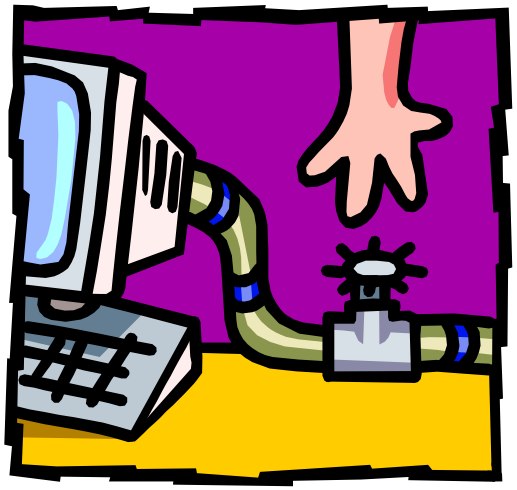
네트워크 보안관리

최근들어, 해킹의 위협은 **UNIX** 혹은 **NT** 서버 뿐만 아니라 포트스캔 및 취약점 검사 등 네트워크 대상으로 이루어지고 있는 실정이다.

이 과목에서는 네트워크의 보안 서비스 및 보안위협 요소와 보안대책에 대하여 다루고 있다.

목 차



Information Security

- **What is a/an (information) security ?**
  - "The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional." *[Information Warfare, July 1996]*
    - 인가되지 않은 정보의 누출, 전송, 수정, 파괴 등으로부터 보호

- **Information Security Objectives**
  - "The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failure of **availability, confidentiality, and integrity**." [OECD 1992]

네트웍 보안서비스

- 네트웍 보안의 목표
  - 비밀성(Confidentiality)
    - Unauthorized access 혹은 inappropriate disclosure로부터 보호
  - 무결성(Integrity)
    - Unauthorized modification or destruction으로부터 보호
  - 가용성(Availability)
    - Denial of service and available in a timely.
  - 신뢰성(Reliability)
  - 접근통제(Access Control)
  - 식별(Identification) & 인증(authentication)
  - 책임추적성(accountability)

Threat against Confidentiality

- **Unauthorized Disclosure**
  - Accidential disclosure may be caused by users, operators, data preparation, output errors, system errors, or communications errors.
  - Violation of established access control procedures
  - Malicious actions taken by personnel
  - Active attempts by authorized personnel to gain access to sensitive information.

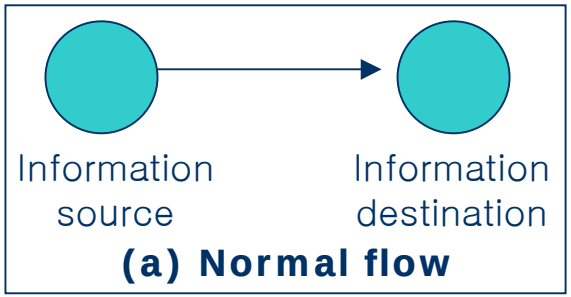
Threat against Integrity

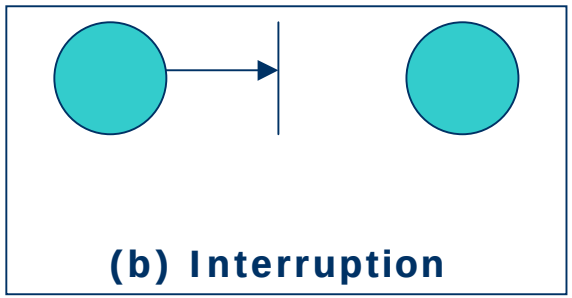
- **Unauthorized Modification**
  - Personnel actively working to sabotage or distrupt network operations/services.
  - Personnel who accidentally interface with network operations/services.
  - External personnel

