주요 기능

구성 및 이중화

- NW의 라우팅 구성 변경이 필요없는 In-Line Transparent 모드 구성
- 모니터링 모드 및 차단 모드를 제공
- 장비 이중화(Active-Active, Active-Standy) 구성 및 Fail-over/ Bypass, LLCF 기능

운영 관리

- 관리자용 Web GUI 환경 및 인터페이스 제공
- 사용자 권한별 접근제어 관리
- 로그 관리 기능(로그감사, 검색 등)
- 원격 접속시 암호화 통신(SSH, HTTPS 등) 기능
- 통합관제(ESM, NMS)와 연동 지원
- 상위기관 룰 연계 기능

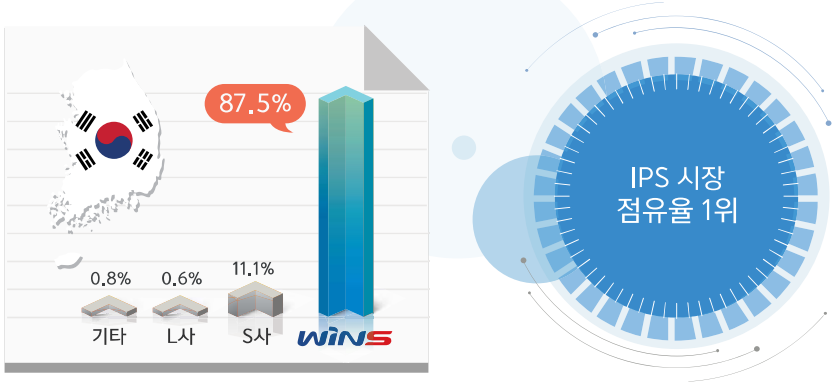
탐지차단 기능

- 유해 트래픽 차단
  - *L7 Signature 기반 탐지 차단
  - *protocol Anomaly 공격의 탐지 및 차단
  - *Fragmentation된 유해 패킷에 대해서도 탐지 및 차단
  - *Offset, String 등을 이용하여 사용자 정의 패턴을 설정
  - *Snort 탐지 규칙 명령어 지원 기능(PCRE)
- Flooding 차단
  - *임의의 IP를 대상으로 임계치 기반의 동적 Flooding 탐지 및 PPS 제어
  - *TCP Flag별 동적 Flooding 제어
- QoS 기능
  - *시스템은 5-Tuple(Src IP주소, Dst IP주소, Src Port, Dst Port, Protocol) 및 TCP Flag 모두 이용하여 복수 조건으로 QoS 정책 설정
  - *TCP Flag는 Syn(Syn/Ack 포함), Psh(Psh/Ack 포함), Fin(Fin/Ack 포함), Rst(Rst/Ack 포함), Ack, 기타 등 다양한 방법의 조합으로 설정
- 암호화 트래픽 탐지 차단 기능
- 국가별 유입 트래픽 모니터링 차단 기능
- IP Pool 을 이용한 Virtural 탐지, 차단

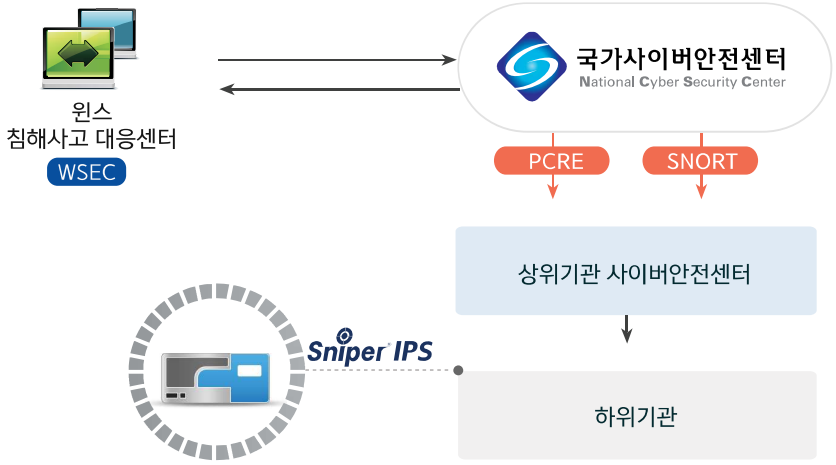
경기도 성남시 분당구 판교로 228번길 17(삼평동) 판교세븐벤처밸리 1동 7층 ㈜ 윈스
TEL. 031-622-8600 FAX 031-622-8601 www.wins21.co.kr

Sniper® IPS

대한민국 대표 침입방지시스템



상위기관 룰 연계 기능 TMS 연동



HTTPS 트래픽 복호화 지원

은닉형 악성코드/DDoS 탐지

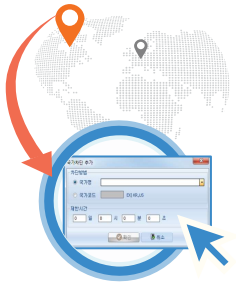
- SSL인증서를 IPS에 설치
- 복호화 후 공격 탐지/방어

암호화 공격 대응은?

국가별 공격 유입 모니터링 및 차단

사이버테러 원천 차단

- 국가별 모니터링
- 정책 최적화



중국발/북한발 유입트래픽 모니터링 필수

제품 성능

	NE 1000	NE 2000	NE 4000	NE 5000	10G
Throughput	400M~1G	2G~4G	4G	10~20G	20~40G
CPU	Intel Xeon Quad Core 2.4Ghz	Intel Xeon Quad Core 2.4Ghz * 2	Intel Xeon Quad Core 2.4Ghz * 2	Intel Xeon Quad Core 2.4Ghz * 2	Intel Xeon Quad Core 2.66Ghz * 2
RAM	6GB/500GB 이상	8GB/500GB 이상	12GB/2TB 이상	12GB/2TB 이상	12GB/2TB 이상
Interface	10/100/1000 *2	10/100/1000 (TX)*4 or 1000(SX/LX)*4	1000BaseSX (LX)*4	10G BaseSR (LR)*4	10G BaseSR (LR)*4
Power	Dual 2중화				