공공부문 클라우드 인식확산 교육

SaaS 서비스 소개 및 공공기관 구축 사례 / 보안

More security,
More freedom

안랩

AhnLab

목차

AhnLab

클라우드 보안의 가치

빠르게 달리려면 브레이크가 필요
클라우드를 이용하려면 보안은 반드시 필요

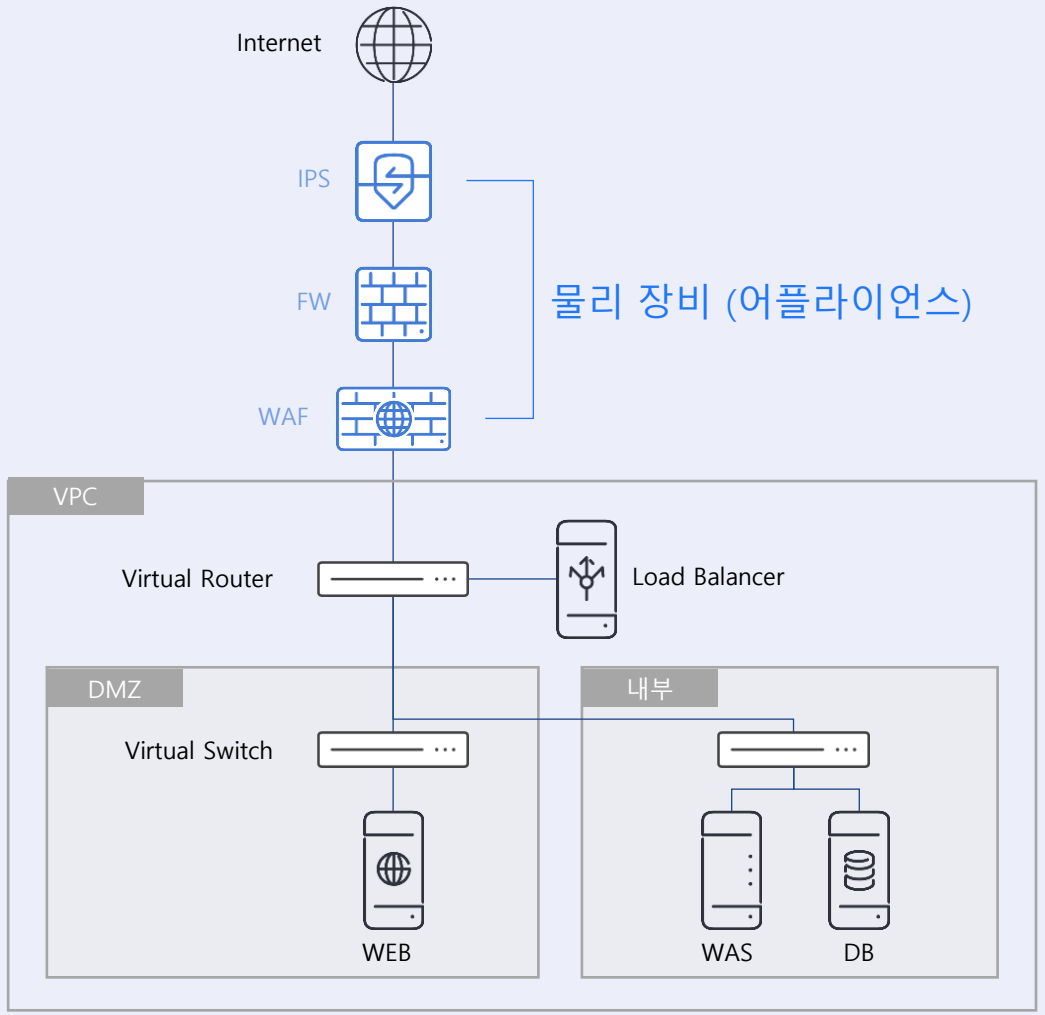
클라우드를 이용하여 혁신을 창출
보안은 혁신을 유지하는 비용 이상의 가치

물리적 네트워크 보안

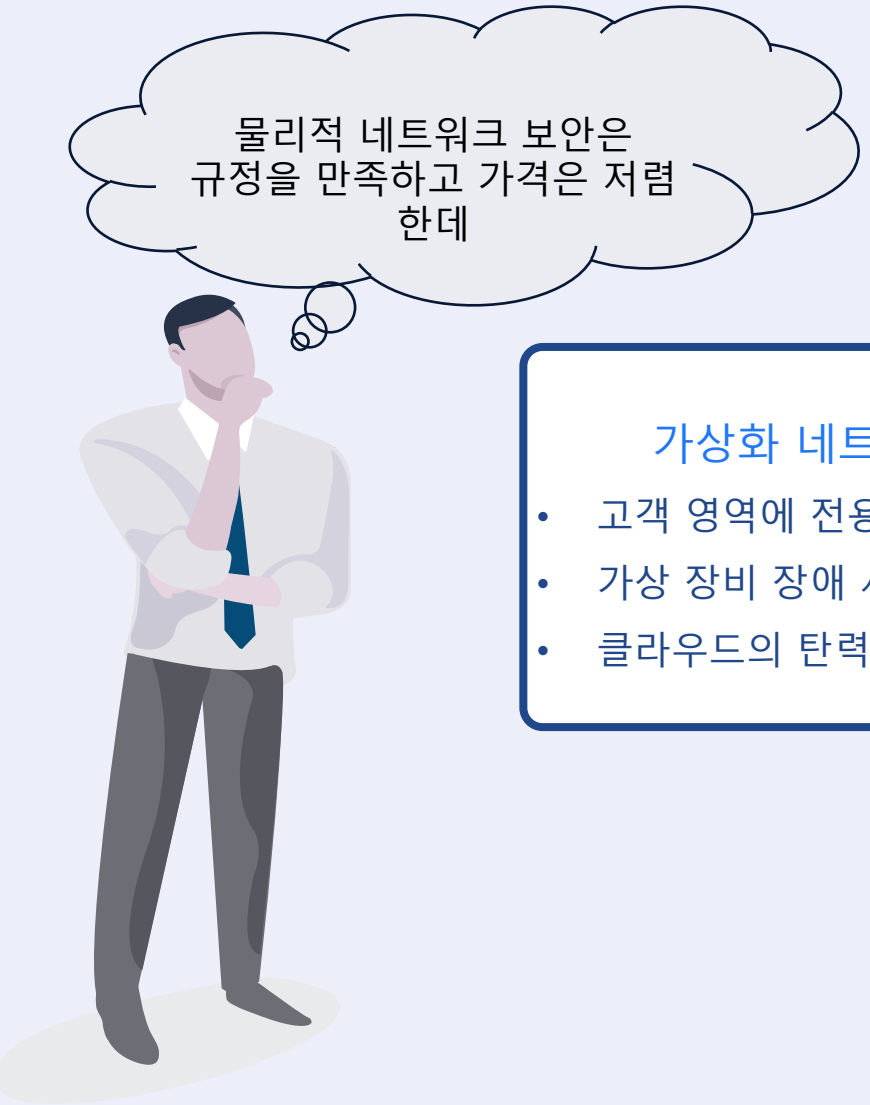
행정 · 공공기관 정보시스템
클라우드 전환 · 통합 사업(7차) 제안요청서

