정보보호

(5111041)

9장

방화벽과 침입 방지 시스템

방화벽의 필요성

- 인터넷 연결이 필수적
  - 하지만 인터넷 연결로 인한 취약점 발생
- LAN 환경을 보호하는 효과적인 방법
- 제어 링크를 설정하는 내부 네트워크와 인터넷 사이에 삽입
  - 하나의 컴퓨터 시스템 또는 두 개 이상의 함께 작업하는 시스템에 설정가능
- 주변 방어에 이용
  - 보안 및 감사에 이용하는 단일 초크포인트
  - 외부 네트워크에서 내부 네크워크를 보호

방화벽 특징

설계 목표

- 외부에서 내부로의 모든 트래픽이 방화벽을 통과해야 함
- 로컬 보안 정책에 정의된 인증된 트래픽은 통과할 수 있어야함
- 방화벽 자체가 침입에 면역이어야 함

방화벽에서 액세스를 제어하고 사이트의 보안 정책을 적용할 기술은 다음과 같다 :

- IP주소와 프로토콜 값: 서비스 제어
- 응용프로토콜: 방향 제어
- 사용자식별: 사용자 인증 및 제어
- 네트워크활동:동작 제어

방화벽의 기능과 한계

기능:

- 단일 초크 포인트 정의
- 보안 이벤트 모니터링의 위치 제공
- 보안과 관련되지 않은 여러 인터넷 기능을 위한 편리한 플랫폼
- IPSec을 위한 플랫폼 제공 가능

한계:

- 방화벽을 우회하는 공격으로부터 보호 불가능
- 내부 위협으로부터 완전한 보호할 수 없음
- 적절하지 않게 보호된 무선 LAN은 외부 조직으로부터 액세스 할 수 있음
- 노트북, PDA, 휴대용 저장장치는 외부에서 감염되어 내부에서 이용될 수 있음

