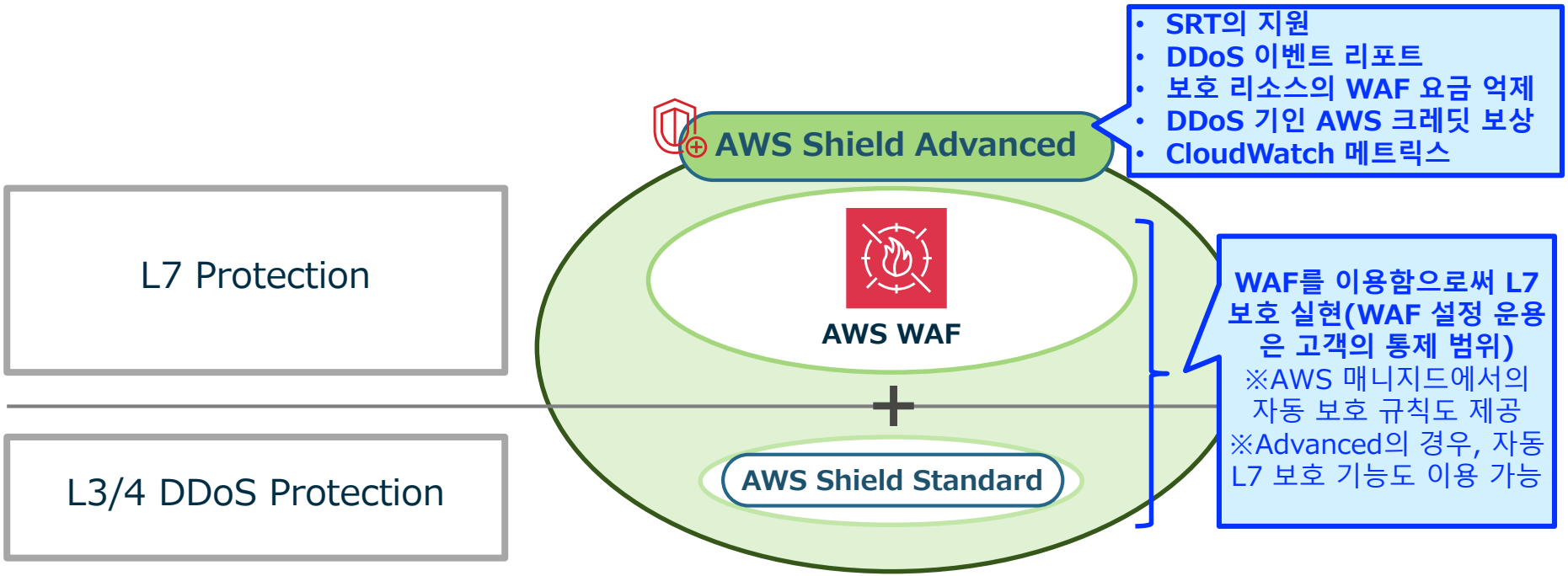
제목에 "DDoS Concession"을 포함하여 "Account & Billing" Support 케이스를 생성하세요

공격 발생 후 15일 이내에 티켓을 생성하고 공격의 영향을 받은 리소스와 관련된 모든 세부 정보 및 공격으로 인해 발생한 비용을 제공하세요



AWS Shield - 요약

L3/4 보호는 AWS Shield Standard로 대응, L7 보호는 AWS WAF로 대응
고급 기능/기업 내 복수 AWS 계정에 대한 보호 옵션을 Advanced가 제공



기능	AWS Shield Standard	AWS Shield Advanced
활성 모니터링		
네트워크 흐름 모니터링	가능	가능
자동 상시 감지	가능	가능
자동화된 애플리케이션(계층 7) 트래픽 모니터링		가능
DDoS 완화		
SYN flood 및 UDP 반사 공격과 같은 일반적인 DDoS 공격에 대한 보호 지원	가능	가능
DDoS 완화 기능에 대한 액세스		가능
사용자 지정 애플리케이션 계층(계층 7) 완화	가능, 사용자가 직접 AWS WAF ACL을 설정 해야함	가능, 사용자가 직접 AWS WAF ACL을 설정하거나 DRT의 도움으로 설정할 수 있음
즉각적인 규칙 업데이트	가능, 사용자가 직접 AWS WAF ACL을 설정 해야함	가능, 사용자가 직접 AWS WAF ACL을 설정하거나 DRT의 도움으로 설정할 수 있음
앱 취약성 보호를 위한 AWS WAF	가능, 사용자가 직접 AWS WAF ACL을 설정 해야함 AWS WAF 요금이 발생함	가능, AWS WAF 요금 발생 하지 않음
가시성 및 보고		
계층 3/4 공격 알림		가능
계층 3/4 공격 과학 수사 보고서 (소스 IP, 공격 벡터 등)		가능
계층 7 공격 알림	가능, 사용자가 직접 AWS WAF ACL을 설정 해야함 AWS WAF 요금이 발생함	가능
계층 7 공격 과학 수사 보고서 (Top Talker 보고서, 샘플링된 요청 등)	가능 사용자가 직접 AWS WAF ACL을 설정 해야함 AWS WAF 요금이 발생함	가능
계층 3/4/7 공격 기록 보고서		가능
DDoS 대응 팀 및 지원		
심각도 높은 이벤트 중 인시던트 관리		가능
공격 중 사용자 지정 완화		가능
사후 공격 분석		가능
비용 보호		
Amazon Route 53 DNS DDoS 요금 배상		가능
CloudFront DDoS 요금 배상		가능
ELB(Elastic Load Balancing) DDoS 요금 배상		가능

Thank you!