- FW, IPS(IDS), DDoS, 서버백신, 접근제어 등 필수 보안서비스 적용 및 국정원 CC인증 제품 활용으로 보안성 강화
- 정보의 특성 등을 고려한 DB암호화, 개인정보 필터 등 보안 강화 적용 전환

보안	WAF	기관별 전체 제공
	IPS or IDS	기관별 전체 제공
	DDoS	기관별 전체 제공
	DB보안(데이터암호화)	4(개)
	서버접근제어	VM전체 적용: 13(개)
	DB접근제어	4(개)
	서버백신	VM전체 적용: 13(개)
	개인정보보호필터링(신규+재활용)	2(개)

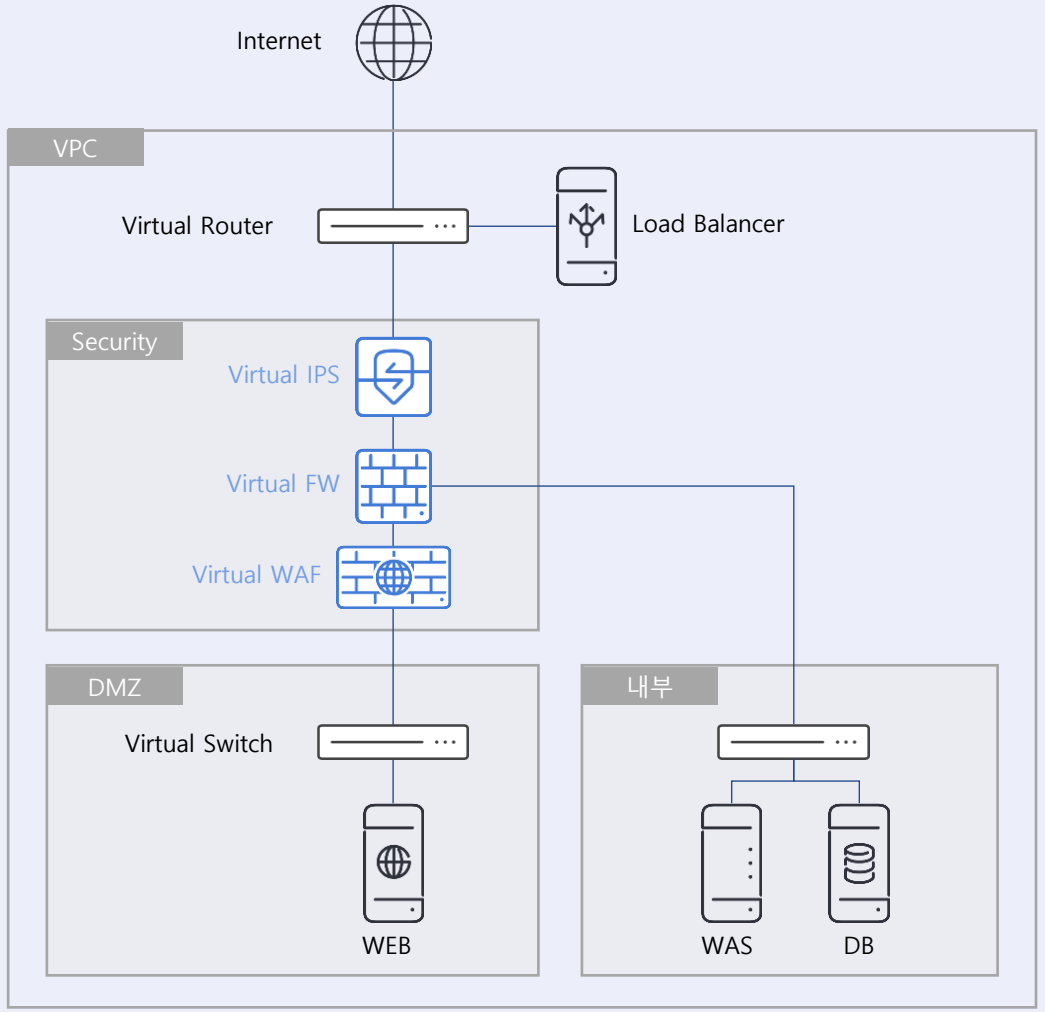


가상화 네트워크 보안



가상화 네트워크 보안 적용

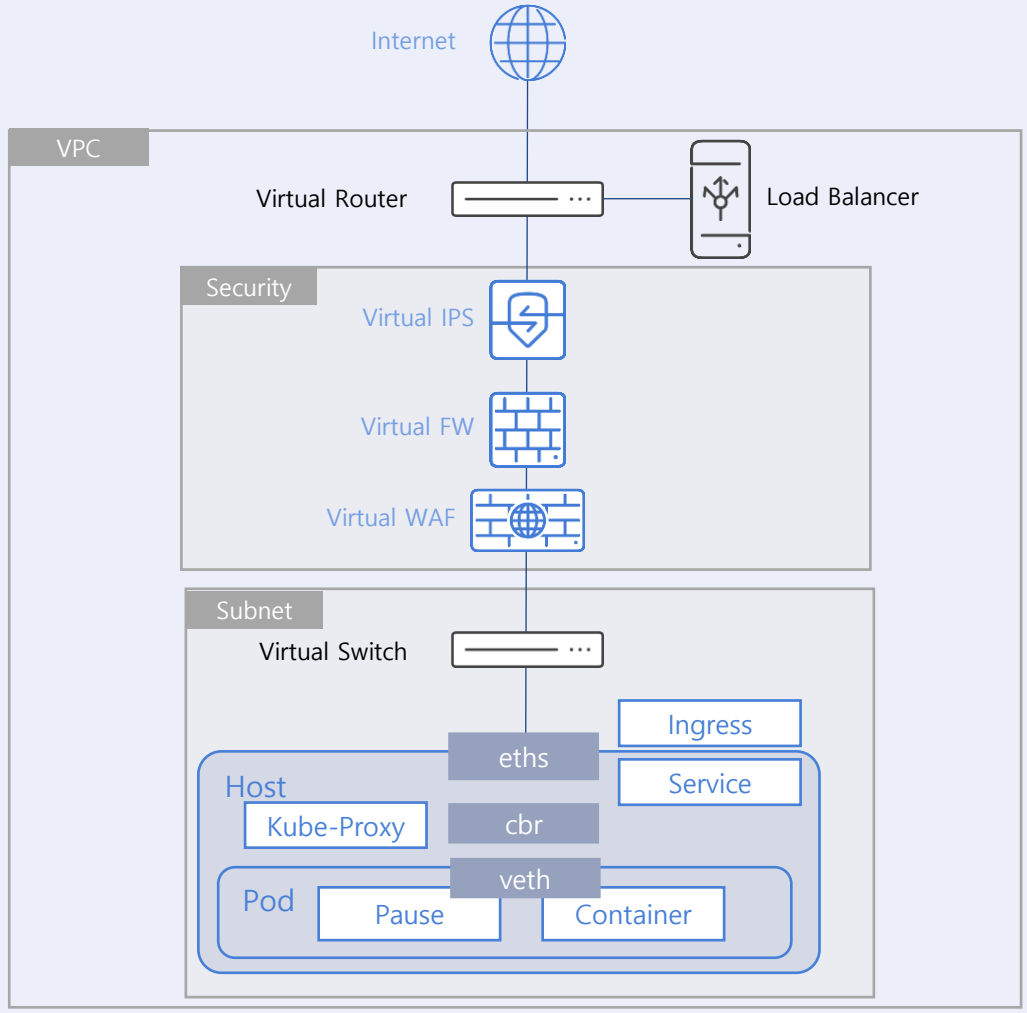
- 고객 영역에 전용 가상 장비
- 가상 장비 장애 시 삭제 후 즉시 재배포
- 클라우드의 탄력적인 구성 지원