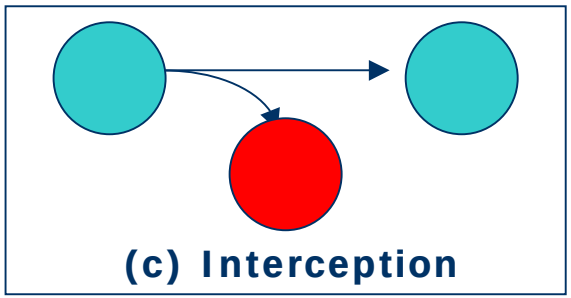
Threat against Availability

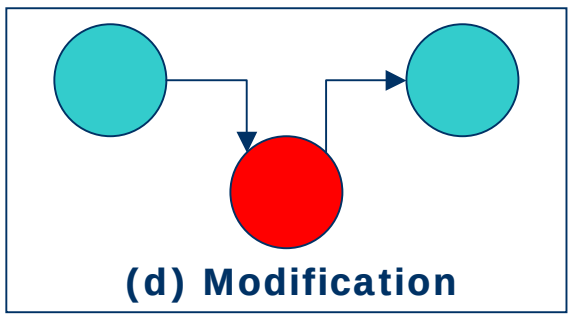
- **Denial of service**
  - Physical destruction of networking segments or subnetworks.
  - Interoperability of networking segments or subnetworks du to equipment malfunction, software failures, or sabotage.
  - Degradation of performance from system saturation, link or bit error rates, or external factors(i.e., weather)
  - Authorzied users prevented physical acess to networking equipment and services
  - Any other condition that results in nonavailability of networking resources to valid users.

