SECUI

네트워크 측면의 내부 정보보호

2014.04.24

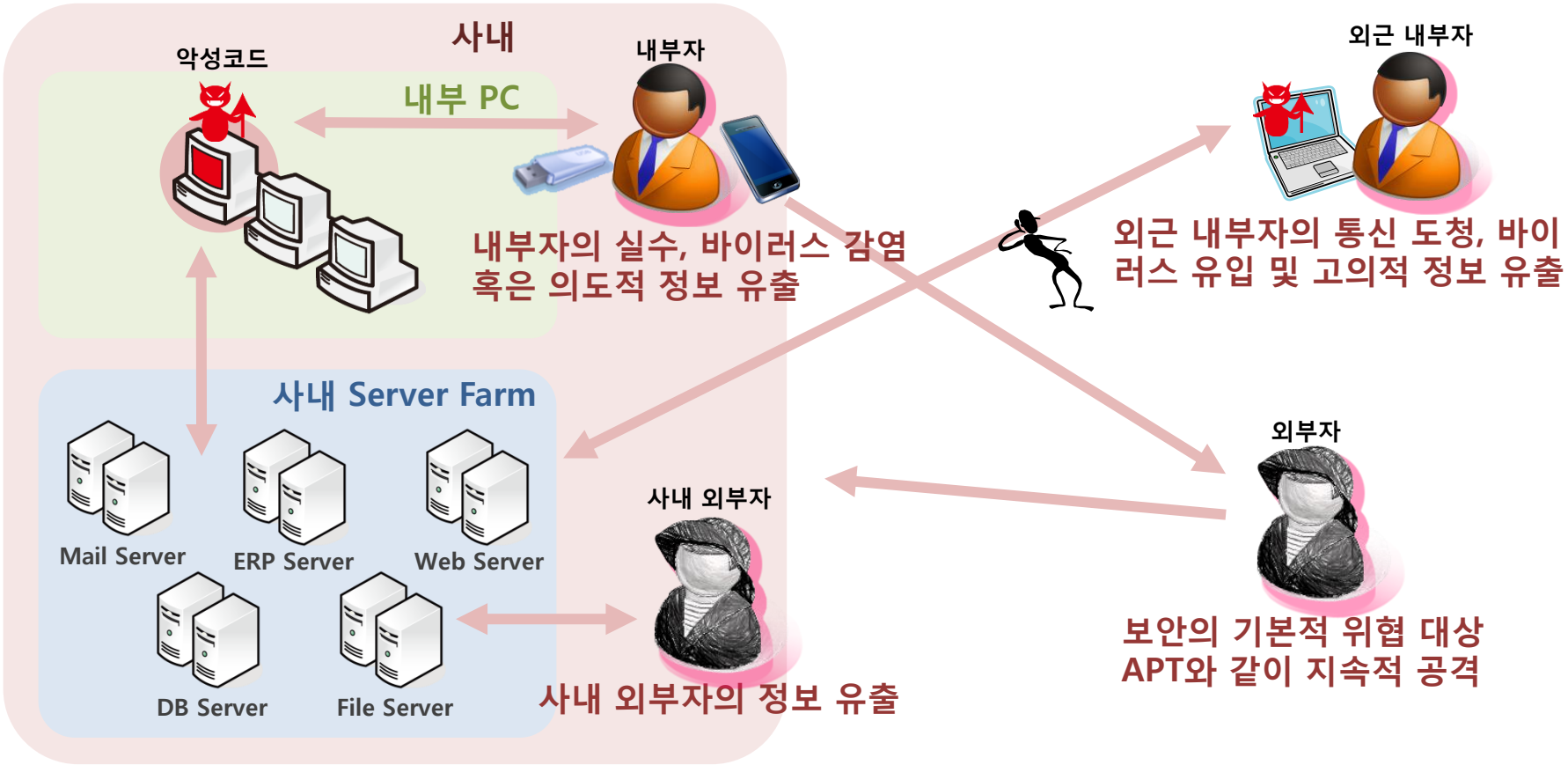
홍기훈 수석

기업의 정보 유출 위협

□ 내부자 및 외부자 위험

○ 내부자의 자료 복사 및 물리적 수단을 통한 유출
- 저장매체 (USB 메모리, 스마트폰, CD, 카메라 등)을 통한 유출

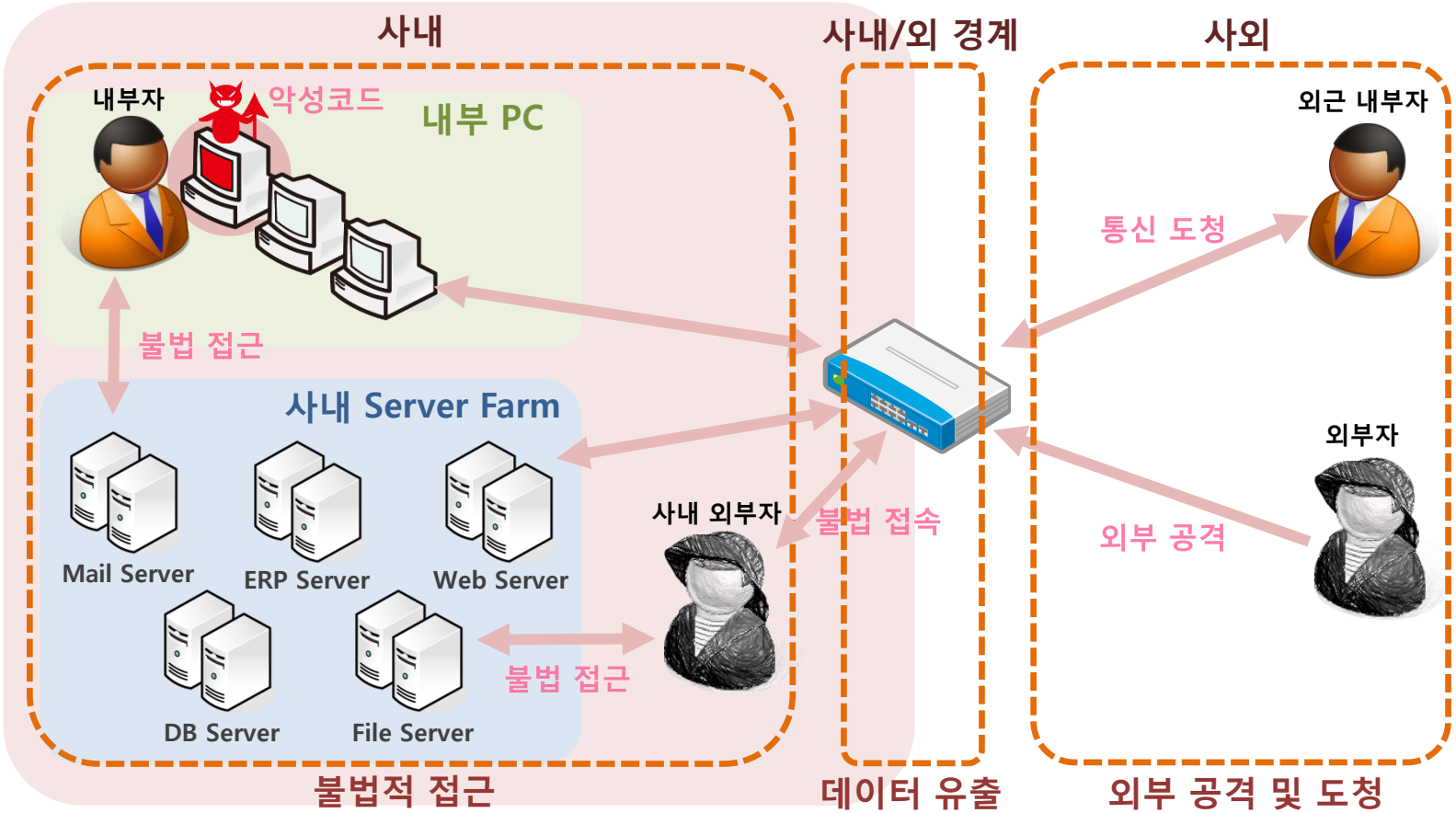
○ 내부자의 네트워크를 통한 유출
- 인터넷을 통해 사용자 실수, 악성 코드 혹은 의도적인 유출 (전송)



구간별 정보 유출 위협

□ 네트워크 구간 별 위협 요소

- ○ 사내 내부
  - 내부자의 권한 없는 불법 접근, 악성 코드에 의한 데이터 접근, 불법적 네트워크 접속
- ○ 사내와 사외 경계
  - 사내 데이터의 외부 유출
- ○ 사외
  - 도청, 외부 공격을 통한 내부 자료 유출, 외근 내부자의 내부 데이터 접근 및 유출



□ 사내 보안에 사원들의 생각