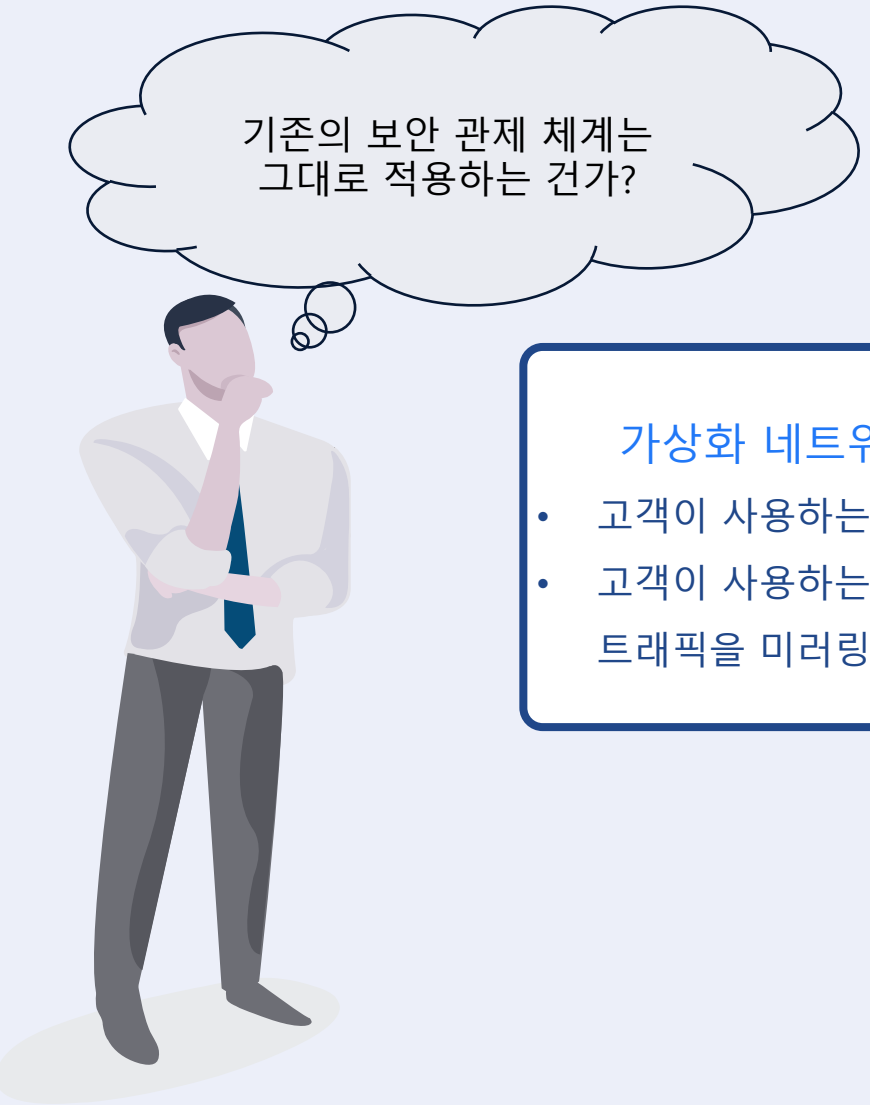
클라우드 네이티브의 가상화 네트워크 보안

가상화 네트워크 보안 적용

- K8S 네트워크 구성에 영향 없음
- 외부에서 K8S로의 CLI 접근 통제
- Host IPS는 Pod, Container 식별

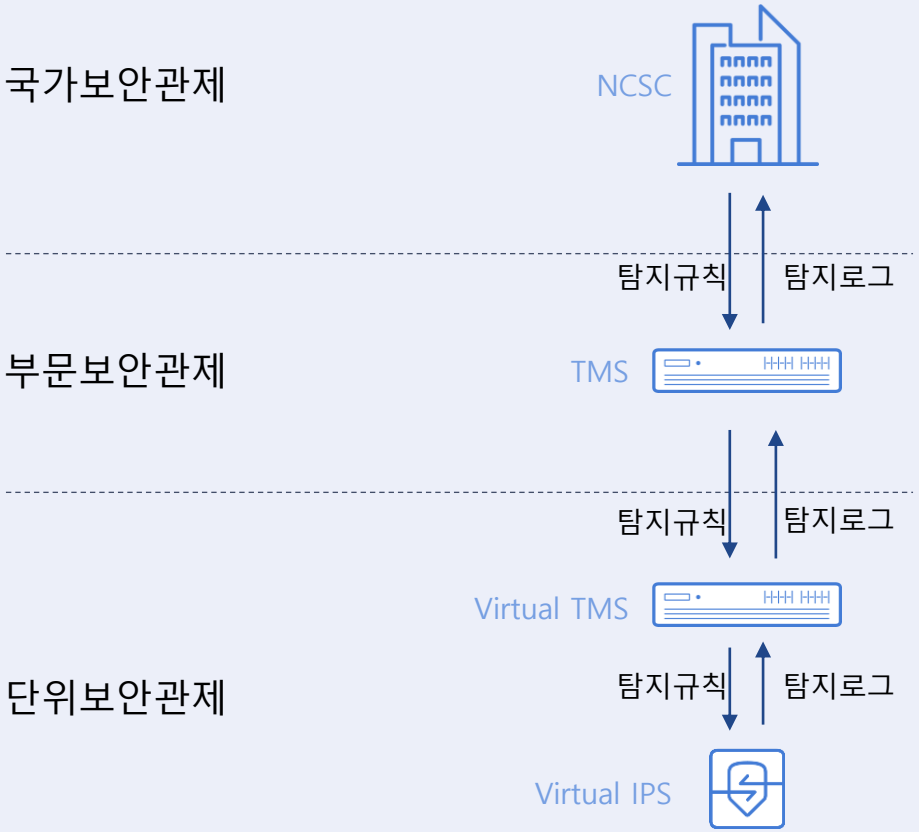


