

AWS와 Splunk를 활용한 DoS(DDoS) 탐지 및 대응 시스템



목차페이지

메인타이틀에 대한 세부 설명을 입력해 주세요.

01

프로젝트 개요

02

전체 아키텍처

03

Splunk 로그 수집 및 탐지

04

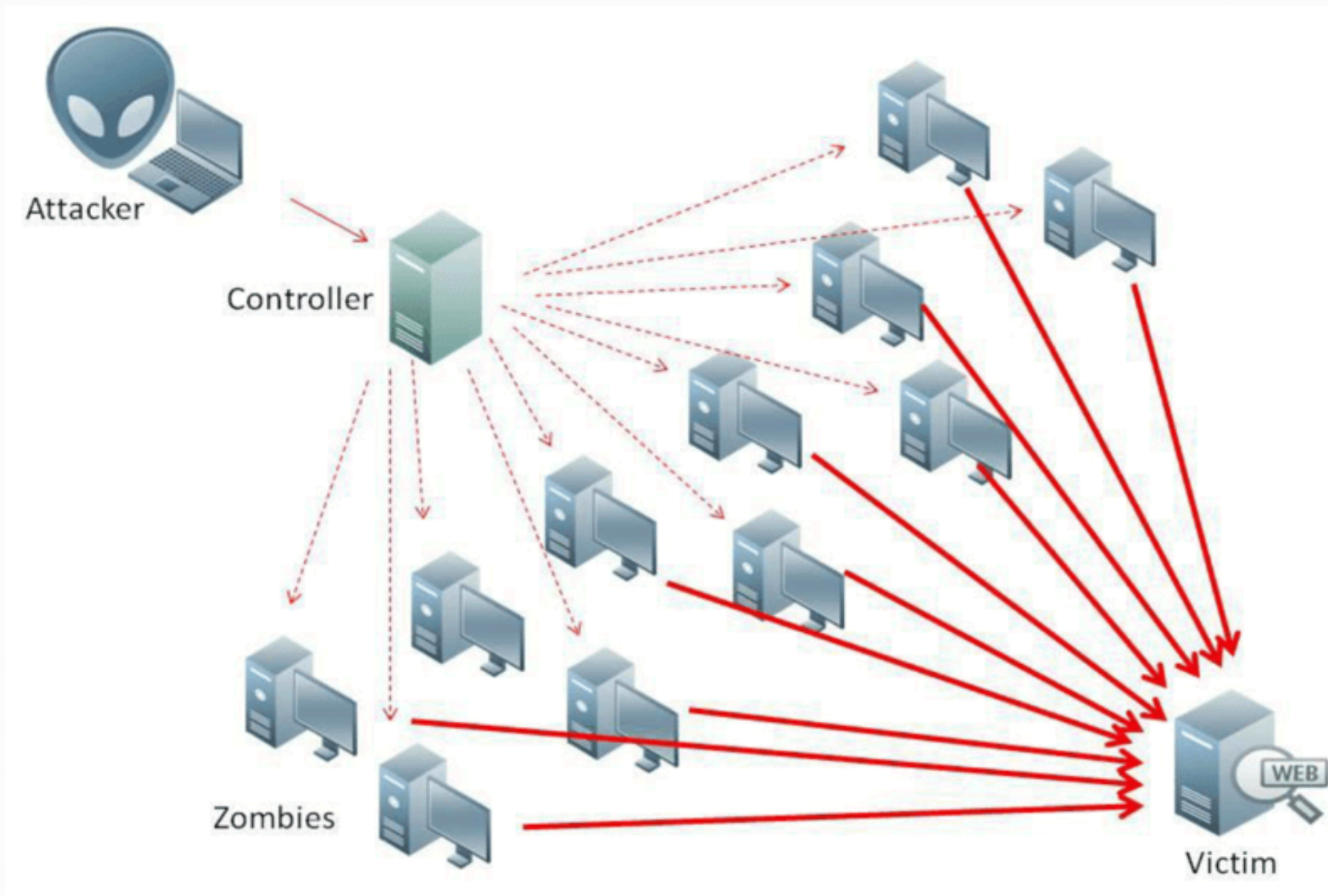
DOS(HTTP flood) 날리기

05

문제점

프로젝트 개요

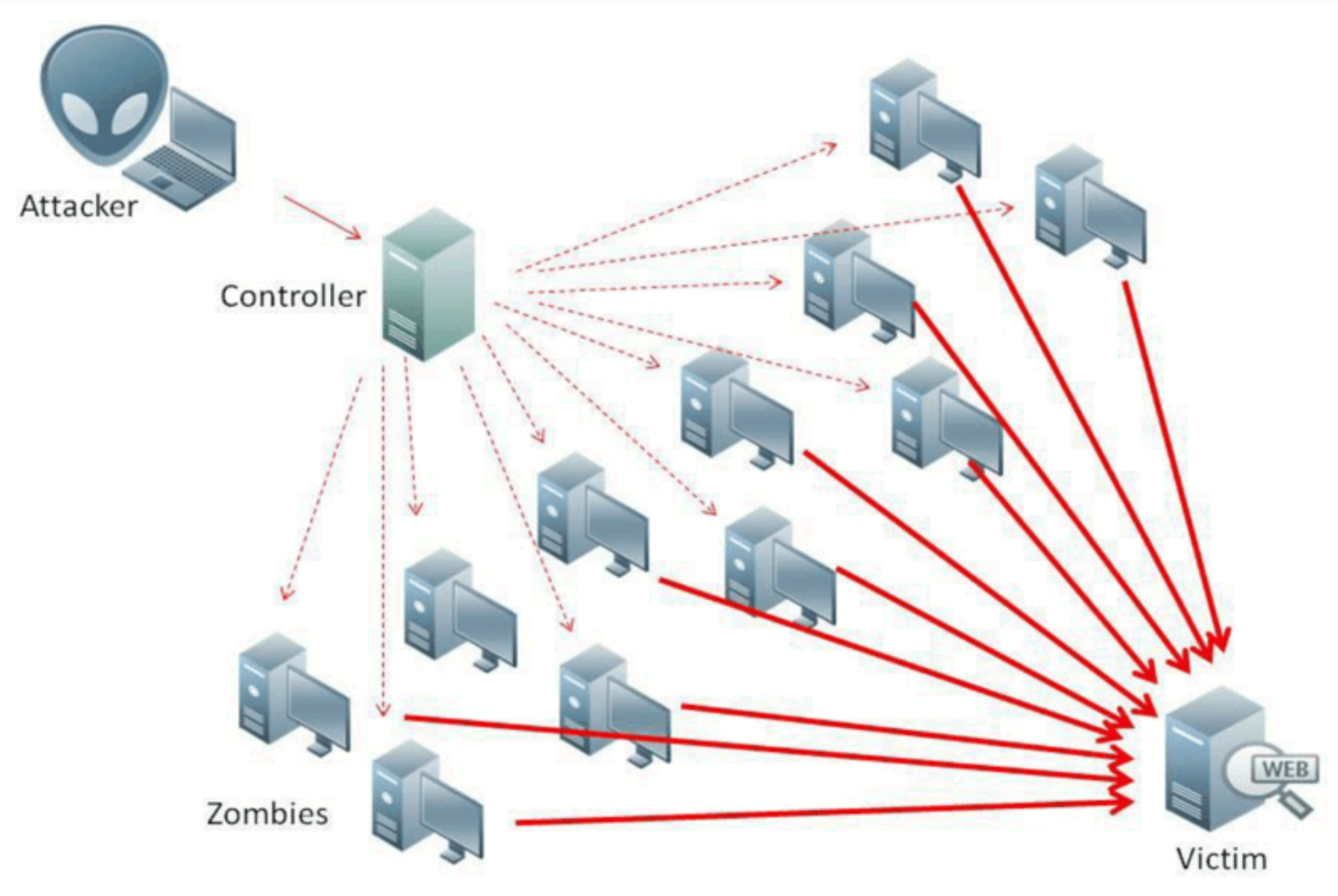
여기 디도스 공격을 당하고 있는 서버가 있습니다.



관리자

프로젝트 개요

공격자가 웹사이트에 짧은 시간 동안 반복적으로 요청을 보내자 서버 로그에는 수많은 접속 기록이 쌓이기 시작합니다.



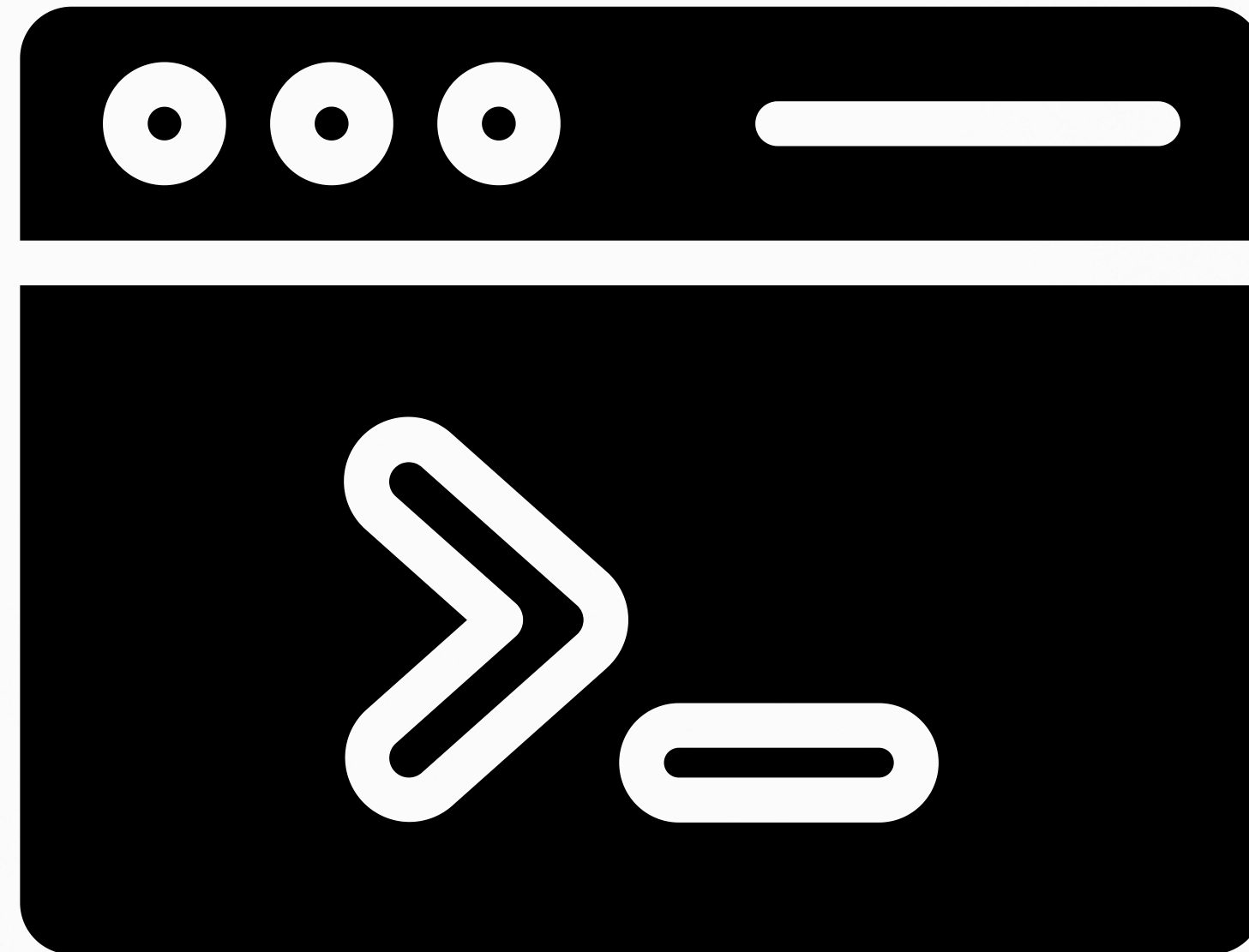
192.168.10.23 - GET /product
188.221.173.107 - GET /product
192.168.10.23 - GET /product
192.221.10.23 - GET /product

