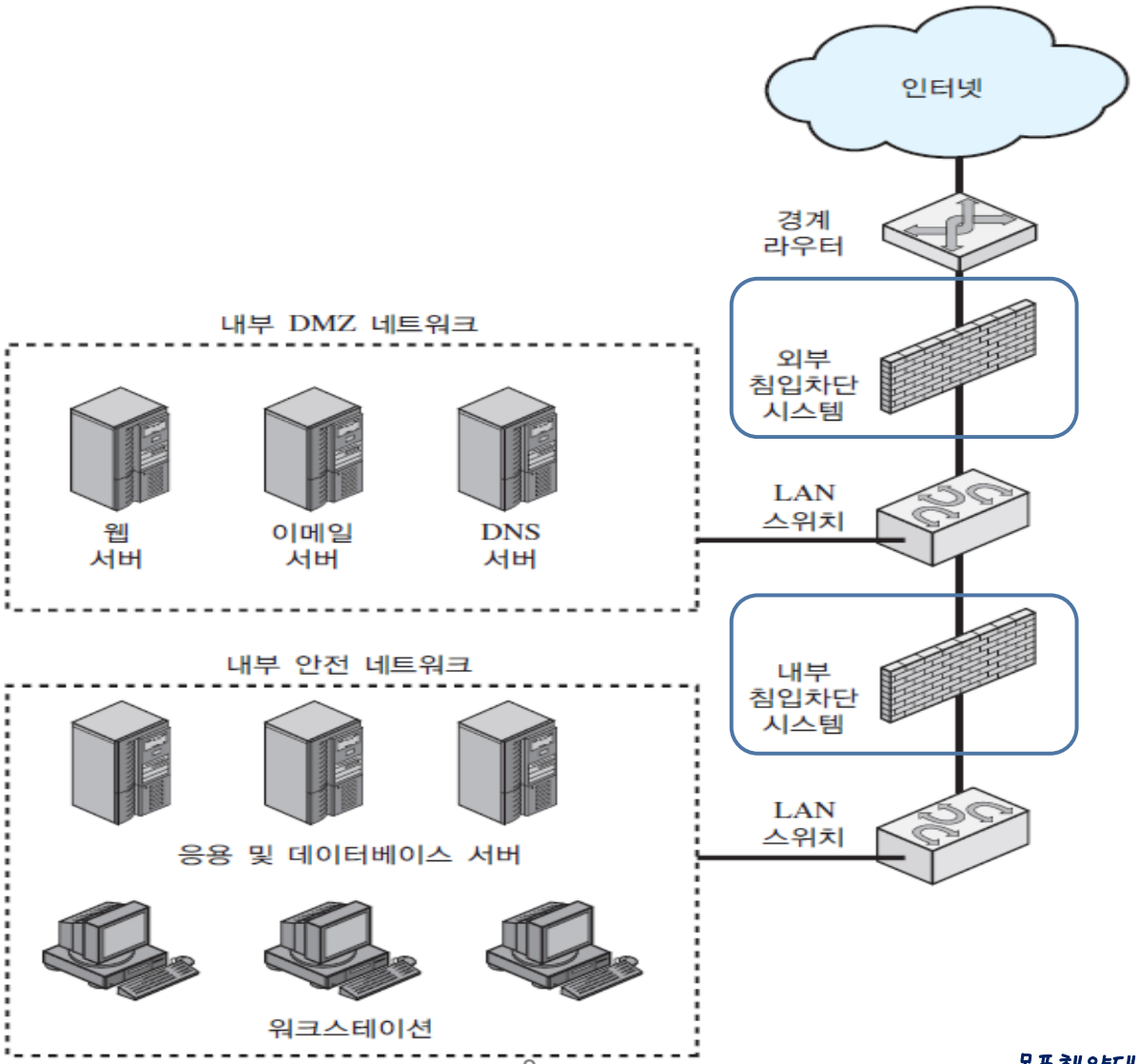
11.5 침입차단시스템 위치와 구성

개요

- 침입차단시스템은 보통 신뢰받지 못하는 트래픽 출처인 외부 네트워크와 내부 네트워크 사이에 위치해서 보호된 방어막을 제공
- 이러한 일반적 원칙을 가지고, 보안 관리자는 필요한 침입차단시스템의 개수와 설치할 장소를 결정해야 함

침입차단시스템 구성 예 (1)



침입차단시스템 구성 예 (2)