클라우드 네트워크 보안 관제

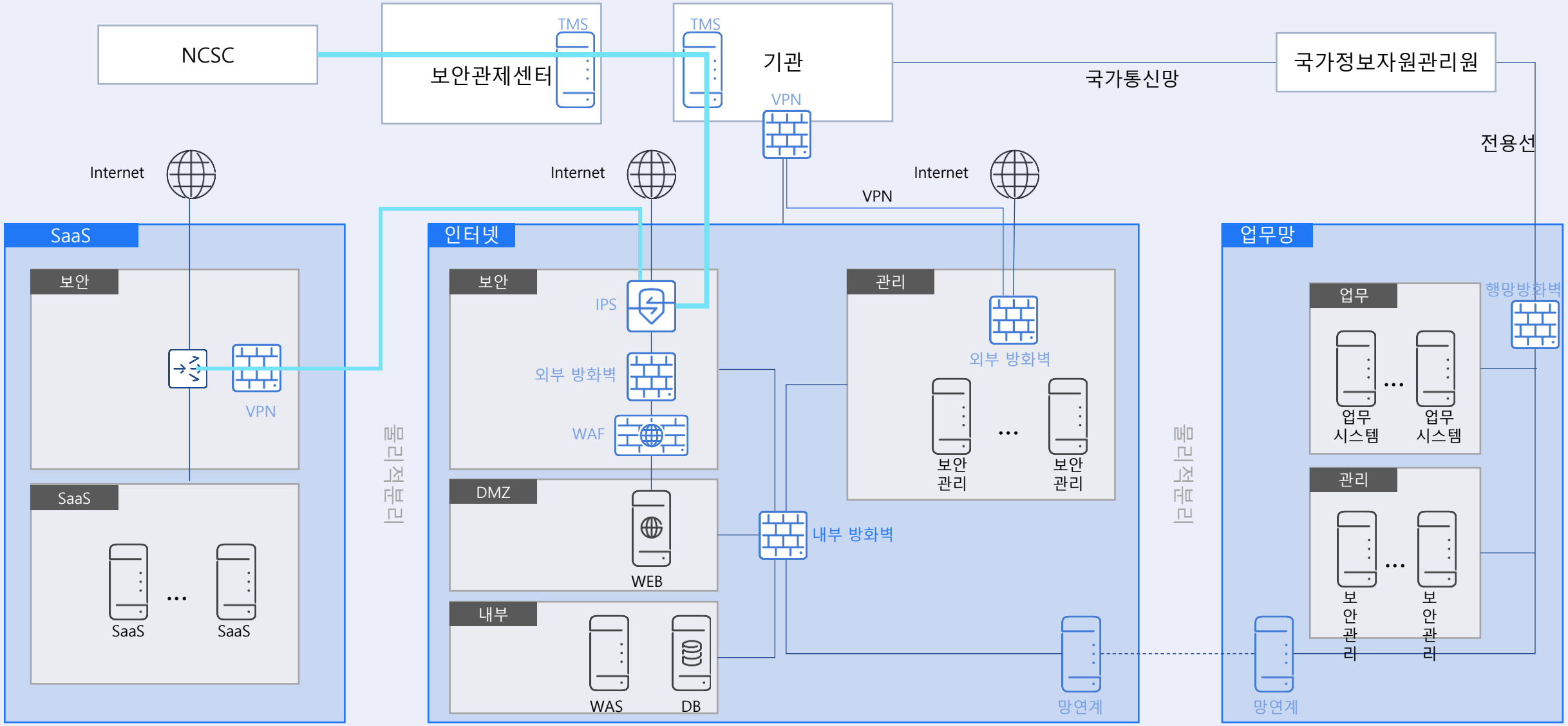


가상화 네트워크 보안 적용

- 고객이 사용하는 IaaS 탐지 지원
- 고객이 사용하는 SaaS로부터 선별된 트래픽을 미러링 받아 탐지 지원



공공 클라우드 네트워크 보안 구성 (예시)