•
•
•
•

프로젝트 개요



기존 CLI에서 tail, grep, sort, uniq 등의 명령어를 사용하면 특정 IP의 요청을 확인할 수 있습니다.



프로젝트 개요

하지만 로그의 양이 많아질수록 문제가 발생합니다.

[illegible]



A large black arrow pointing right towards a large black question mark.



솔직히 CLI 로 분석 하는건 눈이 아프고 귀찮습니다.



편한거 추구

프로젝트 개요



프로젝트 개요



좋은점? 뭐하는 거?

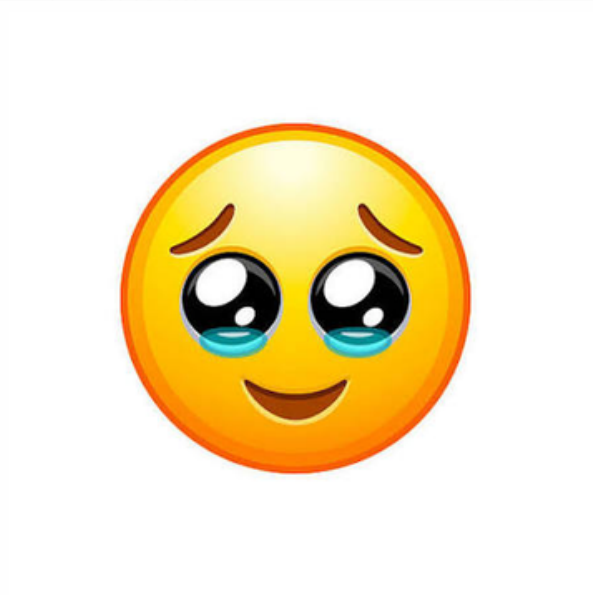
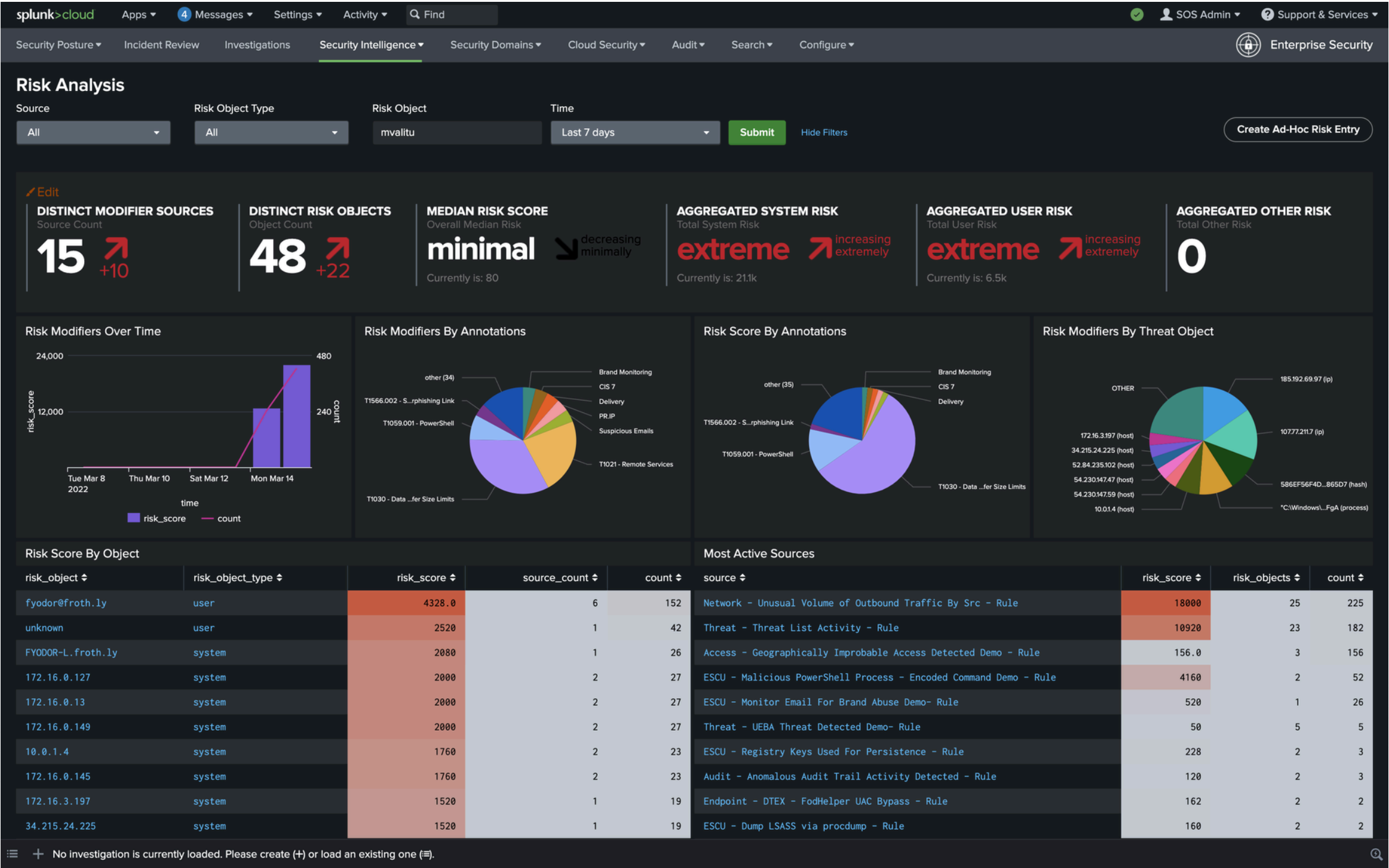
프로젝트 개요



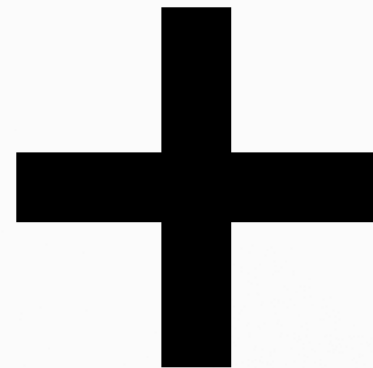
머신 데이터를 수집, 검색, 모니터링, 분석 및 시각화하는 데이터 플랫폼 솔루션.
서버, 애플리케이션, 네트워크 장비 등에서 발생하는 대규모 로그 데이터를
실시간으로 통합 관리하여 비즈니스와 보안 통찰력을 제공

프로젝트 개요

가장 좋은거(특징): 대시보드화 가능



프로젝트 개요



프로젝트 개요



사실 Grafana,Datadog,Wazuh 여러 가지 유사 도구 들이 있다

프로젝트 개요



그중 저는 Splunk 를 사용 해보고자 합니다.

프로젝트 개요



← 사실상 업계 표준

포춘 100대 기업 중 90% 이상 사용: 미국 Fortune 100
대기업 중 90곳이 넘는 기업이 보안 및 로그 분석을 위해
Splunk를 사용하고 있습니다.

