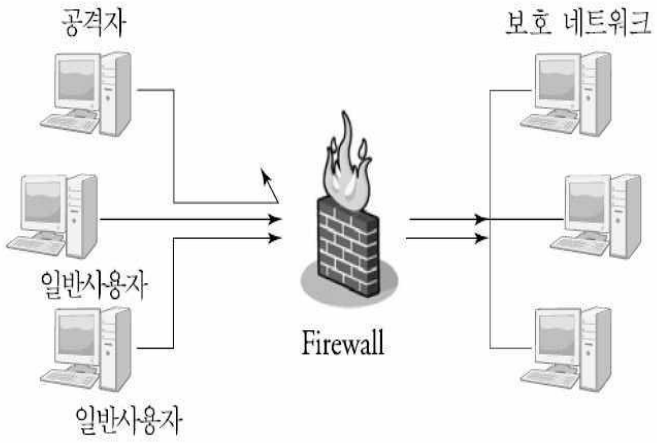
정보보호

07 정보보호시스템

침입차단시스템

- 방화벽(firewall)
- 외부의 불법적인 침입으로부터 내부망을 보호하기 위한 네트워크 정보보호 시스템 중 하나
- 내부 정보자산을 보호하고 외부로부터 유해 정보 유입을 차단하기 위한 정책과 이를 지원하는 하드웨어 및 소프트웨어 총칭
- 외부망과 연동되는 유일한 접점으로서 각 서비스별로 요구한 시스템의 IP 주소와 포트번호를 기반으로 서비스를 제공하거나 차단하기 위해 설정된 정책에 따라 상호 접속된 내외부 망 트래픽에 대한 감시와 기록 유지



침입차단시스템의 장단점

- 장점
  - 취약한 서비스의 보호
    - 보안취약점이 발견된 서비스에 대한 제어 가능
  - 접근 통제
    - 인증받지 못한 사용자의 망 접속 차단 가능
  - 효율적 통제
    - 유일한 접속점이므로 효율적 통제 가능
  - 로그와 통계
    - 감사 및 통계, 트래픽 분석 자료로 활용 가능
- 단점
  - 네트워크의 속도 저하
  - 서비스에 대한 불편
    - 정책에 부합하지 않은 새로운 서비스 사용 불가
  - 특정 서비스에 대한 거부
    - 새로운 서비스, 또는 동적 포트를 이용하는 서비스의 경우 불가
  - 수동적인 보호
    - IP와 포트번호를 기반으로 보호하므로 적법한 IP, 포트로 위장하는 경우 불가
  - 악의적인 내부사용자 공격에 취약
  - 우회하는 서비스 통제 불가
  - 새로운 형태의 공격 대처 불가

침입차단시스템 동작원리

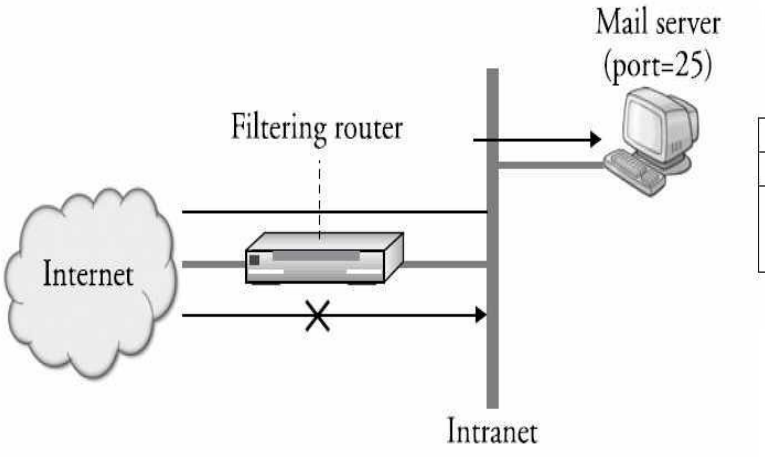
- 정당한 사용자는 이용이 가능하도록 보장하고, 비인가된 사용자는 접근을 불허하여 네트워크 보호
- 동작 계층
  - 응용 계층
  - 트랜스포트 계층
  - 네트워크 계층
- 필터링

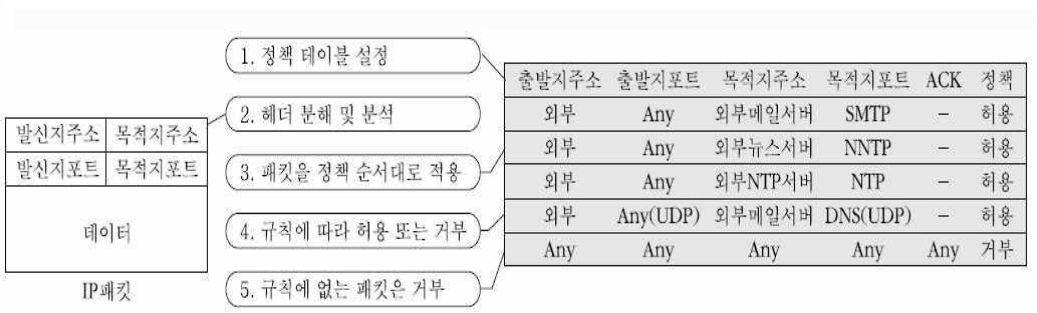
침입차단시스템 종류

유형	구축 형태
패킷 필터링(packet filtering)	듀얼 홈드 호스트 (dual homed host)
응용 계층형(application layer)	베스천 호스트(bastion host)
서킷 레벨형(circuit level)	스크린드 호스트(screened host)
하이브리드형(hybrid)	스크린드 서브넷(screened subnet)

패킷 필터링 (1)

- OSI 3, 4 계층을 이용하는 방법
- IP 주소와 포트 번호로 정책 수립
  - 발신지와 목적지 IP 주소에 대한 차단
  - 보안에 취약한 상위 프로토콜에 대한 차단



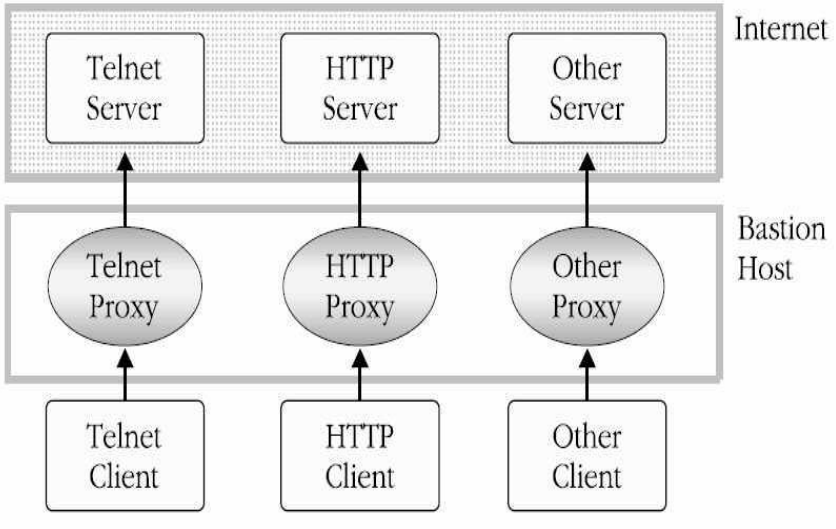


패킷 필터링 (2)

- 특징
  - 다른 방식에 비해 처리 속도 우수
  - 사용자에게 투명성 제공
  - 기존에 사용하고 있는 서비스와 새로운 서비스에 대한 정책 수립 가능
  - TCP, UDP, ICMP 등에 대한 패킷 통제 가능
  - IP spoofing, TCP SYN flooding 차단 가능
  - TCP/IP 헤더 조작 패킷에 대한 방어 불가능
  - 단순 공격에 대한 차단은 가능하나 모든 형태의 공격을 막기 위한 정책 수립은 불편하고 복잡
  - 침입차단시스템을 통과한 경우 내부 망에 대한 접근이 자유롭고 사용자 인증 불가능
  - 호스트가 많을수록 복잡하고 성능 저하

응용 레벨 (1)