○ 출처 : 한국 경제 기사, "사내보안 필요하지만...10명중 6명 스트레스"

- 마크로밀엠브레인이 지난 4~7일 직장인 517명을 대상으로 벌인 설문조사

○ 사내 보안에 대한 사원들 인식

- 63.6% : 사내 보안 탓에 스트레스를 받은 경험이 있다.
  - 42.7% : 보안 때문에 업무에 차질을 빚은 경험이 있다.

○ 가장 불만을 갖는 사내 보안은 ?

- 25.7% : 회사 출입증 유무
- 25.3% : USB 반입·반출 금지
- 22.1% : 개인 메일 사용 금지
- 4.4% : 출퇴근 시 가방 엑스레이 검사

○ 사내 보안의 필요성에 동의하지만 업무에 방해가 될 정도로 불편함에 불만

□ 내부자 정보 유출에 대한 대응 방안

○ 각 목적별 전용 보안 프로그램으로 제어

- 전용 프로그램으로 적합한 보안 목적 달성
  - 바이러스 백신, PC 관리, 문서 보안 프로그램, PC 방화벽 등 여러 보안 프로그램 설치
- 고비용 및 관리적 문제 발생
- 내부자들의 불만 증가
  - 소프트웨어 충돌, 컴퓨터 자원 점유로 느려짐 등

