KSIDC
Korea Server Hosting Inc

KS Korea Server Hosting 코리아서버호스팅

IPS보안관제

- 클라우드 부문 미래창조경영우수기업 대상
- 3년 연속 한국소비자만족지수 1위
- 2010년부터 랭키닷컴 IDC 분야 1위 유지
- 한국정보방송대연합 인증 정보보호준비도 평가
- 한국클라우드산업협회 인증 클라우드 확인제
- 한국품질혁신우수기업 선정
- 한국인터넷진흥원 시행 고객만족우수기업
- IDC부분 기술혁신 대상
- 대한민국 신성장동력 미래선도기업

코리아서버 호스팅은 보다 차별화된 유지관리로 기업과 개인의 전략적 파트너가 되겠습니다.

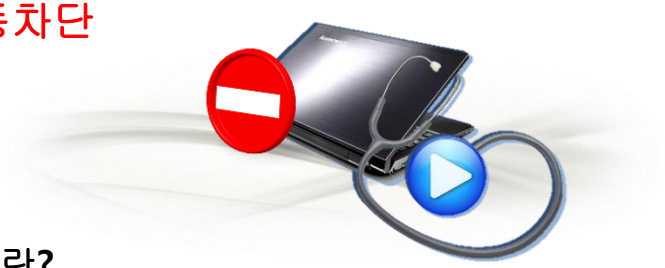
서울시 서초구 서초동 1710-1 SK 브로드밴드 IDC 센터
TEL : 02-593-8320 FAX : 02-6264-8321

IPS 보안관제

KSIDC
Korea Server Hosting Inc

철통보안 IPS 보안관제로
실시간 탐지 및 자동차단

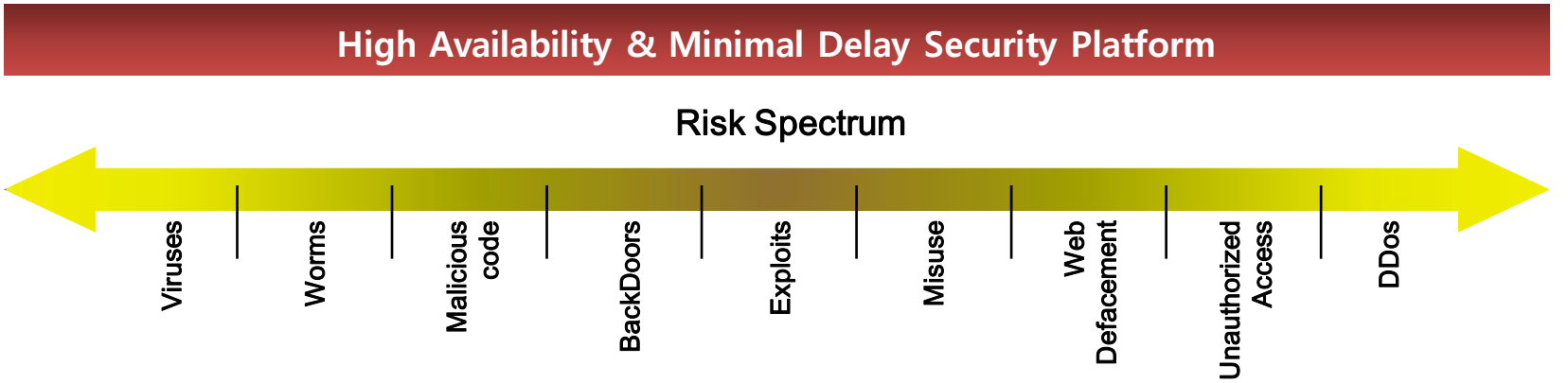
- 실시간 탐지 및 방어
- 내부정보 유출 방지
- 웅급상황 지속적인 패치
- 간편한 설치 및 운영



❖IPS 보안관제 서비스란?

네트워크상의 불법침입의 탐지/방어를 능동적으로 수행, 자동으로 해결책을 제시함으로 실시간 패킷처리, 오탐지를 최소화, 변형 공격과 오용 공격의 탐지, 각각의 상황에 맞는 실시간 반응 기술을 적용한 보안존을 구성하여 실시간으로 탐지/방어하는 서비스입니다.