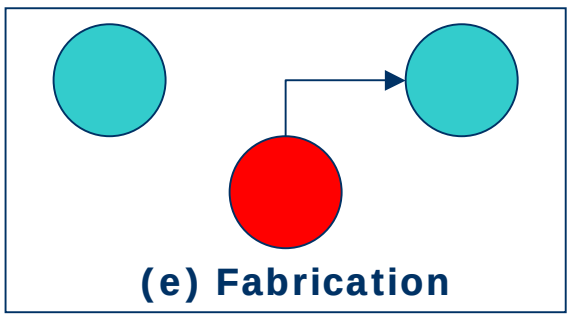
네트워크 보안 위협요소







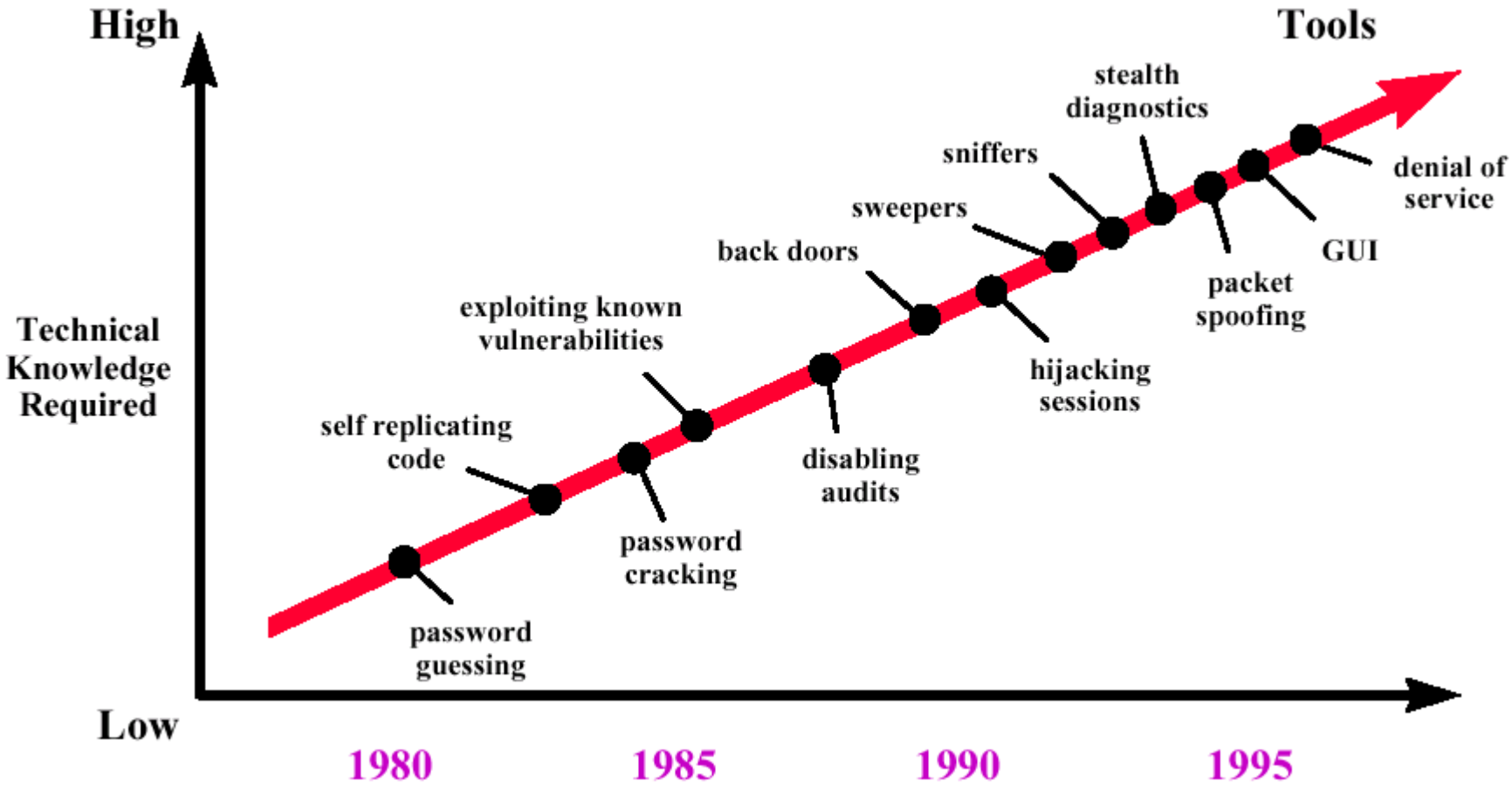




네트워크 보안 위협요소

- **ISO 7498-2** 에서 분류한 보안위협
  - 위장(Masquerade)
  - 불법적인 연합/연대(Illegal association)
  - 비 인가된 접근(Non-authorized access)
  - 정보의 누출(Leakage of information)
  - 정보 전송량 분석(Traffic analysis)
  - 데이터 수정 또는 파괴(Data modification or destruction)
  - 메시지 순서 변경(Invalid message sequencing)
  - 부인(Repudiation)
  - 서비스 방해(Denial of Service)