- OSI 상위 7계층에 적용
- 각 서비스별 프록시(proxy) 데몬이 있어 '응용 레벨 프록시 게이트웨이' 또는 '응용 레벨 게이트웨이"라고 지칭
- 패킷 필터링 기능 외에도 서비스별 접근 제어, 바이러스 검사 등 가능
- 모든 인바운드, 아웃바운드에 대한 로그 가능

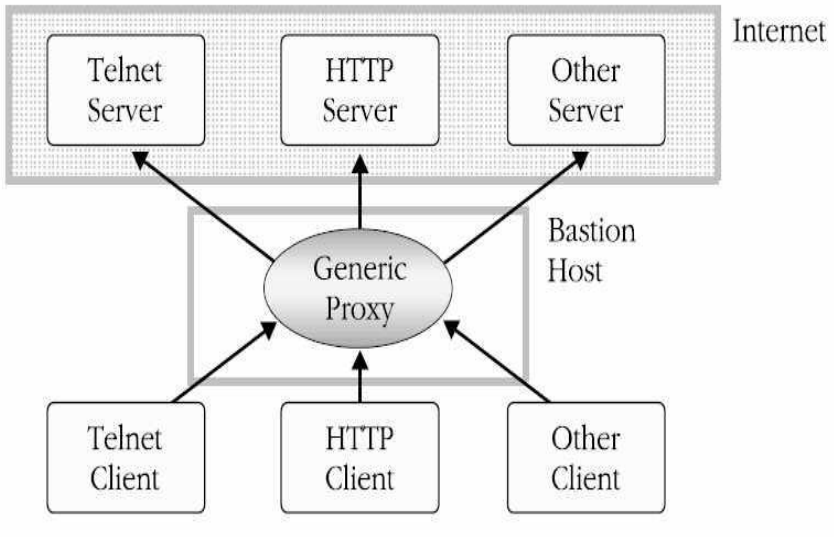


응용 레벨 (2)

- 특징
  - 프록시를 통해서만 연결이 가능하므로 직접적인 세션이 발생하지 않으며, 따라서 내부 망 주소를 숨길 수 있음
  - 강력한 로그 및 감사 기능 가능
  - 최상위 계층에서 처리하므로 처리속도가 늦고, 따라서 고속의 장비가 요구됨
  - 새로운 서비스를 도입하는 경우 프록시 서버가 개발되어야 하므로, 빠른 대처가 어렵고 유연성 부족
  - 사용자에게 투명한 네트워크 제공이 어려움

서킷(Circuit) 레벨

- '서킷 게이트웨이'라고도 함
- OSI 5-7 계층에서 존재
- 어느 응용도 이용할 수 있는 일반적 프록시 존재
- 서킷 게이트웨이를 이용할 수 있는 특별한 클라이언트 필요
- 클라이언트가 설치된 클라이언트만 서킷 생성 가능
- 특징
  - 내부망의 IP 주소 은닉 가능
  - 수정된 클라이언트가 탑재된 시스템은 투명성 제공 가능
  - 수정된 클라이언트가 반드시 필요

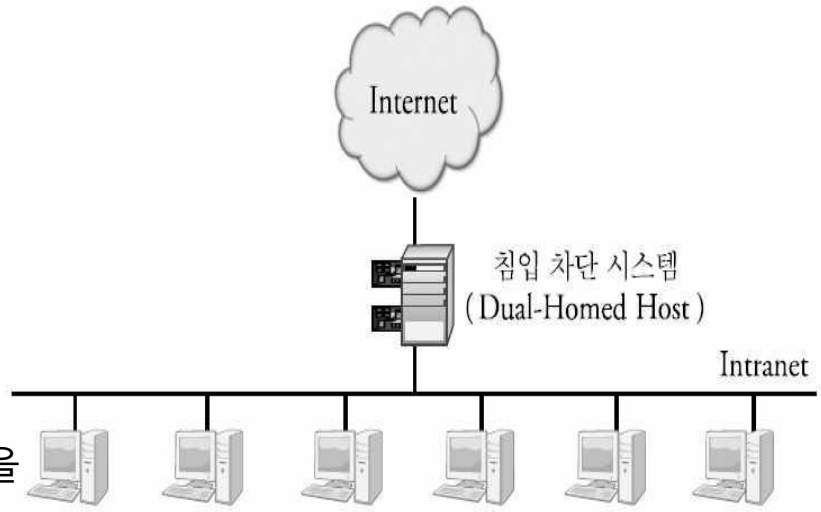


하이브리드

- 여러 형태의 침입차단시스템을 복합적으로 구성
- 현재 사용되고 있는 대부분의 침입차단시스템의 형태
- 특징
  - 가장 효과적인 정책 수립 가능
  - 다양한 환경에 적용 가능
  - 효과적인 정책 수립을 위해 구축, 관리의 복잡성 검토 필요
  - 복잡한 구성으로 인한 정책 설정의 복잡, 시스템 부하로 인한 전체 네트워크 영향 등을 고려해야 함

듀얼 홈드 호스트

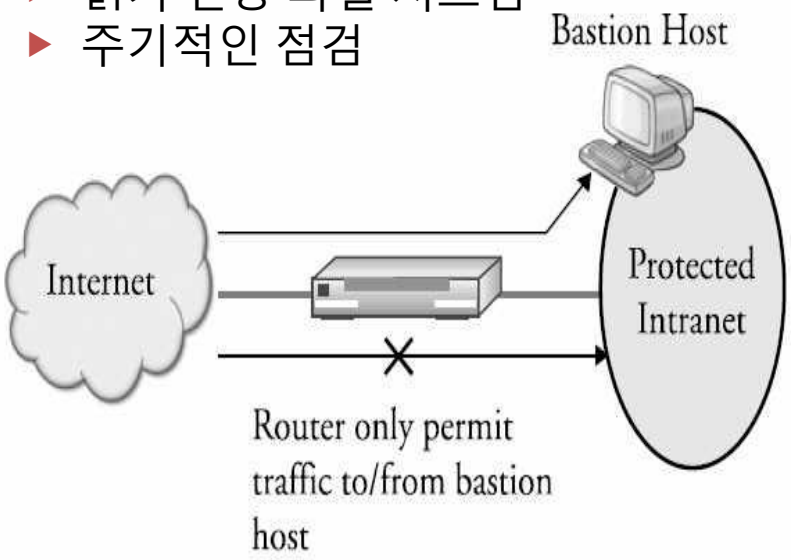
- 두 개의 네트워크 인터페이스를 갖는 호스트로 하나는 외부, 다른 하나는 내부와 연결
- 두 인터페이스 사이에서 필터링 수행
- 규칙을 통과한 패킷을 전달(forwarding)
- 일반적인 응용계층 침입차단시스템이 이러한 형태를 취함
- 단 하나의 노드만을 가지고 있으므로 안전하며, 모든 데이터 분석이 가능하고 로그 가능
- 한대의 장비만을 요구하므로 비용이 적게 들고 설계, 유지 보수 간편
- 로그인 프로세스를 통한 공격 가능
- 단 한대로 구성되므로 해당 시스템이 공격 당했을 때 취약
- 각각의 서비스에 대한 정책 수립이 복잡



베스천 호스트

- 방화벽 관리자가 중점적으로 보호해야 할 내부망의 호스트
- 신뢰할 수 없는 외부 네트워크에 대한 인터페이스로 동작
- 자주 침입을 받기 쉽고, 유일한 관문 역할을 함
- 일반 사용자의 계정을 생성하지 않고, 해킹 대상이 될 수 있는 어떠한 서비스도 제공하지 않음