KSIDC의 보안관제 서비스는 네트워크 상위단에서부터 일반존과 보안존을 구분하여 보안존을 3단계로 구성되며 1차 백본의 유해트레픽 차단, 2차 IPS의 능동형방어시스템 구축, 3차 KS방화벽으로 구축하여 보안 전문 엔지니어가 365일 24시간 보안관제하여 드립니다.



IPS 보안관제

KSIDC
Korea Server Hosting Inc

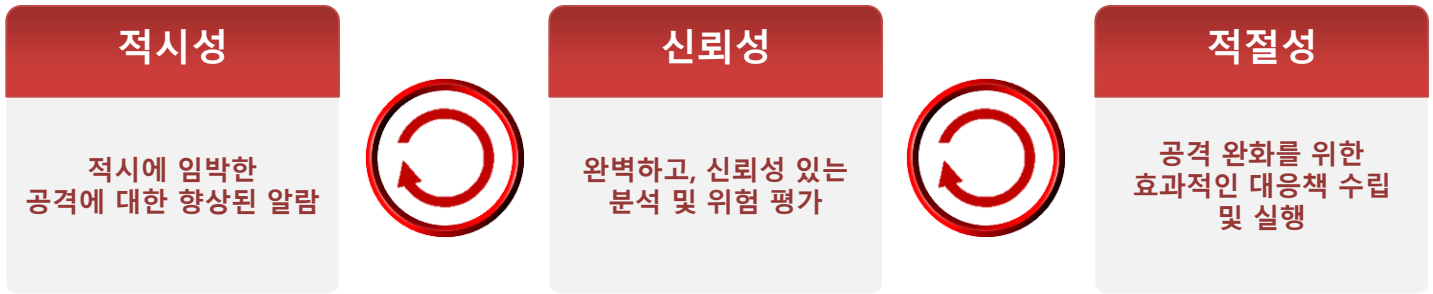
❖필요성 및 도입효과

IPS 보안관제

KSIDC
Korea Server Hosting Inc

✓기대효과

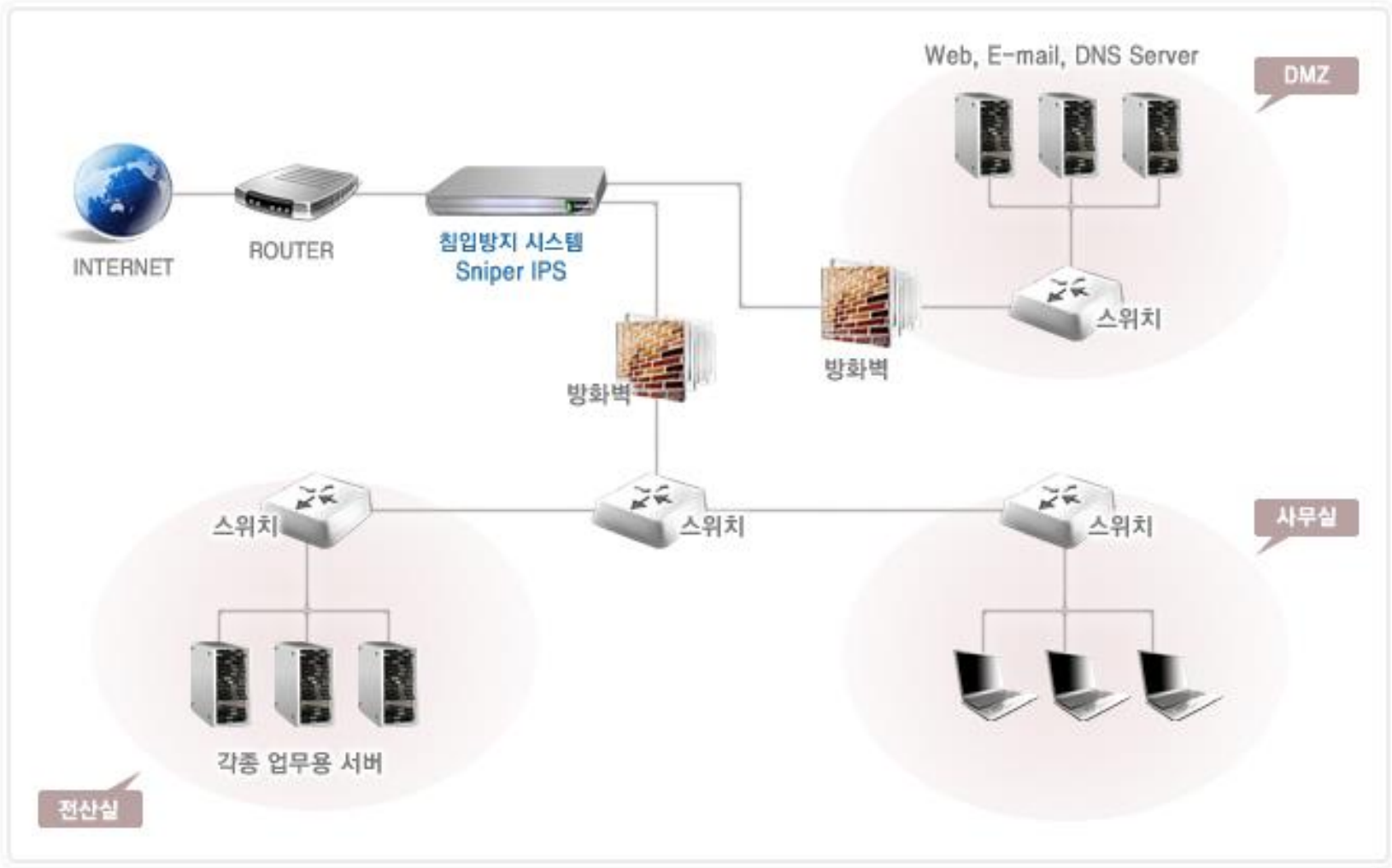
- 내부 사용자(지점사용자)의 감시 → 내부 보안 강화
- 내부 서버/네트워크 장애시 문제 파악 및 대처 가능
- 사용자의 웜바이러스 감염 유해트래픽 차단
- 유해트래픽 차단 → 기존 네트워크의 가용성 향상
- 알려지지 않은 유해트래픽에 대한 대응 가능
- DoS, DDoS로 부터의 내부 네트워크 자원의 보호
- 업무단절 및 지연을 유발하는 웜을 포함하는 대형 해킹공격에 대한 조속한 대응
- 서버의 서비스 생존성 보장으로 대고객 만족 및 조직 경쟁력 확보
- 제품 도입으로 인한 정보 자산의 보호효과는 도입 비용을 천문학적으로 능가
- 효율적인 QoSPolicy 수립, 트래픽 품질 보장 및 SLA 개념 강화