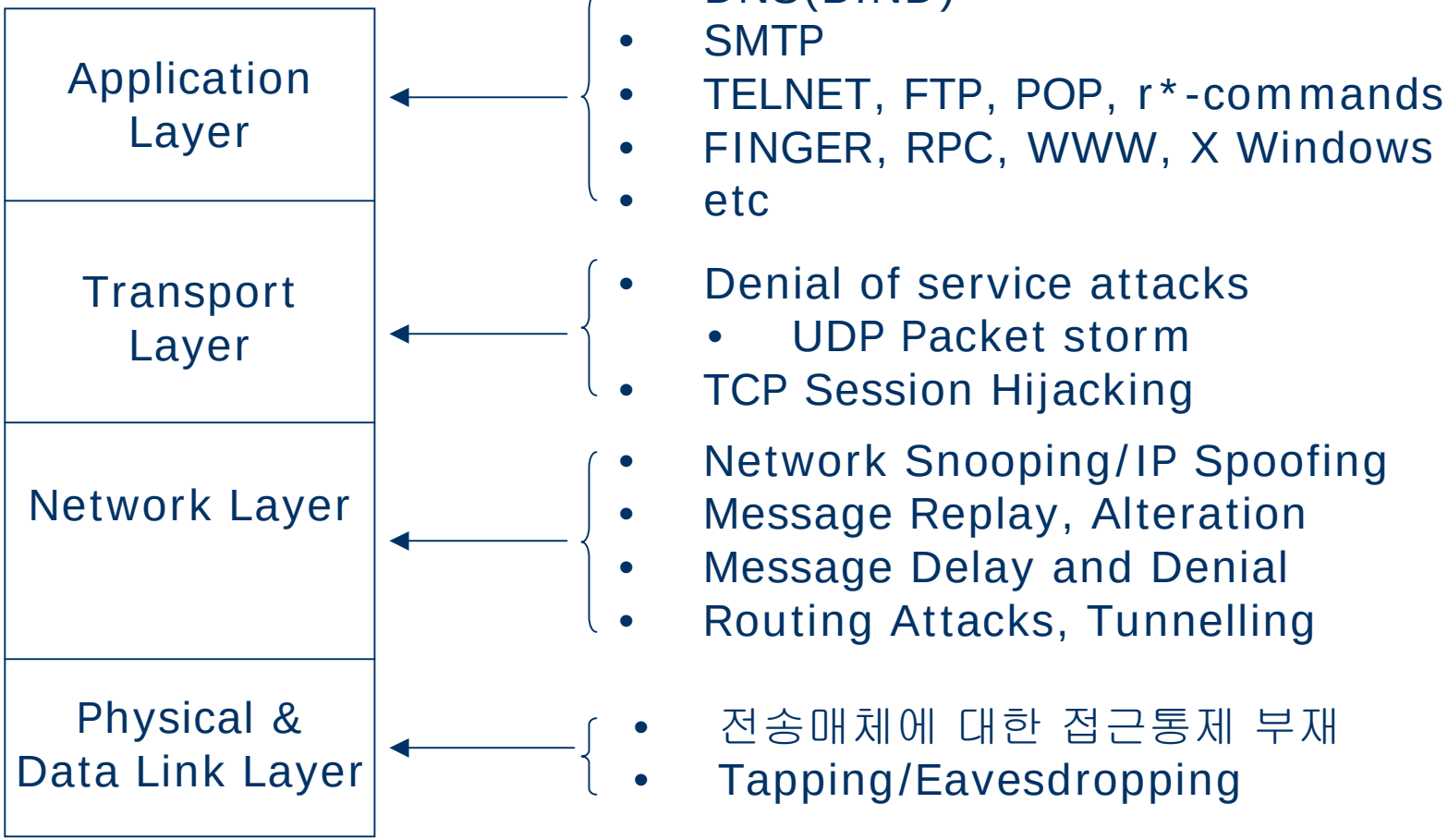
Intrusion Techniques



네트워크 보안취약점

- 네트워크 보안취약점
  - 물리적 보안취약점(tapping/traffic flow)
  - TCP/IP 프로토콜 설계 및 구현상의 취약점
  - 적절하지 못한 자원공유 및 접근제어
  - 네트웍 서버(서비스)의 취약점 및 강력한 인증서비스의 부재
  - 단일화된 보안관리의 어려움
- 네트워크 취약점 공격기법
  - 네트웍을 통한 정보수집
    - 포트스캔(port scanning), 취약점스캔(vulnerability scanning)
  - 네트웍 패킷 분석/변조
    - 스니핑(sniffing), 스푸핑(spoofing), Session Hijacking
  - 네트웍 서버 공격(데몬 프로세스의 버그 이용)
  - DoS/DDoS 공격

