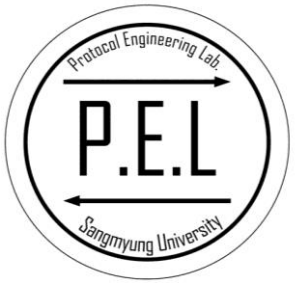


네트워크 보안 에센셜
(11장 침입차단시스템)

Sa-rang Wi (sarang@pel.smuc.ac.kr)
Protocol **E**ngineering **L**ab., **Sangmyung** University

Content

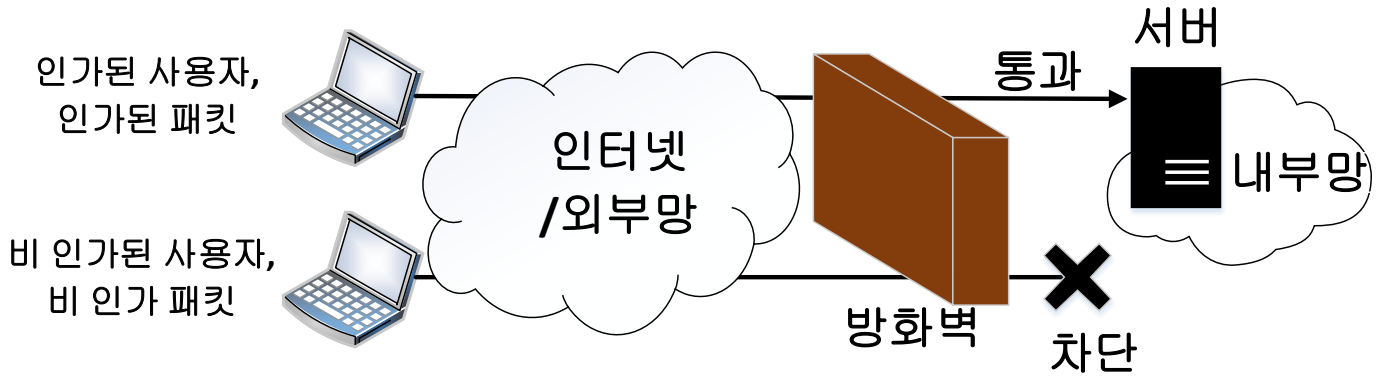
- 침입 차단 시스템
- 침입 차단 시스템의 특성
- 침입 차단 시스템의 유형

침입 차단 시스템

- **침입차단시스템(firewall)의 필요성**
  - 네트워크를 위협하는 공격 유형
    - ✓ 서비스 거부 공격(Dos: Denial of Service)
    - ✓ 패킷 가로채기(Packet sniffing)
    - ✓ 송신측 주소 위조(IP spoofing)
    - ✓ 패킷 내용 변조(modification)
  - 네트워크 위협요소가 증가함에 따라 네트워크에 대한 효율적이고 안전한 보안 정책 수립 및 시스템 도입이 요구

침입 차단 시스템

- **침입차단시스템 (firewall) 의 정의**
  - 외부의 불법 사용자들의 침입으로부터 내부를 보호하기 위한 정책 및 이를 지원하는 하드웨어와 소프트웨어를 총칭
  - 방화벽이라고도 함.
  - 내부의 신뢰성 있는 네트워크와 외부의 신뢰성 없는 네트워크 사이에 위치



침입 차단 시스템의 특성

- **침입차단시스템(firewall)의 설계 목표**
  1. 안에서 밖으로 나가는 모든 트래픽과 밖에서 안으로 들어오는 트래픽 모두 침입차단 시스템을 통과해야 함
     - ✓ 침입차단시스템을 통하지 않고 지역네트워크로 접근하는 것을 물리적으로 차단
  2. 허가된 트래픽만 통과
  3. 안전한 운영체제를 갖는 신뢰 시스템을 사용해야 함