vTrusGuard 소개

FW, VPN, IPS 등 통합 클라우드 네트워크 보안

침입차단
커널 / 플래폼의 핵심 기술 보유
클라우드 환경에 최적화된 트래픽 처리

VPN
IPSec / SSL VPN 핵심 기술 보유
Fierwall / IPS 정책과 연동
MFA 지원
키보드 보안 지원

IPS
IPS 핵심 기술 보유
기본 IPS 시그니처 제공
보안 위협 모니터링 인프라 지원

C&C 탐지 차단
C&C BlackList 기반 탐지 및 차단
C&C 리스트 정기 업데이트

Anti-Malware
자체 개발 Stream Based Anti-Virus 엔진 적용

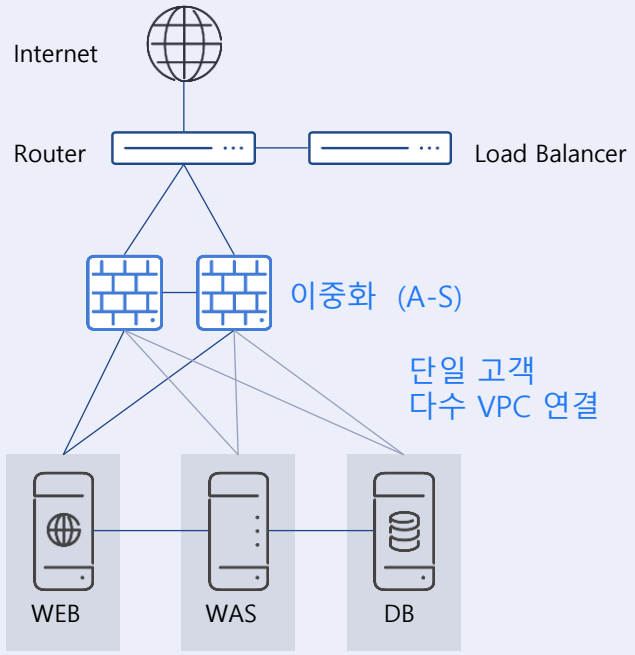
Anti-Mal Site
AhnLab ASD 체계로 정보를 수집 모니터링 및 분석하여 대응

설정
이중화 구성
다수 VPC, Subnet 관리 지원

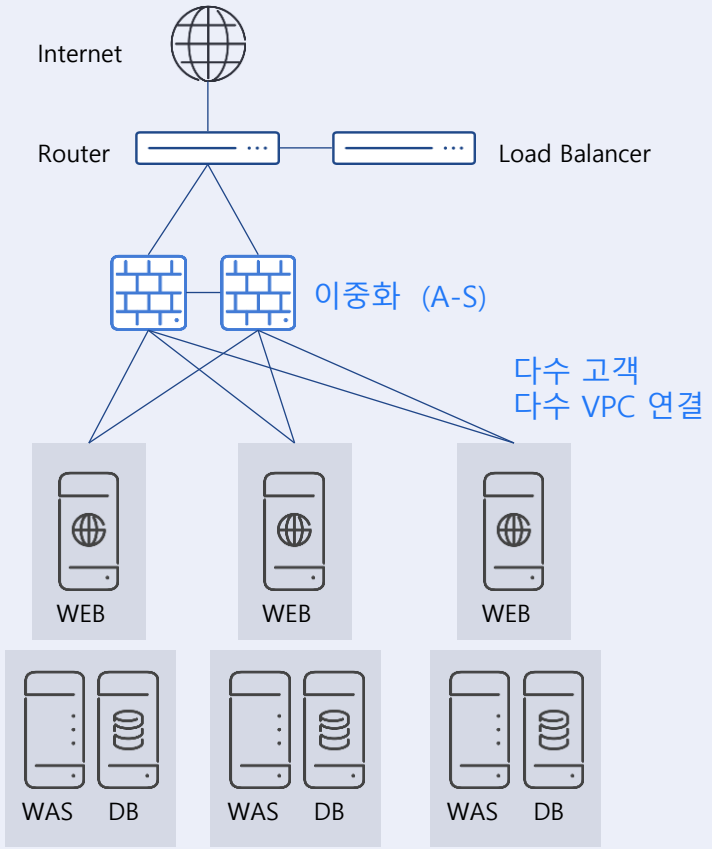
구분	vTrusGuard	Security Group	NACL
대상	네트워크, 인스턴스, Pod, Container	인스턴스	네트워크, 인스턴스
설정	IP/Port/Protocol, 도메인, URL, 사용자 등	IP/Port/Protocol	IP/Port/Protocol
제어	출발지, 목적지 양방향	출발지,목적지 허용	출발지,목적지 양방향
정책	약 65,000개	최대 2,500개	최대 10개 ACL
로그	저장	저장 X	저장 X

