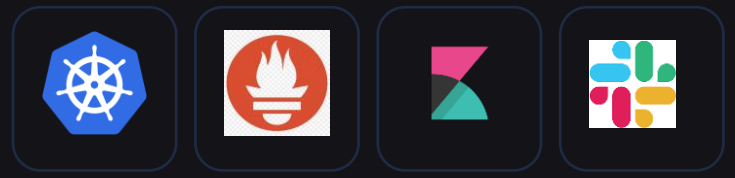
kt cloud
TECH UP



통합 보안 게이트웨이 구축

Integrated Security Gateway

팀 BBQ

조장 배OO – Slack

조원 주OO – Monitoring

조원 조OO – ELK stack

조원 민OO – GKE, Terraform

조원 조OO – Gateway, DB

잦은 보안사고

배경 및 경위

보안 인식의 부재와 위험

경제 경제일반

“쿠팡, 퇴사자 인증키 방치...3370만명 정보 유출 원인 됐다”

최민희 “기본적인 내부 보안 절차도 안 지켜”

뉴스1 · 1일 전 · 네이버뉴스

공격 차단으로는 부족해...**사이버보안** 핵심은 탐지·복구

인공지능(AI) 시대가 본격화되면서 **사이버보안**의 기준도 달라지고 있다. 앞으로는 공격을 완벽히 차단하는 것이 아니라 얼마나 빨리 탐지하고 복구하는지에 따라 기업 경쟁력이 좌우될 것이라는 진단이 나온다. 4일 업...

연합뉴스 · 3시간 전 · 네이버뉴스

국정원 **사이버보안** 실태평가서 중앙·광역 우수 0곳

IT 통제·재해복구 대비 미흡 정부업무평가 반영·배점 확대 국가정보원이 중앙부처, 광역지자체, 공공기관 등 152개 기관을 대상으로 실시한 **사이버보안** 실태평가에서 우수 등급을 받은 중앙부처와 광역지자체가 '제로'...