방화벽의 유형

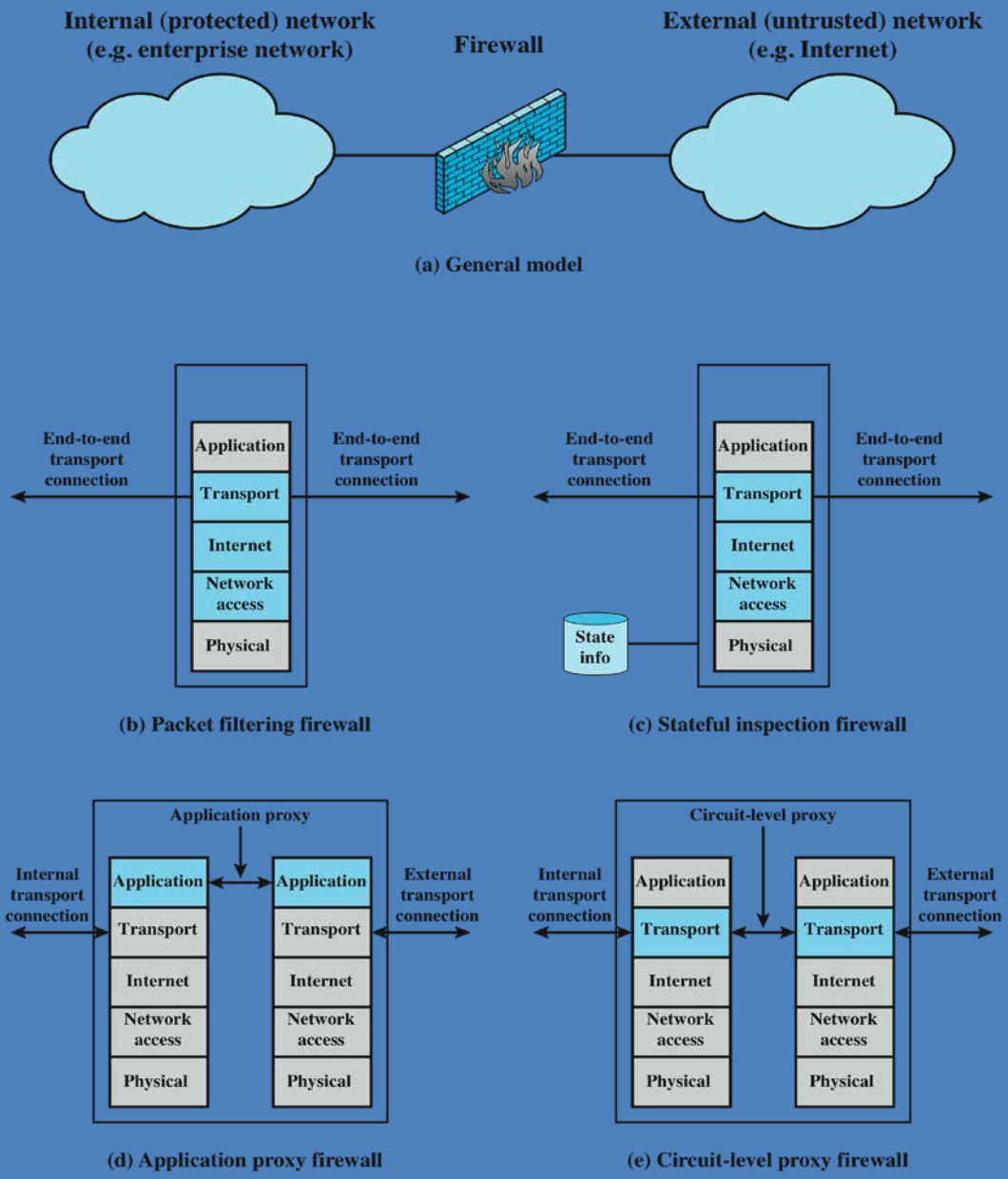


Figure 9.1 Types of Firewalls

패킷 필터링 방화벽

- 들어오고 나가는 각각의 IP 패킷에 규칙을 적용
  - IP 또는 TCP 헤더의 매치에 기반한 규칙의 일반적인 리스트
  - 규칙의 매치를 기반으로 전송 또는 폐기

필터링 규칙은 네트워크 패킷에 포함된 정보를 기반으로 함
• 송신자 IP 주소 • 수신자 IP 주소 • 송수신 전송 계층 주소 • IP 프로토콜 필드 • 인터페이스

- 두 가지 기본 정책:
  - 기본 제거 정책 – 명확히 허용된 경우를 제외하고 금지
    - 더 보수적, 제어, 사용자에게 가시적
    - 정부, 군, 회사 등
  - 기본 전달 정책 – 명확히 금지되지 않는 한 허용
    - 관리와 사용이 쉽지만 덜 안전한 방법
    - 대학교 등

패킷 필터링 예

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

패킷 필터의 장점과 단점

- 장점
  - 간단함
  - 일반적으로 사용자에게 투명하고 매우 빠름
- 단점
  - 응용프로그램의 특정 취약점 또는 기능을 이용한 공격을 방지할 수 없음
  - 제한적인 로깅 기능
  - 고급 사용자 인증을 지원하지 않음
  - TCP/IP 프로토콜 버그를 이용한 공격에 취약
  - 부적절한 설정이 위반으로 이어짐

패킷 필터링 방화벽에 대한 공격 형태

- IP 주소 Spoofing
  - 시스템 내부 사용자의 호스트 주소를 출발지 address로 spoofing → 내부망 침투
- 출발지 routing attack
  - IP, 포트 정보만 분석하고 routing 정보를 분석하지 않는 방화벽에 침투
  - 방화벽을 우회하는 detour route로 공격
- Tiny fragment attack
  - 방화벽이 TCP/IP 헤더 정보를 확인할 수 없도록 헤더의 사이즈보다 작은 크기로 패킷을 fragmentation

상태 기반 검사 방화벽

아웃바운드 TCP 연결 디렉토리를 생성에 의한 TCP 트래픽에 엄격한 규칙

- 각각 현재 설정된 연결의 항목이 있음
- 패킷 필터는 이 디렉토리의 항목 중 하나의 프로파일에 맞는 패킷에 대한 높은 번호의 포트로 들어오는 트래픽을 허용

패킷 정보의 리뷰 뿐만 아니라 TCP 연결에 관한 정보의 기록

- 시퀀스 넘버에 따른 공격을 방지하기 위해 TCP 시퀀스 넘버를 추적
- FTP, IM 및 SIPS 명령과 같은 프로토콜 데이터 검사

예제
상태기반 방화벽 연결 상태 테이블

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Table 9.2 Example Stateful Firewall Connection State Table [WACK02]