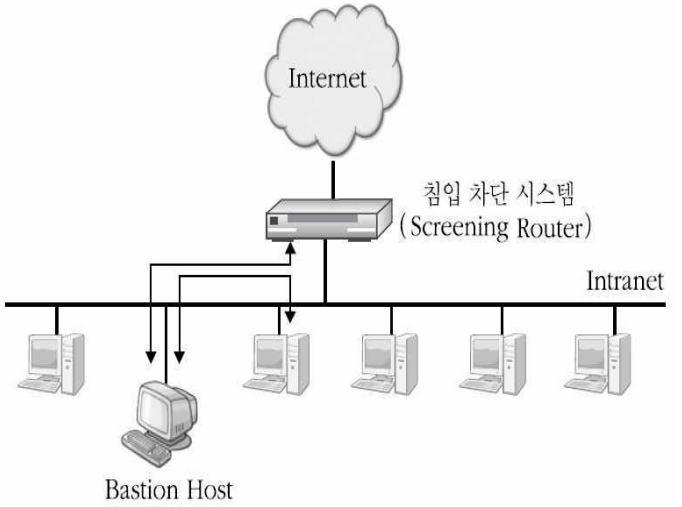
- 콘솔로만 로그인 가능
- 불필요한 유틸리티 모두 제거
- 불필요한 커널 서비스 제거
- 동적 라우팅 테이블 금지
- 요구되는, 최소한의 서비스만 설치
- 개별적인 파티션에 감사기록 저장
- 읽기 전용 파일 시스템
- 주기적인 점검



스크린드 호스트 게이트웨이

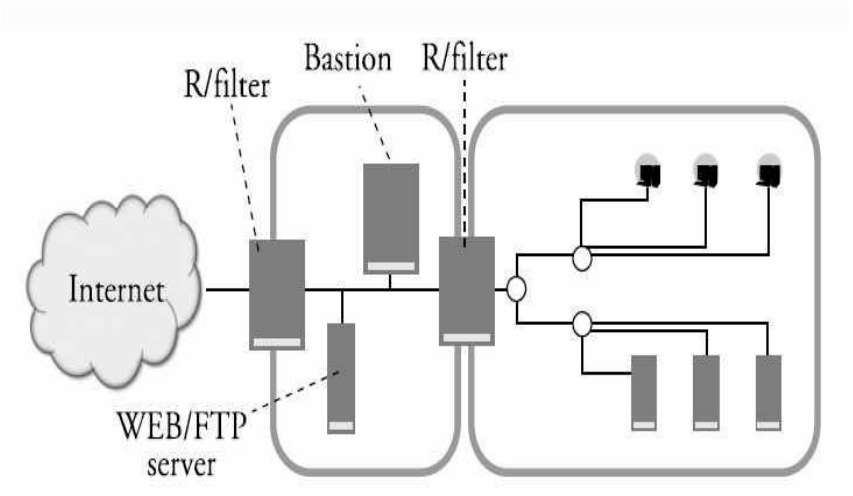
- 패킷필터링 라우터의 한 포트는 외부망에 연결, 다른 포트는 내부망에 연결되어 있고, 베스천 호스트가 내부망에 존재하는 경우를 지칭
- 패킷 필터링 라우터에서 정해진 정책에 따라 유입되는 패킷의 수락 여부 결정
- 수락된 패킷은 모두 베스천 호스트로 보내짐
- 베스천 호스트는 내부 및 외부 네트워크에 대한 인증 작업 수행

- 특징
  - 스크리닝 라우터와 베스천 호스트 두단계를 거치므로 비교적 안전
  - 두 개의 장비만을 설치하므로 간편
  - 베스천 호스트의 보호가 비교적 용이하고, 처리속도도 빠름
  - 모든 트래픽이 베스천 호스트를 거쳐가므로 자원 낭비 가능성
  - 스크리닝 라우터의 설정이 잘못되는 경우 우회하는 공격 가능



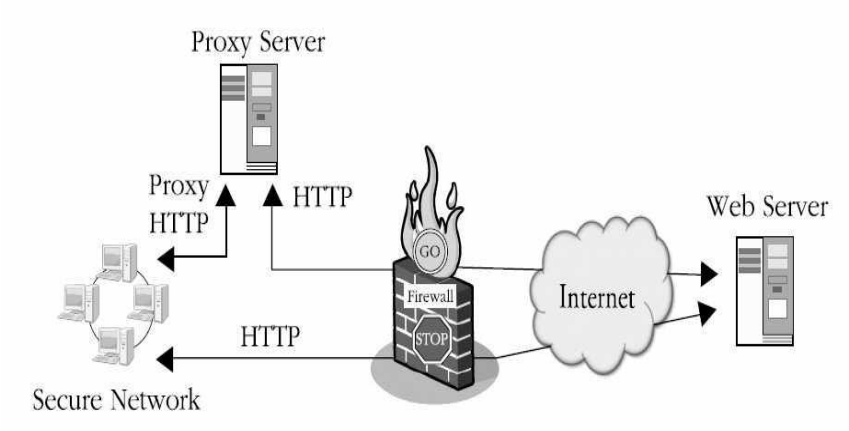
스크린드 서브넷 게이트웨이

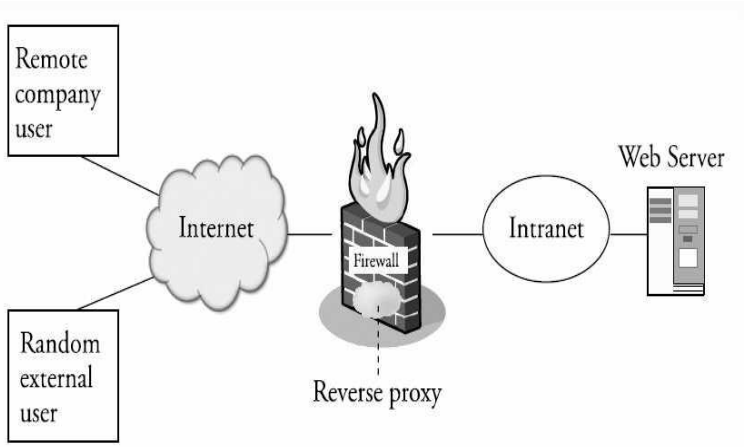
- 외부 네트워크와 내부 네트워크 사이에 하나 이상의 경계 네트워크를 두어 분리
- DMZ(비무장지대)
  - 외부 접속이 많은 시스템 구성
- 3단계 보안을 거치므로 안전한 네트워크 구성 가능
- 베스천 호스트가 공격당해도 내부 망까지 들어올 수 없음
- 설치 및 유지 보수 복잡
- 여러 단계를 거치므로 속도 저하, 비용 증가



침입차단 시스템 구축시 고려사항

- 네트워크 접속 정책 결정
  - 허용된 작업 외 모두 거부 ?
  - 불허된 작업 외 모두 허용 ?
- 모니터링 제어
  - 허용 또는 거부할 대상에 대한 리스트 작성
- 비용
- 서비스 설치 및 구성
  - ftp 서비스 구성
    - 익명 계정, 업로드 허용 시 악성 자료 검사
  - http 서비스 구성
    - 접근 권한 최대한 제한
    - 모바일 코드에 대한 유입 통제





침입차단시스템 구축 절차

- 보호할 내부 네트워크 자산에 대한 위험 분석
- 보호대상 판별
- 제공할 서비스 구분
- 보안 정책, 네트워크 구성 및 서비스 방식에 대한 전체적인 보안 정책 수립
- 침입차단시스템 설치
- 패킷 필터링 라우터 설치
- 애플리케이션 게이트웨이 설치
- 서브네트워크 호스트간의 보안 정책 수립
- 보안관리자의 보안 인지에 대한 교육 및 유지

