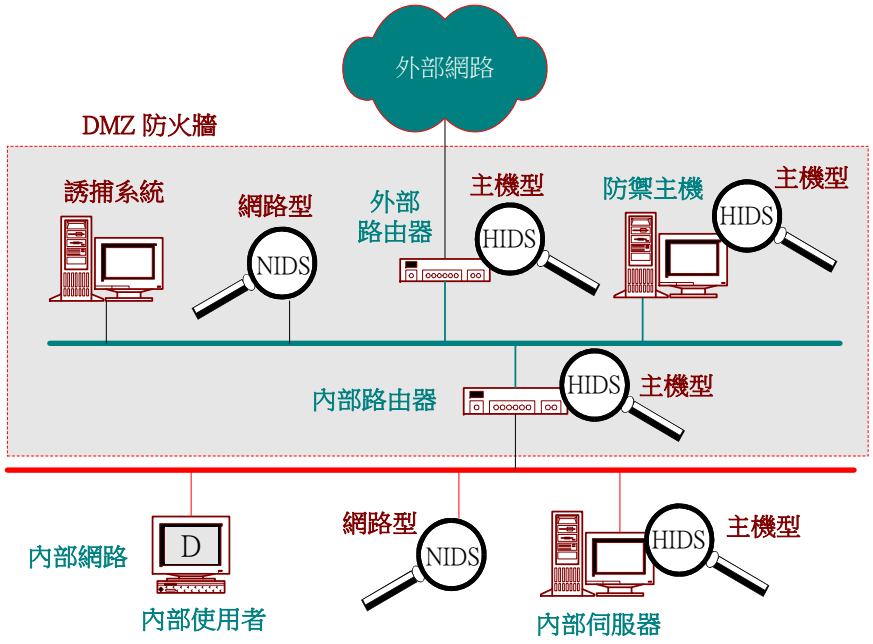
主機型入侵偵測系統－伺服主機

伺服主機入侵偵測

- 系統日誌
  - Lastlog、xferlog、httpd、syslogd、klogd、message
- 安全稽核 ：如, Windows Server

日期	時間	使用者名稱	電腦名稱
事件 ID	來源	型態	類別
事件描述及建議解決方法			
額外資料			



主機型入侵偵測系統－伺服主機

- 伺服主機入侵偵測
  - 主機阻斷偵測
    - 毀滅性攻擊
      - 直接格式化磁碟機
      - 刪除重要檔案
      - 關掉電腦電源
      - 切斷網路連線
    - 過載攻擊
      - 行程攻擊（Process Attack）
      - 磁碟攻擊（Disk Attack）