# 파이어월

# 파이어월

- premises network (**자체 네트워크**)**과 인터넷 사이에 배치되어 경계**(perimeter)**를 형성**
  - On-premise : **클라우드 이용과 반대**, **자체 전산실 서버에 직접 설치해 운용**

| 비즈니스 요구 | 온프레미스 | 퍼블릭 클라우드 |
|---|---|---|
| 데이터 센터 단일 테넌트(컴플라이언스용) | O | X |
| 매우 안전한 데이터 암호화 | O | O |
| 맞춤형 하드웨어, 특수 목적의 시스템 | O | X |
| 용량을 손쉽게 확장 및 축소 가능 | X | O |
| 인프라에 대규모의 정기적인 투자 필요 | O | X |
| 종량제 결제, 사용량 기반 가격 책정 | X | O |
| 완전한 데이터 가시성 및 관리 권한 | O | X |
| 내장형의 자동화된 데이터 백업 및 복구 | X | O |
| 제로에 가까운 중단 시간 위험 | X | O |

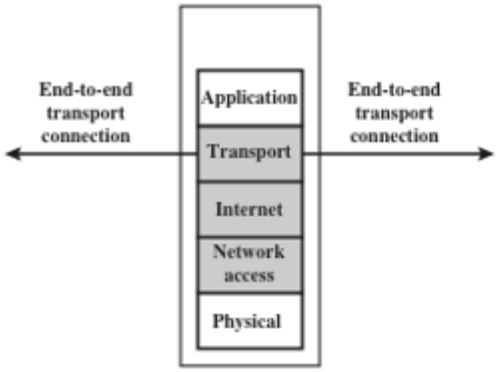
- perimeter **는** Internet-based attacks**을 방어하는** a single choke point
- a single computer **또는** a set of two or more systems

# 파이어월 정책

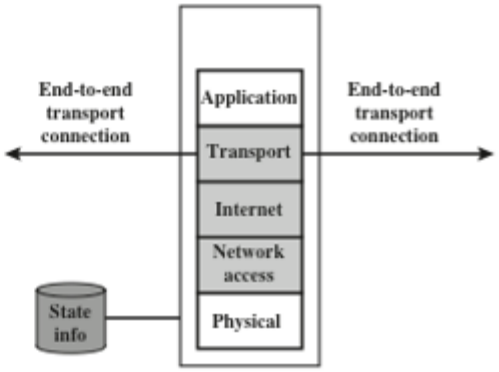
- IP Address and Protocol Values
  - source or destination addresses and port numbers
  - direction of flow
- Application (Protocol)
  - **허용하는 프로그램**
- User Identity
  - IPSec **등의 인증 메커니즘과 결합하여 사용자** id **기반 접근** : **일반 접근제어**
- Network Activity
  - **시간 대 등**

