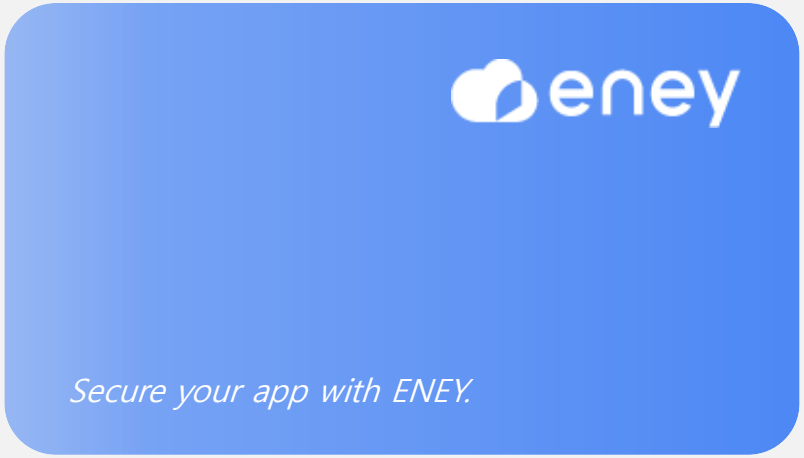
STANDARD PROPOSAL

깔끔하고, 심플한 보안존 클라우드



SERVICE

01. ENEY.CLOUD 필요성

개발자와 엔지니어가 없이도 클라우드 운영관리가 가능합니다.

클라우드 보안을 위해서는 방화벽/WAF가 필요하다.

- 클라우드 운영을 위해서는 방화벽과 WAF(웹방화벽)이 필수 이다. **구축 시 초기 비용이 많이 든다.**

보안 전문인력이 필요하다.

- 클라우드 운영을 위해서는 보안 전문인력이 필요하다. 따라서 전문기관에 외주용역을 맡기거나, 전문이력을 채용하면 **높은 고정비가 발생한다.**