침입탐지시스템

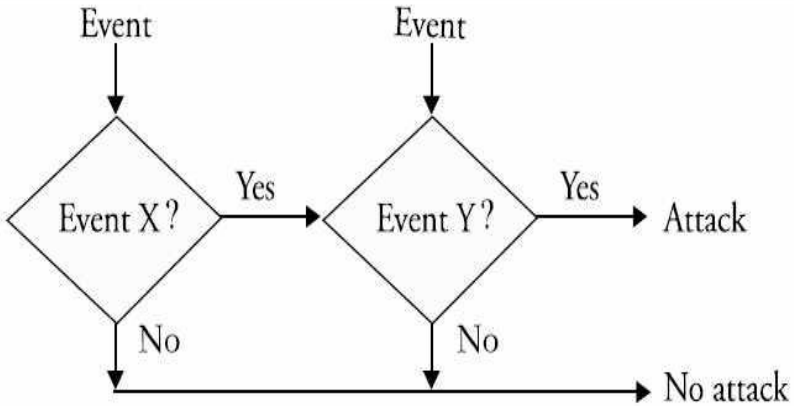
- IDS(Intrusion Detection System)
  - 탐지 대상 시스템에 대한 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 이를 불법적인 행위와 구별하여 침입 여부에 대한 기록과 통보를 통해 대응하도록 하는 기능
  - 단순 탐지 기능을 넘어서 침입패턴 데이터베이스와 전문가시스템을 이용하여 네트워크나 시스템을 실시간 모니터링
  - 발생 가능 오류
    - 오경보 (false alarm, false positive)
    - 경보 실패 (no alarm, false negative)
- 특징
  - 외부로부터 공격 뿐만 아니라 내부 공격도 탐지 가능
  - 침입차단시스템의 경우 인정된 IP로부터의 공격은 막을 수 없지만 IDS는 방어 가능
  - 통계 분석, 호스트의 파일이나 로그 모니터링, 네트워크 트래픽 상의 비정상적인 패턴 탐지에 유용
  - 자체적인 방어보다는 관리자로 하여금 위협에 대한 경고를 알리는 차원의 역할
  - 자체적으로 위험을 차단하는 적극적인 행위는 행하지 않음
- 구성 요소
  - 정보 수집
  - 가공 및 축약
  - 분석 및 침입 탐지
  - 보고 및 조치

침입탐지 시스템 분류 – 데이터 소스

- 호스트 기반 침입탐지시스템
  - host based IDS
  - 시스템 내부에 설치되어 내부 사용자들의 활동을 감시하고 해킹 시도 탐지
  - 애플리케이션 로그, 시스템 로그 등의 정보를 운영체제로부터 획득
  - 호스트마다 설치되어야 함
- 네트워크 기반 침입탐지시스템
  - network based IDS
  - 네트워크의 패킷을 캡처하여 네트워크를 경유하는 모든 패킷을 분석하여 침입 탐지
  - 네트워크 단위로 설치
  - 잘못된 패킷에 대한 정보나 포트 스캔에 대한 정보 획득 가능
  - 네트워크의 상황을 인지하고 있으므로 네트워크 측면 대응 가능
  - 모든 패킷을 재조립하여 분석하므로 네트워크의 부하가 큰 경우 패킷 누락(drop) 발생
  - 암호화된 패킷은 분석 불가

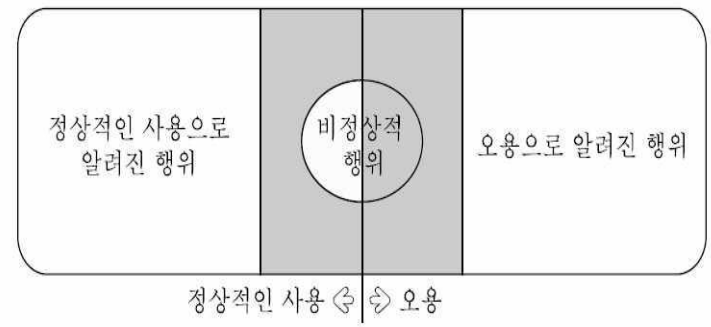
침입탐지 시스템 분류 – 침입 모델(1)

- 오용(misuse) 탐지
  - 알려진 공격법(known-attack)이나 보안 정책에 위반하는 행위에 대한 패턴을 패턴 DB로부터 찾아서 특정 공격 탐지
  - 지식기반(knowledge-based) 탐지라고도 함
  - 자신이 가지고 있는 지식에 기반을 두고 있으므로 탐지에 대한 정확도가 높음
  - 패턴 데이터베이스의 지속적인 갱신 필요
- 새로운 취약성에 대한 최신 정보 유지가 쉽지 않음
- 취약성 분석에 대한 시간 소비형 업무 필요
- 매우 낮은 잘못된 경보율
- 보안시스템에 의해 제안된 분석이 세밀하므로 방어 또는 수정이 용이

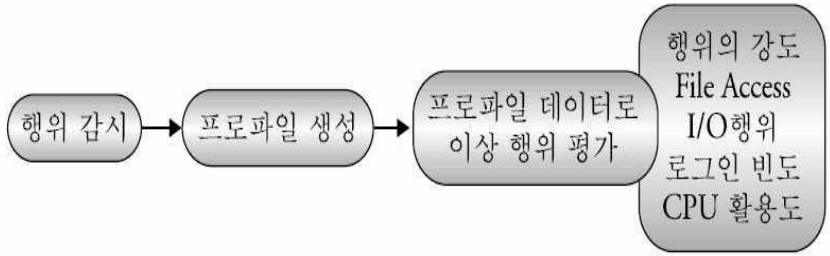


침입탐지 시스템 분류 – 침입 모델(2)

- 비정상적 행위(anomaly) 탐지
  - 시스템 사용자가 정상적이거나 예상된 행위로부터 이탈하는지의 여부를 조사함으로써 탐지
  - 정상적 또는 유효한 행동 모델을 다양한 방법으로 수집
  - 생성된 정보를 바탕으로 만든 탐지모델과 모든 행동을 비교
  - 높은 확률의 잘못된 경보 문제
  - 임계치를 두어 경보를 울리는 정량 분석법도 가능하나 임계치에 대한 설정 필요



- 통계적 분석법의 경우 주기적인 데이터의 변경이나 유지 보수가 필요없지만 확률적인 오차와 오탐율이 높다는 문제
- 신경망 분석법
  - 학습을 통해 신경망을 만들고 적용
  - 비정상과 정상을 구분하는 명확한 기준 설정에 어려움
- 행위기반 탐지 방법
  - 높은 잘못된 경고율
  - 시간에 따라 변화하는 행위 프로파일에 대한 주기적인 재설정 필요
  - 학습기간동안 탐지 불가

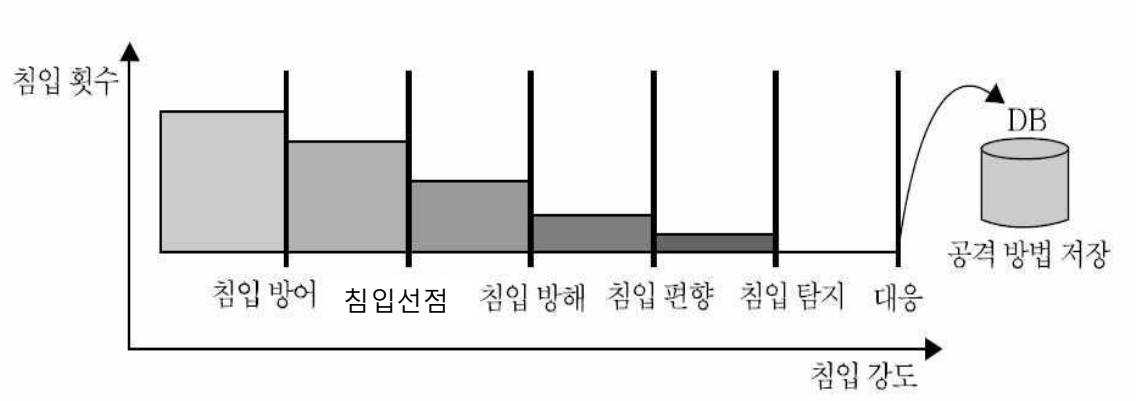


침입탐지시스템의 기능과 한계

- 기능
  - 강력한 보안정책은 IDS의 핵심 기술
  - 비정상적인 네트워크 트래픽에 대한 정보를 저장, 제공 가능
  - 공격 식별, 증거 포착
  - 보안관리자에게 실시간으로 경고하고, 통합 방어 전략 하부 구조로 활용 가능
- 한계
  - 모든 위협을 탐지할 수는 없음
  - 잘못된 경보와 경보 실패 발생 가능
  - 광범위한 공격으로 IDS 자체의 마비 가능
  - 네트워크 기반 IDS의 경우 고속 네트워크에서 효과적인 동작이 어려울 수도 있음
  - 구축되기 전에 충분한 테스트 과정 필요