어플리케이션계층 게이트웨이

- 또한 어플리케이션 프록시라고 함
- 어플리케이션계층 트래픽의 중계 행위
  - TCP/IP 어플리케이션을 이용한 사용자 접촉 게이트웨이
  - 즉, 서버와 클라이언트간 직접적인 end-to-end TCP 커넥션을 허용하지 않음
  - 사용자 인증
  - 서버와 사용자 사이의 원격 호스트와 중계 TCP 세그먼트의 게이트웨이 접촉 어플리케이션
- 각 어플리케이션에 대한 프록시 코드가 있어야 함
  - 어플리케이션 기능의 지원이 제한될 수 있음
- 패킷 필터 보다 안전한 경향
- 단점은 각 연결에 대한 추가 처리에 대한 오버헤드

서킷 레벨 게이트웨이

서킷 레벨 프록시

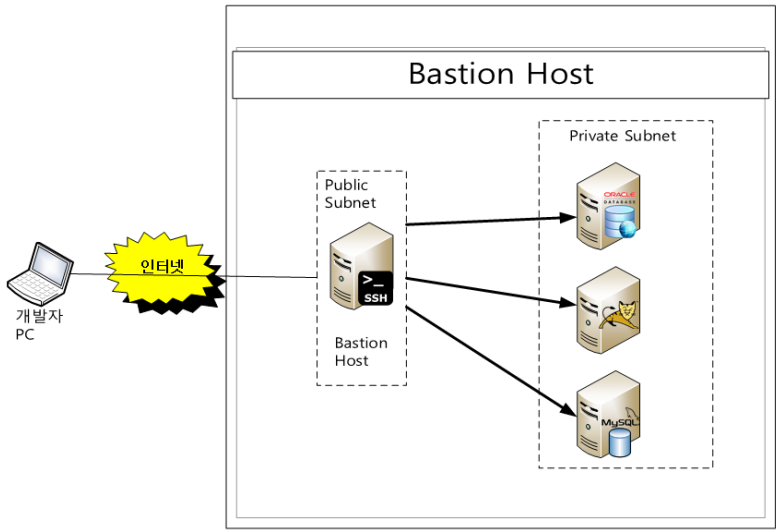
- 두 TCP 연결을 설정, 내부 호스트에 자체 TCP 사용자와 외부 호스트에 하나 사이에 설정
- 직접적인 end-to-end TCP 커넥션을 허용하지 않음
- 검사 컨텐츠 없이 다른 하나의 연결로부터 TCP 세그먼트를 중계
- 보안 기능은 연결 허용의 결정으로 구성
- 내용분석 X (응용레벨게이트웨이와 다른점임)

내부 사용자가 신뢰할 수 있을 때 일반적으로 사용

- 어플리케이션 계층 게이트웨이 인바운드와 서킷 레벨 게이트웨이 아웃바운드에 이용할 수 있음
- 낮은 오버헤드

베스천 호스트

- 시스템 식별은 네트워크 보안의 중요한 장점
- 어플리케이션 계층 또는 서킷 레벨 게이트웨이의 플랫폼 역할
- 보호된 네트워크에 접근하기 위해 유일하게 외부에 노출되는 호스트
- 일반적인 특징:
  - 보안 O/S 실행, 필수적인 서비스만
  - 사용자 인증이 프록시 또는 호스트에 액세스할 수 있음
  - 각 프록시는 기능을 제한할 수 있고, 호스트에 액세스할 수 있음
  - 각 프록시는 작고, 간단하며, 보안을 검사
  - 각 프록시는 독립적, 비 특권(non-privileged)
  - 제한적인 디스크 사용, 따라서 읽기 전용 코드