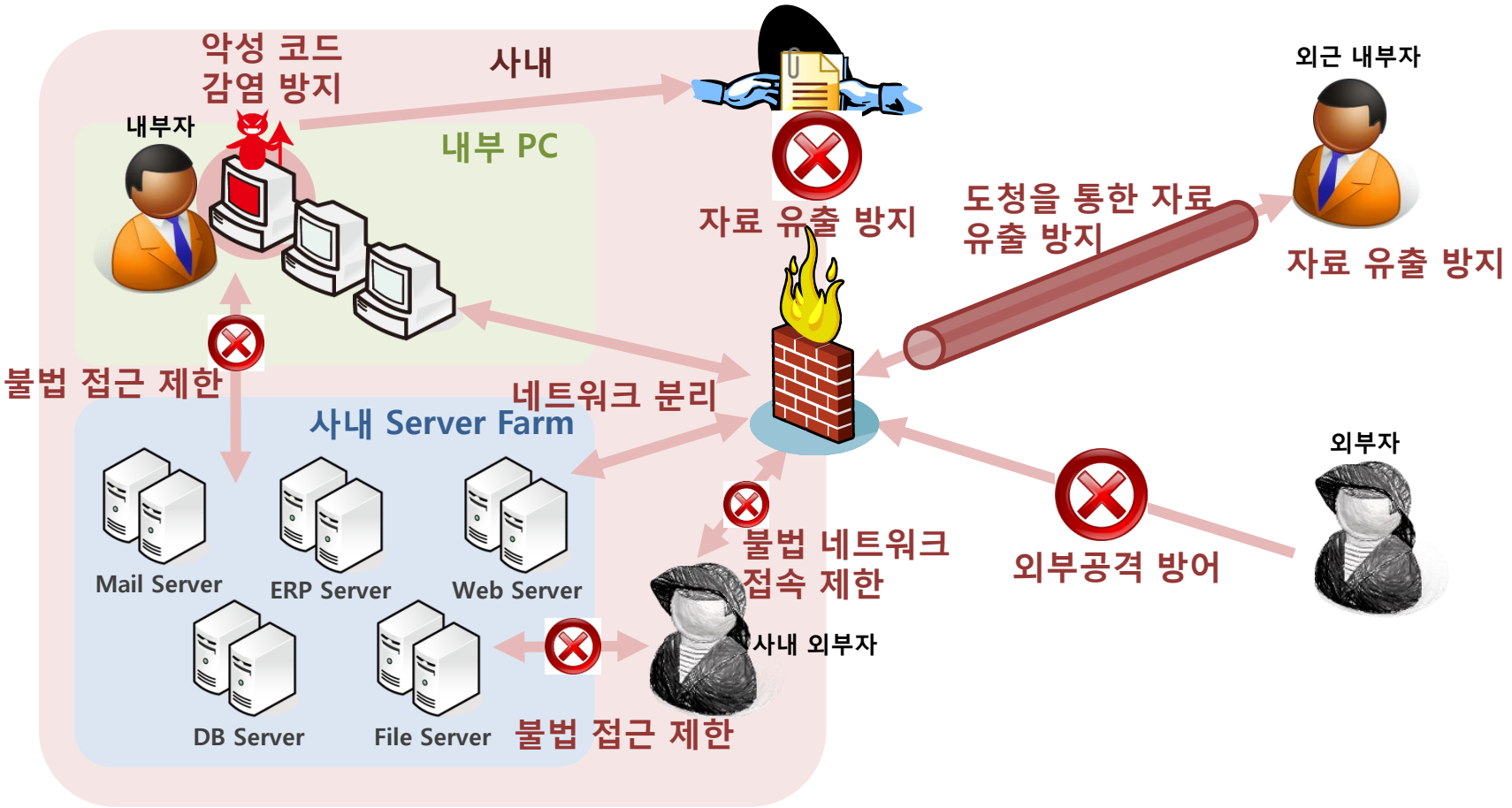
○ 네트워크기반 솔루션으로 제어

- 네트워크단에 네트워크 보안 솔루션 적용
- 저비용 및 단일 장비로 관리 용이
- 내부자 시스템(PC)에 직접적인 간섭없이 적용 가능
- 내부자가 네트워크단 제어를 인지하기 어려움
- 초기 보안 적용 모델로 적합

□ 내부자 및 외부자 정보 유출 방지

○ 네트워크를 통한 유출 방지

- 사용자 실수, 악성 코드 혹은 내부자의 의도적 유출 등



네트워크 기반의 정보 유출 방지 보안 기능들

□ 사내 제어 기능

○ 역할 및 권한 기반 내부 네트워크 제어
- 방화벽 (내부 분리 및 제어) / 사용자 인증 기능
- NAC (내부 접속 사용자 제어)

○ 악성 코드 감염 방지
- 악성 코드 검사 / 스팸 메일 검사
- 악성 URL 차단 서비스 / 카테고리기반 웹필터 서비스

□ 사내 / 사외 경계 제어 기능

○ 외부 정보 유출 방지
- DLP (Data Loss Prevention)
- 애플리케이션 제어
- IPS를 통한 관리자 정의 시그니처

○ 암호화된 정보 유출 방지
- SSL 트래픽 검사 기능을 통한 암호화 데이터 검사

□ 사외 제어 기능

○ 외부 통신 도청 방지
- IPSec / SSL VPN

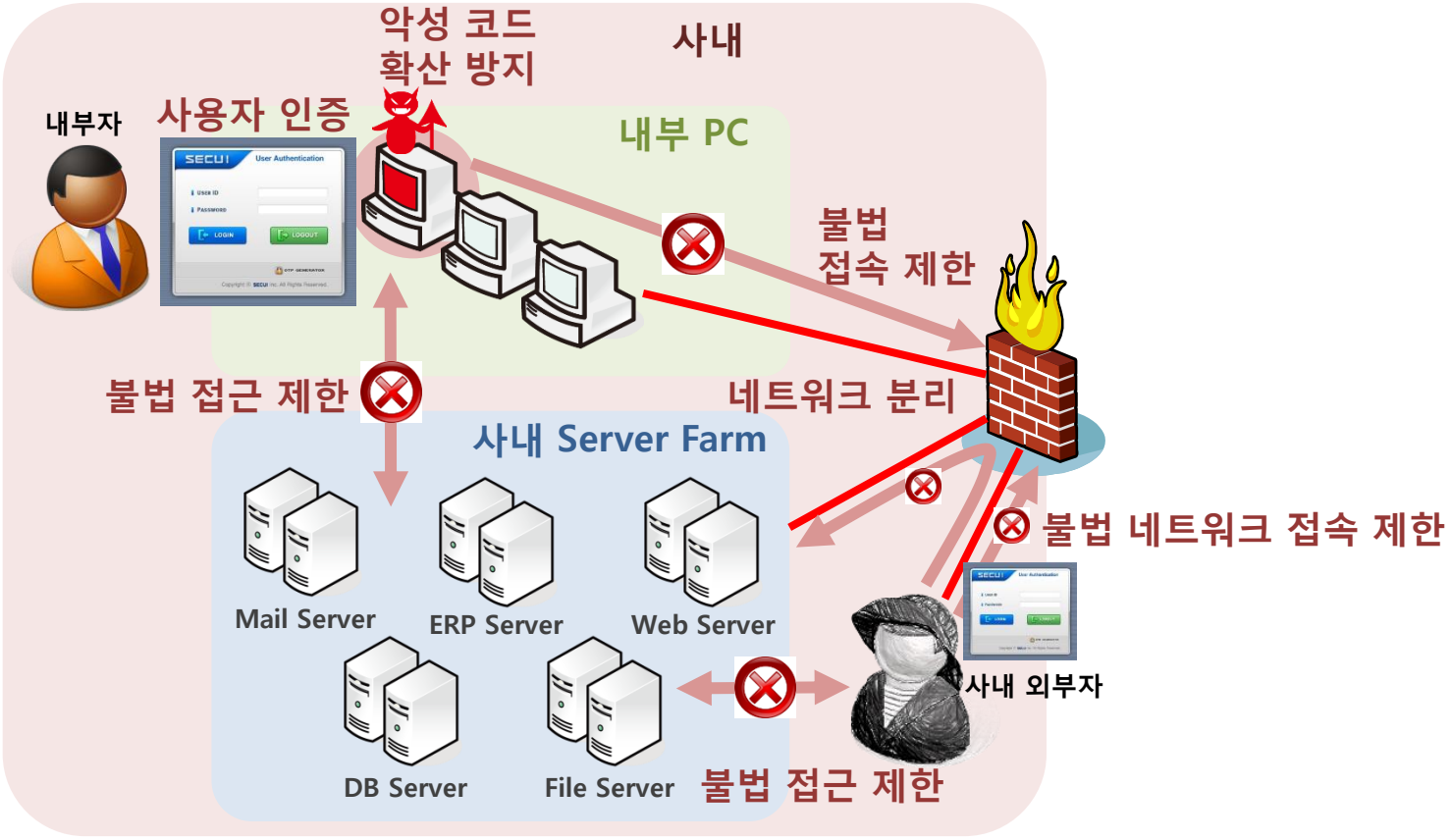
○ 외부 공격 방어
- APT(Advanced Persistent Threat: 지능형 지속 위협) 방어 기능
- 방화벽 및 응용 계층 보안 기능들