02. ENEY.CLOUD 특·장점

Necessity ●---------- Service Value ----------● Necessity

확장성

타사 클라우드,
기존 레거시 장비에
모두 적용가능

검증된 사업자

300곳 이상의
B2B기업 유료 이용 중

클라우드.데이터, 비대면서비스
바우처 공급사업자

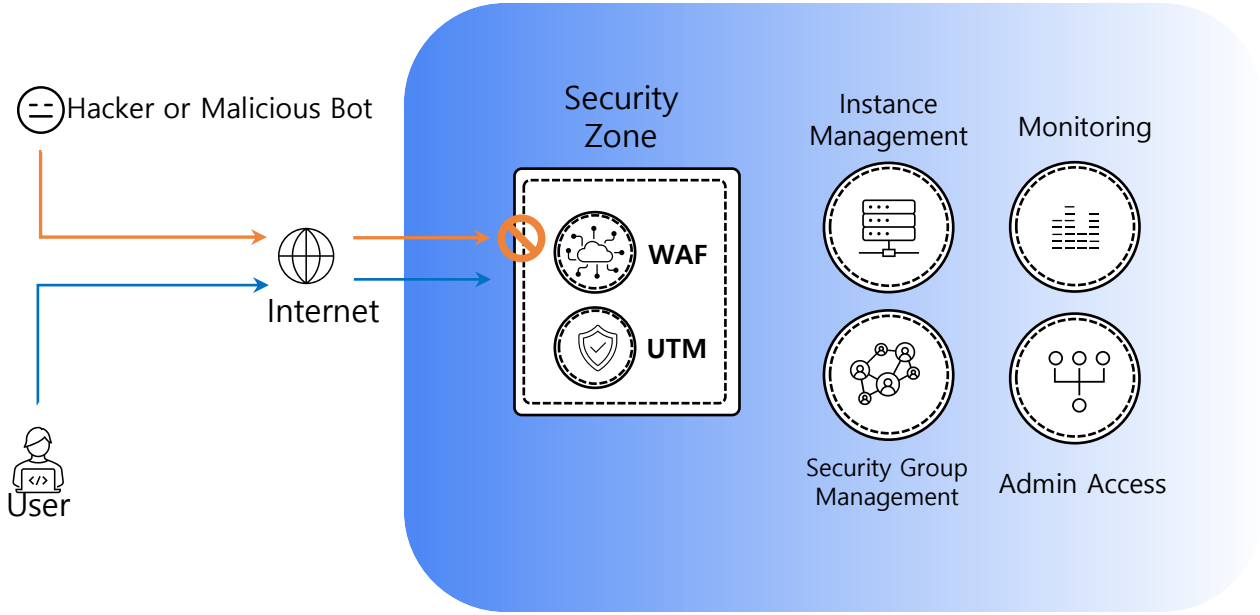
자동화

네트워크 보안 엔지니어가 없
어도, 전문지식이 없어도 가능

개발자와 엔지니어가 없이도 클라우드 운영관리가 가능합니다.

클라우드 컴퓨팅에 대한 지속적인 네트워크 보안 모니터링을 하면, 네트워크 보안 문제 발생시 빠르게 문제를 해결하고, 미래의 예상되는 문제를 예방할 수 있습니다.

서비스 구성도



퍼포먼스 분석

- 클라우드 컴퓨팅 파워 퍼포먼스 실시간 확인

트래픽 분석

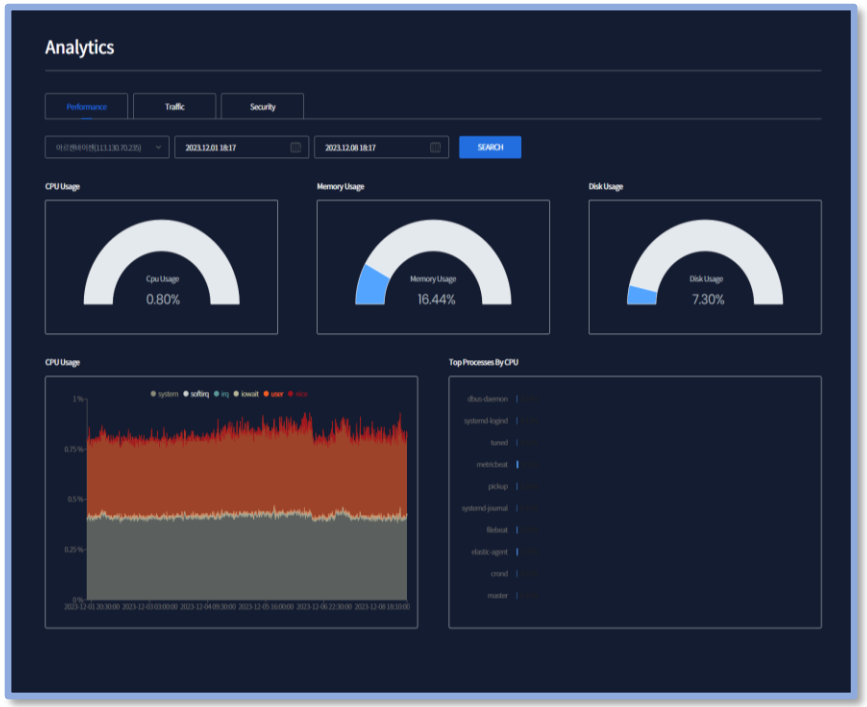
- 네트워크별 현황을 확인

네트워크보안 분석

- 네트워크 보안 이벤트를 확인

04. 퍼포먼스 분석

컴퓨팅파워 퍼포먼스 분석을 통해 간접적으로 시스템의 이상 징후를 확인 할 수 있습니다.