프로젝트 개요

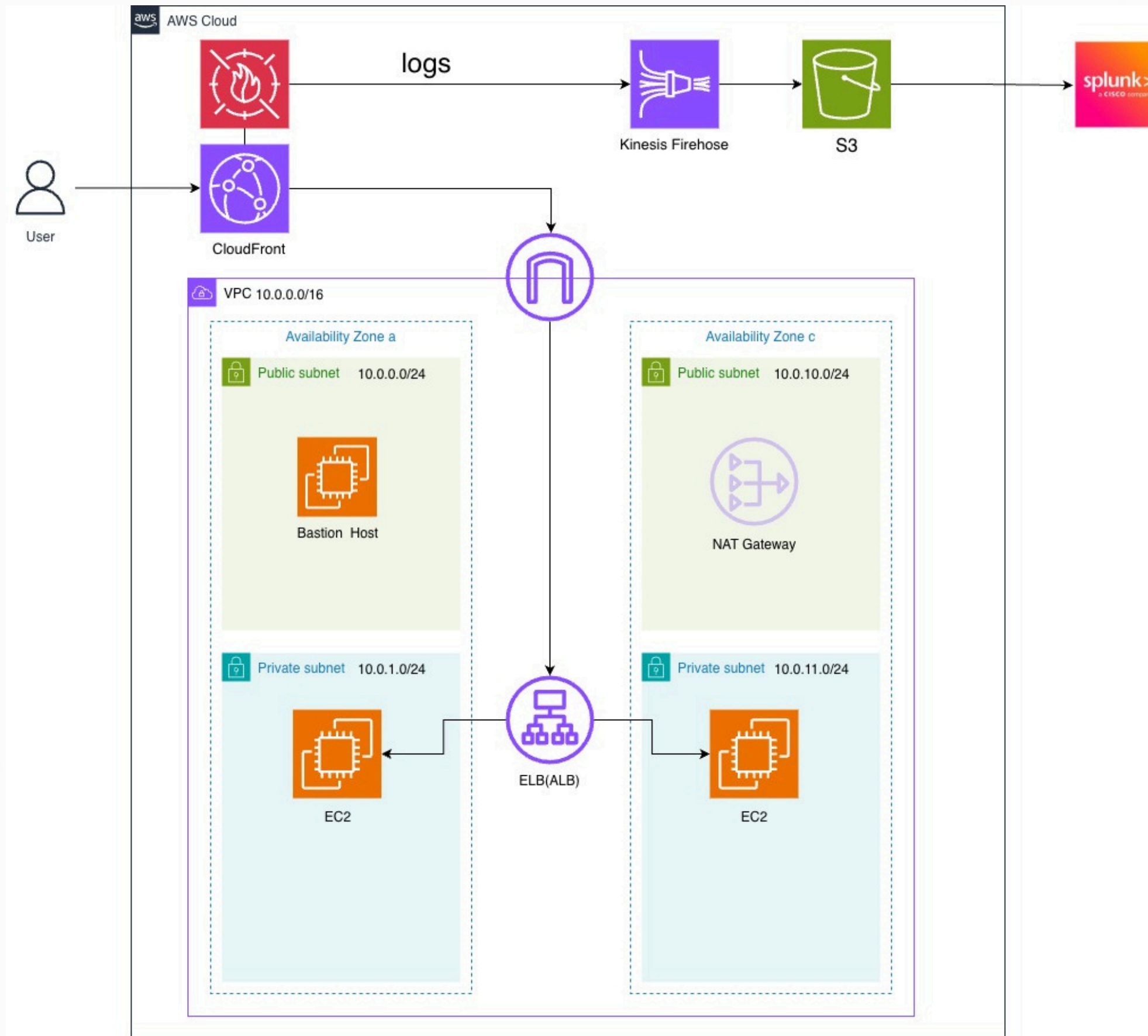


← 사실상 업계 표준

포춘 100대 기업 중 90% 이상 사용: 미국 Fortune 100
대기업 중 90곳이 넘는 기업이 보안 및 로그 분석을 위해
Splunk를 사용하고 있습니다.

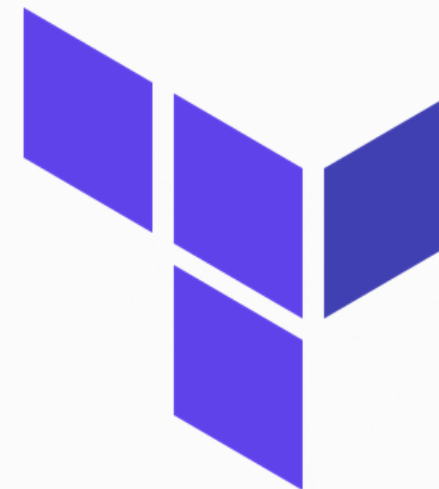
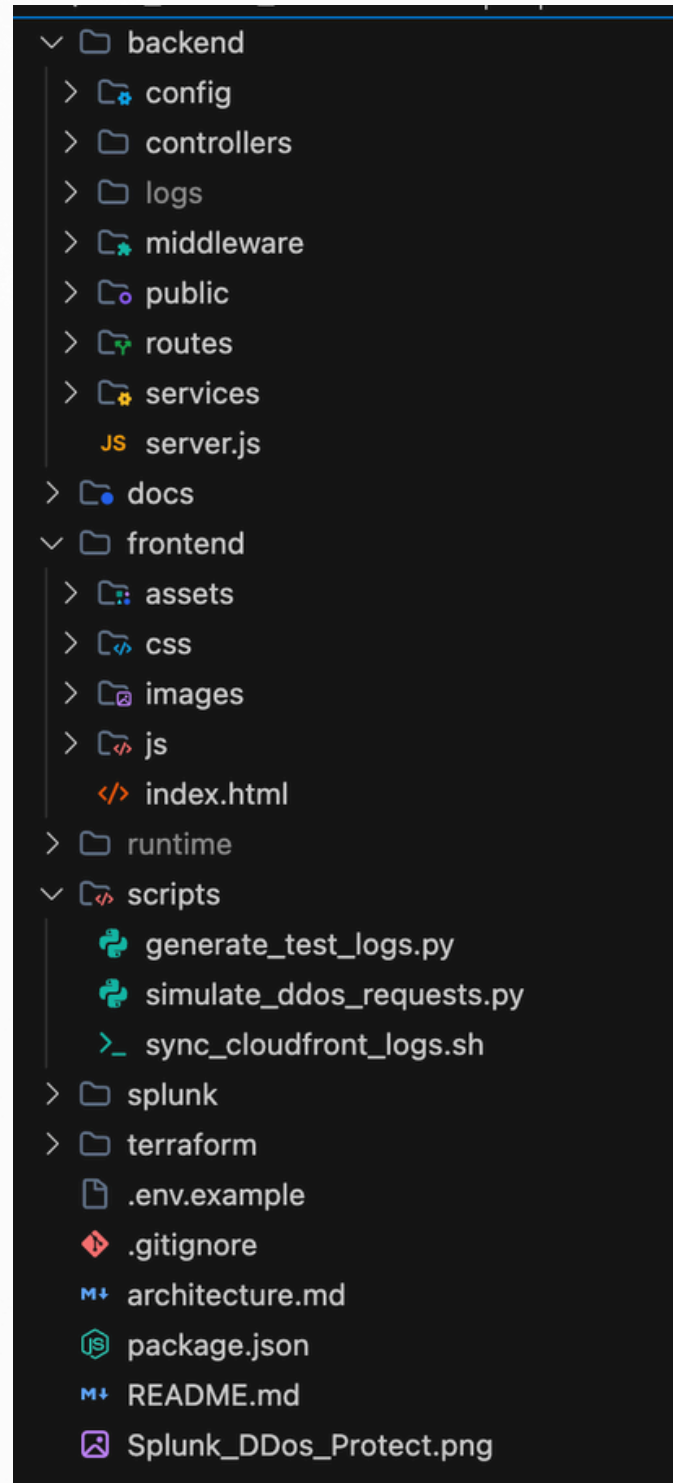
단점: 조금 많이 비쌘

전체 아키텍처



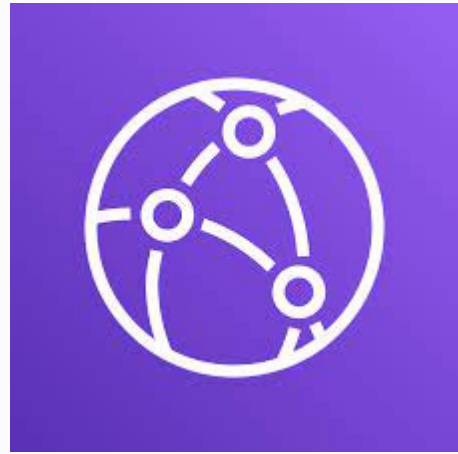
전체 아키텍처

skill



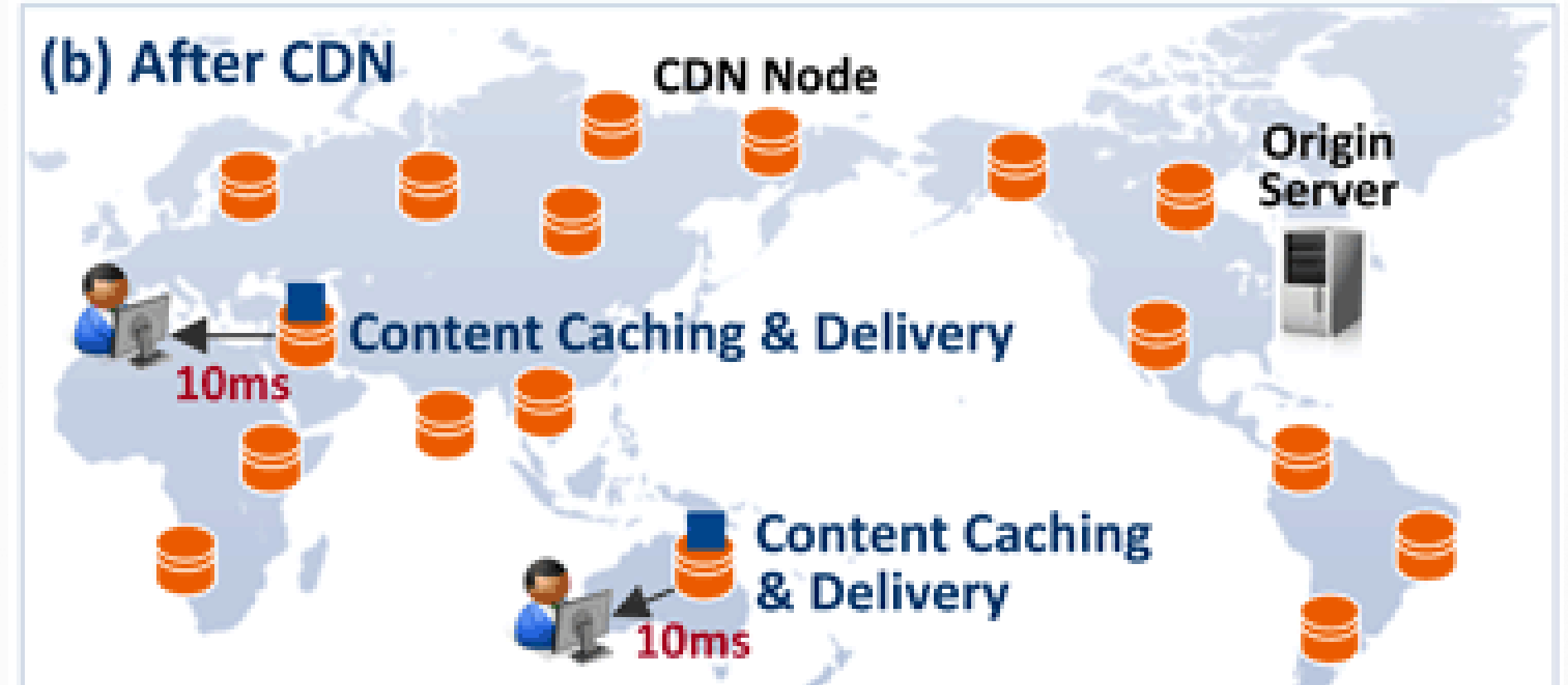
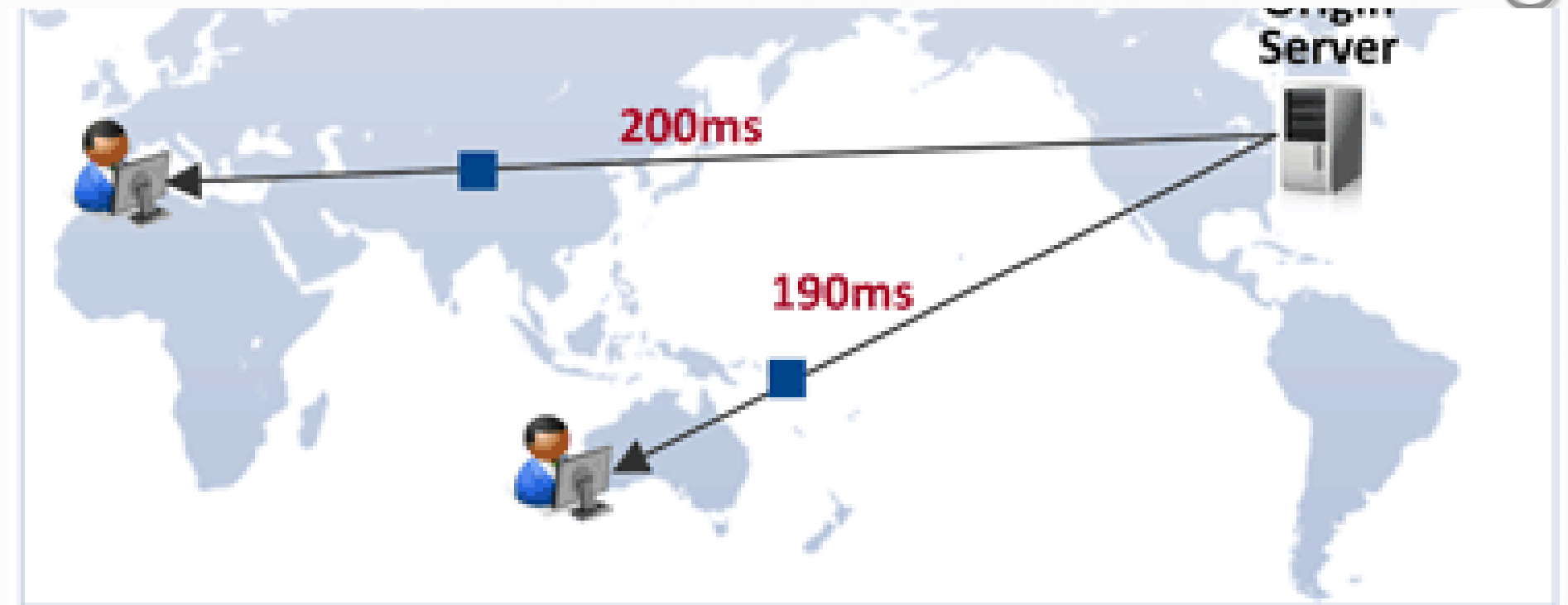
단락 텍스트