내부 네트워크 접근 제어

□ 권한 기반 내부 네트워크 관리

○ 방화벽을 통한 내부 네트워크 분리 및 제한적 접속 허용
- 사용자 인증 기능을 통해 허용된 사용자만 네트워크 접속 허용

○ NAC(Network Access Control)을 통한 네트워크 접속 관리
- 동일 LAN에서 이웃 컴퓨터로의 접근 제한



악성 코드 제어 (1/2)

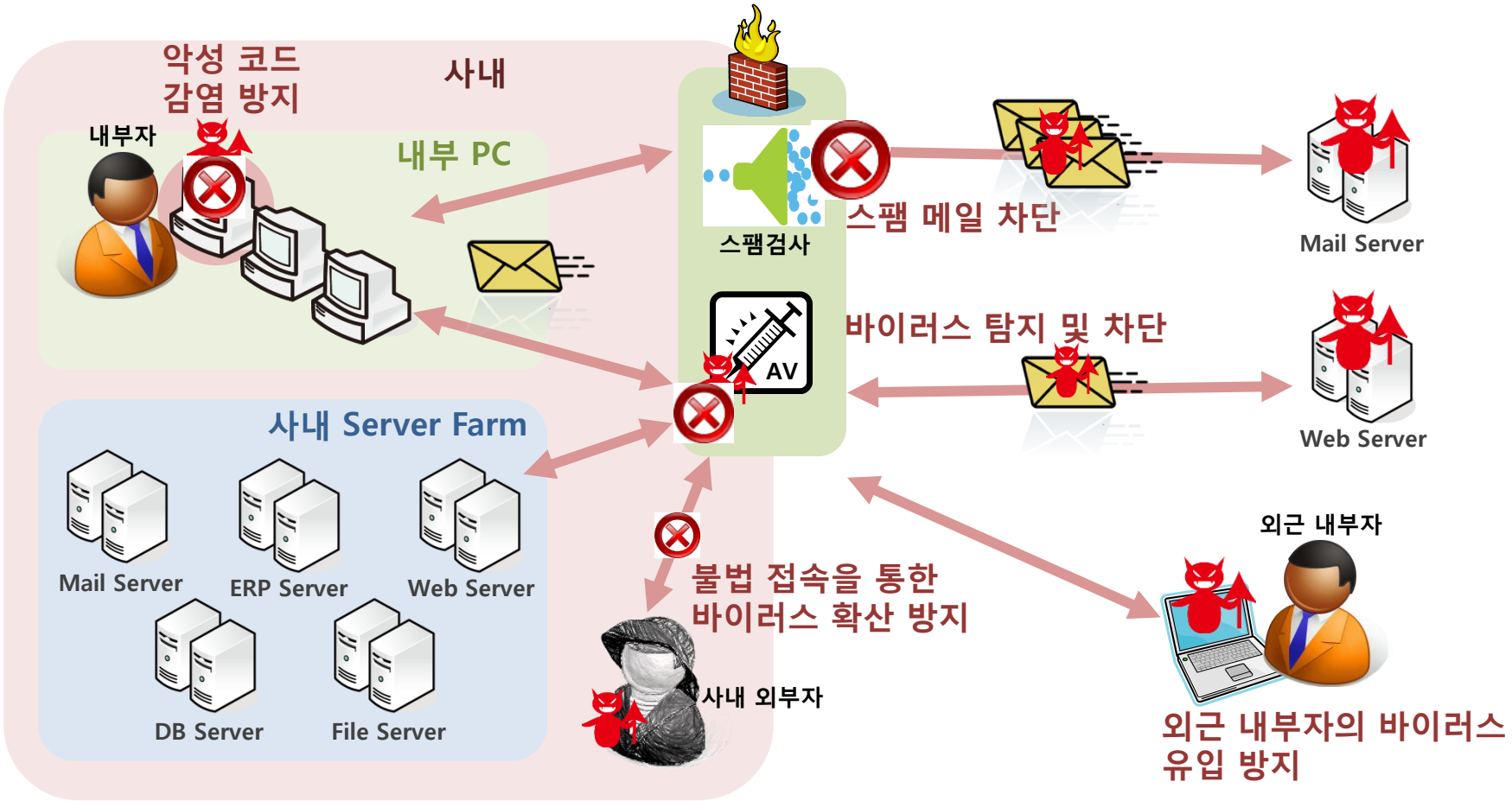
□ 악성 코드 유입 방지

○ 바이러스 검사 (E-mail, Web, FTP 등)