TCP / IP 보안취약점



Network/Port Scanning

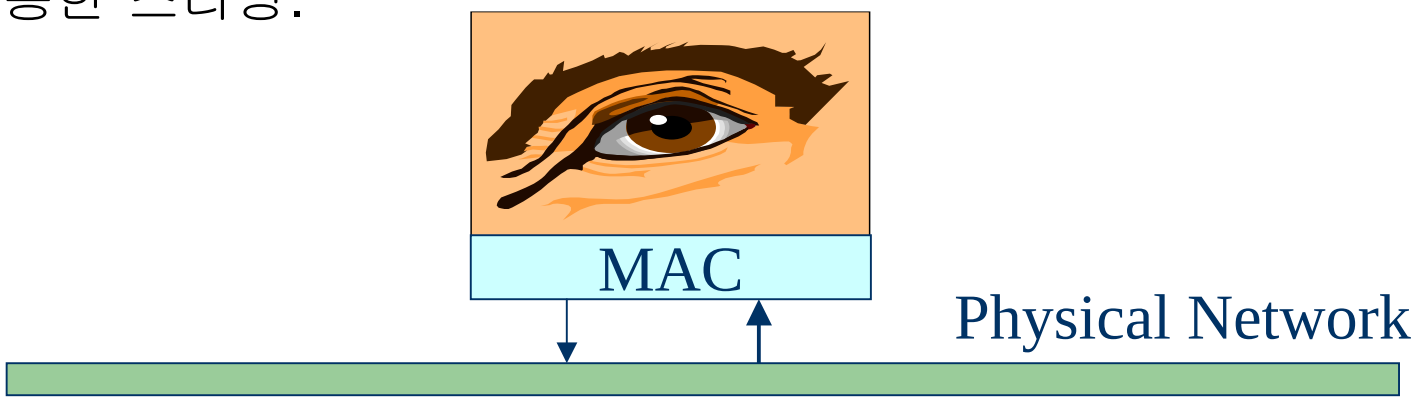
- **Ping sweeps**
  - to find which machines are alive
- **TCP scans**
  - looking for services the intruder can exploit
- **UDP scans**
  - to send a gabage UDP packet to the desired port.
  - Most machines will response with an ICMP “destination port unreachable” message.
- **OS identification/detection**
  - sending illegal(or strange) ICMP or TCP packets.
- **Account scan**

Vulnerability Scanning

- 네트웍 기반의 취약점 탐지 도구
  - ISS(Internet Security Scanner)
  - SATAN(Security Administrator's Tool for Analyzing Networks), SAINT
  - Vulnerable CGI Scanner

Packet Sniffing

- **Shared medium**
  - Ethernet/FDDI 등은 전송매체를 공유한다.
  - 동일 세그먼트의 모든 호스트는 네트웍 트래픽을 볼 수 있다.
- **Server sniffing**
  - On switched networks
- **Remote sniffing**
  - Network bandwidth가 낮은 경우, RMON enabled hosts를 이용한 스니핑.



Remote Attacks

- **What are some common exploits?**
  - CGI scripts
  - Web Server attacks
  - Web Browser attacks
  - SMTP(Sendmail) attacks
  - Access(login, file access, password cracking, etc)
  - IMAP, POP
  - IP Spoofing
  - Buffer Overflows
  - DNS attack
  - etc.,

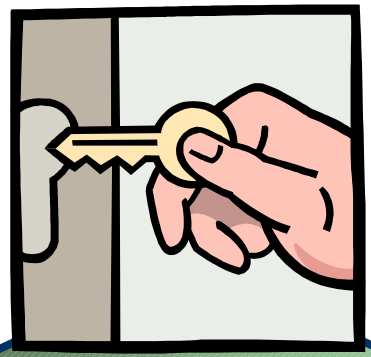
Buffer Overflow

- **What is a buffer overflow attack ?**
  - 버퍼의 길이보다 더 큰 문자열 데이터를 입력할 경우, 스택 프레임의 중요자료구조(stack frame pointer / return address)를 변경하여 임의의 주소로 점프, 임의의 명령을 수행시키는 것이 가능하다.
  - 이러한 문제는 C/C++로 작성된 프로그램에서 흔히 발생한다. 왜냐하면, 버퍼의 경계검사(boundary check)를 수행하지 않는다.
  - DNS overflow
  - statd/mountd overflow
  - POP

DoS/DDoS

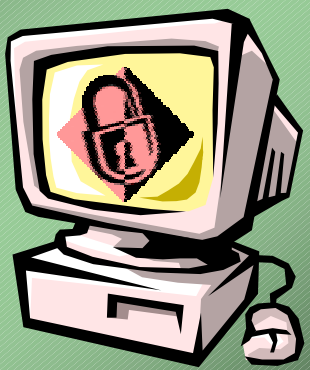
- **Ping-of-Death**
  - Sends an invalid fragment, which starts before the end of packet, but extends past the end of packet.
- **SYN Flood**
  - Sends TCP SYN packet(which start connections) very fast.
- **Land/Latierra**
  - Sends forged SYN packet with identical source/destination address/port.
- **WinNuke**
  - Sends OOB/URG data
    on a TCP connection
    to port 139(NetBIOS Session/SMB).