- 외부 침입차단시스템
- DMZ(demilitarized zone) 네트워크
  - 내부 침입차단시스템과 외부 침입차단시스템 사이에 위치
  - DMZ 영역 안에 한 개 이상의 네트워크된 장치들이 존재
  - 외부에서 접속할 수 있어야 하며 보호되어야 할 시스템은 주로 DMZ 네트워크에 배치
  - 보통 DMZ 안에 있는 시스템은 회사의 웹사이트, 이메일 서버 또는 DNS 서버와 같이 반드시 외부로 연결할 수 있어야 함

침입차단시스템 구성 예 (3)

- 내부 침입차단시스템
  - 내부 침입차단시스템은 외부 침입차단시스템보다 더 엄격한 필터링 능력 보유
    - 기업 내부 서버와 워크스테이션 보호
  - 내부 침입차단시스템은 DMZ 관점에서 보면 양방향 보호
    - DMZ에서 시작된 공격 보호
    - 내부 보호된 네트워크에서 시작된 공격 보호
  - 다수의 내부 침입차단시스템을 사용해서 내부 네트워크의 일부를 서버로부터 보호

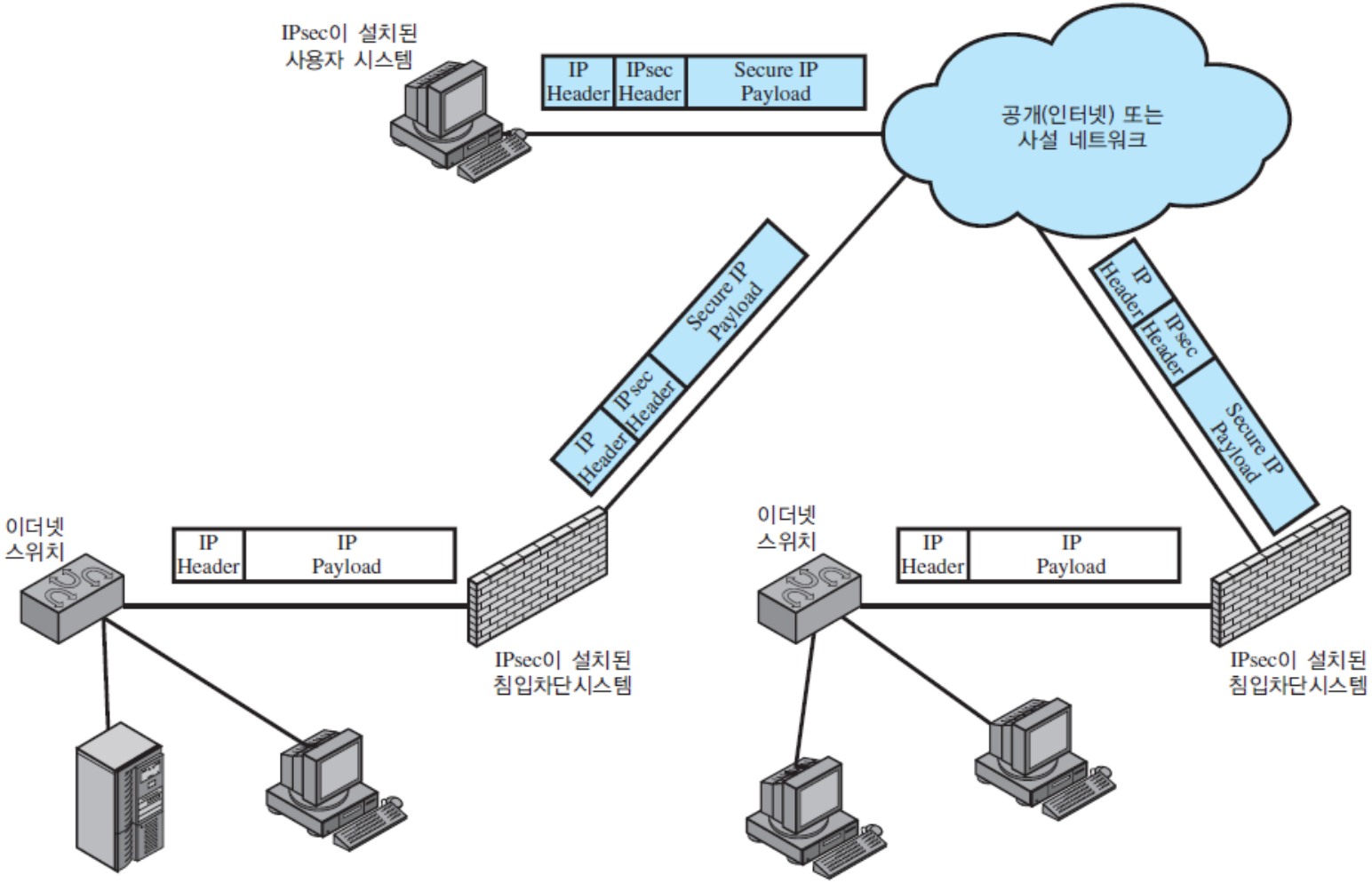
VPN (1)