○ 스팸 메일 검사

- 악성 코드의 배포에 사용되는 스팸 메일 차단

□ 구간 별 바이러스 확산 방지

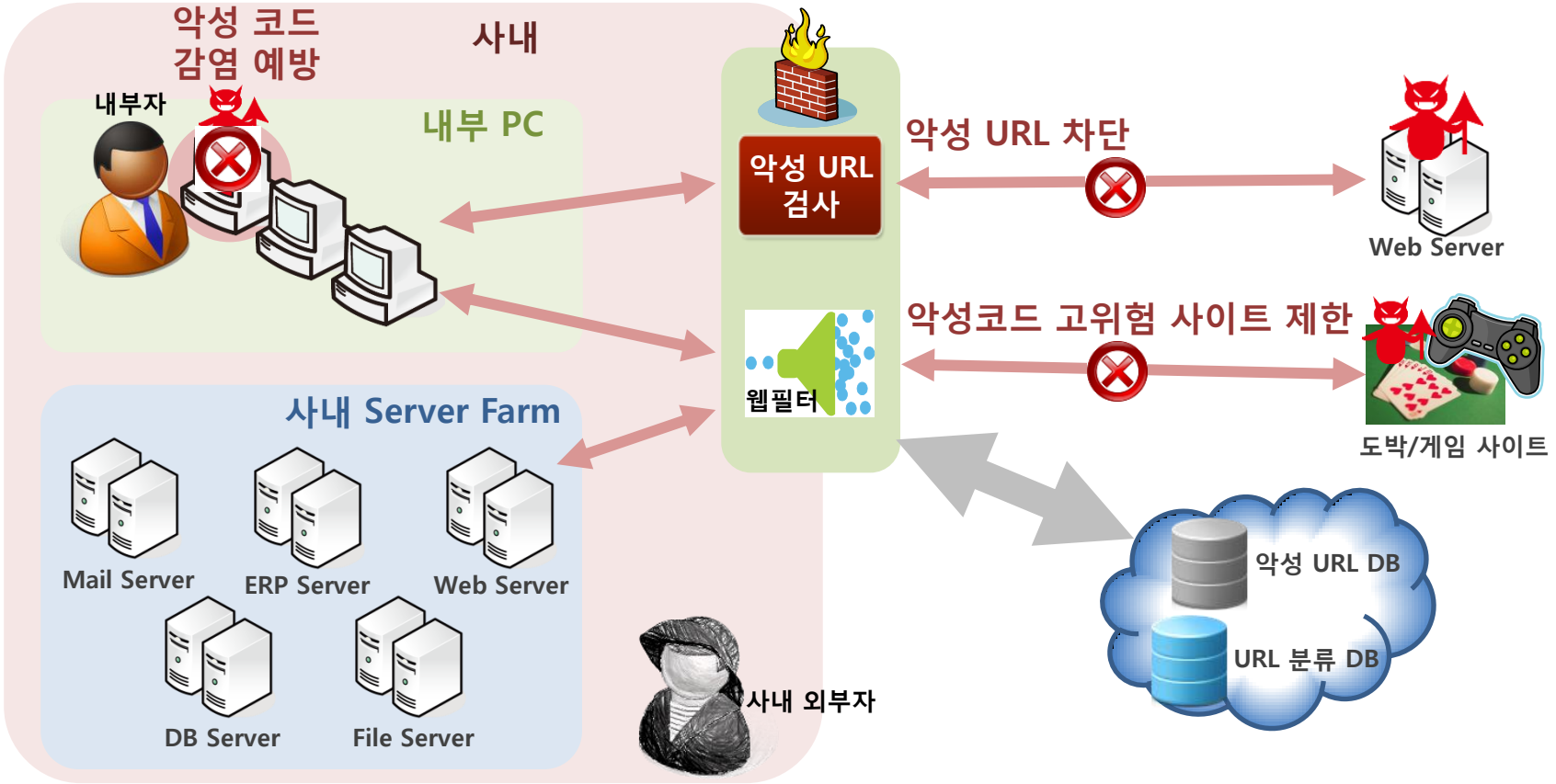


악성 코드 제어 (2/2)

□ 악성 코드 유입 방지

○ 악성 URL 차단 서비스
- 클라우드기반 악성 URL 차단 (사이트 검사 후 DB화)