컴퓨팅 파워 퍼포먼스 분석

- **CPU Usage** 인스턴스의 실시간 CPU 사용량 확인
- **Memory Usage** 인스턴스의 메모리 사용량 확인
- **Disk Usage** 인스턴스의 Disk 사용량 확인
- **CPU Usage** CPU 사용량을 그래프로 확인
- **Top Processes By CPU** 실행중인 프로세스를 점유율 순으로 확인

05. 네트워크 트래픽 분석

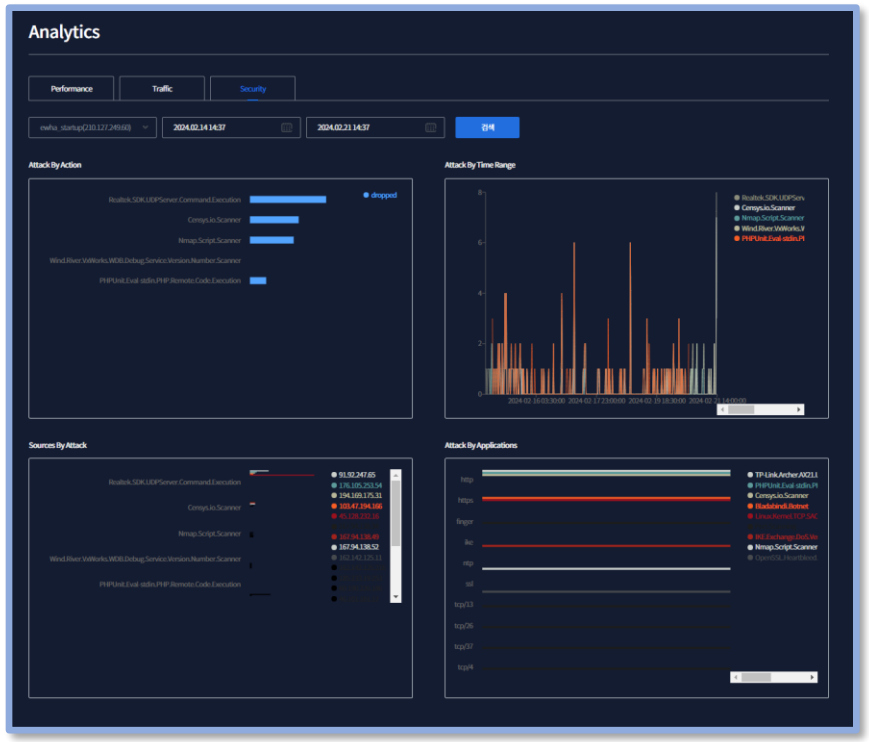
대상 네트워크, 분석기간을 선택 후 검색하여 해당 기간의 인스턴스 사용량을 모니터링 합니다.

네트워크 트래픽 분석

- **Network Traffic** 실시간 네트워크 트래픽 정보 확인
- **Bytes By Protocol** 접속한 프로토콜 및 포트별 네트워크 통신량 확인
- **Bytes By Sources** 접속한 IP 별 네트워크 통신량 확인
- **Bytes By Destination** 접속한 목적지 IP 별 네트워크 통신량(Bytes) 확인

06. 네트워크 보안 분석

대상 네트워크, 분석기간을 선택 후 검색하여 해당 기간의 인스턴스 사용량을 모니터링 합니다.



네트워크 보안 분석 이벤트

- **Attack By Action** 어떤 공격활동이 탐지 및 차단되었는지
- **Attack By Time Range** 공격시도를 시간 별로 확인
- **Sources By Attack** 공격시도가 어떤 주소에서 출발하였는지
- **Attack By Applications** 어떤 서비스 포트를 통해 공격시도가 발생하였는지 확인

