TCP/IP 교과서

11장 TCP/IP 보안

11.1 | 방화벽은 무엇인가

~~11.2 | 공격 기술~~

~~11.3 | 침입자들이 원하는 것은 무엇일까~~

~~11.4 | 요약~~

~~11.5 | Q&A~~

~~11.6 | 워크숍~~

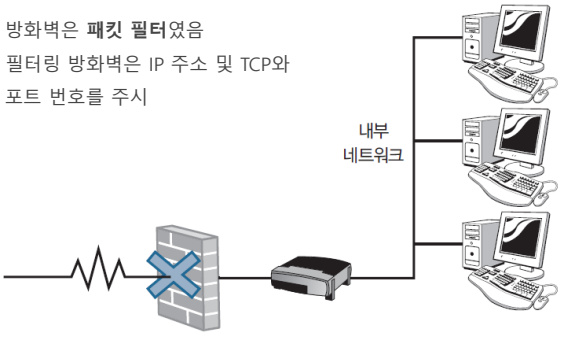
~~11.7 | 핵심 용어~~

11.1 방화벽은 무엇인가

TCP/IP 교과서

- 방화벽은 네트워크 통로에 위치한 장치로 네트워크의 인바운드(inbound) 패킷 헤더를 검사, 수락 또는 거부
- 실제로 방화벽이 라우터는 아니지만, 방화벽 기능이 종종 라우터에 내장되어 있음
- 전달 결정은 온전히 주소 지정에 기반하는 것이 아니라 네트워크에서 허용되는 트래픽 유형에 대해서 네트워크 소유자가 구성한 규칙을 기반으로 함

- 초기 방화벽은 **패킷 필터**였음
- 패킷 필터링 방화벽은 IP 주소 및 TCP와 UDP 포트 번호를 주시



11.1 방화벽은 무엇인가

TCP/IP 교과서

» 룰 셋(Rule Set)

번호	외부(From)		내부(To)		동작
	IP 주소	포트	IP 주소	포트	
1	Any	Any	147.168.100.100	80	Allow
2	Any	Any	Any	Any	Deny

- 첫 번째 룰 셋 : 외부(External)에서 접근하는 모든 시스템에 내부의 147.168.100.100 시스템의 80번 포트에 대한 접근을 허용(Allow)
- 두 번째 룰셋 : '명백히 허용하지 않은 서비스에 대한 거부'를 적용하기 위한 것으로, 룰 셋을 통해 명시적으로 허용하지 않으면 모두 차단

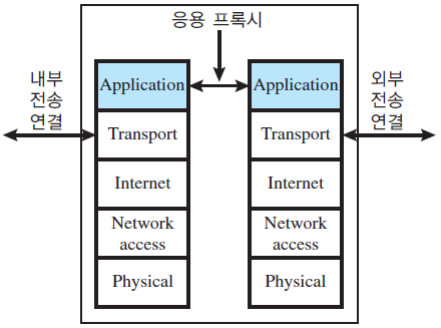
❖ 패킷 필터 방화벽의 한계

- 바이러스는 파일 등을 통해 감염되므로 근본적으로 방화벽이 영향을 미치기 어려움
- 일부 웜은 막을 수 있지만 정상적인 서비스 포트에 대해 웜이 공격을 시도할 때는 막을 수 없음

11.1 방화벽은 무엇인가

TCP/IP 교과서

» 응용 레벨 게이트웨이(Proxy server)



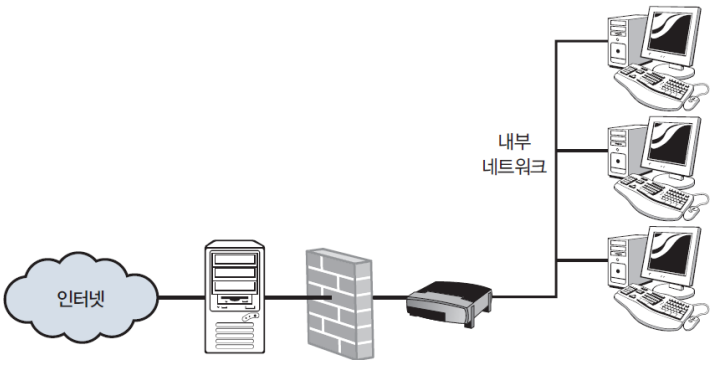
- **응용-레벨 트래픽의 중개자 역할 수행**
- **패킷 필터보다 더 안전**
- **응용 레벨에서 들어오는 모든 트래픽을 로깅하고 감사하는 것이 용이함**
- **응용 별로 프록시 서버를 구축해야 함**
- **내부와 외부 2개의 연결이 연결이 요구되며 그에 따른 처리량 증가**
- **응용별 프록시 서버 기능을 제공하여 패킷 필터링 방식과는 달리 외부와 내부 네트워크 간의 직접적인 패킷 교환을 허용하지 않는다.**

11.1 방화벽은 무엇인가

TCP/IP 교과서

» DMZ

- 많은 기관이 FTP 서버, 이메일 서버 및 인터넷으로부터 접근할 수 있는 다른 시스템을 유지하고 있음



11.1 방화벽은 무엇인가

TCP/IP 교과서

» DMZ

- 방화벽 간의 공간
- 방화벽 뒤에 로컬 자원을 배치하고, 방화벽 앞에 인터넷에 접근이 가능한 자원을 배치하는 기술은 일반적으로 소규모 네트워크에서 사용
- DMZ는 공개 인터넷보다 안전하지만 내부 네트워크보다는 안전하지 않은 중간 수준의 보안을 유지