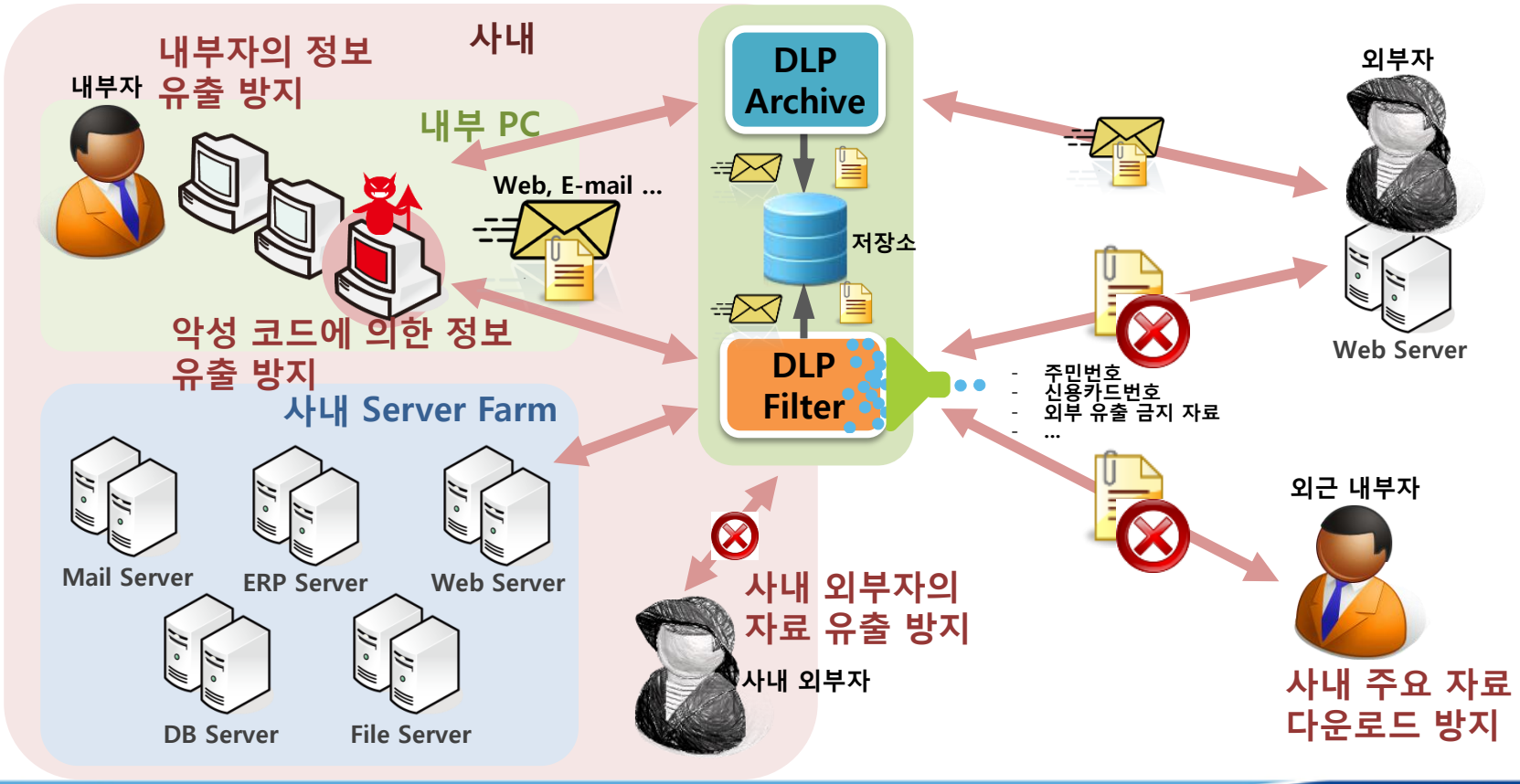
○ 카테고리기반 웹필터 서비스
- 웹 사이트 분류별 접속 제어 기능
- 사내에서 악성코드 고위험 사이트 (도박, 게임 등)의 접속 제어



외부 정보 유출 방지 (1/2)

☐ DLP (Data Loss Prevention)

- ○ 내부 정보 유출 방지 (FTP, E-mail, Web 등)
- ○ Content Filter
  - 문서 및 메일의 특정 내용 및 특정 조건에 해당하는 컨텐츠의 **필터** 기능
- ○ Content Archive
  - 덤프 및 로깅 기능 (특정 프로토콜 컨텐츠의 **저장** 기능)
  - 웹, 메일 본문, 첨부파일 등 (프로토콜 메시지 및 데이터)



외부 정보 유출 방지 (2/2)

□ Application Control

○ 어플리케이션 접근제어를 통한 데이터 유출 방지

- 웹메일, 웹 업로드, 클라우드 서비스, SNS, 노트 기능 등

□ IPS를 통한 관리자 정의 시그니처

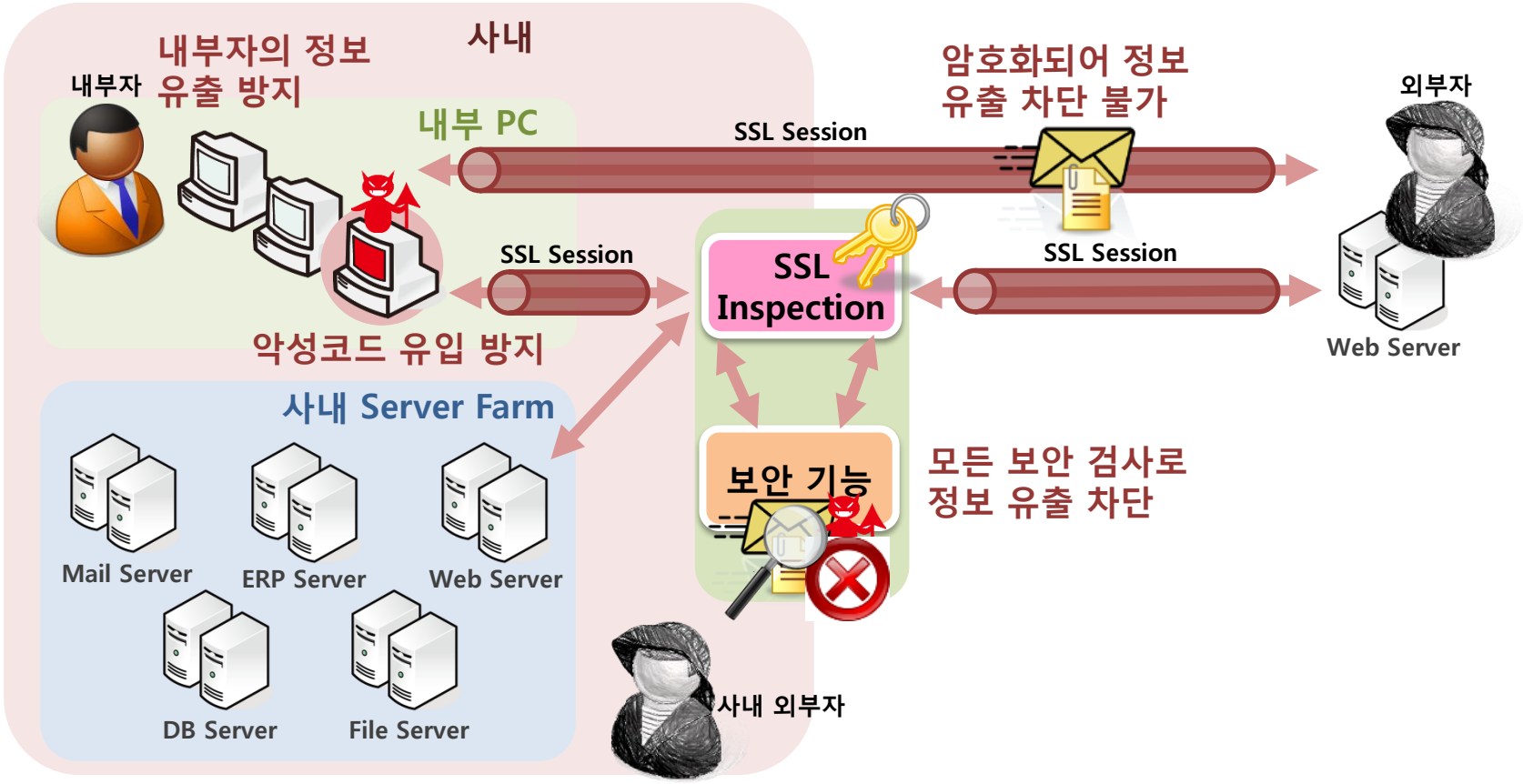
- Packet /Protocol Preprocessing
- 시그니처 기반 탐지
- 행위 기반 탐지
- 애플리케이션 세션 차단