호스트 기반 방화벽

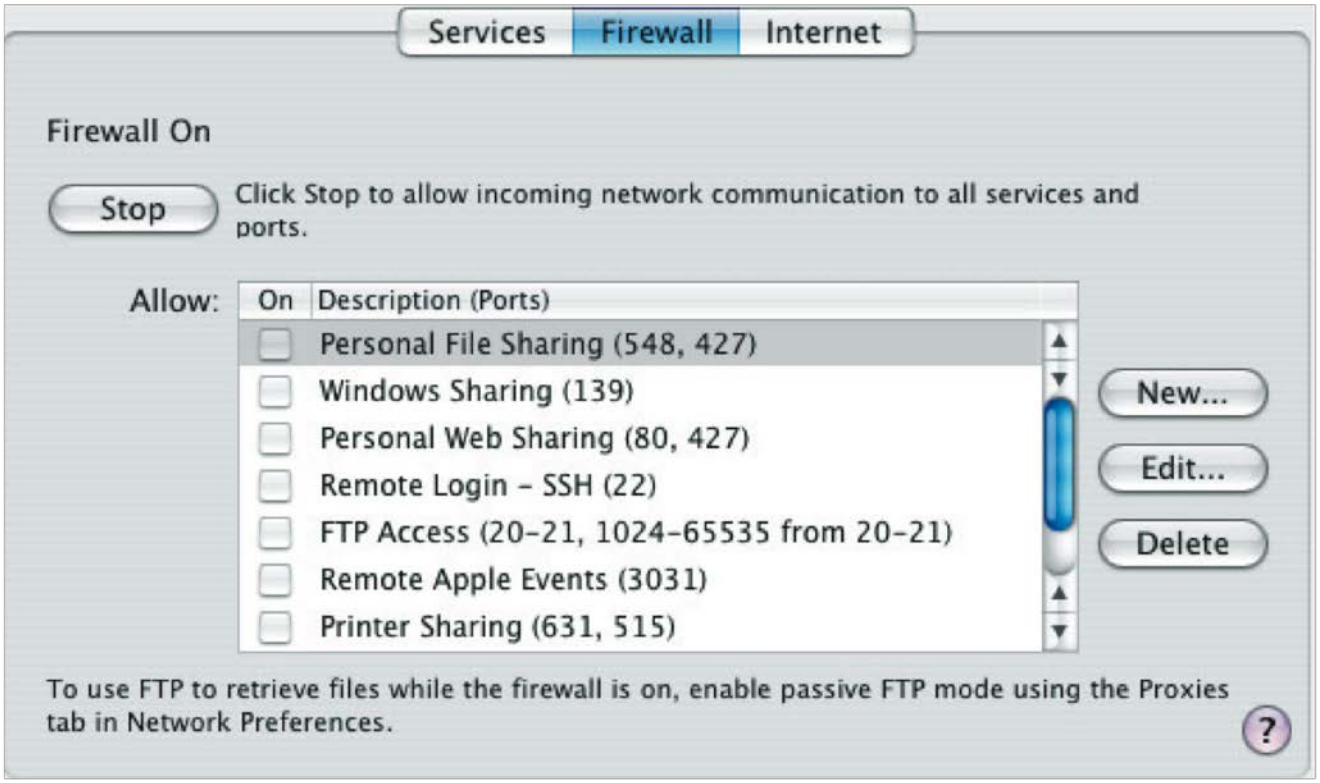
- 각각의 호스트를 보호하는데 사용
- 운영체제에서 사용하거나 부가적인 패키지형태로 제공할 수 있음
- 패킷의 흐름을 필터링하고 제한 함
- 일반적인 위치는 서버