계획

모든 요청을 “중앙 게이트웨이”로 통제

게이트웨이 레벨에서 “표준 보안 정책”을 이용하여 트래픽 통과

① 트래픽/전송량 중앙 통제

- Rate Limiting: 사용자·IP별 호출 제한
- Payload Size Limit: 응답 크기 상한
- 스크래핑·대량유출 물리적 차단

② 인증/인가 중앙화

- 게이트웨이에서 JSON Web Token(JWT) 검증
- 퇴사자/협력사 계정 사용: 블랙리스트 즉시 반영

③ 통합 가시성

- 요청/응답 로그를 중앙 수집
- “누가/언제/무엇을” 감사 추적
- 실시간 모니터링·경보 기반 대응

핵심 메세지

- 여러 서비스에 흩어진 보안 기능을 중앙 한 곳으로 모아 정책/감사/관제를 표준화해서 사고 대응 시간을 줄인다

작업 흐름: 차단 → 관제 → 추적

1 정상 요청

- 정상 사용자가 서비스를 이용하는 평소 트래픽
- 게이트웨이가 통과시키고, 기록을 남김
- HTTP code: 200

2 공격 시도

- 비정상적인 대량 요청/스캔/권한없는 접근 같은 수상한 트래픽
- 게이트웨이가 차단시키고, 차단 사유를 기록
- HTTP code: 502

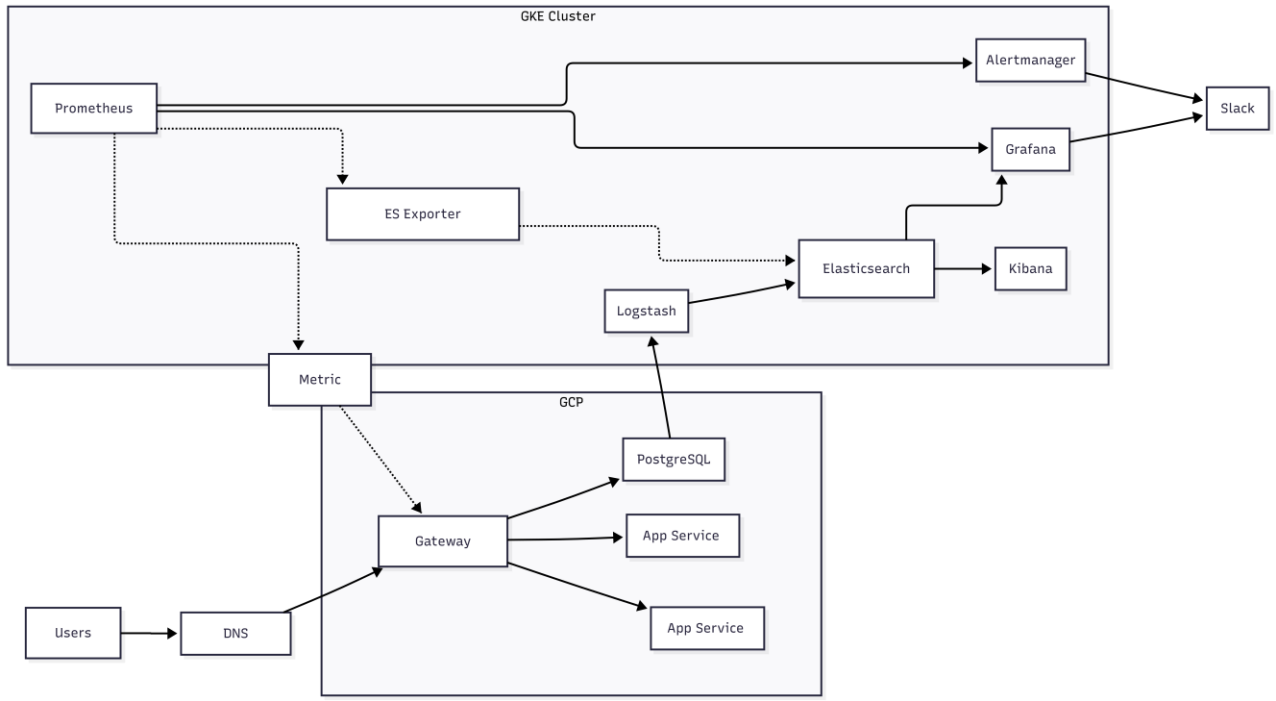
3 관제

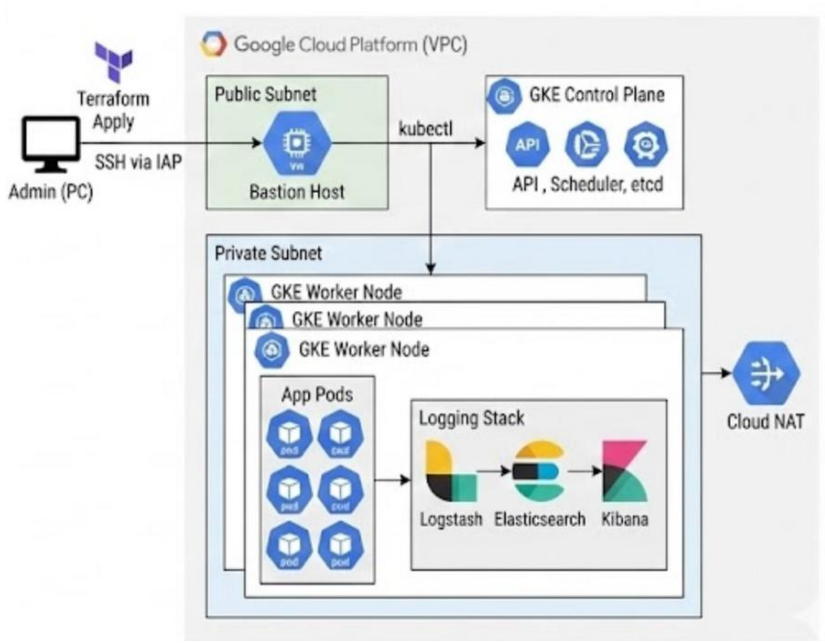
- 요청 급증/오류율 상승을 확인하여, 현재 이상징후가 있는지 파악
- 대시보드/알림으로 에러율, 요청량 등의 신호를 확인

4 추적

- 어떤 IP/계정이 어떤 엔드포인트를 호출했는지 검색
- 대시보드를 확인하여 특정 시간대의 로그 횟수와 로그에 있는 IP/계정, HTTP 코드 등을 확인