네트워크 보안대책



물리적 보안대책

기술적 보안대책



관리적 보안대책

Objectives

- 네트웍 보안**(Protection)**의 목표
  - Avoidance
  - Prevention
  - Detection
  - Containment & Response
  - Recovery
  - Improvement

관리적 보안대책

- **Developing a network scurity policy**
  - What resources are we trying to protect?
  - Which people do we need to protect the resources from?
  - How likely are the threats?
  - How important is the resource?
  - What measures can be implemented to protect the resource?
  - How cost effectively and in what time frame can these be implemented?
  - Who authorises users?
- **Security Strategy**
  - Everything is forbidden unless explicitly permitted.
  - Everything is permitted unless explicitly forbidden.

Security Policy

- **Network Service Access Policy**
  - higher-level, issue-specific policy
    - Allow no access to a site from the Internet, but allow access from the site to the Internet; or, in contrast,
    - Allow some access from the Internet, but only to selected systems such as information servers and e-mail servers.
- **Firewall Design Policy**
  - lower-level policy
    - Permit any service unless it is expressly denied; or
    - Deny any service unless it is expressly permitted.
- **System Specific Policies**

물리적 보안대책

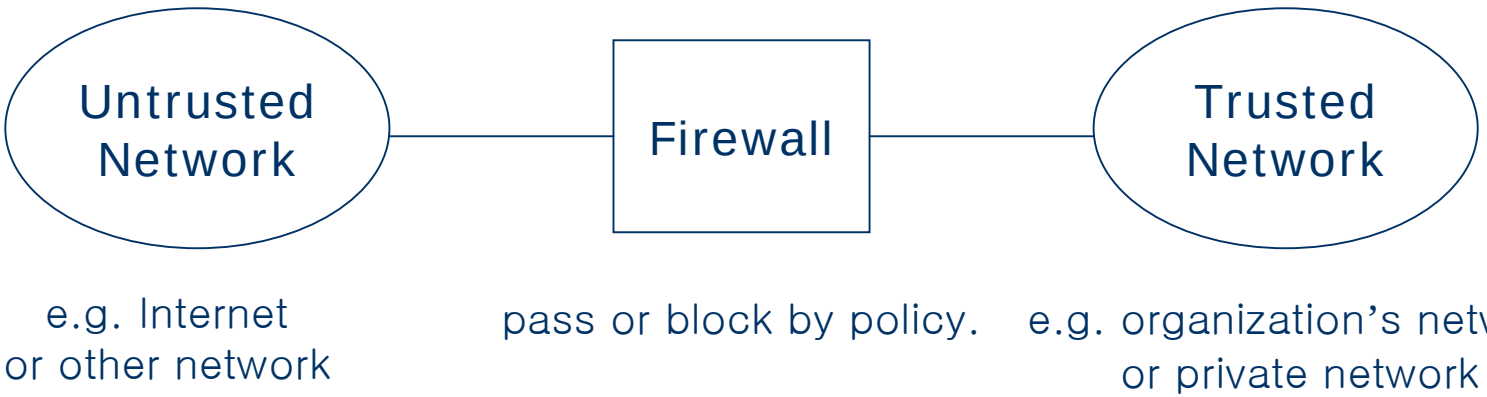
- **Objectives of physical layer security**
  - 전송매체에 대한 접근통제
  - to protect the entire physical service data bit stream
  - to provide traffic flow confidentiality.
    - connection confidentiality and traffic flow confidentiality
  - The primary mechanism that applies to the physical layer to implement these services is *total encipherment of the data stream*.