- 인바인드 패킷/ 아웃바인드 패킷
  - 방화벽 입장에서 인바인드는 외부 네트워크에서 들어오는 패킷이고 아웃바인드는 밖으로 내보내는 패킷

침입 차단 시스템의 특성

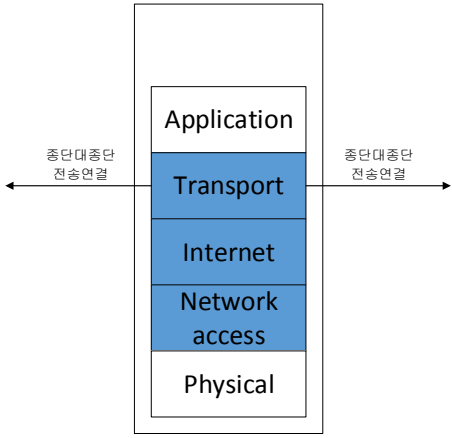
- **침입 차단 시스템의 주요 기능**
  - 접근 통제 기능
    - ✓ 호스트, 사용자 , 서비스의 속성을 기초로 내부 네트워크에 대한 접근 통제
    - ✓ 패킷 필터링 규칙 이용
  - 식별 및 인증 기능
    - ✓ 내부 네트워크로 접근하려는 사용자 또는 컴퓨터의 신원을 식별하고 인증(ex)패스워드)
  - 보안관련 사건의 위치 추적 기능
    - ✓ 모든 트래픽은 침입차단시스템을 통과하므로 모든 접속 정보에 대한 기록 유지
    - ✓ 이러한 기록인 로그 정보를 이용해 접근 통계, 취약성점검, 추적기능 제공
  - 암호화 기능
    - ✓ 기밀성, 무결성기능 제공
  - 주소변환(NAT)
    - ✓ IP 주소 변환 기능

침입 차단 시스템의 유형

- **침입 차단 시스템의 유형(침입차단의 대상 네트워크 계층에 따라)**
  - 패킷-필터링 방화벽(Packet filtering firewall)
  - 상태기반 패킷 검사 방화벽(Stateful Packet inspection firewall)
  - 응용 프로그램 수준의 방화벽
    - ✓ 프록시 서버(proxy server)
    - ✓ 회선-레벨 게이트웨이(circuit-level gateway)

침입 차단 시스템의 유형

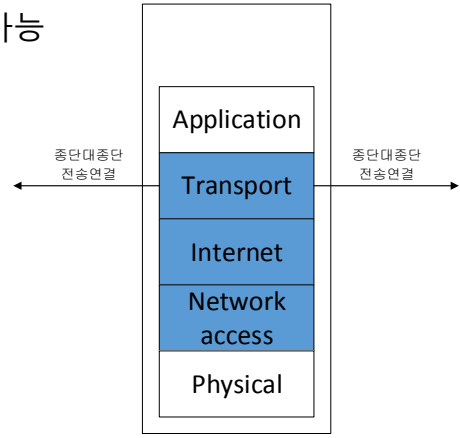
- **패킷-필터링 방화벽(packet filtering firewall)**
  - IP주소와 Port 번호를 이용해 패킷을 허용하거나 Drop하는 방식
  - OSI 7계층 중에서 네트워크계층과 전송 계층에서 동작
    - ✓ 출발지 IP, 목적지 IP
    - ✓ 출발지 Port, 목적지 Port
  - 필터링 순서:
    - ✓ 보안정책설정 > 패킷분석 > 패킷을 보안 정책 순서대로 적용 > 보안 정책에 따라 허용 또는 거부 > 보안정책이 정의되지 않으면 2가지 디폴트 동작 (모두 부인 or 모두 승인) 중 1개 수행



(a) 패킷 필터링 침입 차단 시스템

침입 차단 시스템의 유형

- **패킷-필터링 방화벽(packet filtering firewall)**
  - 장점
    - ✓ OSI 7 모델에서 네트워크 계층과 전송 계층에서 처리되기 때문에 다른 방식에 비해 처리속도가 빠름
    - ✓ 사용자가 쉽게 사용할 수 있음
  - 단점
    - ✓ 경계선 방어 지원 불가
    - ✓ 가변적인 포트를 사용하는 서비스나 다중 포트를 가진 서비스를 처리하기 어려움
    - ✓ 들어오는 패킷 ,나가는 패킷에 대한 규칙을 다 정해야 함
    - ✓ 상위계층을 검사하지 않기 때문에 특정 응용 프로그램을 이용한 공격 방어 불가능
    - ✓ 보안 정책에서의 접속제어 규칙의 개수 및 순서에 따라 부하 가중

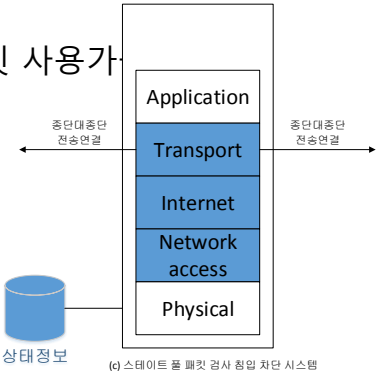


(a) 패킷 필터링 침입 차단 시스템

침입 차단 시스템의 유형

- **상태기반 패킷검사 방화벽(Stateful Packet inspection firewall)**
  - 패킷 필터링 방식과 같이 네트워크 계층에서 패킷 필터링 및 TCP 연결에 관한 정보를 기록하는 시스템