# 파이어월 종류

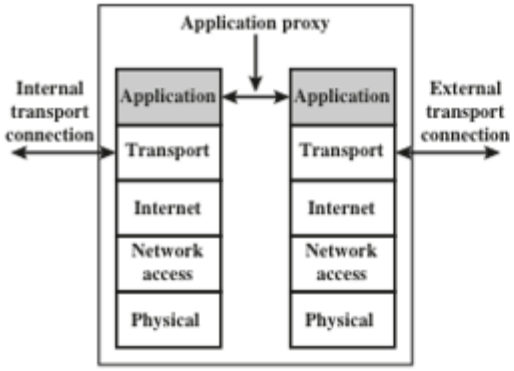




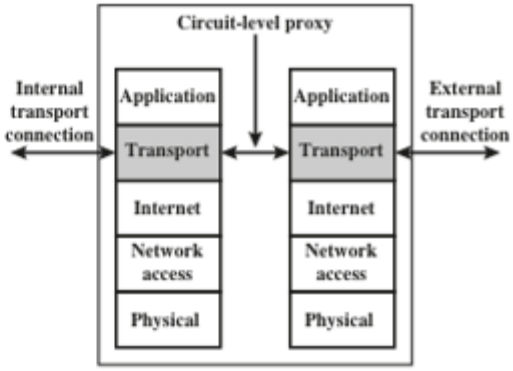

(b) Packet filtering firewall




(c) Stateful inspection firewall




(d) Application proxy firewall

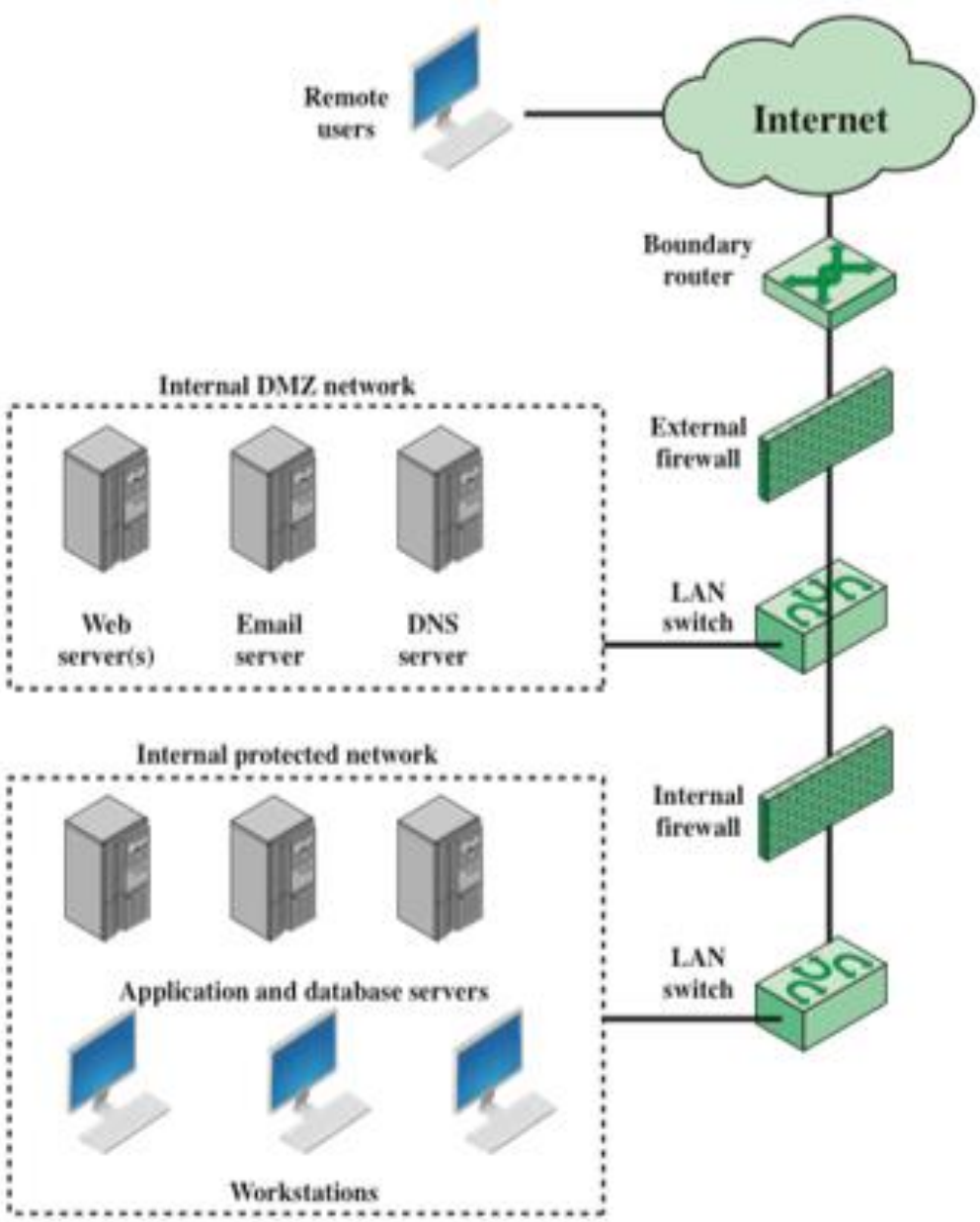



(e) Circuit-level proxy firewall

# BASTION HOST

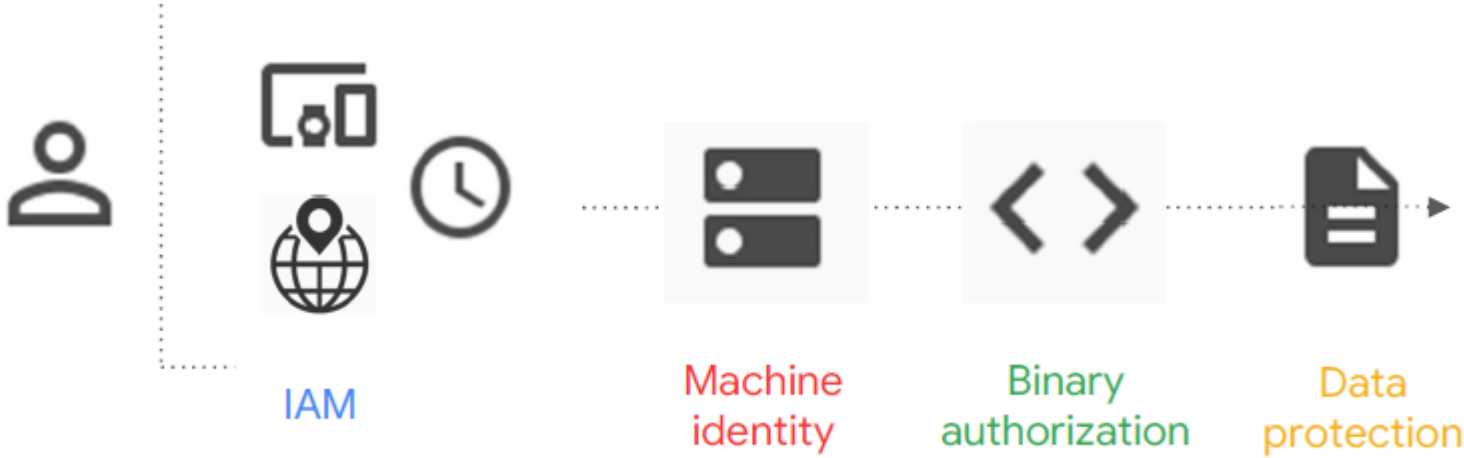
- application-level or circuit-level proxy
- **특징**
  - Secure OS**에서 동작**
  - **네트워크 관리자만 이용**
  - **각** proxy**는 일부 기능 만 수행**
  - **각** proxy**는 일부 서버만 담당**
  - Audit**을 강화**, **모든** traffic**을 로깅 하는 등**

# 파이어월 구성 예


Remote users
Internet
Boundary router
Internal DMZ network
External firewall
LAN switch
Web server(s)
Email server
DNS server
Internal protected network
Internal firewall
LAN switch
Application and database servers
Workstations

