

PNU Cloud Access Security Broker (CASB)

클라우드 내 서비스에 대한 접근 제어, 데이터 보호, 모니터링 및 위협 식별 기능을 제공하는 클라우드 접근 보안 브로커 (CASB)

적용분야



Zero Trust



Multi Cloud



기업/공공 자산



네트워크 보안

연구목적

- 클라우드 내 서비스에 대한 접근 제어 관리의 어려움과 네트워크를 통한 데이터 유출 및 내외부 위협이 증가함에 따라, **클라우드 환경을 보호하기 위한 Broker 기반 보안 강화** 필요
- CASB는 클라우드 서비스와 사용자 사이에서 중개자로서 보안 통제 지점 역할을 수행하여 기업이 클라우드 서비스를 보다 안전하게 활용할 수 있도록 접근 관리, 데이터 보호, 사용자 모니터링 및 위협 탐지 등의 다양한 보안 정책을 적용할 수 있도록 지원함
- As-Is**: 기존의 CASB는 SaaS 영역에서 발생하는 사이버 공격 및 데이터 유출을 줄이는 데 기여해왔으나, IaaS 및 PaaS 등의 클라우드 인프라 영역에 보안을 제공하는데 한계를 가짐
- To-Be**: **멀티 클라우드 인프라에 대한 접근 제어, 데이터 보호, 사용자 모니터링 및 위협 탐지 등의 보안 기능을 제공하기 위해 CASB를 개발**하였음

연구내용

Cloud Access Security Broker (CASB)

CASB Client

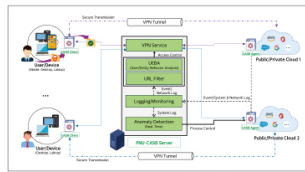
클라우드 서비스 사용자의 단말기에서 실행되는 프로그램으로 VPN 연결을 통한 네트워크 보안 기능과 악성 문서 업로드 방지를 위한 위협 요소 제거 기능 제공

CASB Server

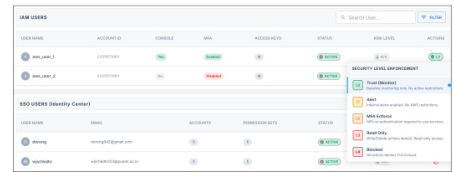
클라우드 사용자 및 서비스를 위한 VPN 인증서 발급 및 VPN 연결 제공, 클라우드 동기화 및 Private IP 할당을 통한 ACL (Access Control List) 생성, 클라우드 서비스 모니터링 및 위협 분석, 클라우드 위험도 기반 세분화된 접근 제어 적용

CASB Agent

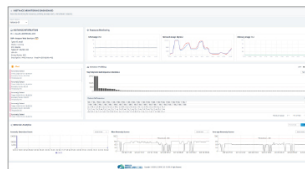
클라우드 서비스를 위한 Agent 프로그램으로 VPN 연결을 통한 네트워크 보안 기능 제공 및 서비스 내 이벤트/시스템 로그 수집 및 전송



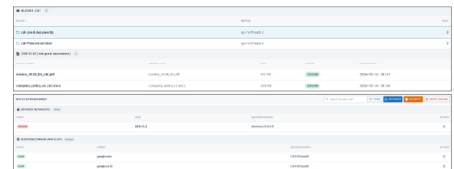
1. CASB 아키텍처



2. 위험도 기반 세분화된 접근 제어 적용



3. 클라우드 서비스 모니터링 및 위협 분석



4. 클라우드 서비스내 악성 행위 방어

기술 경쟁력

기존기술

- SaaS 앱 을 대상으로만 보안 기능을 적용하기에 IaaS, PaaS 등의클라우드 인프라를 대상으로 한 CASB 기술이 부재함
- 멀티 클라우드 환경을 대상으로 통합적인 클라우드 접근 제어 기술의 부재로 인한 정책 관리의 어려움

기술적 한계

- 적용 범위: SaaS 앱을 대상으로만 보안 기능 제공
- 접근 제어: SaaS 앱 대상 접근 제어 기능 제공
- 위협 탐지: 네트워크 트래픽 및 리소스를 통한 위협 탐지

기술 차별성

- 클라우드 인프라를 대상으로 세분화된 접근 제어, 데이터 보호, 사용자 모니터링, 위협 탐지 등 보안 기술을 제공하는 CASB 제안
- 멀티 클라우드 환경을 대상으로, 자동화된 클라우드 동기화 및 접근 제어 리스트 생성 및 세분화된 접근 제어 정책 적용

기술적 우위

- 적용 범위: 멀티 클라우드 인프라를 대상으로 보안 기능 제공
- 접근 제어: 멀티 클라우드 대상 세분화된 접근 제어 기능 제공
- 위협 탐지: 실시간 시스템 로그 분석을 통한 위협 탐지
- 프로파일링: 인프라 모니터링을 통한 패턴 분석 및 프로파일링

대상기술

지식 재산권

발명의 명칭

프라이빗 클라우드 환경에서의 제로샷 학습 기반 비정상 행위 탐지 방법 및 시스템

출원(등록)번호

10-2024-0133547

출원(등록)일자

2024.10.02