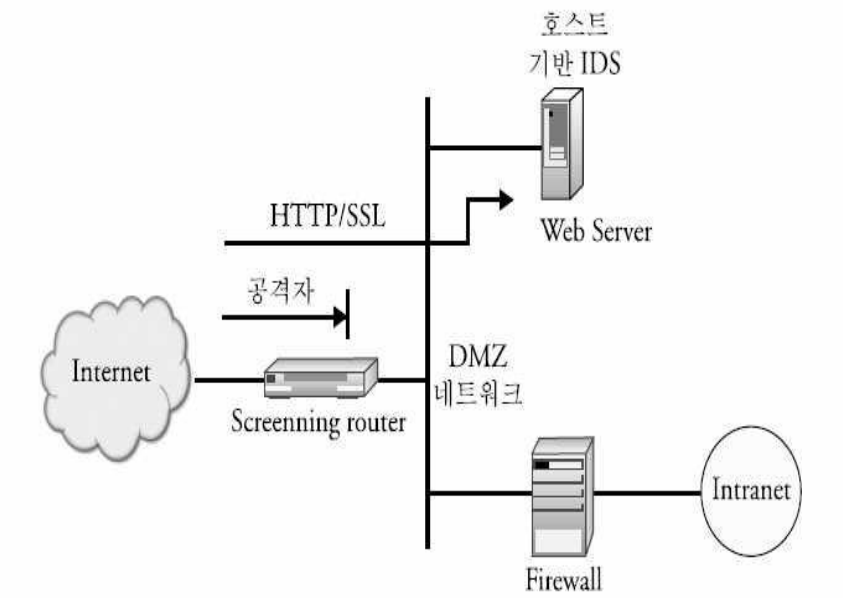
침입 대응

- 침입방어(Intrusion Prevention)
  - 무력화
- 침입 선점(Intrusion Preemption)
  - 공격자에 대한 공격
- 침입 방해(intrusion Deterrence)
  - 공격 대상 은닉 등
- 침입 편향(Intrusion Deflection)
  - 허니 팟
- 침입 탐지(intrusion Detection)
- 대응

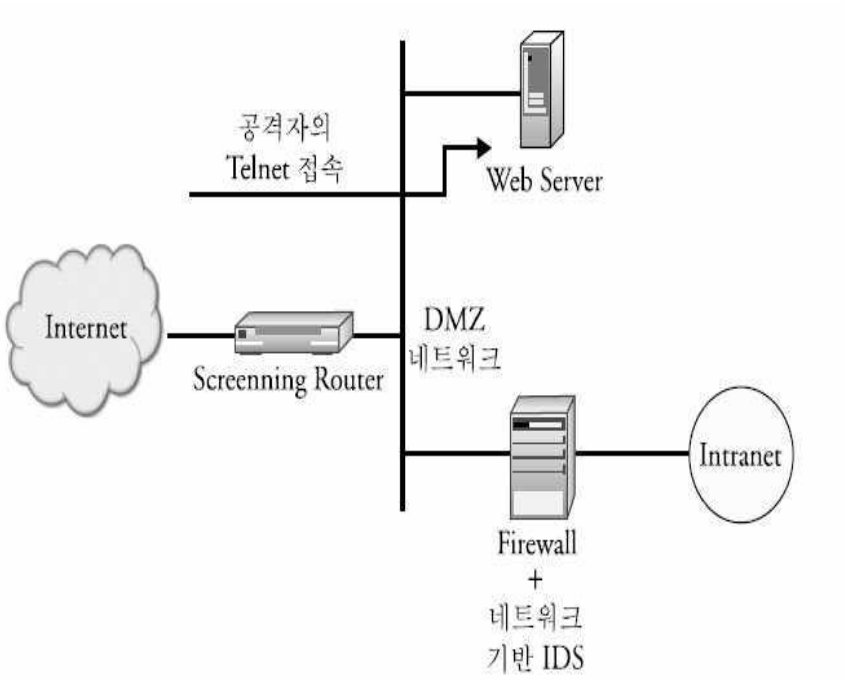


침입탐지시스템을 포함한 망 구성(1)

- 침입탐지시스템과 웹서버

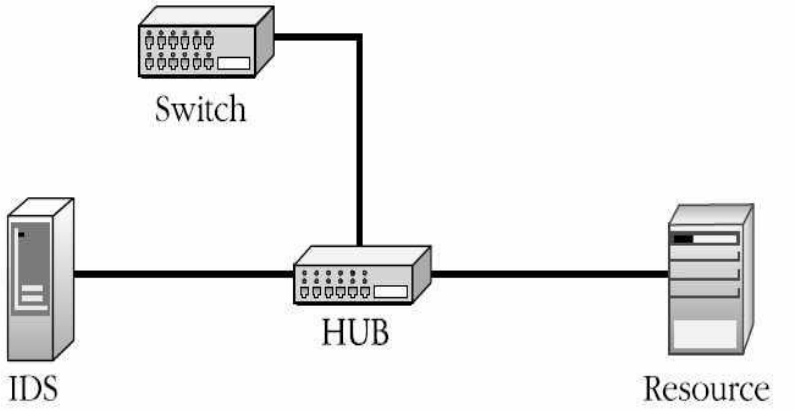


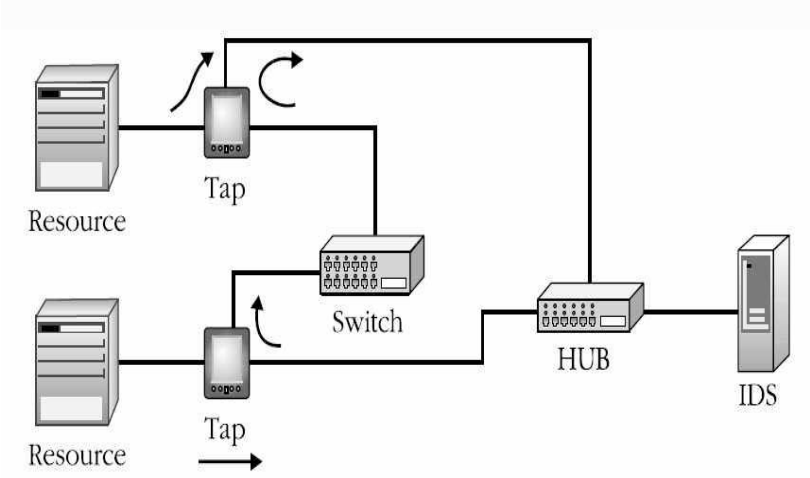
- 침입탐지시스템과 침입차단 시스템



침입탐지시스템을 포함한 망 구성(2)

- 네트워크 기반
  침입탐지시스템과 스위칭 허브





침입탐지시스템과 환경

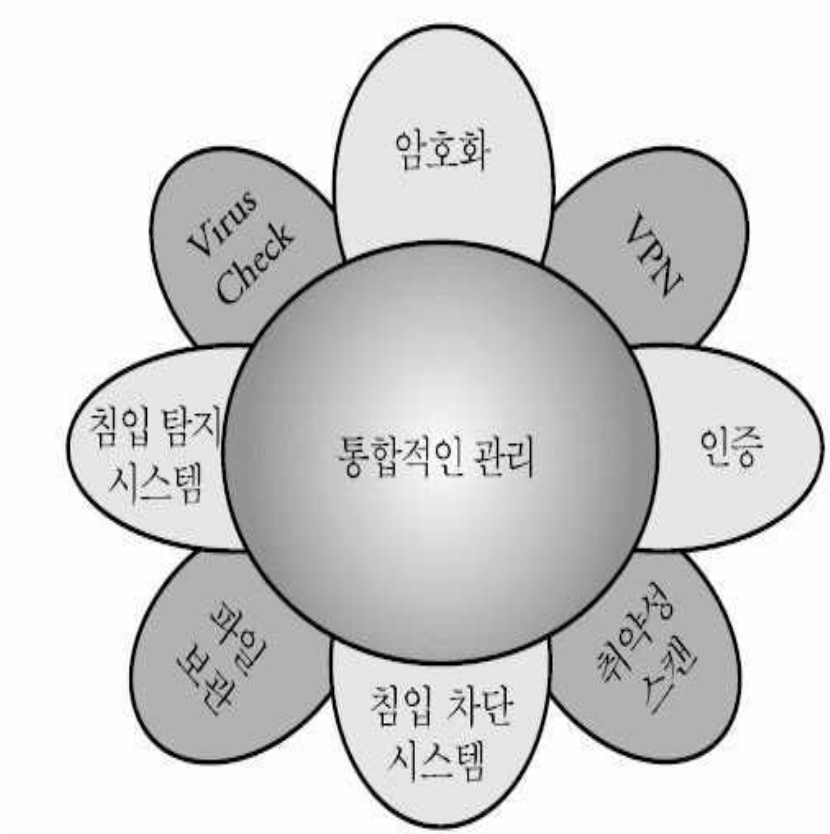
- IDS와 VPN
  - VPN을 사용하는 경우 데이터를 암호화해서 전송하므로 네트워크 기반 IDS는 침입을 탐지할 수 없음
  - 호스트 기반 IDS 사용하면 로그와 감사 데이터를 이용하여 애플리케이션 수준 IDS 운영 가능
- 네트워크 기반 IDS와 고속 네트워크
  - IDS 탐지 속도보다 네트워크 속도가 빠르면 패킷 누락(drop) 현상 발생
  - 해당 IDS의 네트워크 수용 임계치를 확인하여 적합한 솔루션을 구축해야 함
  - 헤더 감사, 데이터 감사 등을 여러 대의 IDS가 작업을 분담하여 수행하거나, 동일한 기능을 갖는 IDS를 복수개 설치하여 작업 수행하는 방안도 가능