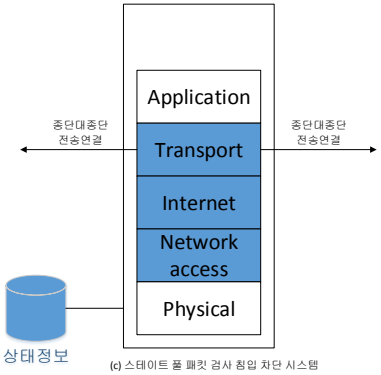
  - 특징
    - ✓ 모든 통신 채널을 추적하는 상태 정보 존재
      - 출발지IP, 목적지IP, 포트번호 등등
      - 추적된 정보들로 인해 다음에 받아야 할 패킷이 무엇인지 알 수 있음
      - 룰셋을 만들 수 있음.
    - ✓ 각 연결의 상태를 감시하기 위해 TCP 헤더에 포함된 특정 값을 검사
      - TCP 트래픽 : 연결 성립, 사용 중, 연결 종료
      - 연결의 상태를 이용해 필터링 하기 때문에 가변적인 포트번호를 사용하는 패킷 사용가



(c) 스테이트 풀 패킷 검사 침입 차단 시스템

침입 차단 시스템의 유형

- **상태기반 패킷검사 방화벽(Stateful Packet inspection firewall)**
  - 장점
    - ✓ 모든 통신 채널에 대해 추적 가능
    - ✓ 한 차원 높은 패킷 필터링 기능 제공
    - ✓ 응용 프로그램 방화벽과 같은 성능감소 발생하지 않음
    - ✓ UDP와같은 비 연결형 패킷도 추적 가능
  - 단점
    - ✓ 상태정보에 DOS 공격으로 인해 거짓 정보가 가득찰 때 장비가 일시적으로 정지되거나 재가동 해야 함
    - ✓ 재 가동 시 상태정보 db가 리셋됨



(c) 스테이트 풀 패킷 검사 침입 차단 시스템

침입 차단 시스템의 유형

- **응용 프로그램 수준의 방화벽(Application Level Firewall)**
  - 패킷을 응용계층(URL,MIME)까지 검사해서 패킷을 허용하거나 Drop하는 방식
  - 응용 서비스(ex) 카톡, MSDN)마다 지원할 수 있는 여부가 다름

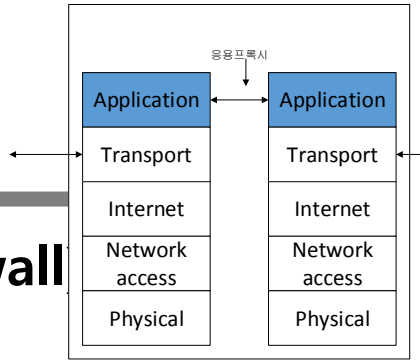
  - 특징
    - ✓ OSI Model 의 7계층까지 작동
    - ✓ 각 서비스 별로 프록시 데몬(백그라운드 프로세스) 이 존재해서 일명 응용프로그램 게이트웨이라고도 함
    - ✓ 사용자 인증 및 파일 전송 시 바이러스검색과 같은 부가 서비스 지원

  - 종류
    - ✓ 프록시 서버 방화벽
    - ✓ 회로레벨 프록시 방화벽

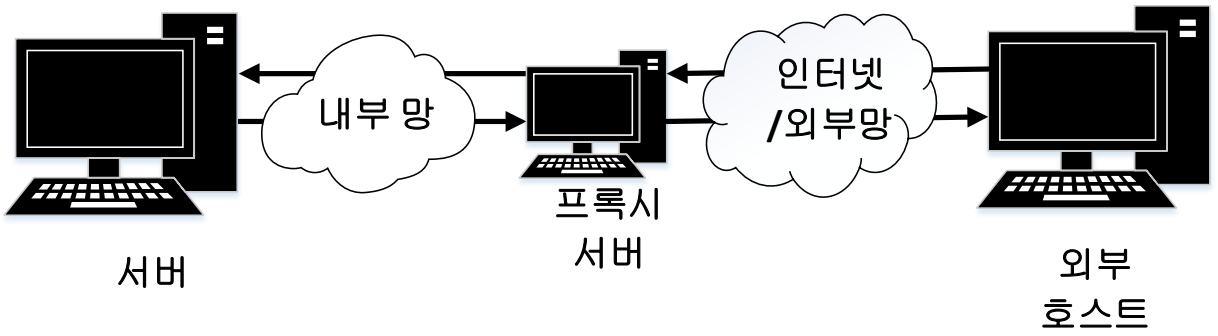
침입 차단 시스템의 유형

- **응용 프로그램 수준의 방화벽(Application Level Firewall)**
  - 장점
    - ✓ 패킷 필터링보다 나은 보안 제공
    - ✓ 외부에 대한 내부망의 완벽한 경계선 방어 및 내부 IP 주소 숨김
    - ✓ 강력한 로깅 및 감사기능 제공
    - ✓ 강력한 인증기능 제공(ex)일회용 패스워드)
  - 단점
    - ✓ 패킷 필터링보다 속도가 느림
    - ✓ 상위 레벨에서 동작하기 때문에 많은 부하를 유발할 수 있음