07. 보안존 서비스 정책

구분		STANDARD	PREMIUM	PREMIUM PLUS	ENTERPRISE
Network	Public IP	○	○	○	○
	IPsec VPN	○	○	○	○
	SSL-VPN	○	○	○	○
	IP/Port 기반 정책 설정	○	○	○	○
방화벽	IPS		○	○	○
	웹 공격 탐지(기본)		○	○	○
	트래픽 Logging			○	○
웹방화벽	웹 공격 탐지(Expert)			○	○
백업	인스턴스 백업(매일)			○	○
보안관제	실시간 모니터링(24x365)				○
	침임탐지 대응				○
	보안정책 및 운영				○
	정기/비정기 보고서 제출				○

www.eney.cloud

Secure Your App

CSASE STUDY

Case 01 비업무 트래픽에 대한 통제를 원하는 기업

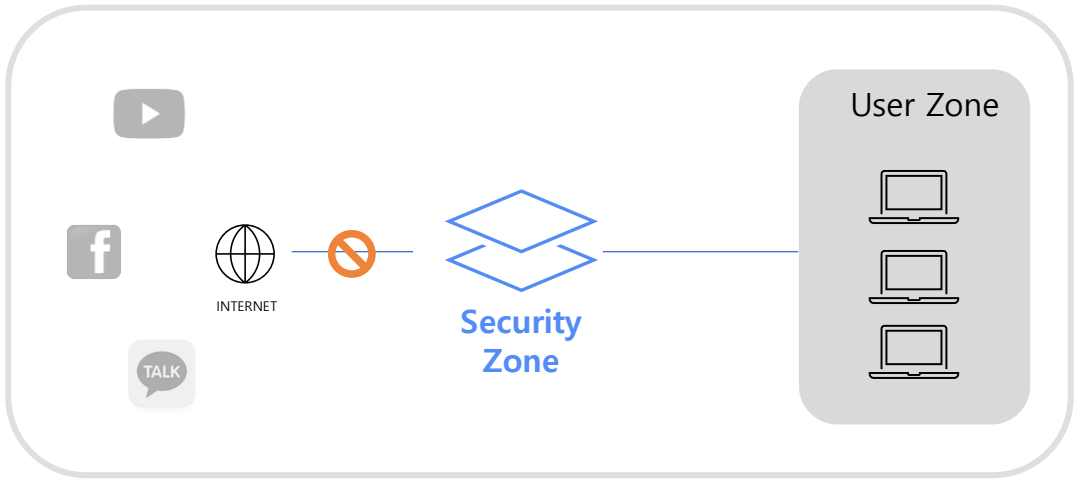
Case 02 외부에서 안전한 접근을 원하는 기업

Case 03 웹방화벽이 필요한 기업

Case 01. 비업무 트래픽에 대한 통제를 원하는 기업

요구사항

- 사내에서P2P 사용에 대해 완벽한차단
- 승인하지 않은 메신저사용금지
- 업무시간에 비업무 사이트사용금지
- 외부로부터의 접근통제
- 다양한 해킹방어