장 점:
• 필터링 규칙을 호스트 환경에 맞출 수 있음 • 보호는 토폴로지에 독립적으로 제공 • 보호의 추가적인 레이어를 제공

개인 방화벽

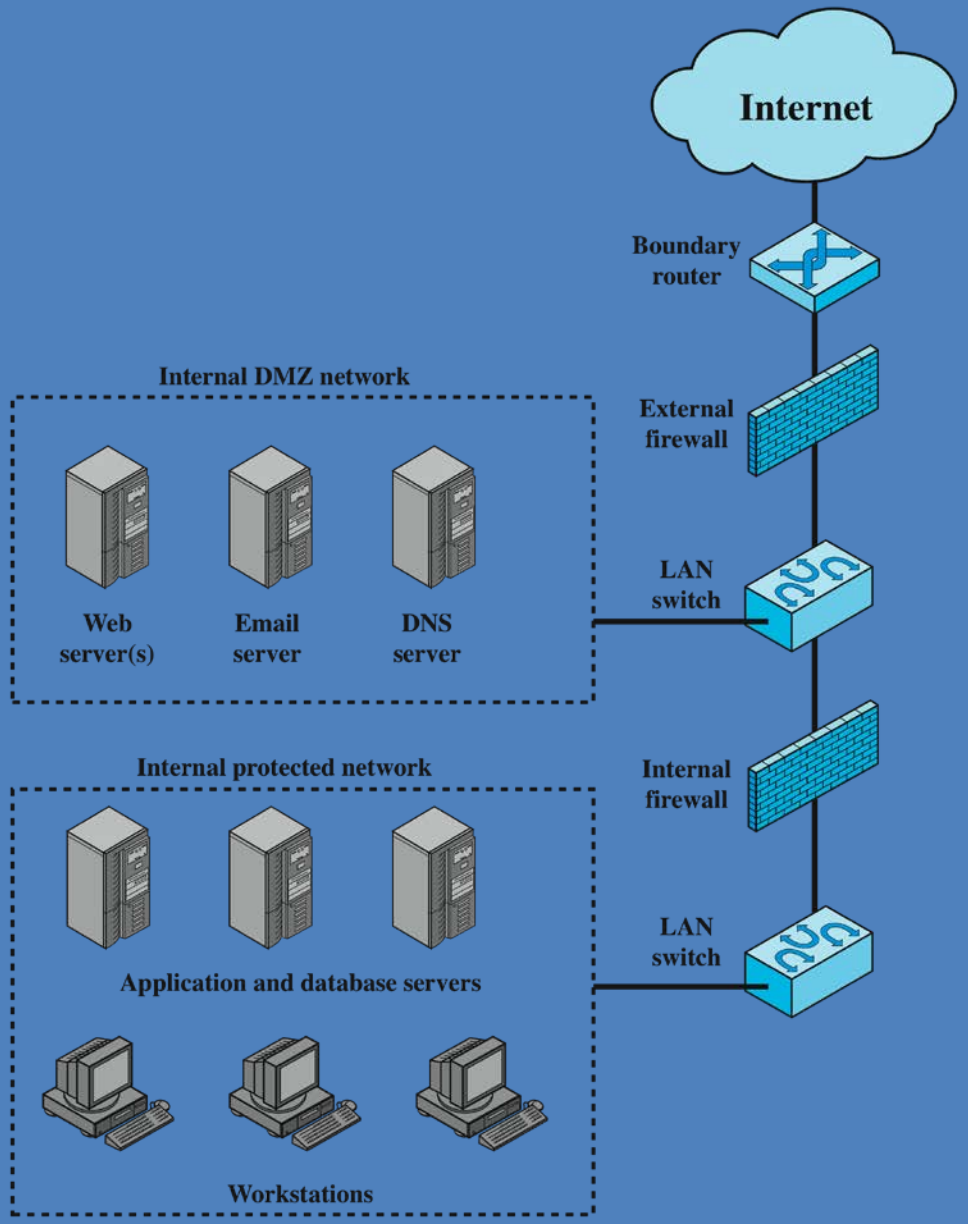
- 개인 컴퓨터 또는 워크스테이션과 인터넷 또는 기업 네트워크 간의 트래픽을 제어
- 가정이나 기업 모두가 사용할 수 있음
- 일반적으로 개인 컴퓨터의 소프트웨어 모듈임
- DSL , 케이블 모뎀, 또는 다른 인터넷 인터페이스에 연결된 홈 컴퓨터의 모든 연결에 위치할 수 있음
- 일반적으로 서버 기반 또는 독립형 방화벽보다 훨씬 덜 복잡함
- 주요 역할은 인증되지 않은 원격 액세스를 거부하는 것
- 또한, 나가는 트래픽의 모니터링으로 웜과 악성코드의 활동을 차단하고 탐지할 수 있음