전체 아키텍처



CloudFront

이미지, 동영상 등 정적·동적 웹 콘텐츠를
빠르고 안전하게 전송하는 AWS의 글로벌
콘텐츠 전송 네트워크(CDN) 서비스



전체 아키텍처



WAF(Web Application Firewall)

웹 애플리케이션으로 들어오는 HTTP/HTTPS 트래픽을 모니터링하고 필터링하는 웹 방화벽.
SQL 인젝션, 크로스 사이트 스크립팅(XSS) 같은 악의적인 공격을 차단 하는 AWS 서비스

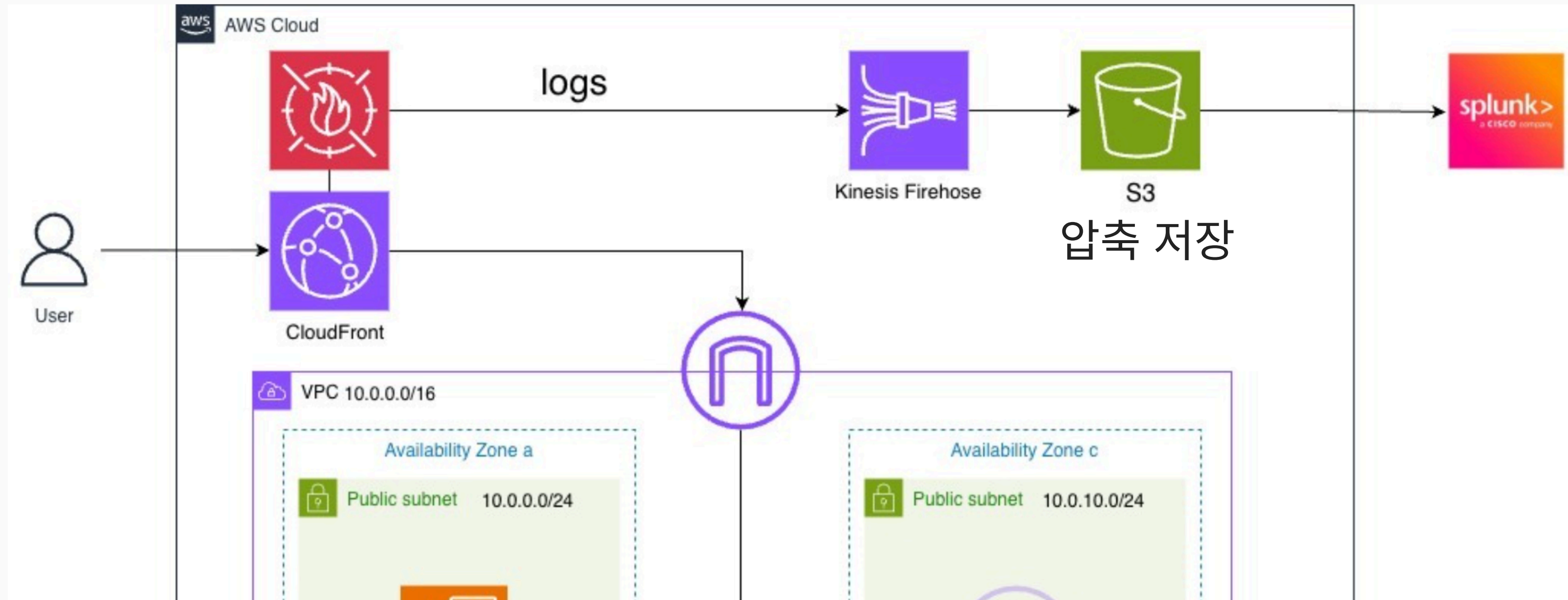
전체 아키텍처



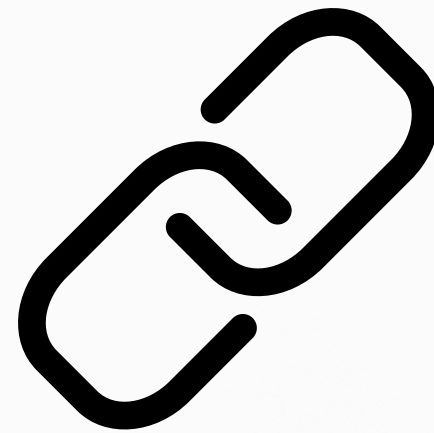
Kinesis Data Firehose

는 실시간 스트리밍 데이터를 인프라 관리 없이 클릭 몇 번으로 Amazon S3, Splunk 등 원하는 목적지로 자동 변환하여 안전하게 전송·저장해 주는 완전관리형(서버리스) 데이터 로드 서비스

전체 아키텍처

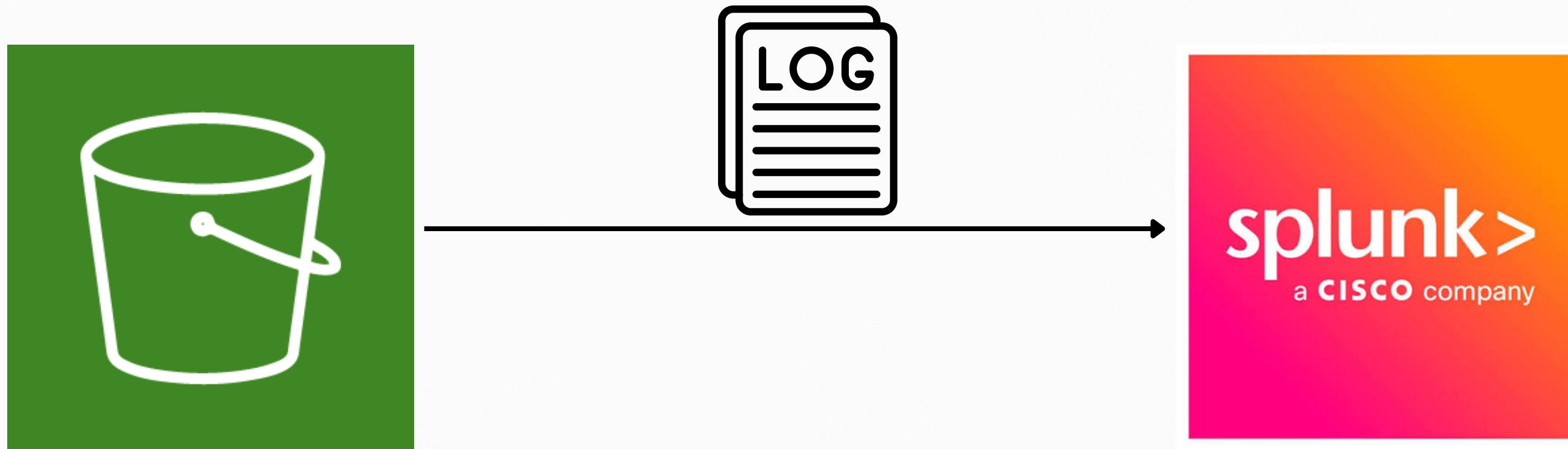


Splunk 로그 수집 및 탐지



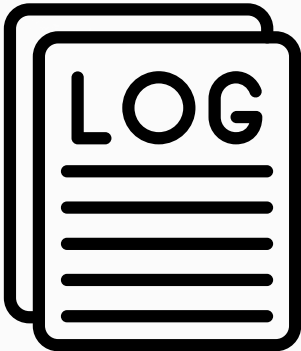
Splunk 로그 수집 및 탐지

자세히는 S3 에 저장 해논 로그 들을 가지고 와야 한다



Splunk 로그 수집 및 탐지

자세히는 S3 에 저장 해논 로그 들을 가지고 와야 한다



SPLUNK DDOS PROTECT DEMO

로컬 저장

보안 이벤트를 전송하는 가상 상점

Shield

Edge Shield Hoodie

CloudFront 엣지를 테마로 한 데모 상품입니다.