암호화 정보 유출 방지

□ SSL 트래픽 검사

○ 클라이언트-서버간 SSL 암호화 통신의 복호화 및 보안 검사 수행

- 암호화된 자료 유출 방지 및 보안검사와 제어 수행
  - DLP, 악성 코드 검사, 웹필터, IPS, 애플리케이션 제어 등

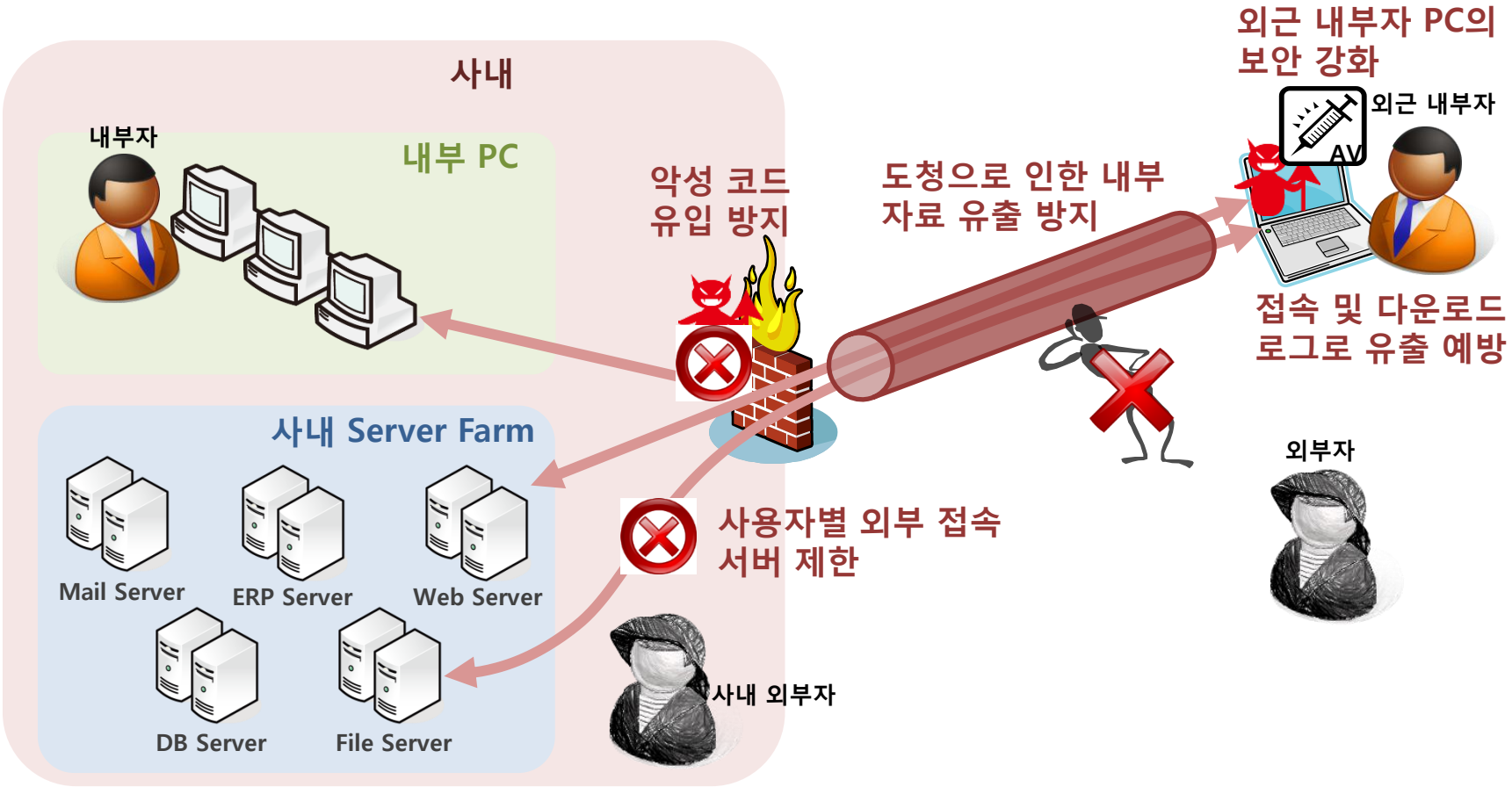


외부 통신 도청 방지

□ 안전한 암호화 터널링

○ IPSec VPN / SSL VPN

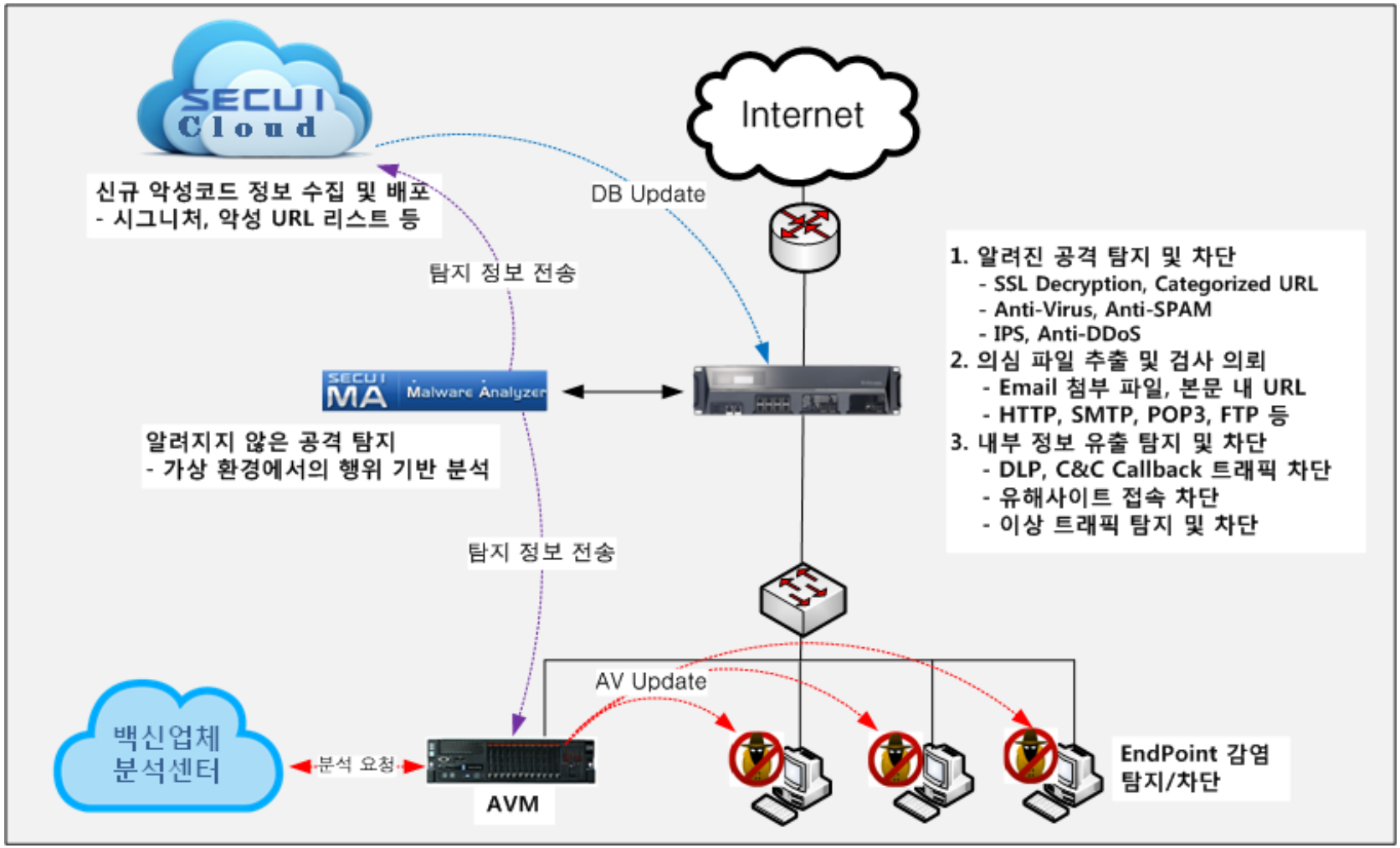
- 강력한 암호화를 통해 외부에서의 도청 방지
- 특정 서버 혹은 특정 기간(출장 기간 혹은 업무 시간)만 외부 접속 허용
- 외근 내부자 PC의 백신, 윈도우 방화벽 강제 사용



외부 공격 방어

□ APT 방어

○ 4단계 방어 체계 구축 (추출 → 분석 → 차단 → 치료)



UTM의 진화

□ UTM(Unified Threat Management) 초기

○ **방화벽 + α (보안 위협 방어)**
- 방화벽(L2~L4) 기능을 기본으로 상위 프로토콜(L5~L7) 보안 기능으로 진화

○ 초기 **대표적인 보안 위협**에 대한 방어 기술 위주로 진화
- 패킷 도청 방어 (IPSec VPN, SSL VPN)
- 침입해킹 탐지를 위한 IDS의 통합 및 차단 (IPS)
- 네트워크단에서 바이러스 탐지 및 차단 (Anti-virus)

□ UTM 현재

○ **보안 + α (관리 기술)**

○ 보안 사고를 사전에 방지하기 위한 여러 **보안 관리 기술** 위주로 진화
- 인터넷 서비스의 다양화에 따라 **서비스 제어 기술**이 대폭 강화

○ **Service-aware 분석 기술**을 통한 세밀한 보안 관리 기능으로 진화
- 웹 서비스 제어 (URL Filter)
- 다양한 사용자 프로그램 혹은 서비스 제어 (Application Control)
- 사용자 접속 제어 및 사용자 인증 (NAC, User Control & Auth.)
- 데이터 유출 방지 (DLP)
- SSL 트래픽 검사

○ **진화된 공격 방어** 기술로 진화
- 웹서버에 대한 공격 방어 (Web Application Firewall)
- 분산 서비스 거부 공격 방어 (DDoS)
- APT (지능형 지속 위협) 방어

Beyond Korea
Go Global

NJOYABLE Culture
INNOVATE Process
CREATIVE Thinking
ENERGETIC Behavior