개인 방화벽 인터페이스 예제



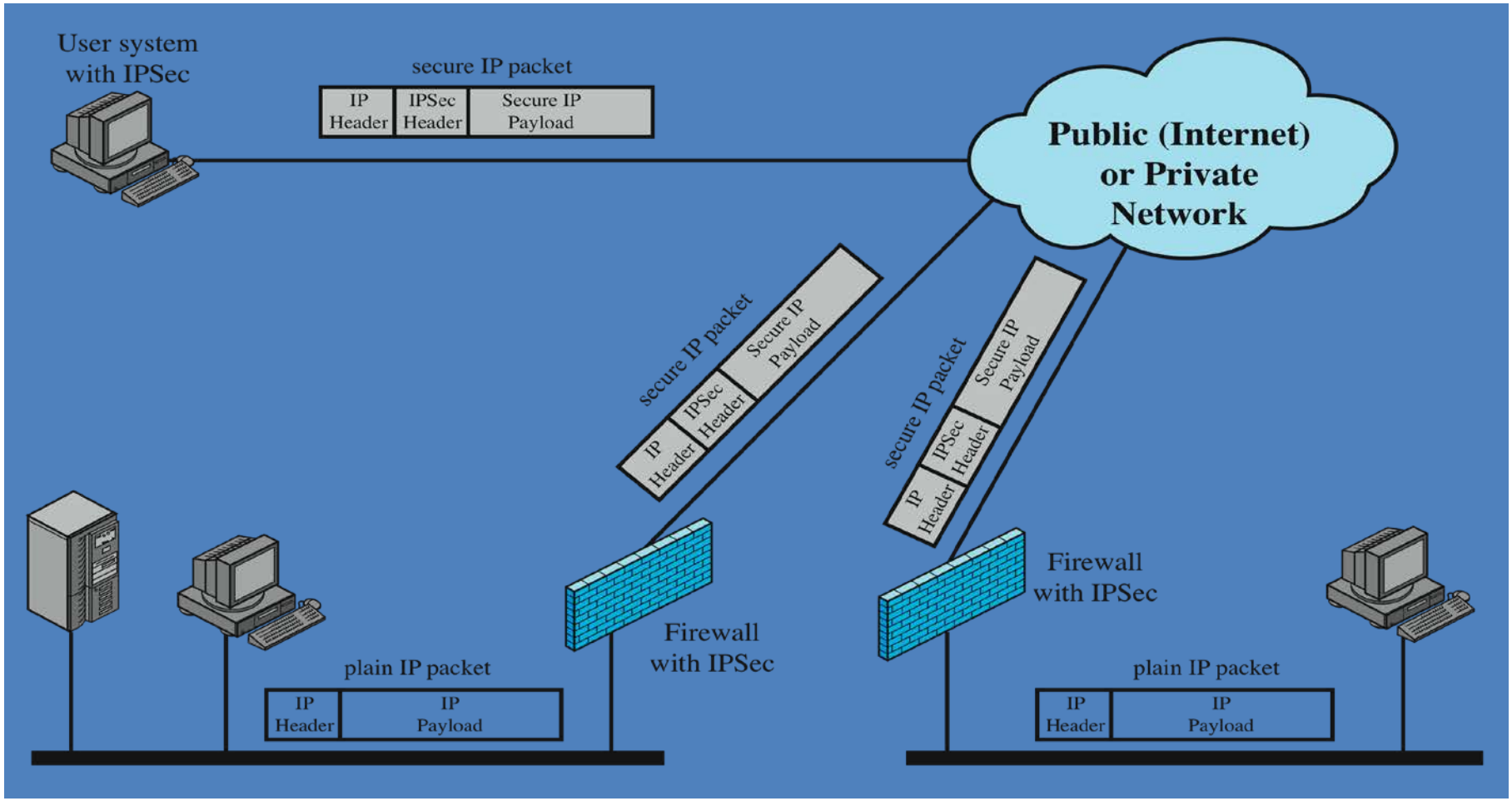
방화벽 구성 예제

- DMZ 네트워크 : 외부에서 접근할 수 있으나 특정 보호조치가 필요한 시스템들이 존재
- 내부 네트워크 : 내부 방화벽에 의해 보호, DMZ 시스템에 자리잡은 악성코드의 공격으로부터 방어



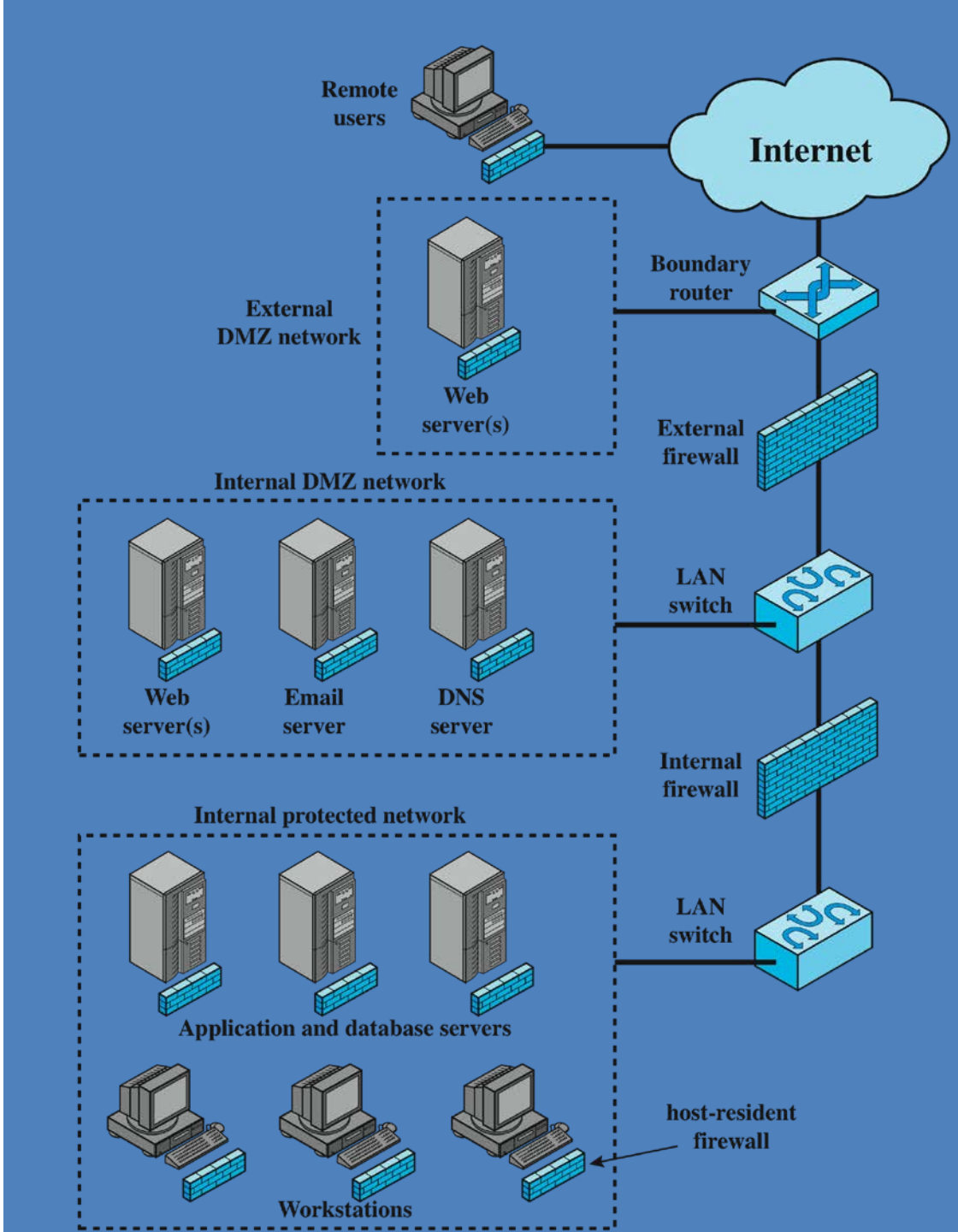
가상 사설 네트워크 (VPNs)