KRW 79000

상품 보기

WAF

WAF Guard Cap

봇 트래픽 차단을 상징하는 캡입니다.

KRW 32000

상품 보기

S3

Log Bucket Tote

S3 로그 저장소 콘셉트의 토트백입니다.

KRW 45000

상품 보기

SPL

Splunk Query Mug

SPL 탐지 쿼리를 떠올리게 하는 머그입니다.

KRW 21000

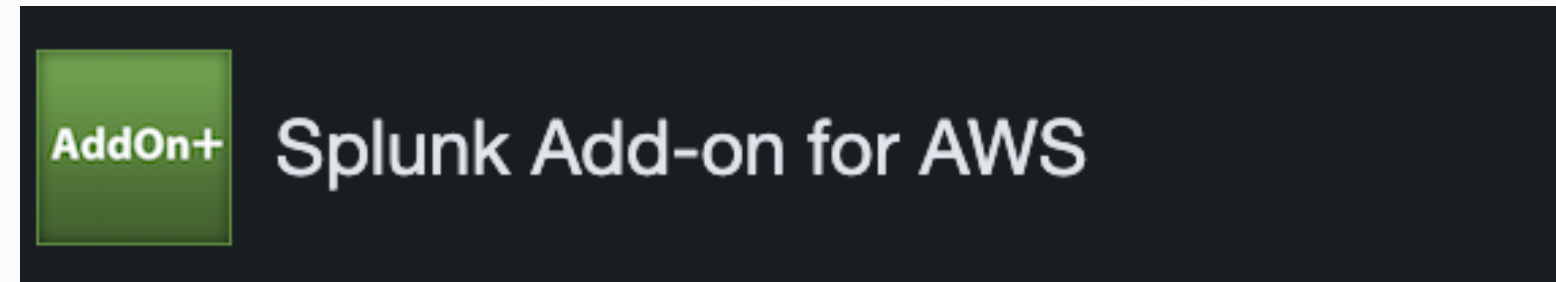
상품 보기

전송 JSON

```
{
  "ok": true,
  "event": {
    "event_type": "product_click",
    "timestamp": "2026-07-12T23:42:43.992Z",
    "session_id": "40f6cdf0-3f55-4147-805a-07d168e4e663",
    "page": "/",
    "product": {
      "id": "waf-cap",
      "name": "WAF Guard Cap",
      "category": "apparel",
      "price": 32000,
      "currency": "KRW"
    }
  },
  "client": {
    "ip": "118.221.173.107, 15.158.3.198",
    "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36",
    "referrer": ""
  }
},
"splunk": {
  "delivered": false,
  "reason": "Splunk HEC is not configured. Set SPLUNK_HEC_URL and SPLUNK_HEC_TOKEN."
}
}
```

Splunk 로그 수집 및 탐지

찾아보니 운이 좋게도 AWS 와 연결 해주는 기능을 지원 해준다.



Splunk 로그 수집 및 탐지



이러면 연결시킬수 있다.

splunk>enterprise

앱 ▾

입력

설정

검색

상태 검사 ▾

입력

Create data inputs to collect data from AWS

Ingesting data from AWS to Splunk Cloud? Have you tried the new Splunk Data Manager yet?
Data Manager makes AWS data ingestion simpler, more automated and centrally managed for you, while co-existing with AWS
Read our [blog post](#) to learn more about Data Manager and it's availability on your Splunk Cloud instance.

3 Inputs

페이지당 10개 ▾

모두 ▾

검색...

i	Input Name ▲	Data Type ⇅	Input Type ⇅	Account ⇅
>	cloudfront_logs	CloudFront Access Logs	Generic S3	Gyeongdaeyoung
>	vpc_flow_logs	Generic S3	Generic S3	Gyeongdaeyoung
>	waf_logs	Generic S3	Generic S3	Gyeongdaeyoung

Splunk 로그 수집 및 탐지

Splunk 는 자체적인 쿼리(SPL)를 이용해 데이터를 분석한다.



```
index=aws earliest=-24h "/api/events/product-click" "product_name=" | rex field=_raw "product_name=(?<product_name>[^&\s\t]+)" | eval
product_name=replace(urldecode(product_name), "\\+", " ") | stats count as clicks by product_name | sort - clicks
```

splunk>Enterprise

메뉴

입

설

Q

상

새로운 검색

index=aws earliest=-24h "/api/events/product-click" "product_name=" | rex field=_raw "product_name=(?<product_name>[^&\s\t]+)" | eval
product_name=replace(urldecode(product_name), "\\+", " ") | stats count as clicks by product_name | sort - clicks

시간 범위: 최근 24시간

Q

221개의 이벤트 (26/07/12 8:35:29.000 ~ 26/07/13 8:35:29.722)

이벤트 샘플링 없음

작업

이벤트

패턴

통계 (5)

시각화

표시: 페이지당 20개

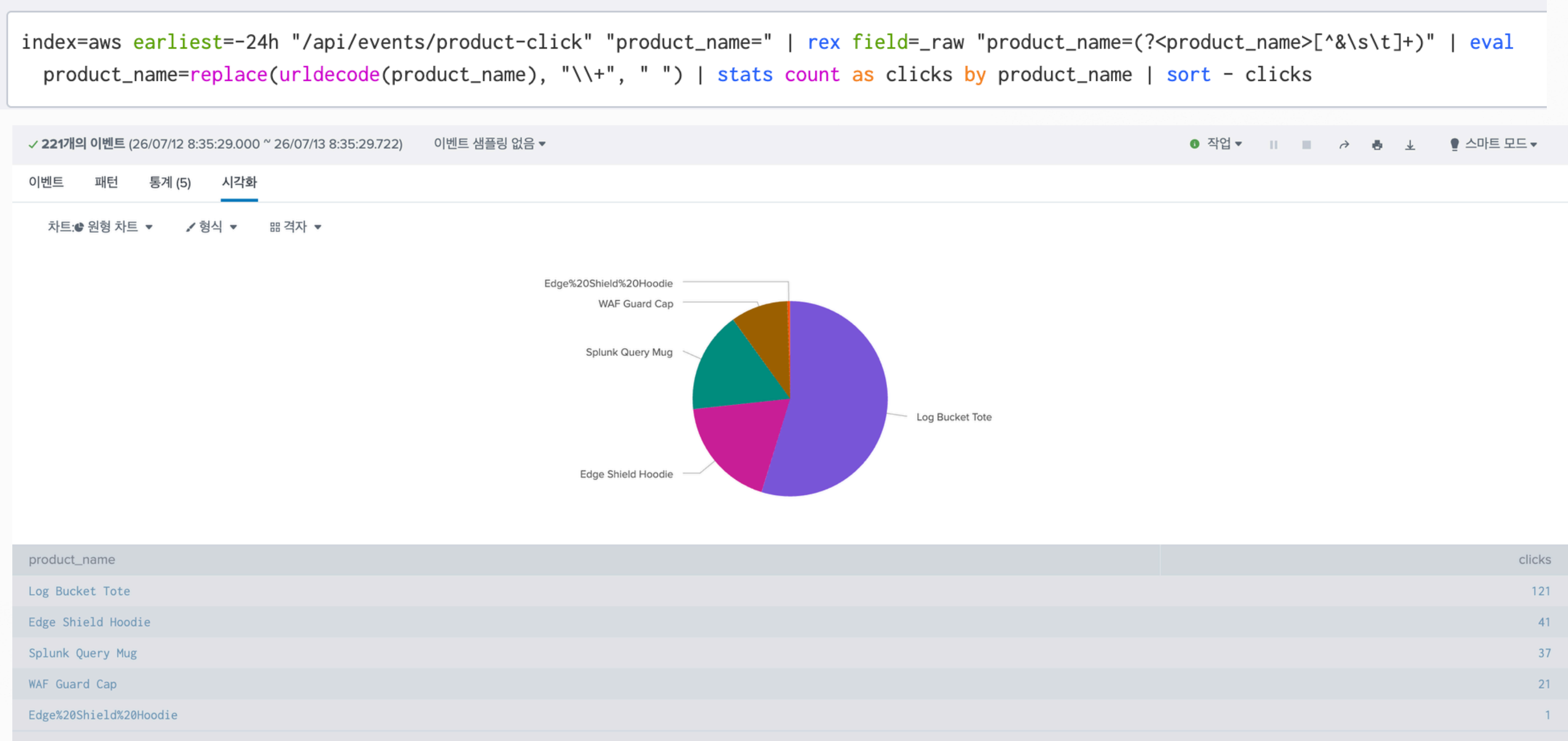
형식

미리보기: 켜기

product_name	clicks
Log Bucket Tote	
Edge Shield Hoodie	
Splunk Query Mug	
WAF Guard Cap	
Edge%20Shield%20Hoodie	