침입탐지시스템의 침입 판정

- 판정하는 방식
  - 공격에 대한 축적된 지식을 바탕으로 공격 판정
  - 정상 행위에 대한 참조 모델 생성 후 정상 행위에서 벗어나는 행위를 찾는 방식
- 지식 기반 침입 탐지(오용 탐지)
  - 전문가시스템(expert system)
  - 시그니처(signature) 분석
  - 패트리넷(petri-net)
  - 상태전이분석(state transition analysis)
  - 유전알고리즘(genetic algorithm)
- 행위 기반 침입 탐지(비정상 행위 탐지)
  - 통계적(statistical) 방법
  - 전문가 시스템 (expert system)
  - 신경망(neural network)
  - 컴퓨터 면역학(computer immunology)
  - 데이터 마이닝(data mining)
  - HMM(Hidden Markov Model)
  - 기계학습(machine learning)

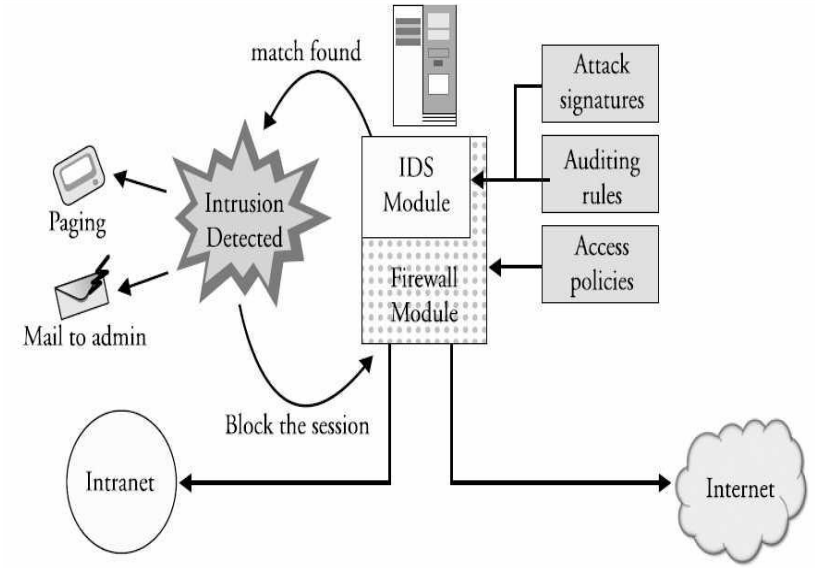
통합시스템

- 통합 보안 관리 (Integrated Security Management)
  - 날로 복잡해지는 보안 제품들에 대해 통일성 제공
  - 운영자의 실수로 인한 패해 최소화
  - 여러 보안 정책과 장비들에 대한 일관되고 통일된 인터페이스 제공

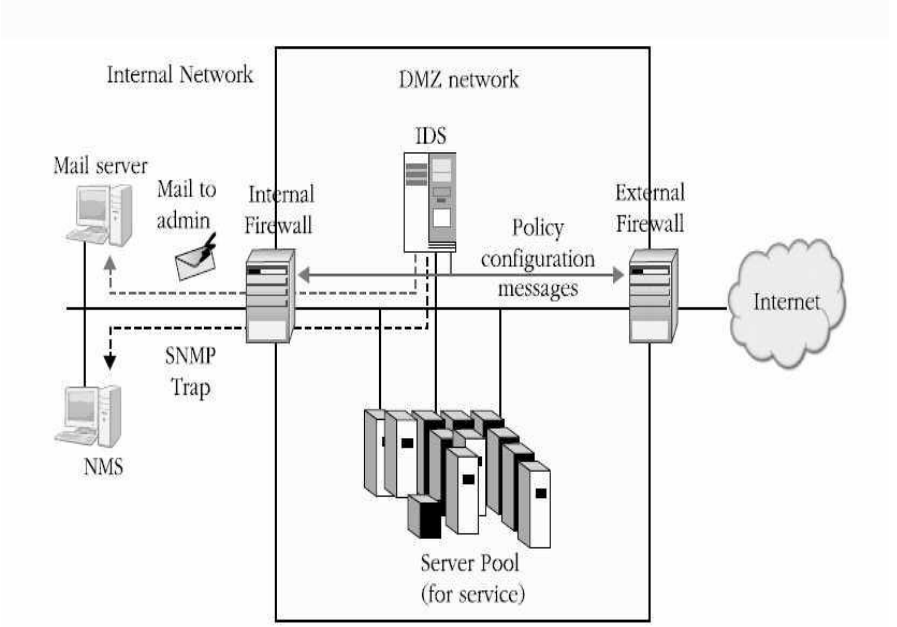


통합시스템 분류

- 혼합형 통합 모델 (Hybrid Integration Model)

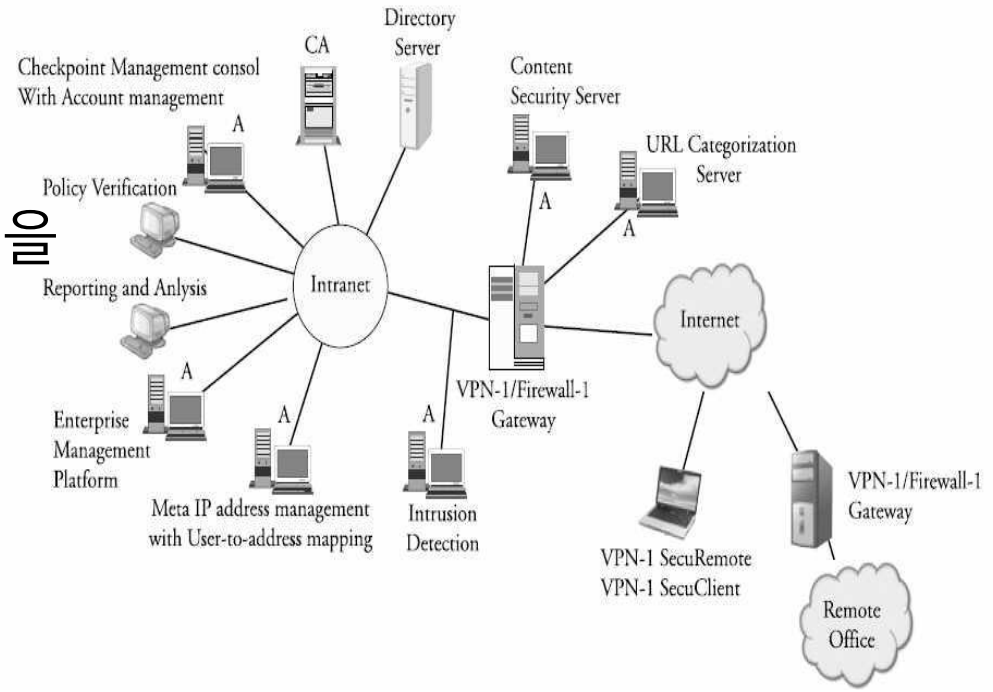


- 연동 통합 모델 (Interoperational Integration Model)