- 공공 네트워크를 이용하되, 하위 프로토콜 계층에서 암호화와 사용자 인증을 통해 안전한 연결 제공.
- 사설 네트워크보다 저렴



분산된 방화벽 구성 예제

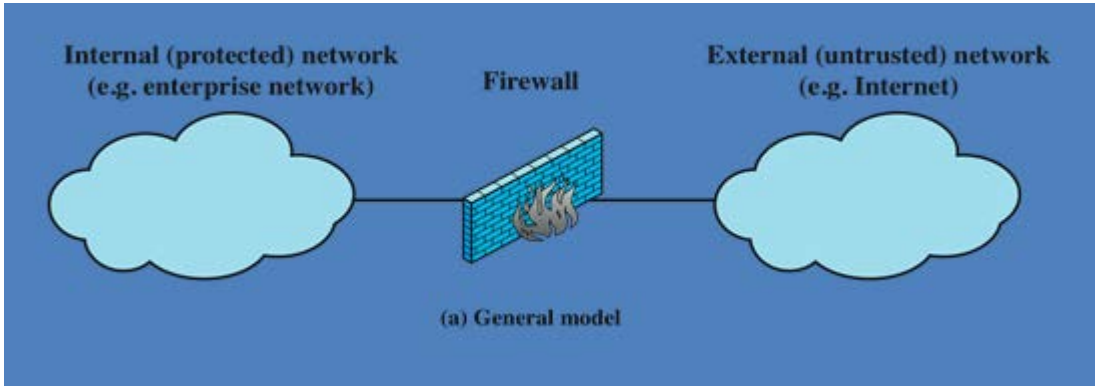
- Stand-alone 방화벽과 다수의 호스트 기반 방화벽으로 구성
- 관리자는 다양한 보안보안 모니터링 측면에서 효율적임