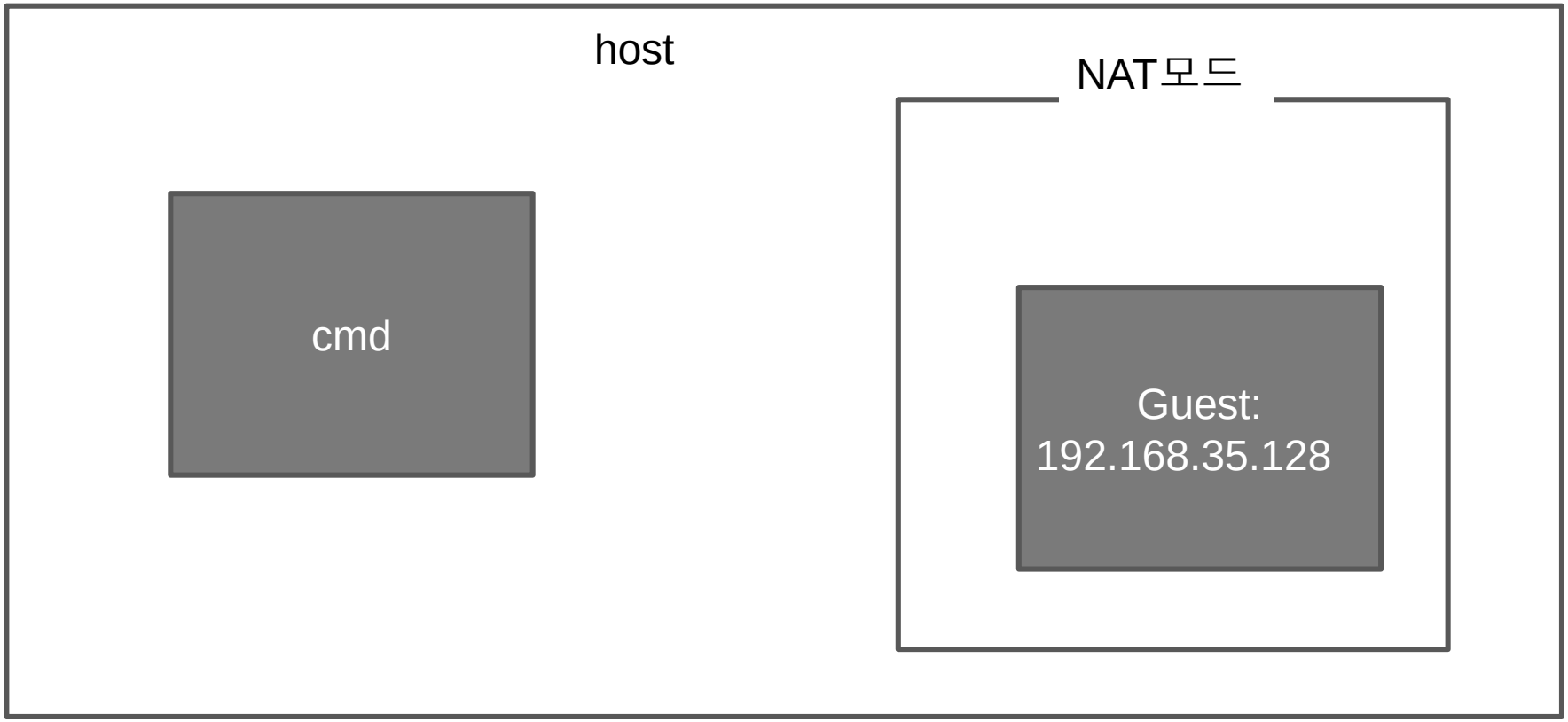
# 제로 트러스트

- Perimeter **보안과 반대**
- **모든 접근에 대해 (강화된) 인증과 접근제어 + 플랫폼 보안**




# 파이어월 실습

# 가상머신 네트워크 구조



# FTP

- ftp login inbound

  $ sudo apt install vsftpd

  $ sudo systemctl start vsftpd

  $ sudo systemctl enable vsftpd

  - Test

```
sean@ubuntu:~/Desktop$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:sean):
```

  - **윈도우**

```
C:₩Users₩user>ftp 192.168.33.128
192.168.33.128에 연결되었습니다.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
사용자(192.168.33.128:(none)):
```

# FIREWALL 기본

- **상태**

  $ sudo su

  # ufw status verbose

- **시작**

  # ufw enable

  ☞ **윈도우에서 ftp 접속 시도 :실패**

- **정책 조회**

  # ufw show raw

# FIREWALL 기본

- **허용과 차단**

  # ufw allow 21

  # ufw status verbose

  ☞ 21**번 허용 후** ftp **접속 다시 시도** : **성공**

- Default rule

  # ufw default deny

# 규칙

- **조회**

  # ufw show raw | grep 21

  **또는**

  # ufw status verbose

- **번호 조회**

  # ufw status numbered

- **규칙의 삭제**

  # ufw delete 1

- **전체 삭제** = inactive

  # ufw reset

  # sudo ufw enable  # inactive -> active

# 규칙

- **서비스 명으로 허용**

  # ufw allow ftp  ( 21/tcp )

- **상충되는 규칙 : 덮어 씀**

  # ufw deny 21/tcp

- **범위가 다른 규칙: 번호가 낮은 규칙이 적용됨**

```
     To                         Action      From
     --                         ------      ----
[ 1] 21                         DENY IN     Anywhere
[ 2] 21/tcp                     ALLOW IN    Anywhere
```

# FROM, TO

- **포트번호 범위**

  # ufw allow 21:30/tcp  #  tcp port  21~30

- **특정 IP 만 허용**
  - ufw allow from <ip address> to <protocol> port <port number>

    # ufw allow from 192.168.33.1  to any port 21

- Rule**을 낮은 번호로** insert

  # ufw insert 1 allow from 192.168.33.1  to any port 21

- **과제** 1: reset **후에**  enable

  # ufw deny 21 **실행 후**

  ftp (tcp) **접속을 허용하도록** rule **추가 후**

  rule **조회**
  - **상기 명령 전체 실행 화면을 캡처** 1.jpg

# APP

- App list

  # ufw app list

  # ufw allow CUPS  # list**에 포함된** app

- App **편집** : /etc/ufw/applications.d/app**이름**

```
[vsftp]
title=vsftp
description=vsftp
ports=21/tcp
~
```

- **반영**

  # ufw reload

- App **단위 허용**

  # ufw allow vsftp