vTrusGuard 구성 및 구축사례

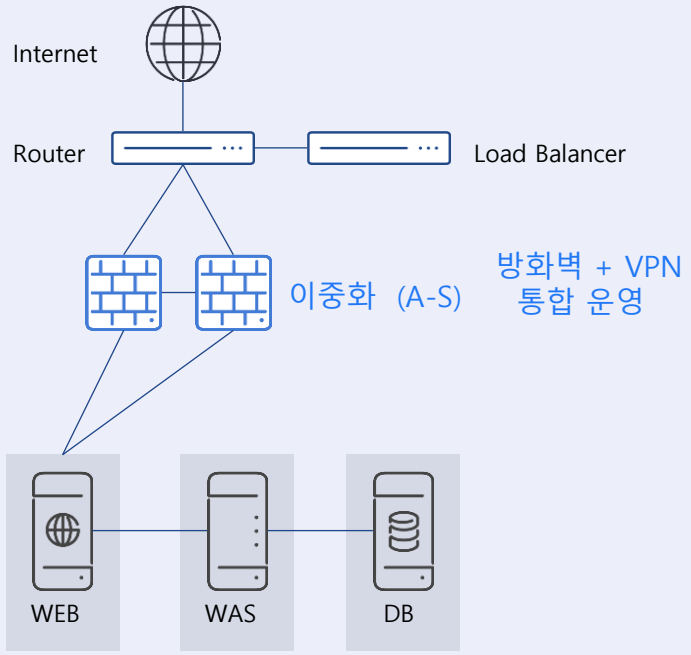
단일 고객의 다수 VPC 통합



다수 고객의 다수 VPC 통합



방화벽, VPN 통합



vAIPS 소개

TMS 구성을 위한 클라우드 최적의 IPS

위협 탐지/차단

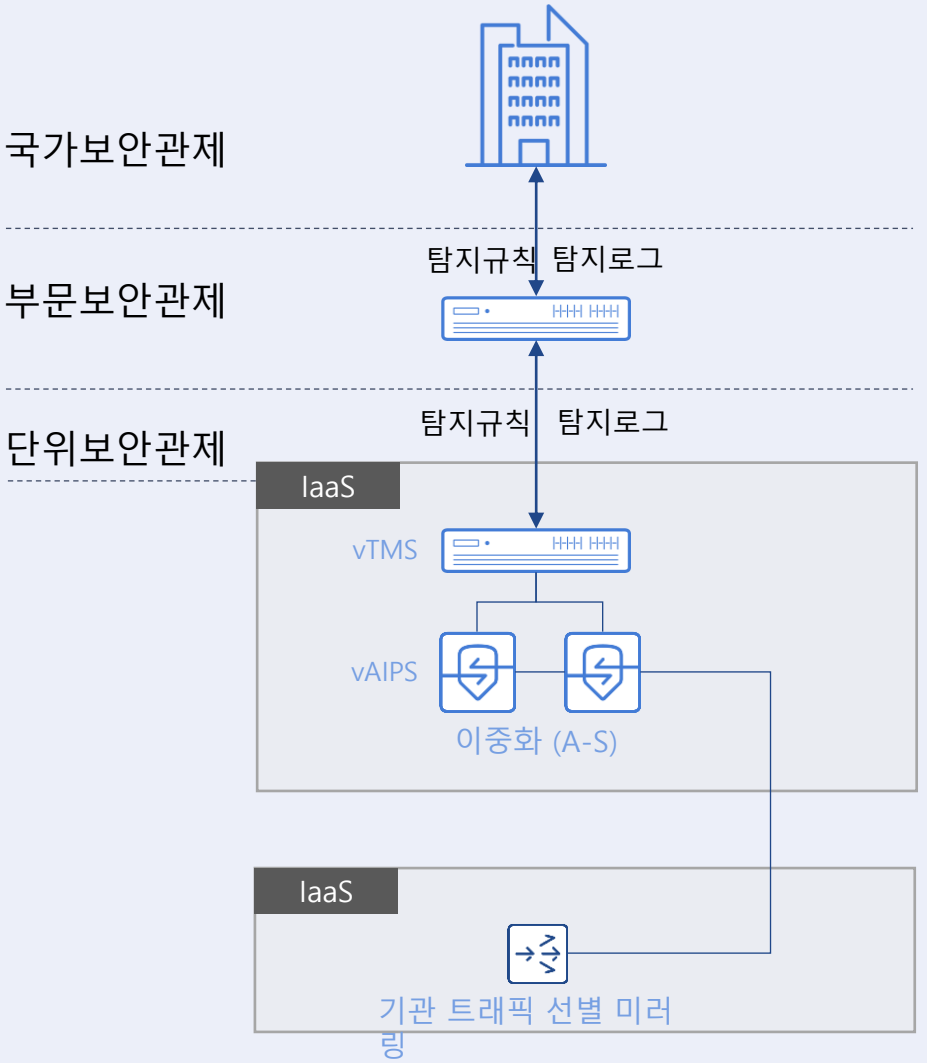
시그니처 기반 위협 탐지/차단
기본 IPS 시그니처 제공
사용자 정의 룰 지원 (Snort, PCRE, Yara)
행위 기반 탐지
비정상 프로토콜 차단
SSL 트래픽 검사
C&C 연결 차단
X-Forwarded-For 헤더 내 실제 IP 추출