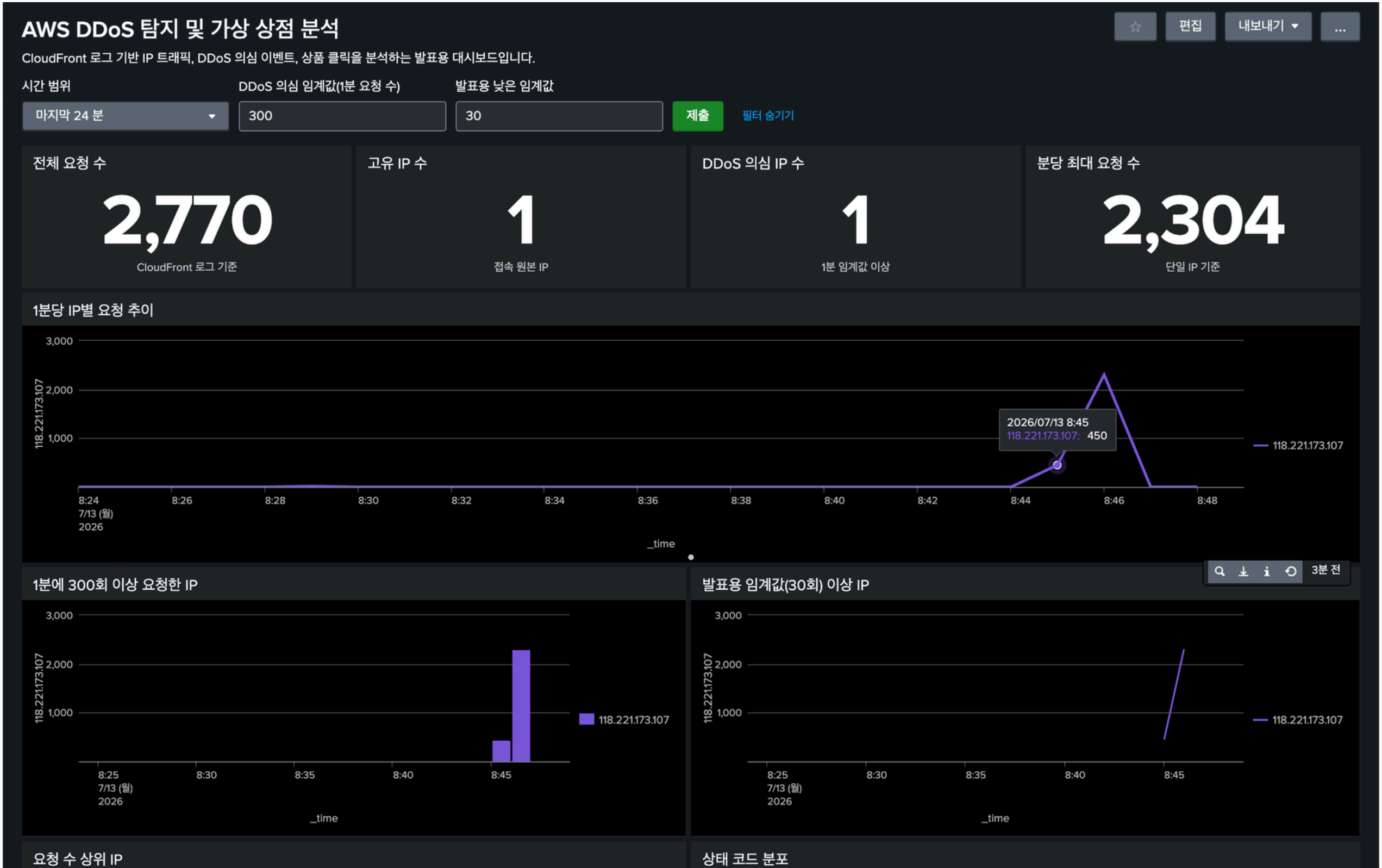
Splunk 로그 수집 및 탐지

이렇게 데이터 시각화가 가능하다.



Splunk 로그 수집 및 탐지

이렇게 자체적으로 대시보드를 만들어봄



Splunk 로그 수집 및 탐지

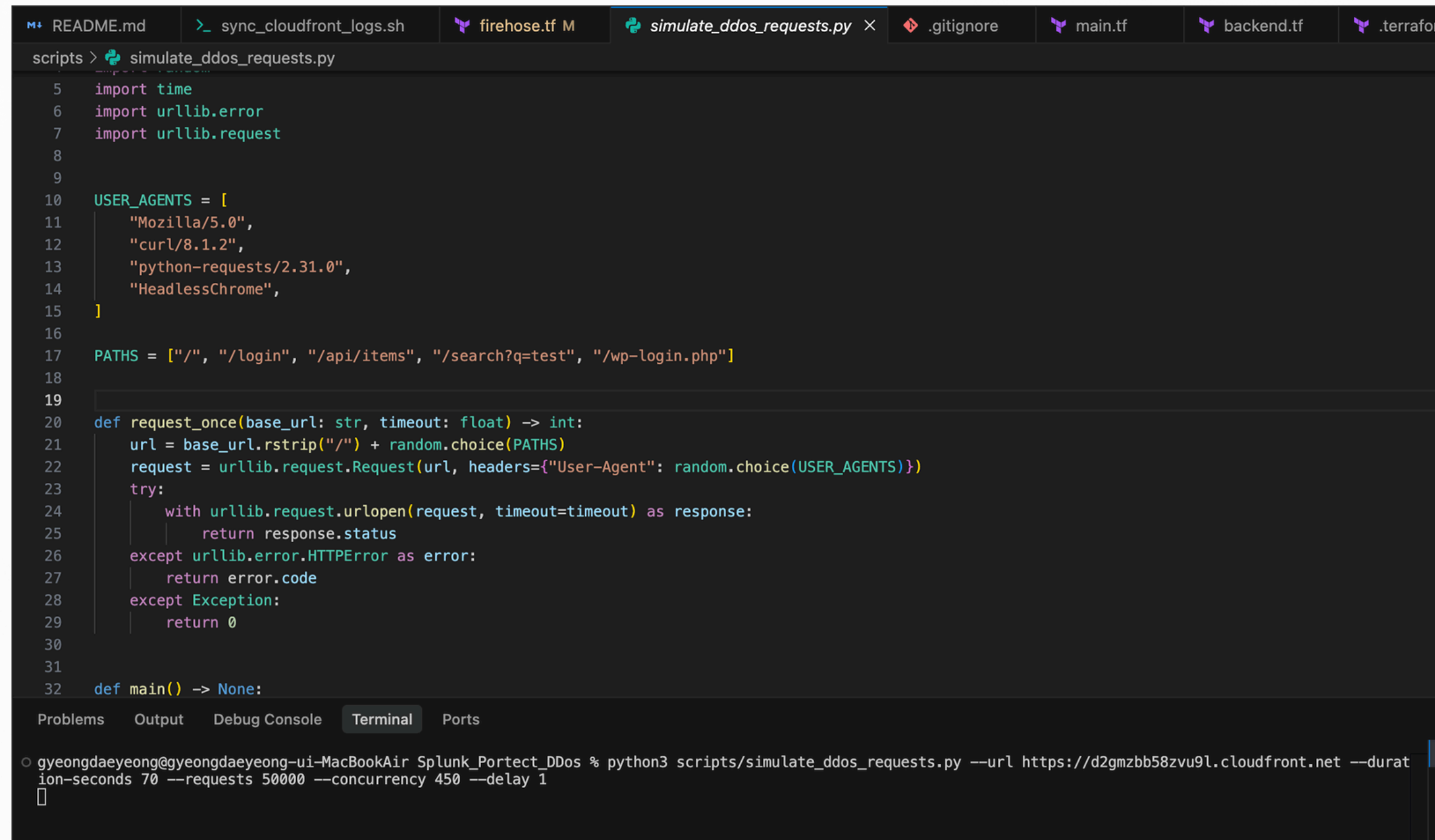
이렇게 자체적으로 대시보드를 만들어봄



DOS 날리기

DOS 를 날려 봄

ChatGPT 가 만듦



```
scripts > simulate_ddos_requests.py
5  import time
6  import urllib.error
7  import urllib.request
8
9
10 USER_AGENTS = [
11     "Mozilla/5.0",
12     "curl/8.1.2",
13     "python-requests/2.31.0",
14     "HeadlessChrome",
15 ]
16
17 PATHS = ["/", "/login", "/api/items", "/search?q=test", "/wp-login.php"]
18
19
20 def request_once(base_url: str, timeout: float) -> int:
21     url = base_url.rstrip("/") + random.choice(PATHS)
22     request = urllib.request.Request(url, headers={"User-Agent": random.choice(USER_AGENTS)})
23     try:
24         with urllib.request.urlopen(request, timeout=timeout) as response:
25             return response.status
26     except urllib.error.HTTPError as error:
27         return error.code
28     except Exception:
29         return 0
30
31
32 def main() -> None:
```

Problems Output Debug Console Terminal Ports

○ gyeongdaeyeong@yeongdaeyeong-ui-MacBookAir Splunk_Portect_DDos % python3 scripts/simulate_ddos_requests.py --url https://d2gmzbb58zvu9l.cloudfront.net --duration-seconds 70 --requests 50000 --concurrency 450 --delay 1

DOS 날리기

Befor



splunk> Enterprise

☑

🔍

📶

⚙️

🔔 1

❓

|

👤 Administrator ▾

⋮

☰

> Search & Reporting

🔍 검색

📈 애널리틱스

📁 데이터 집합

📄 보고서

🔔 경고

📊 대시보드

📦 모듈

AWS DDoS 탐지 및 가상 상점 분석

☆ 편집 내보내기 ...

CloudFront 로그 기반 IP 트래픽, DDoS 의심 이벤트, 상품 클릭을 분석하는 발표용 대시보드입니다.

시간 범위

DDoS 의심 임계값(1분 요청 수)

발표용 낮은 임계값

제출

필터 숨기기

전체 요청 수

0

CloudFront 로그 기준

고유 IP 수

0

접속 원본 IP

DDoS 의심 IP 수

0

1분 임계값 이상

분당 최대 요청 수

결과를 찾을 수 없습니다.

1분당 IP별 요청 추이

결과를 찾을 수 없습니다.

1분에 300회 이상 요청한 IP

결과를 찾을 수 없습니다.

발표용 임계값(30회) 이상 IP

결과를 찾을 수 없습니다.