OPSEC (Open Platform for Secure Enterprise Connection)

- Checkpoint 사가 제안한 통합 보안 솔루션을 위한 API와 표준안
- 침입차단시스템, 침입탐지시스템, 안티바이러스 등의 시스템을 하나로 연동
- SVN(Secure Virtual Network)이라고 불리는 구조를 기반으로 VPN 게이트웨이를 위한 보안시스템에 적용 가능



보안 운영체제 (1)

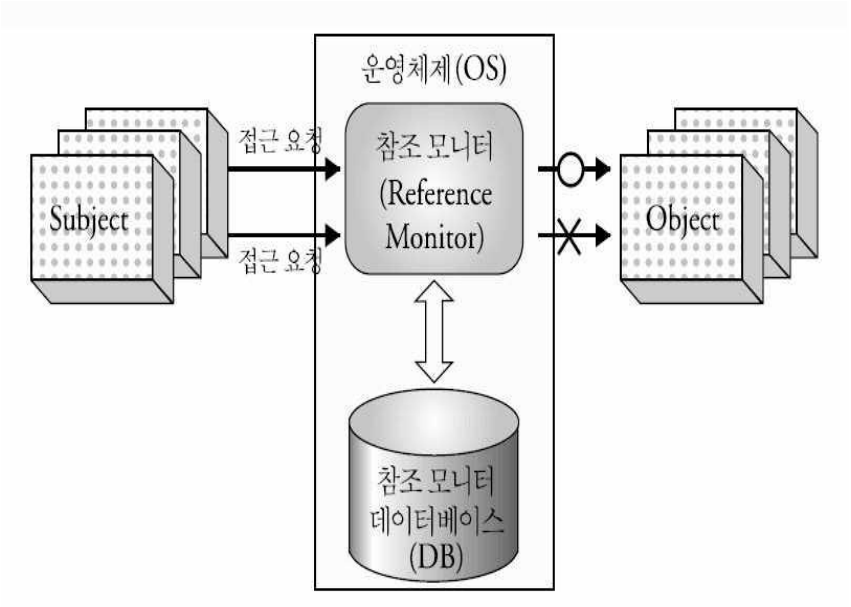
- 운영체제 내에 보안 기능을 위한 보안 커널을 이식한 운영체제
  - 사용자에 대한 식별과 인증
  - 강제적 접근 통제
    - 접근제어정책
    - 인증사용정책
    - 암호화 사용정책
  - 임의적 접근 통제
    - 신뢰된(trusted) 경로
    - 보호된(protected) 경로
  - 재사용 방지
  - 침입 탐지 등
- 보안 운영체제의 필요성
  - 응용 프로그램 수준의 정보보호시스템은 부분적인 보안 적용으로 인해 고비용 발생
  - 운영체제의 버그 등 자체 취약성을 이용한 공격 증가 => 패치나 업그레이드 등 임시 방편적인 취약성 수정 대응
  - 운영체제 커널에 보안 기법을 가미한 보안 운용체제를 개발하면 보다 효율적인 보안 시스템 구축 가능

보안 운영체제 (2)

- 보안 커널
  - 참조모니터 개념을 구현한 하드웨어, 펌웨어, 혹은 소프트웨어로 시스템 자원에 대한 접근을 통제하기 위해 기본적인 보안 절차를 커널에 구현한 컴퓨터 시스템
  - 보호 대상 객체에 대한 모든 접근에 대한 검토를 보장
  - 보안 메커니즘의 독립성이 보장되고, 모든 보안 기능이 단일 코드 집합에 의해 수행하도록 하여 무결성 유지, 커널에 대한 분석, 검증 가능
- 보안 커널 설계
  - 운영체제 소스 코드에 보안기능을 추가하거나 적재 가능한 커널 모듈에 보안 기능만 추가적으로 구현하는 방식으로 개발
  - 반드시 제공하여야 하는 사항
    - 운영체제의 기본 개념을 기반으로 설계
    - 외부로부터의 공격 방어 기능과 함께 탐지 기능을 통한 역추적 가능
    - 시스템 자원에 대한 통제가 가능하고 모든 자원 관리 가능
    - 모든 운영상의 접근과 행위 감시
    - 각종 프로그램과 환경 설정 변경에 대한 기록
    - 인증을 통한 신분 확인

보안 운영체제 (3)

- 참조 모니터(Reference Monitor)
  - 보안 커널의 가장 중요한 부분
  - 객체에 대한 통제 기능
  - 감사, 식별, 인증, 보안 매개변수 설정 등의 보안 메커니즘과 데이터를 교환하면서 동작
  - 운영체제 측면에서 사용자가 특정 객체에 대한 접근 권한이 있는지, 특정 동작이나 행위를 할 수 있는 지 여부를 검사, 감시하는 기능
  - 주체와 객체 사이의 모든 정보를 대상으로 하는 보안 모듈
  - 항상 호출되는 프로세스



보안 운영체제 (4)

- 요구사항
  - 사용자와 프로그램을 가능한 최소의 권한으로 운영
  - 우연 혹은 의도적인 공격으로부터 손상을 최소화해야
  - 충분한 분석과 검증이 가능하도록 작고 단순한 보호 메커니즘이 들어있는 경제적인 보안시스템이어야
  - 충분한 검토가 가능하도록 상대적으로 작고 주요한 보안 메커니즘에 의존해야
  - 해당 기능을 공개함으로써 개방형 설계 지향해야
  - 직접적, 우회적인 모든 접근에 대한 검사를 통한 완전한 중재 및 조정이 가능해야
  - 객체에 대한 접근은 하나 이상의 조건에 의해 결정되어, 하나를 우회해도 객체 보호가 이루어져야
  - 공유 객체는 정보 흐름 가능성이 있는 채널을 제공하므로 최소화해야
  - 보안 메커니즘 사용이 용이하고 우회 가능성이 적어야

접근통제 모델링 (1)

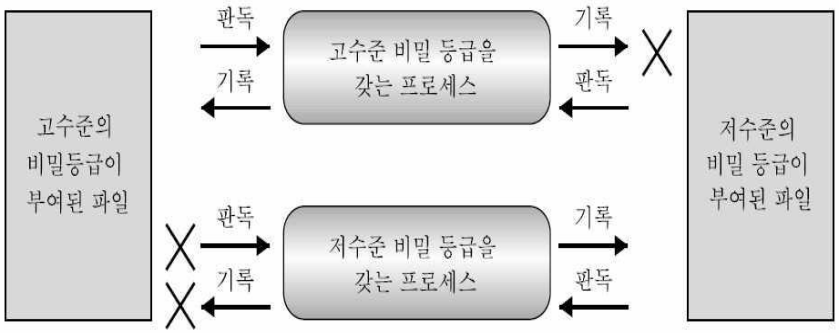
- 임의적 접근 통제
  - 주체나 그것에 속한 그룹의 ID에 근거하여 객체에 대한 접근을 제한하는 방법
  - 최초 객체에 내포된 DAC(Discretionary Access Control) 관계는 복사된 객체로 전파 불가능
  - 주체의 ID에만 의존하고 객체의 데이터 의미에는 지식이 없으므로 ID가 도용될 경우 DAC 체계가 파괴될 수 있음
  - 소유자의 재량에 근거하여 데이터 보호와 공유가 이루어짐

- unix의 ACL(Access Control List)

ID	Type	Permissions Granted	Permissions Denied	Time of day Restrictions	Location Restrictions
S. Smith	Indivisual	read, modify, manage			
team members	group	read			
auditors	role	read	modify, manage		
Contractor	group	read, modify	manage	8:00-18:00 Mon-Fri	Only local terminals