IPS 보안관제

KSIDC
Korea Server Hosting Inc

❖서비스 구성도

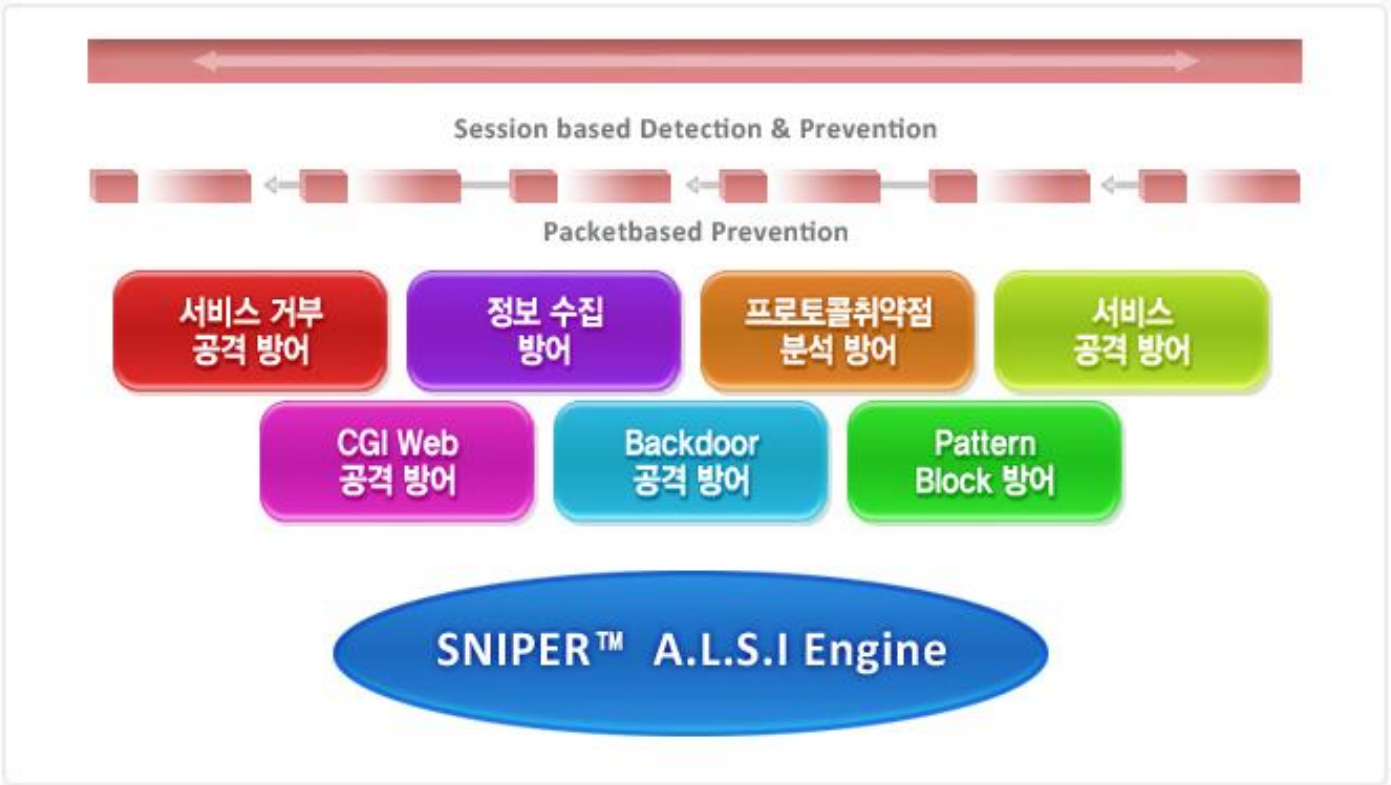


IPS 보안관제

KSIDC
Korea Server Hosting Inc

❖ IPS Architecture

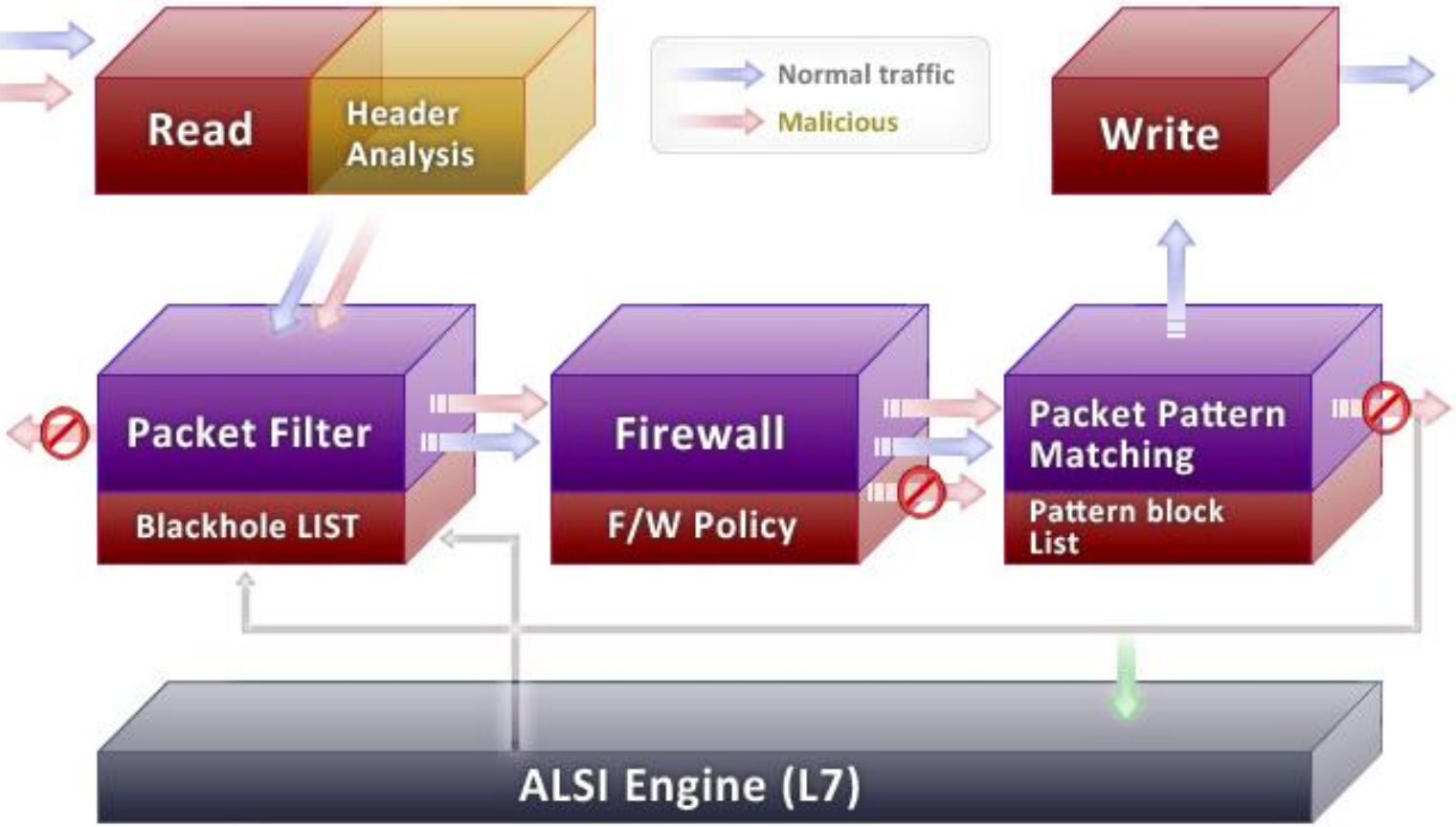
- SNIPER-IDS 기술에서 진보된 Application Level Stateful Inspection Engine 개발
- Switch, Firewall 에서 발생되는 False Negative 방지를 위한 SNIPER-A.L.S.I Engine
- 여러 Signature 룰 축약하여 탐지함으로써 Directory Traverse, WEB CGI 공격 등 다양한 형태의 공격도탐지 가능하며,탐지 속도 또한 향상된 기술
- TCP Connection-Oriented 기반 공격시 정교한 세션조합으로 해킹공격을 분석하는 기술



IPS 보안관제

KSIDC
Korea Server Hosting Inc

✓Engine Flow



IPS 보안관제

KSIDC
Korea Server Hosting Inc

❖IPS Specification[기능]

IPS Specification		
System	Stand-Alone Management	○
	콘솔별도	X
	Web Management	○
	SLI 암호화	○
	CLI Support	X
	Transparent Mode	○
	Security Certification	CC(공통평가기준)
Real-time Monitoring	실시간탐지/방어정보	○
	트래픽 추이/네트워크 부하	○
	프로토콜별 점유율	○
Detection Block Method	Application Level Stateful Inspection	○
	Dynamic Black List	○
	One-way 공격방어	○
	Defragmentation	○
	Reassembly	○
	Forensic Support	○

IPS Specification		
Detection Categories	Dos	○
	스캔공격(Probing)	○
	서비스공격	○
	프로토콜 취약성	○
	Backdoor	○
	Web CGI	○
	Worm	○
	Anomaly	○
	사용자정의	○
	Import/Export Signature	○
	라이브업데이트	○
	Signature Scheduling	○
	시그네쳐수	1500+
	Critical 문제시 24시간 대응	○
Actions	Detect Only	○
	Block	○
	Allow	○
	Alert	○
	Log	○