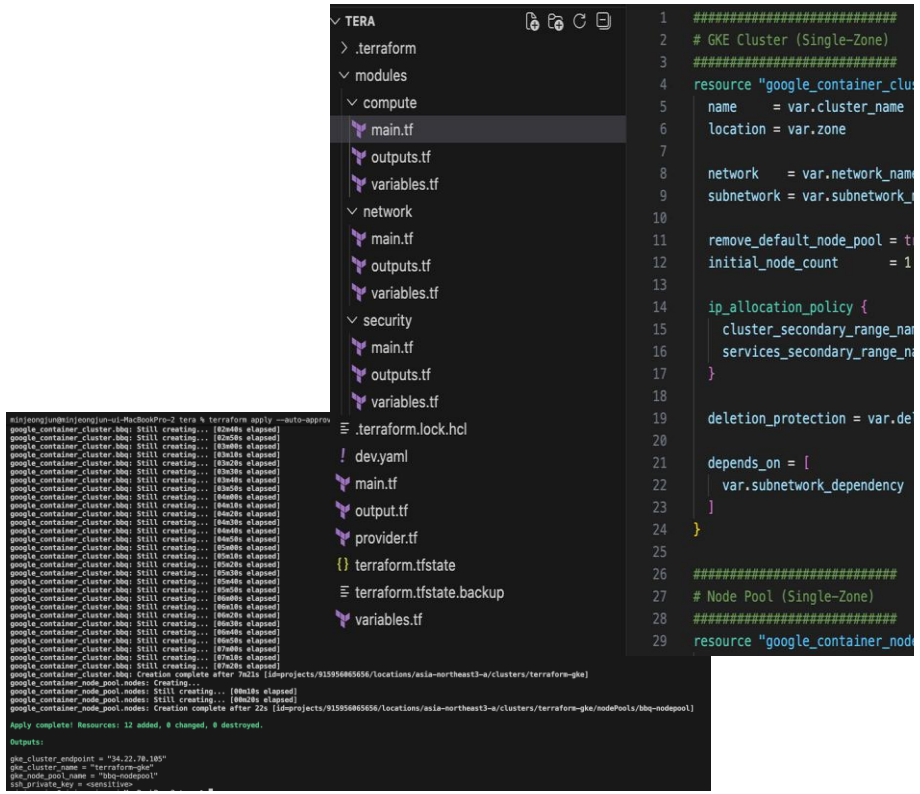
시스템 아키텍처 및 구성


GKE Cluster
Prometheus
Alertmanager
Grafana
Slack
ES Exporter
Elasticsearch
Kibana
Logstash
Metric
GCP
PostgreSQL
Gateway
App Service
App Service
Users
DNS


Google Cloud Platform (VPC)
Terraform
Apply
SSH via IAP
Admin (PC)
Public Subnet
Bastion Host
kubectl
GKE Control Plane
API
API , Scheduler, etcd
Private Subnet
GKE Worker Node
GKE Worker Node
GKE Worker Node
App Pods
Logging Stack
Logstash
Elasticsearch
Kibana
Cloud NAT

시스템 아키텍처 및 구성

코드형 인프라 관리 (IaC)



- 전체 인프라 코드화:
  - VPC, Subnet, Cloud NAT, LB 등 네트워크 인프라 구성
  - Private GKE 클러스터 및 노드 풀 프로비저닝
  - IAP 기반 Bastion Host VM 생성 및 방화벽 규칙 설정

- 주요 특징 및 전략
  - 모듈 기반 구성
  - 네트워크, 컴퓨팅, 보안 등 리소스별로 모듈을 분리하여 재사용성 및 관리 효율성 증대
  - IaC를 이용한 배포시간이 수기 작업 대비 약 **76.7%** 단축
  - 배포 안정성 확보
  - terraform plan을 통한 사전 검증 후 apply 실행으로 휴먼 에러 최소화

사고를 막는 최소 세트

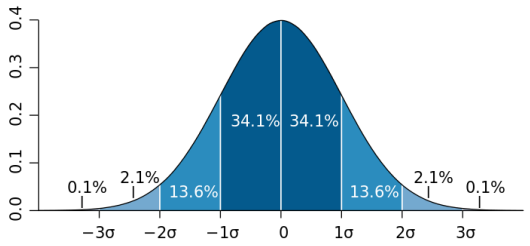
차단(Prevent)

- Rate Limit: IP/사용자별 호출 제한
- Payload 제한: 대량 응답 차단
- 퇴사자/비정상 계정 블랙리스트
- 권한 기반 라우팅(서비스별 접근)

탐지(Detect)