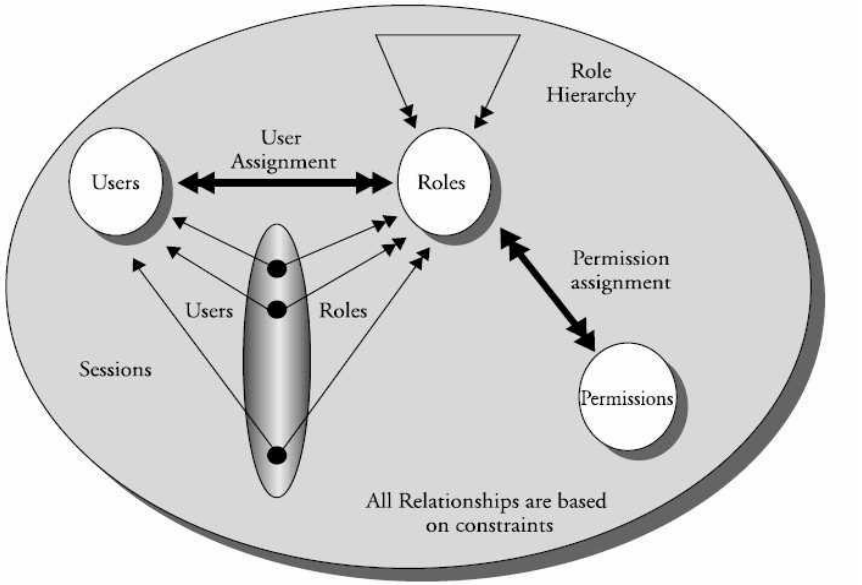
접근통제 모델링 (2)

- 강제적 접근 제어
  - 보안에 대한 민감성을 가지고 있는 객체에 대해 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제한하는 방법
  - 객체의 소유자에 의해 변경할 수 없는 접근 통제 관계 정의
  - 최초 객체가 가지고 있는 MAC(Mandatory Access Control)은 복사된 객체로 전파
  - 데이터 공유를 시스템이 결정
- 다중 등급 모델(Multi Level Model)
  - DAC와 MAC 포함
  - 주체 및 객체에 등급을 부여하여 접근을 통제



접근통제 모델링 (3)

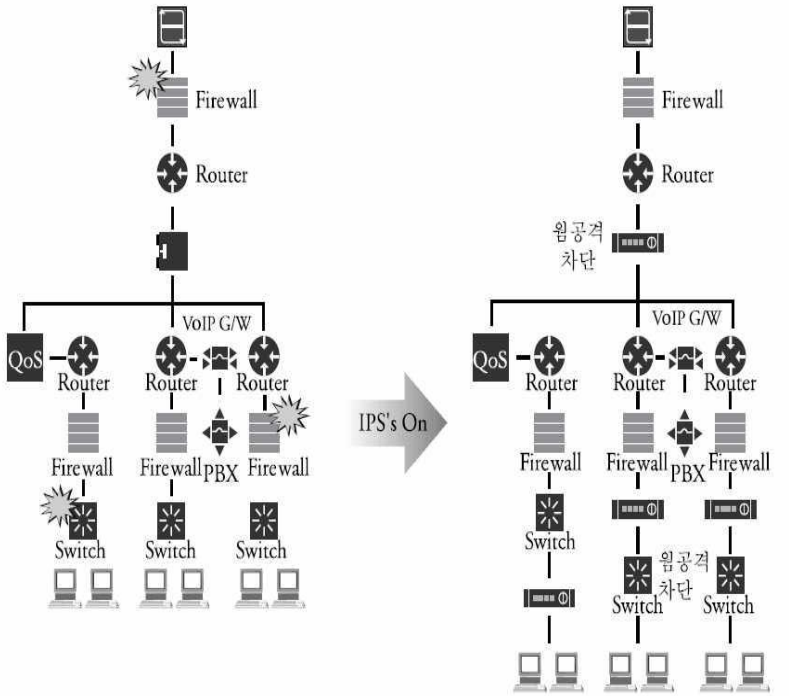
- 역할 기반 접근 통제 모델
  - 사용자의 역할 및 직능에 따라 접근을 통제하는 방식
  - 중앙관리자가 접근 권한을 통제
  - 비임의적 접근 통제라고도 함
  - 사용자의 역할 및 직능별 권한의 관리가 용이
  - 자원에 대한 보안이 효율적으로 이루어질 수 있음
  - 기업 및 공공기관의 자원 보호에 대한 효율적인 통제 기능
- 장점
  - role을 이용 상호 관계 설정 최소화
  - 사용자에게 특정 업무를 수행하기 위한 최소한의 권한만 부여 가능
  - role 중 분쟁의 소지가 있는 role을 한 사용자에게 집중하는 것을 방지할 수 있음
  - 업무 수행에 필요한 모든 추상적인 권한을 role로 정의 가능



침입 방지시스템 (1)

- IPS(Intrusion Prevention System)
- 잠재적인 위협을 인지한 후 이에 즉각적인 대응을 하기 위한 네트워크 보안 기술 중 예방적 차원의 접근 방식
- 네트워크 관리자가 설정해 놓은 일련의 규칙에 기반을 두고 즉각적인 행동을 취할 수 있는 능력을 가지고 있어야 함
- 네트워크 트래픽을 감시하여 부당한 패킷이 들어오는 경우 해당 IP 주소 또는 포트로 들어오는 트래픽을 봉쇄하고, 합법적인 트래픽은 가용성 제공
- 개별적인 패킷, 트래픽 패턴 모두 감시하고 대응하는, 보다 복잡한 감시와 분석 수행

- 탐지기법
  - 주소 대조
  - HTTP 스트링과 서비스트링 대조
  - 일반 패턴 대조
  - TCP 접속 분석
  - 변칙적인 패킷 탐지
  - 비정상적 트래픽 탐지
  - TCP/UDP 포트 대조



침입 방지시스템 (2)

- 침입차단시스템과 침입탐지시스템의 기능을 결합한 형태
  - 정책 기반 접근제어는 개방된 포트를 이용한 공격에는 한계
  - 침입탐지시스템은 침입자에 대한 판단을 할 뿐 차단 기능이 없음
- 탐지와 차단을 동시에 수행
- 다양하고 지능적인 침입기술에 대한 다양한 방법의 보안 기술을 이용하여 침입이 일어나기 전에 실시간으로 침입을 막고, 알려지지 않은 방식의 침입으로부터 네트워크와 호스트 보호
- 최소한의 구성과 고객화로 관리자의 업무 경감

- 필요성
  - 능동적인 보안 필요성 증대
  - 해킹 기법의 고도화, 지능화에 따른 크래킹의 원천적 차단 및 방지 기능 필요
  - IDS, Anti-Virus, Secure-OS등 기존 보안 시스템의 대응 능력 한계
  - 서비스 제한을 통한 보안이 아닌, 중요 데이터에 대한 응용 보안에 대한 요구

침입 방지시스템 (3)

- 호스트 기반 IPS
  - 커널 레벨의 시스템 콜 수행 정보를 기반으로 미리 설정된 보안 위반 분석 정책을 적용하여 보안 위반 여부를 분석하는 행위 기반 침입 방지 수행
  - 주요 기능
    - 버퍼 오버플로우 공격 방지
    - 포맷 스트링 공격 방지
    - 경주 상황 공격 방지
    - 루트 쉘 획득 방지
    - 암호 추측 공격 방지
    - 다중 프로세스 생성 공격 방지
    - Disk Excess 공격 감시
    - Memory Excess 공격 감시
- 네트워크 기반 IPS
  - 응용 계층에서 패킷 분석을 수행하는 흐름 제어 기반 침입 방지 수행
  - 침입 방지 능력과 빠른 반응 속도를 위해 네트워크 상에 위치
  - 세션기반 탐지 지원
  - 주요 기능
    - IP/ARP Spoofing 공격 방지
    - DoS. DDoS 방지
    - fragmentation/segmentation 공격 방지
    - Protocol 변조 공격 방지
    - Portscan 공격 방지
    - 정상 트래픽에 위배되는 공격 방지
    - I/Worm, Virus, Backdoor 공격 방지
    - 유해사이트 접속 방지
    - 우회공격 방지