외부 연동

AhnLab TMS와 연동
Syslog에 의한 로그 전송
NCSC 연동 지원

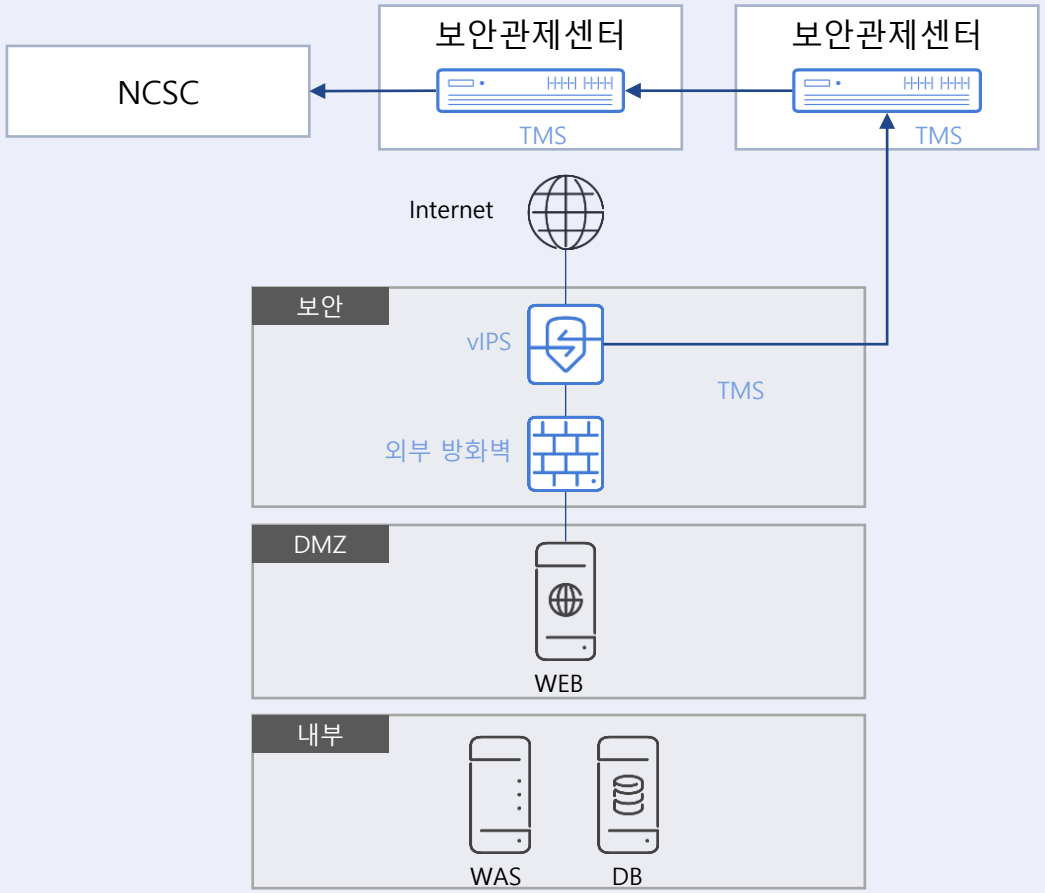
설정

이중화 구성
다수 VPC, Subnet 관리 지원

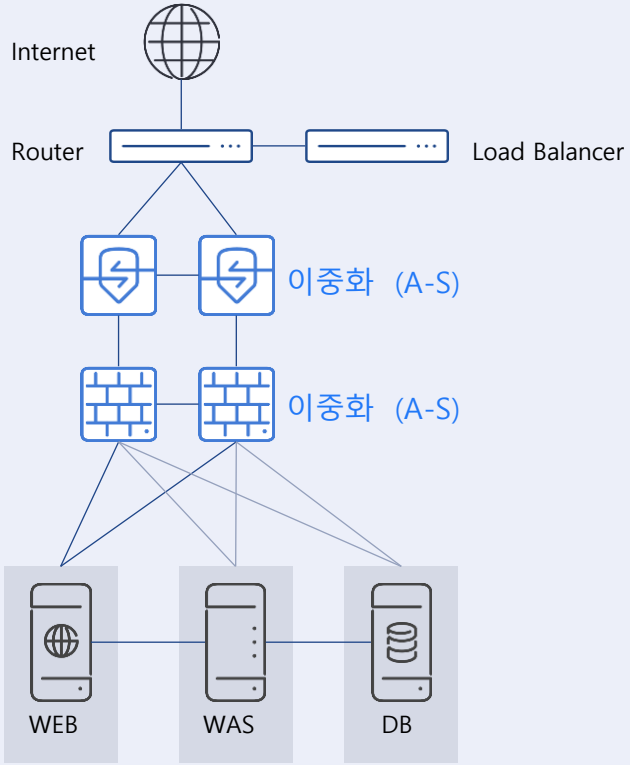


vAIPS 구성 및 구축 사례

고객의 기구축된 TMS를 이용하여 NCSC 연동

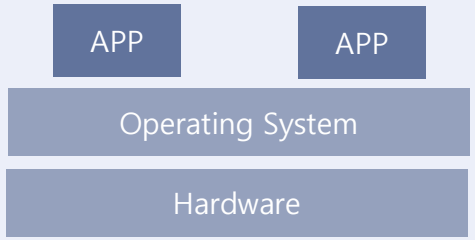


방화벽과 이중화 구성



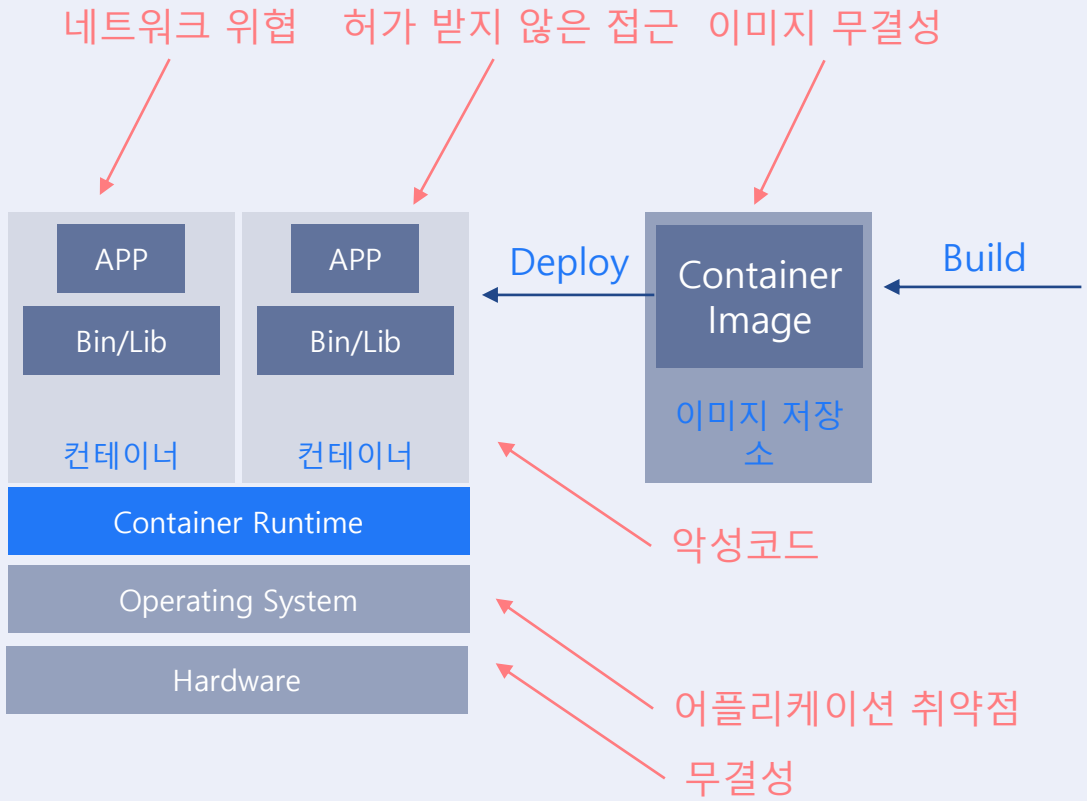