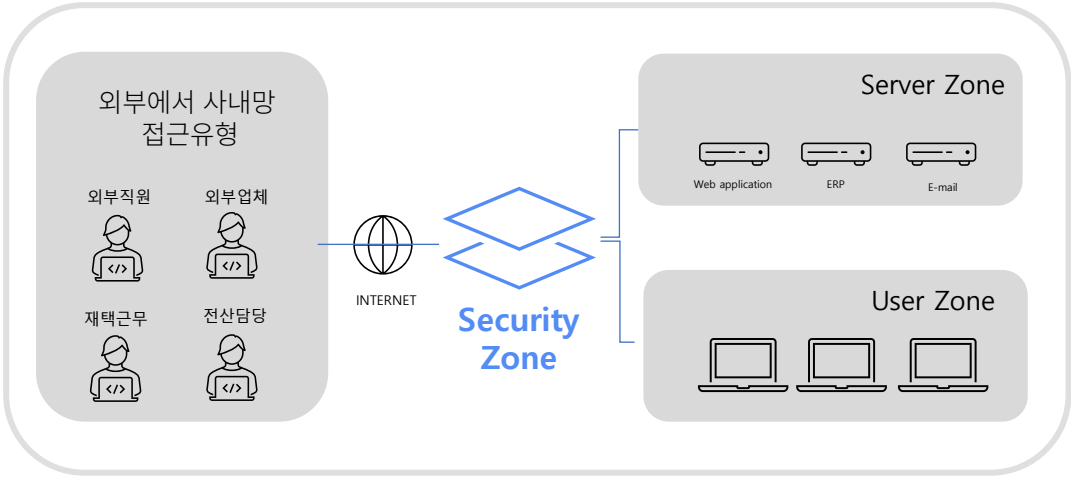


방화벽을 구매 또는 소프트웨어 방화벽을 설치하려면, 고정비용이 발생과 전문 엔지니어가 필요합니다.
에네이클라우드를 이용하면 빠른 시간 안에 방화벽 구현이 가능하며, 알고리즘 기반으로 운영자동화가 가능합니다.

Case 02. 외부에서 안전한 접근을 원하는 기업고객

요구사항

- 지정된 근무지 이외의 외부에서 내부 시스템으로 무분별한 접근이 허용되어 있어 보안이 취약함
- 외부에서 사내망으로 안전한 접근방법 필요
- 접근하는 사용자에 따라 권한차단부여
  (외근직원/외부업체/재택근무/전산담당)

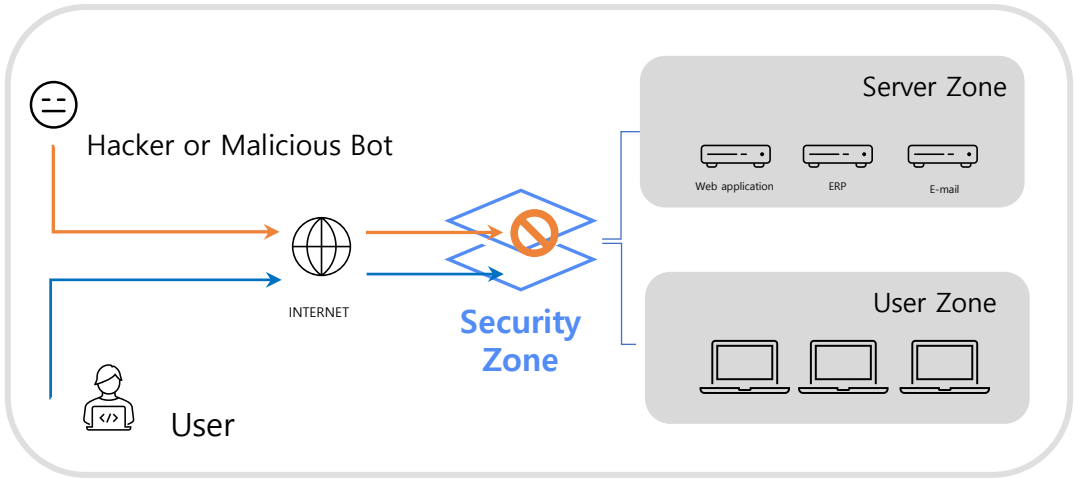


SSVPN 기능을 통해 안전하게 기업내부 사내망 자원을 사용 할 수 있습니다. 사용자의 담당업무와 권한에 따라 사용자를 그룹화하여 차등권한을 부여 할 수 있으며, 사용자들의 접속 및 접근 기록을 통해 감시가 가능합니다.

Case 03. 웹방화벽이 필요한 기업

요구사항

- 로그분석을 통해다양한 백도어발견
- 로그분석후 해당백도어 제거
- 공격자가 설치한 다양한 악성코드 설치확인 및 제거
- 중국으로부터의 SQL Injection 공격 차단
- 컨텐츠 복사 시도 차단



악성코드 대량유포로 인한 웹서버 부하증가로 서비스장애가 발생되었으나 에네이클라우드 보안존을 활용하여 부하증가 현상이소멸 되었습니다.

