11.2 침입차단시스템 특성

침입차단시스템의 설계목표

- 안에서 밖으로 나가는 모든 트래픽과 밖에서 안으로 들어오는 트래픽 모두는 반드시 침입차단시스템을 통과
  - 침입차단시스템을 통하지 않고 내부 네트워크에 접근하는 것을 물리적으로 차단
- 지역 보안정책에 의해 정의된 트래픽 같은 허가된 트래픽만 통과
  - 다양한 유형의 보안 정책
- 침입차단시스템 자체는 침투에 면역성을 가지고 있어야 함
  - 안전한 운영체제를 갖춘 신뢰시스템 사용

접근제어와 사이트 보안정책 수행 4가지 일반적인 기술 (1)

- 서비스 제어(Service control):
  - 안에서 밖으로, 혹은 밖에서 안으로 접근할 수 있는 인터넷 서비스 유형 결정
  - TCP(UDP) 포트 번호를 근거로 필터링
  - 프록시 소프트웨어를 이용하여 각 서비스 요청을 전달하기에 앞서 수신하고 해석
  - 자체적으로 웹서비스나 메일서비스와 같은 서비스 운영
- 목적지 제어(Direction control):
  - 특정 서비스 요청을 시작하거나, 침입차단시스템 통과를 허용할 때 목적지를 결정

접근제어와 사이트 보안정책 수행 4가지 일반적인 기술 (2)

- 사용자 제어(User control):
  - 어느 사용자가 접근을 시도하는지에 따라 서비스 접근을 제어
  - 일반적으로 경계 안의 사용자에게 국한
  - 외부사용자가 보내서 안으로 들어오는 트래픽에도 적용 가능
- 행동 제어(Behavior control):
  - 특정 서비스를 어떻게 사용할 지 제어
  - 예: 스팸을 제거하기 위해 전자메일을 필터링
  - 예: 외부에서 시도하는 접근에 대해 내부 웹 서버의 일부 정보만 접근하도록 제한

침입차단시스템 역할 범위

- 단 하나의 길목을 두어 불법사용자가 보호 네트워크에 들어오는 것을 막고, 취약한 서비스가 네트워크에서 나가고 들어오는 것을 금지하고, 다양한 종류의 IP 스푸핑과 라우팅 공격으로부터 보호
  - 단일 시스템이나 시스템의 한 단위에서 보안 기능을 독립적으로 운영
  - 하나의 길목만을 지킴으로 보안 관리 단순화
- 보안관련 사건의 위치 추적과 감사와 경고를 구현
- 보호 범위 밖의 서비스
  - 안전하지 않은 무선 LAN
  - 내부 침입차단시스템으로 통제되지 않는 로컬 시스템 사이의 무선 통신
- 휴대장치 사용
  - 랩톱, PDA 또는 휴대용 저장장치는 외부 감염 가능
  - 내부에서 사용시 문제점 발생