클라우드 가상환경 보안

물리적 서버



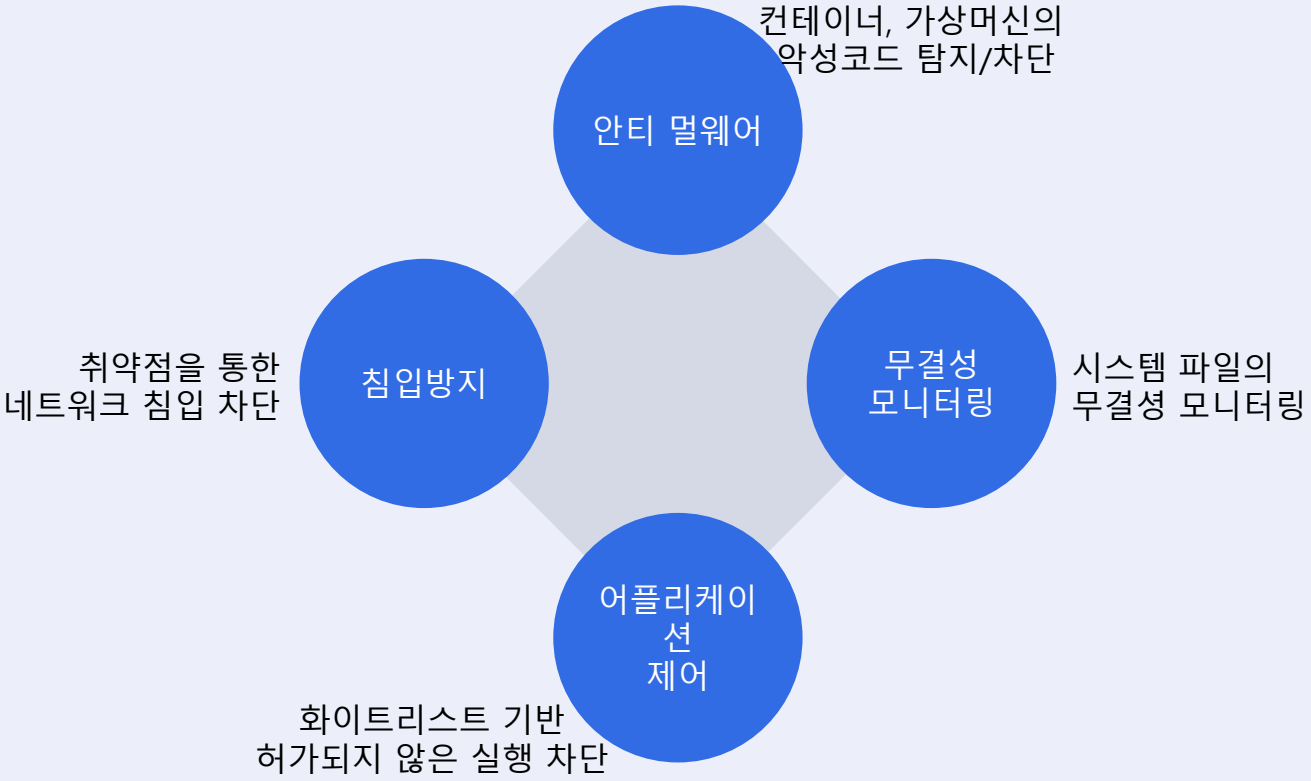
하이퍼바이저에 의한 가상화

컨테이너에 의한 가상화

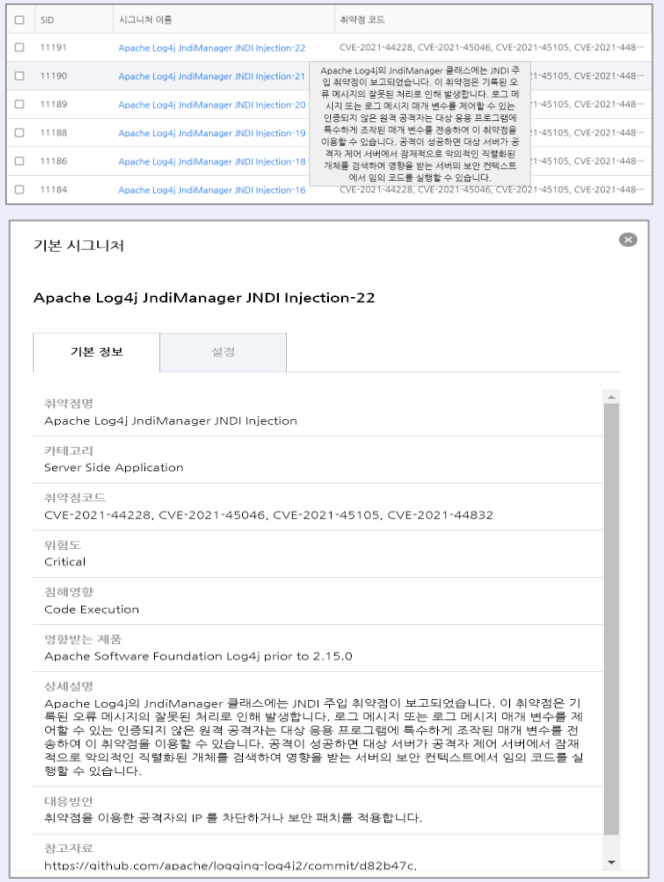


AhnLab CPP 소개

AhnLab CPP 주요 기능



제로데이 공격 방지



- 2021.12.10
  Apache Log4j 취약점(CVE-2021-44228) 발표
- 2021.12.11
  AhnLab CPP의 IPS 시그니처 긴급 대응

More security, More freedom

감사합니다

AhnLab