- 로그 표준화 + 중앙 저장(ELK)
- 메트릭 기반 이상징후(급증/오류율)
- 대시보드에서 실시간 관제
- 알림(슬랙) 연동은 확장 영역

일반적인 이상치



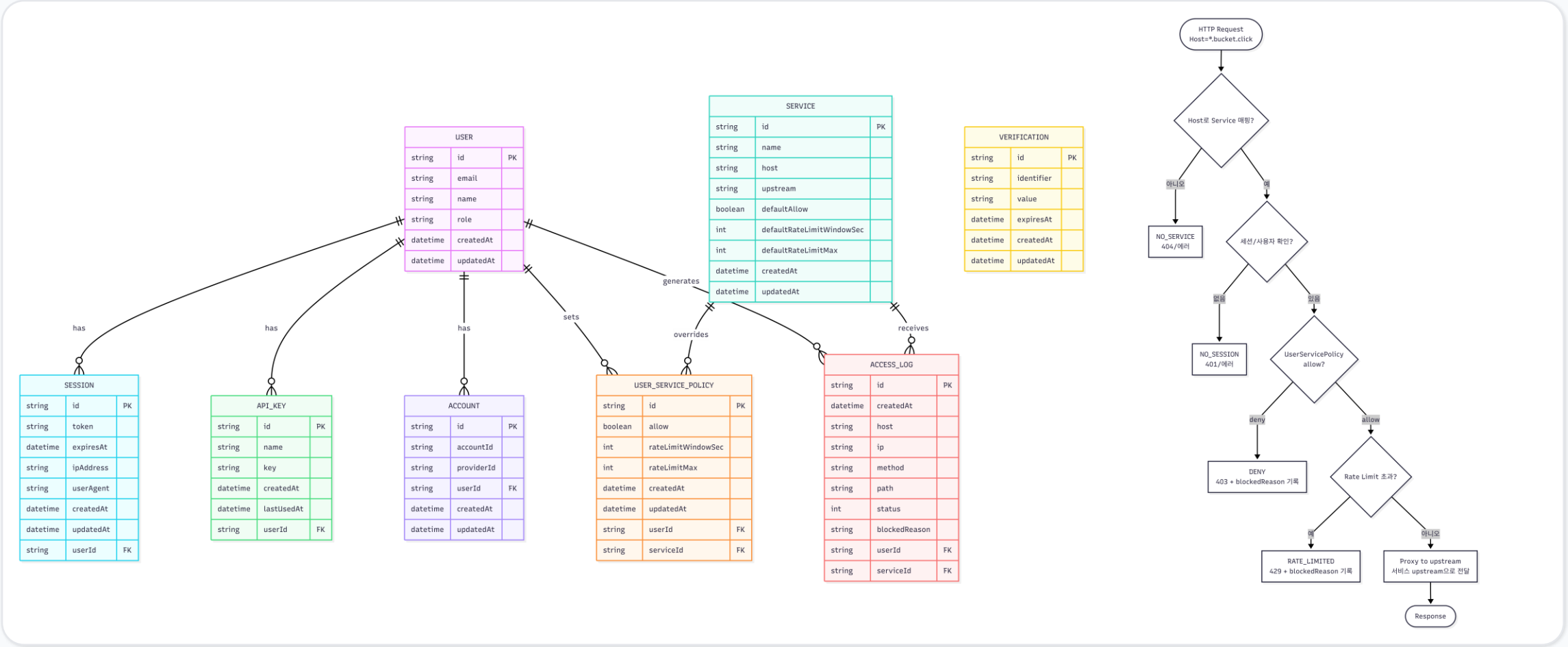
- 일반적인 통계에서 이상치는 3σ, 약 0.1%
- 이 프로젝트에서는 모수 값이 적고, 실제 작동을 확인하고자 하기에 보편적인 값을 확인하여 훨씬 적은 값을 이용
- 보편적인 값은 표를 참조

구분	보편적인 이상치 기준 (Threshold)
로그인	연속실패 100회 NIST SP 800-63B-4(2025)
용량	2-3배 Google SRE Team(2016)
시간	평소 패턴의 이탈 Cain et al. (2024)

구분	설정한 이상치 기준 (Threshold)
로그인	1분 내 **5회~10회** 연속 실패
용량	응답 크기 **평균의 3배** 초과 (또는 10MB)
시간	**00시 - 06시**

※ 시간은 경고 알림, 로그인과 용량은 게이트웨이 수준 차단

게이트웨이 아키텍처


USER
string id PK
string email
string name
string role
datetime createdAt
datetime updatedAt
SERVICE
string id PK
string name
string host
string upstream
boolean defaultAllow
int defaultRateLimitWindowSec
int defaultRateLimitMax
datetime createdAt
datetime updatedAt
VERIFICATION
string id PK
string identifier
string value
datetime expiresAt
datetime createdAt
datetime updatedAt
has
has
has
sets
generates
overrides
receives
SESSION
string id PK
string token
datetime expiresAt
string ipAddress
string userAgent
datetime createdAt
datetime updatedAt
string userId FK
API_KEY
string id PK
string name
string key
datetime createdAt
datetime lastUsedAt
string userId FK
ACCOUNT
string id PK
string accountId
string providerId
string userId FK
datetime createdAt
datetime updatedAt
USER_SERVICE_POLICY
string id PK
boolean allow
int rateLimitWindowSec
int rateLimitMax
datetime createdAt
datetime updatedAt
string userId FK
string serviceId FK
ACCESS_LOG
string id PK
datetime createdAt
string host
string ip
string method
string path
int status
string blockedReason
string userId FK
string serviceId FK
HTTP Request
Host=*.bucket.click
Host로 Service 매핑?
아니오
예
NO_SERVICE
404/에러
세션/사용자 확인?
없음
있음
NO_SESSION
401/에러
UserServicePolicy
allow?
deny
allow
DENY
403 + blockedReason 기록
Rate Limit 초과?
예
아니오
RATE_LIMITED
429 + blockedReason 기록
Proxy to upstream
서비스 upstream으로 전달
Response