- VPN: virtual private network
  - 상대적으로 안전하지 않은 네트워크를 이용해서 상호 연결
  - 보안을 제공하기 위한, 암호와 특별한 프로토콜을 사용하는 컴퓨터로 구성
- 기업망 구성
  - 워크스테이션, 서버와 데이터베이스가 하나 이상의 LAN으로 연결된 형태
  - 비용 절감과 WAN 관리업무 위임을 위해 공공망을 통한 사이트 연결 가능
  - 재택근무자의 경우 공공망을 통한 회사 시스템 접속
  - 기타 모바일 사용자의 회사 시스템 접속
  - 이때 보안 문제 해결 필요

VPN (2)

- 공공망 사용에 따른 보안 문제
  - 도청 문제
  - 허가 받지 않은 사용자의 접근
- VPN 필요성
  - 안전하지 않은 네트워크인 인터넷을 통한 안전한 연결을 위해 하위 프로토콜 계층에서 암호와 인증을 사용
  - 전용선을 사용하지만 양단에서 동일한 암호화 인증 시스템에 의존하는 사설 네트워크보다는 일반적으로 저렴
- 암호화는 침입차단시스템 소프트웨어나 라우터에 의해 수행
- 가장 보편적인 프로토콜 메커니즘은 IP 레벨에서 수행되는 IPsec

VPN (3)


IPsec이 설치된
사용자 시스템
IP Header
IPsec Header
Secure IP Payload
공개(인터넷) 또는
사설 네트워크
IP Header
IPsec Header
Secure IP Payload
IP Header
IPsec Header
Secure IP Payload
이더넷
스위치
IP Header
IP Payload
IPsec이 설치된
침입차단시스템
이더넷
스위치
IP Header
IP Payload
IPsec이 설치된
침입차단시스템

VPN (4)

- 침입차단시스템 내부에 있는 별개의 박스에서 구현하는 경우
  - 이미 암호화가 되어 침입차단시스템을 통과
  - 접근통제, 로깅, 바이러스 스캐닝과 같은 기능 수행 불가
- 침입차단시스템 외부에 있는 경계 라우터에서 구현하는 경우
  - 덜 바람직

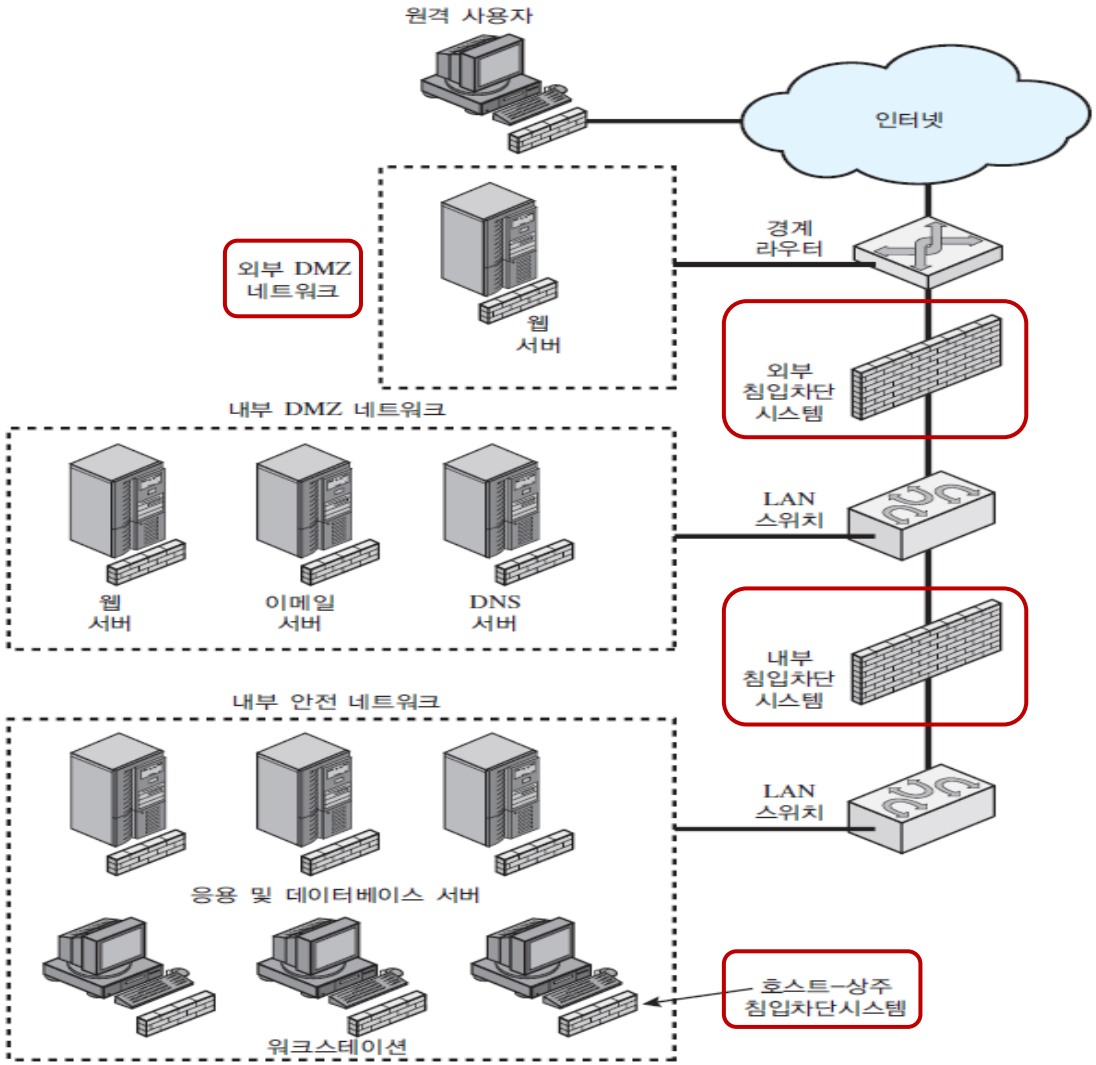
분산 침입차단시스템 (1)