기능별 상세

F/W 방화벽

Firewall

구분	기능상세
Packet Filtering	Protocol, SRC/DST IP, Port, Interface 별로 패킷 필터링 지원
	방화벽 정책 별 출발지 호스트에 대한 허용세션 제안기능지원
	방화벽정책별 PPS 제한기능을 이용한 Rate Limit 제공
	방화벽정책별IP그룹, Port 그룹, 시간그룹 사용지원
Stateful Inspection	세션의 상태를 보전하여 New/Established/Related/Invalid 구분하여 관리
	세션 상태에 대해 세션timeout 값 변경지원
NAT	Static/Dynamic NAT/PAT 지원
	Source NAT/Destination NAT 지원
	SMAP/DMAP NAT 지원
Group Configuration	IP/Port/Time 그룹지원
Session 관리지원	세션 타임아웃 시간설정, 세션 별 로그생성, 세션 초기화기능지원

VPN

구분	기능상세
Support to Standard IKE & IPSEC	IPSEC표준을 준수하며 동일장비 및 타사장비와의 연동지원
	표준IKE 지원을 통한안정적인Key 관리지원
	ESP/AH프로토콜지원
Tunneling	정책기반, 경로기반IPSec터널지원
Encryption algorism	DES , AES (128, 192, 256), 3DES
Hash algorism	MD5,SHA1 , SHA256
Support To Muti line	Fail-Over, Active-Active 지원
IPv6지원	IPv6 IPSec 기능지원
SSL	SL기능지원(무료)
XAUTH 기능지원	Radius서버를 이용한 Xauth지원
모바일VPN	모바일 FortiClient를 통한 VPN터널링 지원
IPSec VPN Client	S/W VPN Program을 통한VPN 통신지원FortiClient

F/W 방화벽

IPS

구분	기능상세
Signature	시그니처기반 탐지기능 제공
Anomaly	비정상행위 트래픽을 탐지 및 자동으로 차단하는 기능제공
Update	주기적인IPS 패턴 업데이트 기능(주기적으로 혹은 수동가능)
격리	공격자 격리기능 제공
The Other	위험도, 타겟, 프로토콜, OS 및 어플리케이션 형태에 따라 선택적 IPS 필터 설정지원
	사용자IPS 시그니처 생성기능 제공

Antivirus

구분	기능상세
Pattern	Virus Pattern DB 자체 보유 및 업데이트
mode	Proxy , Flow 제공
The Other	압축된 파일형태의 바이러스차단기능, Wildlist의 Virus100% 차단
	공격자 격리기능 제공

Web Filtering

구분	기능상세
오버라이드	Administrative , User 지원
Grade to internet	Fortiguard를 통한등급 및 종류별 사이트차단
	웹콘텐츠 차단기능지원
The Others	로컬래이팅 추가지원

Networking

구분	기능상세
QOS	정책별로 대역폭 제한 및 인터페이스별 대역폭 설정지원
VDom	가상 도메인 지원
DHCP	Interface별 server , Relay 지원
MODE	NAT/ROUTE/Transparent지원
HA	Active–Standby , Active –Active 지원
Addressing mode	Static , DHCP, PPPoE 지원
The Other	Dynamic Routing (RIP. OSPF, BGP , Multicast)
	Static Routing (Static , Policy)
	DDNS 지원
	무선 컨트롤러 기능제공(FortiAP 연동가능)

WAF

OWASP TOP 10 취약점 대응이 가능합니다.

구분	기능상세
Broken Access Control	Parameter Tampering, Invalid URL, Directory Traversal 등
Cryptographic Failures	Privacy Filtering, Input Content Filtering등
Injection	SQL Injection, Stealth Commanding, Cross Site Scripting등
Insecure Design	Error Handling, Parameter Tampering, Directory Traversal 등
Security Misconfiguration	Directory Listing, Error Handing, XXE Injection등
Vulnerable and Outdated Components	User Defined Pattern, Custom Rule
Identification and Authentication Failures	Cookie Poisoning, SQL Injection, Directory Traversal 등
Software and Data Integrity Failures	Insecure Deserialization
Security Logging and Monitoring Failures	탐지로그 모니터링 및 연동(운영환경)
Server-side Request Forgery	File inclusion

Thank You