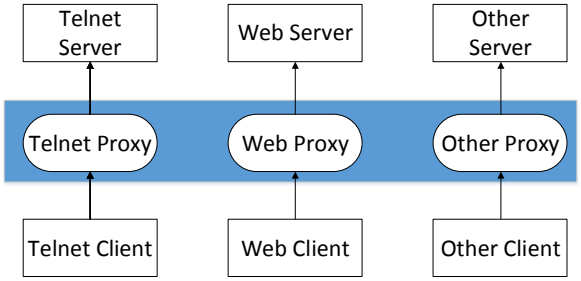
침입 차단 시스템의 유형



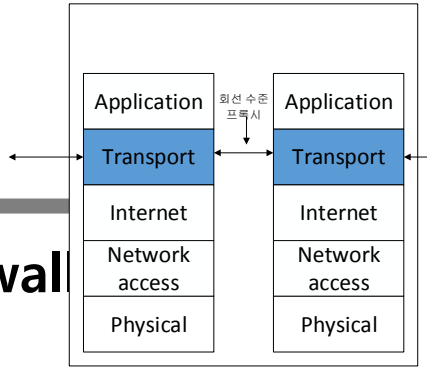
- **응용 프로그램 수준의 방화벽(Application Level Firewall**
  - 프록시 서버 방화벽
    - ✓ 네트워크에 진입 혹은 나가는 패킷을 응용 프로그램 수준까지 검토해 악의적인 정보가 있는 지 검토 및 목적지시스템까지 전달



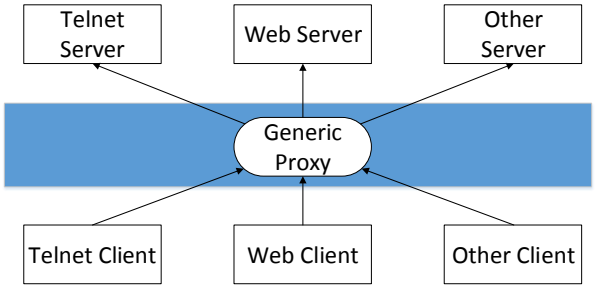
  - 프록시 서버 방화벽의 기타 기능-캐시
    - ✓ 사용자가 한번 방문한 사이트 정보를 미리 저장해 원하는 사용자에게 제공
    - ✓ 방화벽 구성 시 속도나 성능 저하 막기 위한 기능



침입 차단 시스템의 유형



- **응용 프로그램 수준의 방화벽(Application Level Firewall**
  - 회로레벨 프록시 방화벽
    - ✓ OSI 모델의 세션층에서 작동하는 방화벽
    - ✓ 요청된 세션이 합법적인지 판단하기 위해 TCP 핸드쉐이크를 모니터링 함
    - ✓ 전송레벨로 제어하는 부분에 있어서 패킷 필터링과 유사
  - 특징
    - ✓ SOCKS(Socket Secure) 프로토콜 사용
      - 프록시를 통한 전송계층 보안 연결이 가능하도록 안전한 프록시 데이터 채널을 형성하는 기능을 일반화한 프로토콜
    - ✓ 프록시 서버가 1개만 사용
      - 프록시 서버에 맞게 클라이언트 프로그램 수정해야 함



침입 차단 시스템의 유형

- **생각해볼 만한 문제**
  - zmap, 쇼단과 같은 스캐너들은 모든 IP주소를 10분 안에 스캔 할 수 있다.
  - 이러한 스캐너들은 공격자들이 공격을 하기 위한 기초 작업으로 활용 가능하다.
  - 스캐너들에 대해 자유로워질 수는 없을까?
    - ✓ 공개 접근 서버 및 장비들의 제한
      - 일단 인터넷에 연결하지 않으면 되지만 그런 경우는 드물기 때문에 내부 네트워크와 외부 네트워크 사이에 외부 네트워크로부터 접근 할 수 없는 방화벽을 세워야 함.
      - 방화벽 내의 IP 필터를 사용해 접근을 제한하고, VPN을 사용하는 것이 좋다.

감사합니다~