- 분산 침입차단시스템(distributed firewalls) 구성
  - 독립된 침입차단시스템 장치
  - 중앙관리통제하에 함께 동작하는 호스트-기반 침입차단시스템
- 관리자
  - 수 백 개의 서버와 워크스테이션상의 호스트-상주 침입차단시스템을 구성
  - 로컬과 원격 사용자 시스템상의 개인 침입차단시스템 구성 가능
- 네트워크 관리자
  - 전체 네트워크 전반에 걸쳐 정책을 세팅
  - 보안을 모니터링

분산 침입차단시스템 (2)

- 인터넷 공격을 막고, 특정 컴퓨터와 응용 프로그램에 맞춘 보호 방법 제공
- 독립된 침입차단시스템은 내부 침입차단시스템과 외부 침입차단시스템을 포함한 전체를 보호

분산 침입차단시스템 구성 예



침입차단시스템 위치와 토폴로지 요약 (1)

- 호스트-상주 침입차단시스템(Host-resident firewall):
  - 개인 침입차단시스템 소프트웨어와 서버의 침입차단시스템 소프트웨어
  - 단독으로 사용하거나, 분산침입차단시스템의 일부로 사용
- 스크리닝 라우터(Screening router):
  - 내부와 외부 네트워크 사이의 라우터에서 패킷 필터링 수행
  - 소규모 사무실/가정 사무실(SOHO) 응용에 적합
- 단일 배스천 인라인(Single bastion inline):
  - 내부와 외부 네트워크 사이의 단일 침입차단시스템 장치
  - 스테이트풀 필터와 응용 프로그램 프록시 구현 가능
  - 소규모에 중급 규모 조직에 적합

침입차단시스템 위치와 토폴로지 요약 (2)

- 단일 배스천 T(Single bastion T):
  - 단일 배스천 인라인과 유사하나 외부에서 보이는 서버가 위치한 DMZ에 있는 배스천 안에 제3의 인터페이스를 가지고 있음
  - 중급 규모에서 대규모 조직에 적합
- 이중 배스천 인라인(Double bastion inline):
  - DMZ가 두개의 침입차단시스템 사이에 존재
  - 대규모 기업과 정부 조직에 적합
- 이중 배스천 T(Double bastion T):
  - DMZ가 배스천침입차단시스템 상의 독립된 네트워크 인터페이스 상에 있음
  - 대규모 기업과 정부 조직에 보편적
- 분산 침입차단시스템 구성(Distributed firewall configuration):
  - 대규모 기업과 정부 조직에 적합

과제

- 11.1, 11.2, 11.3, 11.4
- 11.8, 11.11