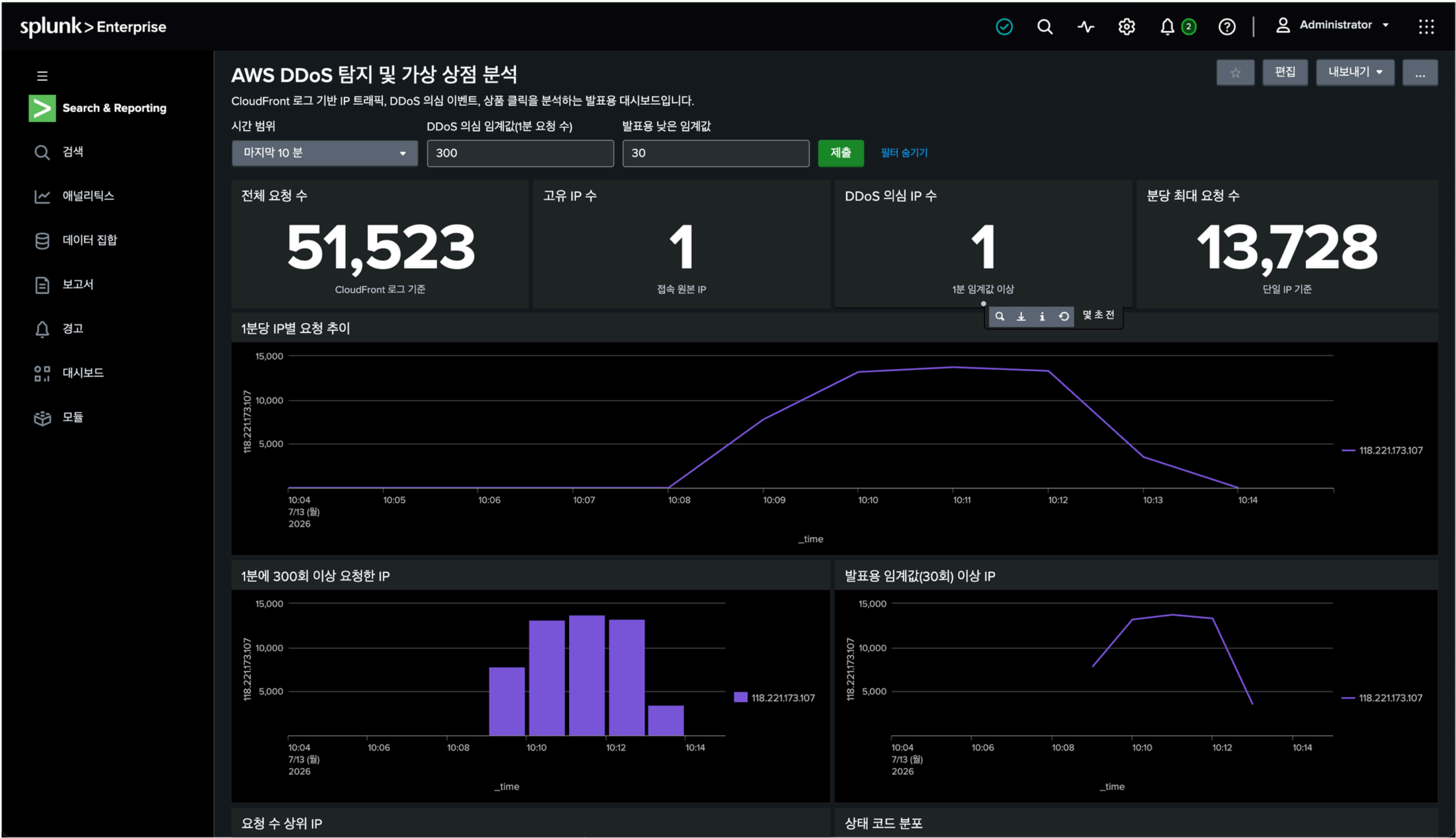
요청 수 상위 IP

🔍 ⬇️ ⓘ ↺ 4분 전

상태 코드 분포

DOS 날리기

After



DOS 날리기



IP 겁나 많이 왔다.

요청 수 상위 IP	
client_ip ↕	requests ↕
118.221.173.107	51523

DOS 날리기



그러면 웹사이트에 들어가서忆케 될까?

DOS 날리기



그러면 웹사이트에 들어가서 억케 될까?

403 ERROR

The request could not be satisfied.

Request blocked. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner.
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.

Generated by cloudfront (CloudFront)
Request ID: WDP--lpEMfY0bSWUd8DN7jBTu7c4k5XAeMFHoFUi2p0tPwt0r0hq4A==

차단 되었다....

DOS 날리기

그러면 웹사이트에 들어가서 억케 될까?

403 ERROR

The request could not be satisfied.

Request blocked. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner.
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.

Generated by cloudfront (CloudFront)
Request ID: WDP--lpEMfY0bSWUd8DN7jBTu7c4k5XAeMFHoFUi2p0tPwt0r0hq4A==

차단 되었다....

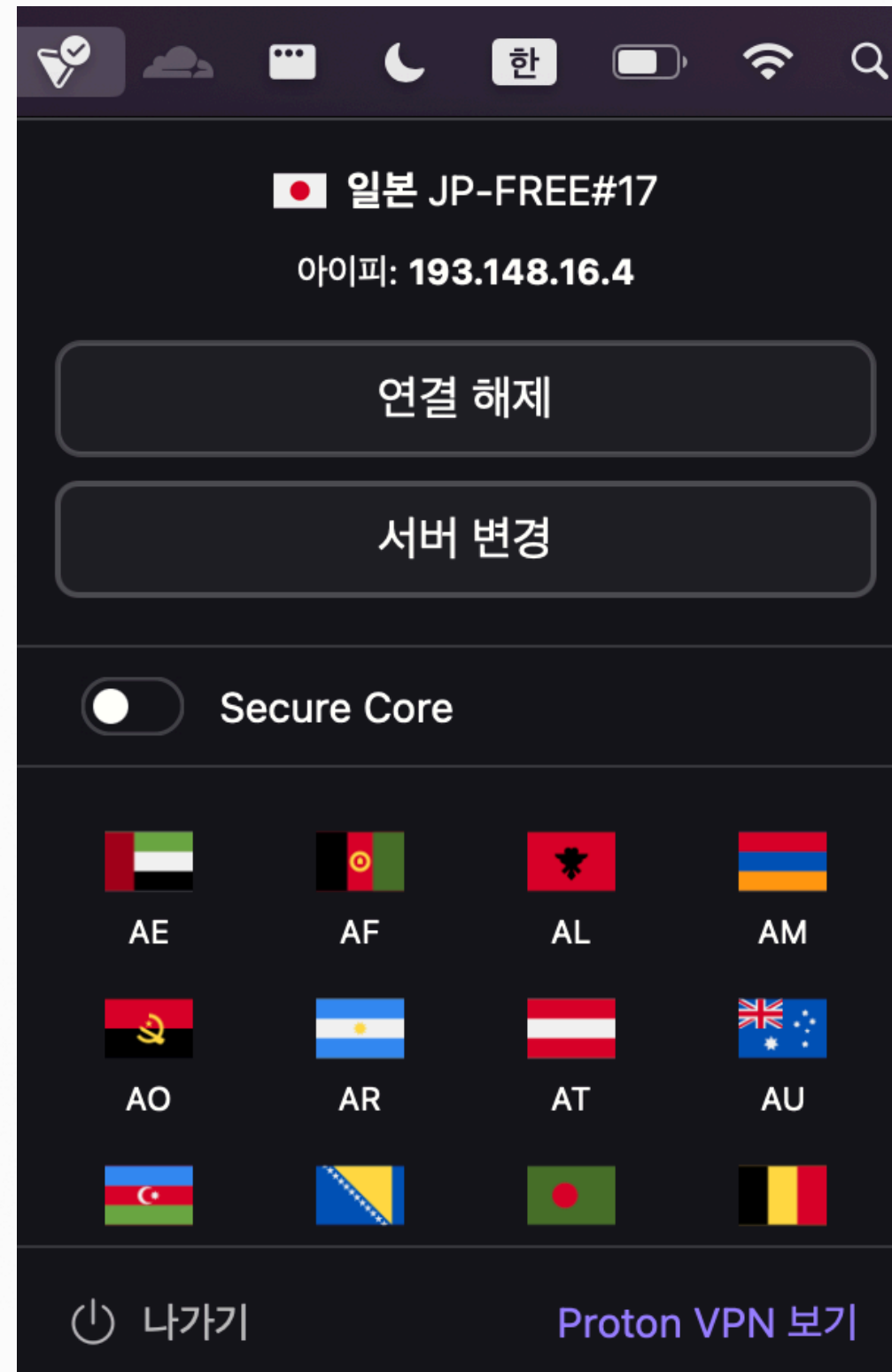


WAF 가 잘 차단 해준 거다. 🙌

IP에서 짧은 시간에 많은 요청을 보내면 WAF가 해당 IP를 차단한다.