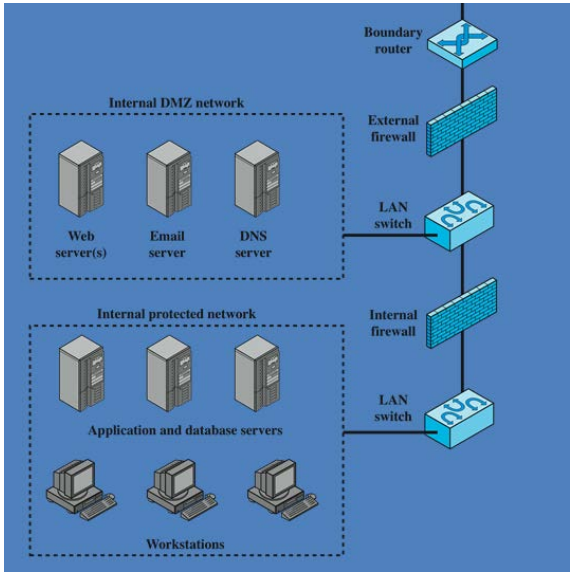


방화벽 토폴로지

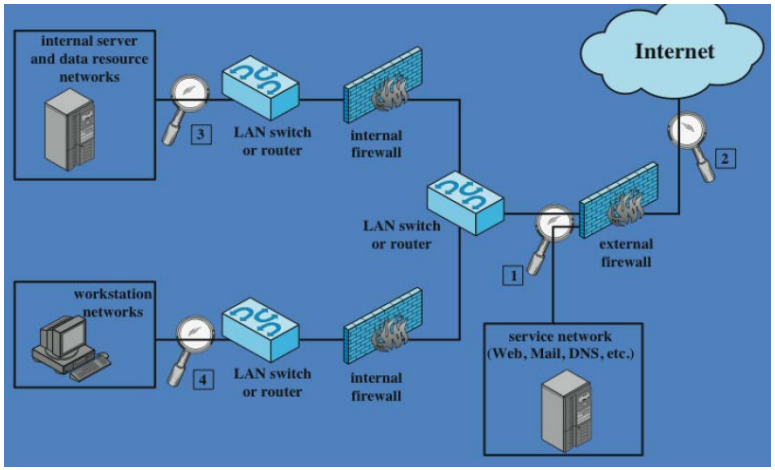
host-resident firewall	•개인 방화벽 소프트웨어와 서버의 방화벽 소프트웨어를 포함
screening router	•무상태(stateless) 또는 전체 패킷 필터링과 내부와 외부 네트워크 사이의 단일 라우터 •작은 사이즈 네트워크에 적합
single bastion inline	•내부와 외부 라우터 사이의 단일 방화벽 장치 •추가적인 네트워크 인터페잇호 가짐
single bastion T	•외부에서 볼 수 있는 서버에 위치한 DMZ에 배스천 의 세 번째 네트워크 인터페이스를 가짐
double bastion inline	•DMZ는 배스천 방화벽 사이에 끼어있음
double bastion T	•DMZ는 배스천 방화벽의 별도의 네트워크 인터페이스에 있음
distributed firewall configuration	•대형 기업 및 정부 기관에서 사용

Bastion inline 구조





Bastion T 구조



침입 방지 시스템 (IPS)

- 보안 제품에 최근에 추가
  - 트래픽을 차단할 수 있는 인라인 네트워크 기반 IDS
  - 방화벽에 IDS 기능을 더한 기능적 추가
- 방화벽과 같이 트래픽을 차단 할 수 있음
- IDS의 개발 알고리즘을 사용
- 네트워크 또는 호스트 기반으로 할 수 있음

호스트 기반 IPS (HIPS)

- 서명(signature)과 이상 탐지 기술을 이용한 공격 식별
  - 서명(signature): 초점은 패킷안에 어플리케이션 페이로드의 특정 컨텐츠에 악성으로 식별된 패턴을 찾는 것
  - 이상(anomaly): IPS는 악성코드를 나타내는 행동 패턴을 찾는 것
- 특정 플랫폼에 맞게 할 수 있음
- 또한 행위 모니터링을 위해 샌드박스 방법을 사용할 수 있음

장점
• **다양한 도구들은 밀접하게 작업** • **위협 방지는 보다 포괄적** • **관리가 쉬움**

네트워크 기반 IPS (NIPS)

- 패킷의 폐기와 TCP연결의 분해의 권한을 갖고 있는 인라인 NIDS
- 서명과 이상탐지를 이용
- 플로우 데이터 보호를 제공할 수 있음
  - 전체 어플리케이션 플로우 컨텐츠를 모니터링
- 악의적인 패킷을 이용하여 식별 가능:
  - 패턴 매칭
  - 상태기반 매칭
  - 프로토콜 이상(anomaly)
  - 트래픽 이상(anomaly)
  - 통계적 이상(anomaly)

Snort 인라인

- Snort는 Inline 동작을 통해 침입 방지 기능 수행이 가능
- Snort 사용자는 패킷 수정보다 그것들을 드롭시킬 수 있는 대체 옵션을 포함
  - 허니팟 구현에 유용
  - 공격자는 실패를 볼 수 있지만 발생한 이유는 알 수 없음