VIPER-N

인터넷전화 보안 게이트웨이

CC : (Common Criteria)
Common Criteria for Information Technology Security Evaluation)

SEPARATE

인터넷전화 교환기 내부를
사설 IP로 구성하여 외부로부터 격리

MONITOR

네트워크 트래픽 상시 모니터링으로
보안 위협 탐지

PROTECT

방화벽 방식의 솔루션으로
외부로부터의 보안 위협 차단

기업내로 유입되는 트래픽을 모니터링하고 VoIP 공격을 사전에 탐지/차단 하는 보안장비로써 국가정보원 “인터넷전화 보안장비 보안기능 요구사항”을 만족하는 IP 기반의 보안 취약점을 이용한 도청, 거부공격, 오용공격, 가로채기, 스팸 등의 다양한 인터넷전화 서비스 대상 공격을 탐지 차단하는 VoIP 전용 보안장비 입니다.
FMC, UC 구축 시 예상되는 NAT Traversal 처리와 기업내 주소정보를 완벽히 차단하는 Topology Hiding 기능 및 RFC3261 SIP 트래픽 암호화 기능을 동시에 제공하는 GATEWAY 방식과 IPT 내부 사용시에도 Transparent 하게 기존 네트워크의 변경이 없는 BRIDGE 방식을 제공하여 어떠한 망환경에서도 도입이 가능합니다.

GATEWAY

망분리
사설/공인 망분리

변환
UDP/TCP<->TLS,
RTP<->SRTP

모니터링
실시간 SIP 메시지 모리터링

탐지
DoS/DDoS 비정상 패킷 탐지

암호화
TLS/SRTP 지원

확장성
IPv4/IPv6 동시 지원

BRIDGE

망유지
망 변경없이 설치

분석
SIP 보안 위협 분석

NAONWORKS AhnLab (08381) 서울시 구로구 디지털로 271, 711호 02.2025.1630 sales@naonworks.com

주요 기능 (Main Function)

분류	기능 내용
보안	인터넷 전화 서비스의 주요 보안 위협 탐지/차단
	Flooding(SIP , TCP , RTP , ICMP 등) 탐지/차단
	VoIP 비정상세션, SPAM, Static/Dynamic ACL 설정을 통한 단말 접근 탐지/차단
	감사/식별 및 인증
	기관내 주소정보 차단을 위한 Topology Hiding
	인증 우회를 통한 불법 사용 탐지/차단
VoIP방화벽	NAT/Firewall 내 VoIP 단말 및 IP-PBX 수용을 위한 음성 방화벽(VoIP NAT)
	B2BUA SIP 메시지 처리로 NAT Traversal
	SIP Trunking 및 SIP Connect 등의 다양한 Call Routing
	외산 IP-PBX 및 VoIP Gateway와 연동
암호화	시그널 및 미디어에 대한 암호화(TLS, SRTP)기능 제공
	국제표준(AES)및 국내표준(ARIA)보안 프로토콜 탑재
	행정기관 인터넷전화 보안규격 Ver.4 지원
	TLS ↔ UDP , RTP ↔ SRTP간 프로토콜 변환
모니터링	장애 대처를 위한 실시간 Call 로그 모니터링
	발생 호 및 인터넷 사업자와 연동여부 상태 모니터링
	다양한 통계 데이터 출력 및 보고서 출력(시간별, 일별, 월별)

주요 특장점 (Features & Benefits)

기능성
- 인터넷 전화 서비스의 주요 보안 위협 탐지/차단
- NAT/Firewall 내 VoIP 단말 및 IP-PBX 수용을 위한 음성 방화벽

안정성
- 하드웨어 일체형 장비로 외부 VoIP 공격에 대한 완벽한 차단
- 이중화 구성이 가능하여 연결된 호에 대한 백업 및 장애에 의한 절체 시 서비스 유지

확장성
- 하드웨어 변경 없이 동시 콜수 확장 및 다양한 Call Routing 구성

편의성
- 사용자 편의적이고 직관적인 GUI 환경으로 편리한 액세스 설정 및 동작
- 별도의 EMS 없이 시스템 관리가 가능하며 다양한 Report 기능 제공

시스템 구조 및 구성 (System Structure & Configuration)