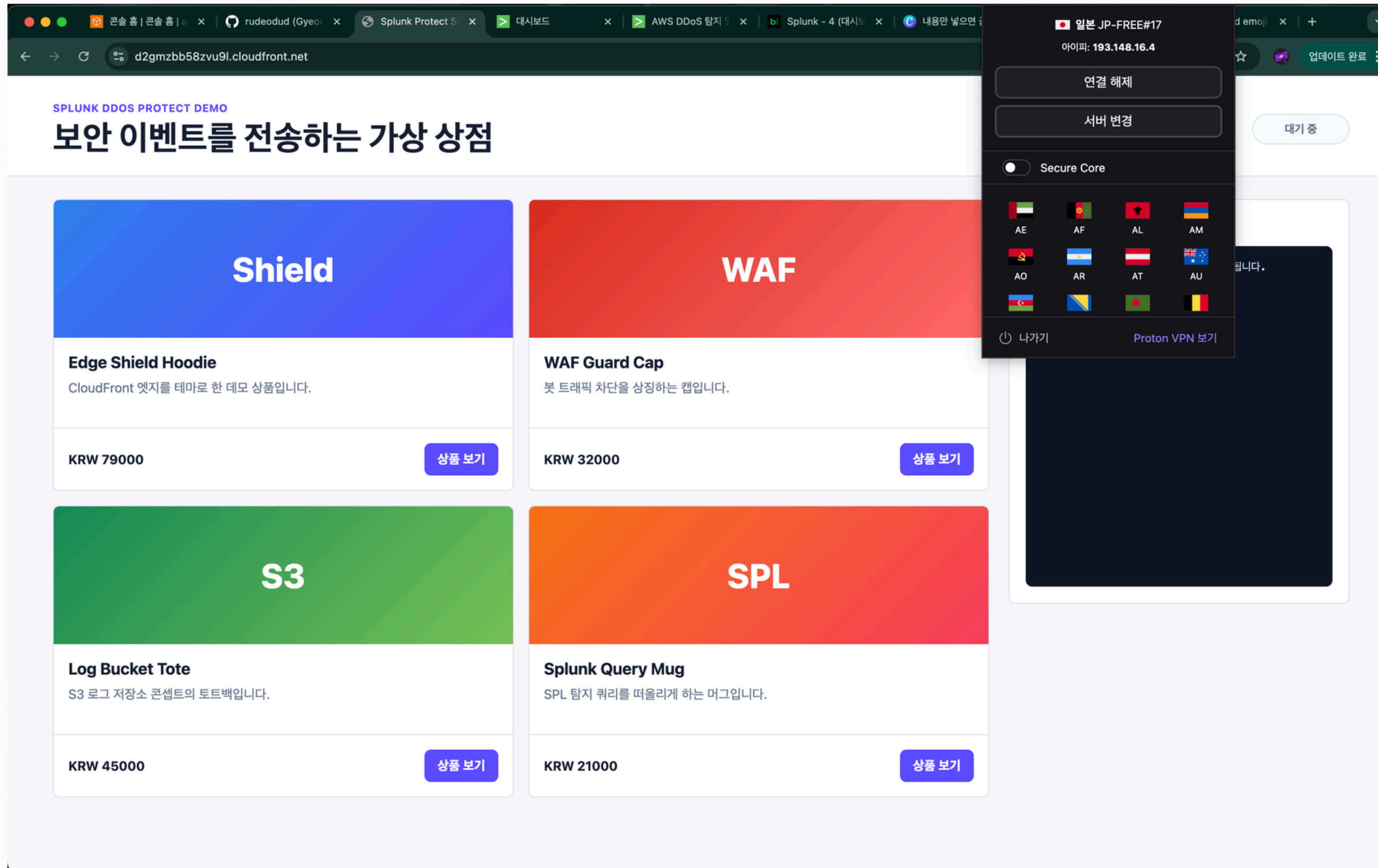
DOS 날리기

그러면 vpn 을 켜 들어가 보자



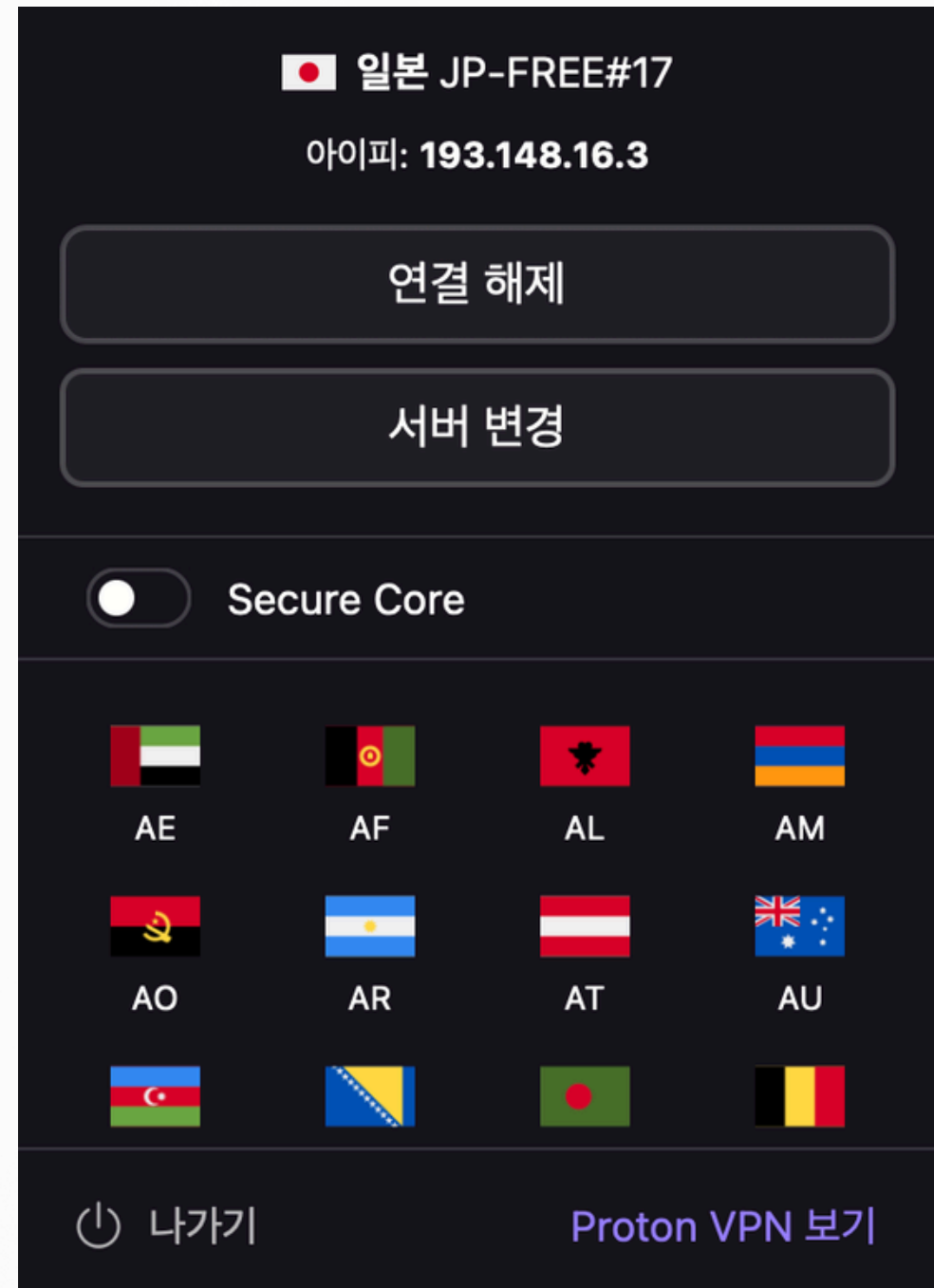
DOS 날리기

잘 들어가진다. 그러면 서버에는 문제가 없다는 거다



DOS 날리기

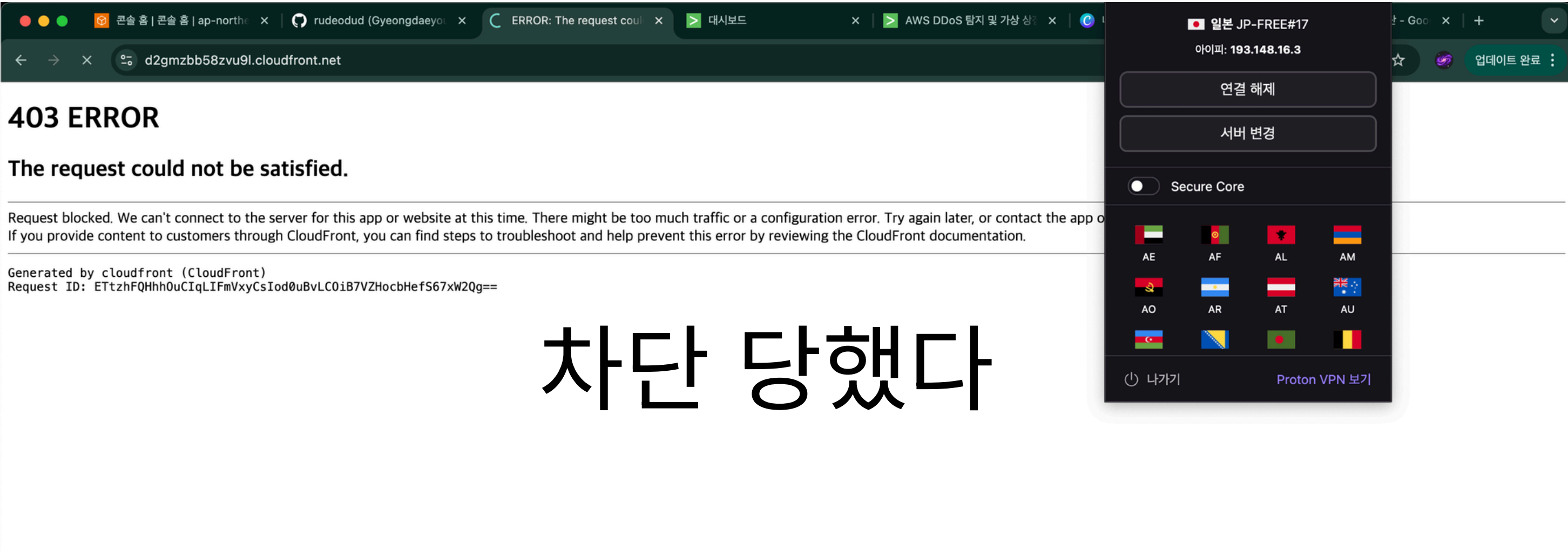
그러면 VPN 을 켜 상태로 DOS 를 날려보자



요청 수 상위 IP	
client_ip ↕	requests ↕
193.148.16.3	6164

DOS 날리기

그러면 VPN 을 켜 상태로 DDOS 를 날려보자

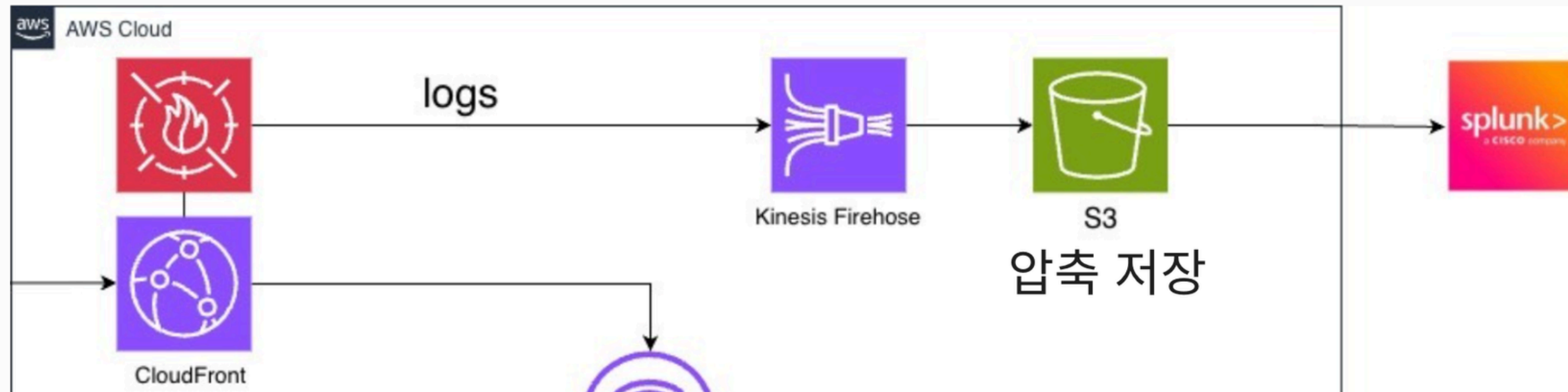


차단 당했다

문제점

느리다.

`./scripts/sync_cloudfront_logs.sh`



감사합니다.