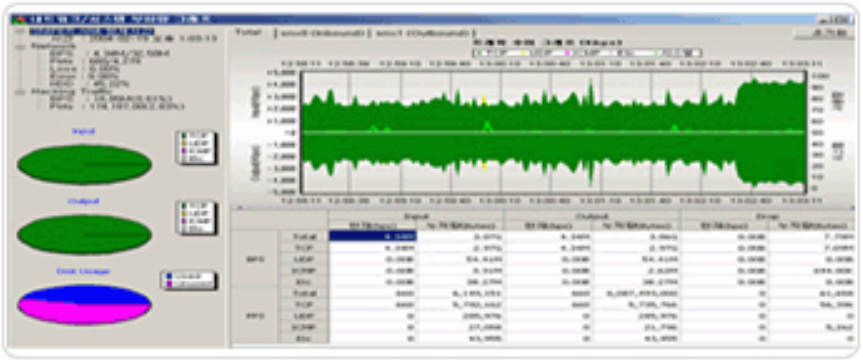
IPS Specification		
Notification /Messaging	E-mail	○
	Screen Display	X
	Alarm Sound	○
	SMS	○
	Script	○
	Syslog	○
	SNMP	○
내부정보유출 방지	E-mail	○
	Telnet	○
	FTP Rlogin	○
	NETBIOS	○
	Raw Data	○
Reports	월별 보고서작성	○
	Customize	○
	File Type	CSV, Excel
Additional Functions	Firewall	○
	Passive Mode	○
	MPLS	○
	이중화 구성(HA)	○
False Positive의 최소화	예외 메커니즘	○
	공격정보튜닝	○
	RawData캡쳐	○
	내부/외부 IP의 설정	○
	ALSI	○

IPS 보안관제

KSIDC
Korea Server Hosting Inc

❖ Real Time Monitoring

- 실시간 세션정보(HTTP, FTP, Telnet 등)및 네트워크 트랜드 확인



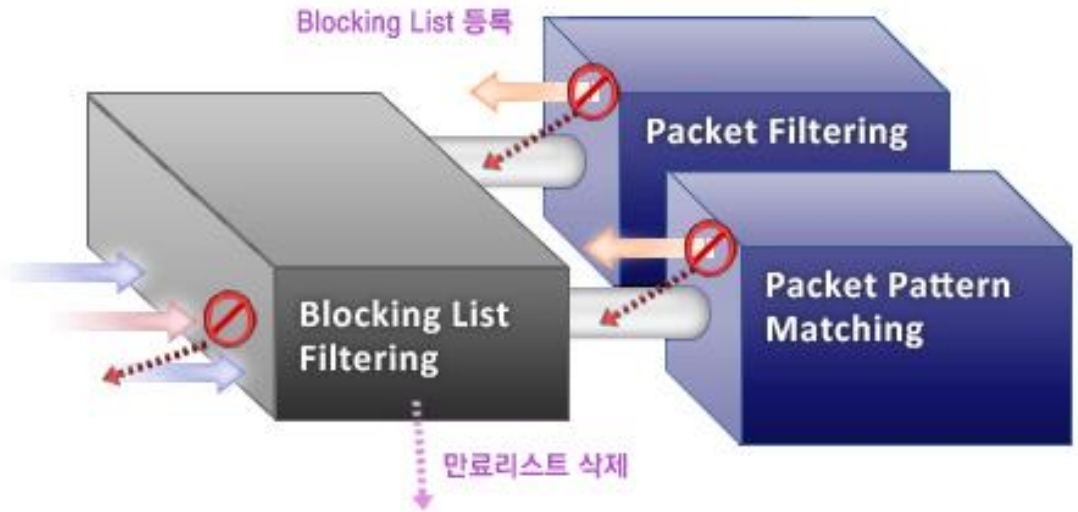
- 실시간 탐지/방어정보(해킹, 유저정의, 네트워크)및 방어상황(방어제한시간 등) 확인

IPS 보안관제

KSIDC
Korea Server Hosting Inc

❖Dynamic Rule 적용

- Filtering & Matching 에 차단됨과 동시에 Blocking List 등록
- Blocking List 만료 후 삭제함으로써 Dynamic Policy Rule 수립
- 수동등록모드 지원



Blocking List 구성요소

- 등록/만료일시
- 차단방법
- 공격/대상주소
- 프로토콜/포트
- 차단사유
- 공격코드
- 공격명