기술적 보안대책

- 침입예방 및 회피(Prevention & Avoidance)
  - 위험분석(자산/위협인식), 위험관리
  - 취약점 탐지 및 보안패치를 통한 취약점 제거
  - 불필요한 서비스 제거
- 침입탐지(Detection & Response)
  - 침입 흔적을 조사(log audit) 및 실시간 모니터링(real-time monitoring)을 통하여 사전/사후 침입탐지
- 침입차단(Protection)
  - Limit unauthorized access from the public network(internet)
- VPN(Encryption & Authentication)
  - 암호화 통신, 강력한 인증절차
- IPSec, PKI

침입차단시스템(Firewall)

- 침입차단시스템(Firewall)이란?
  - 외부 사용자들이 내부 네트워크에 접근하지 못하도록 하는 장치
  - 라우터나 패킷 필터링, 프록시(Proxy) 소프트웨어가 수행중인 독립 시스템 또는 전용 하드웨어를 이용



침입차단시스템(Firewall)

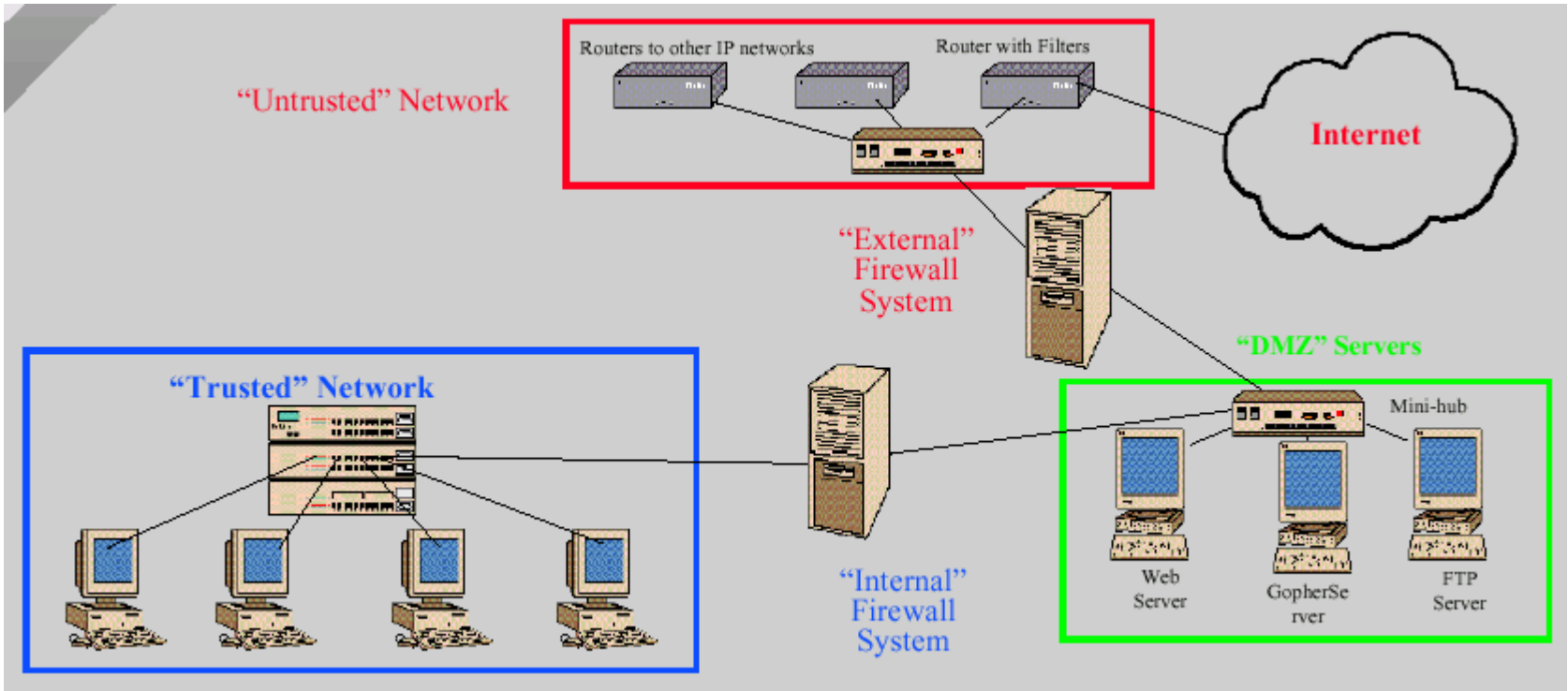
- **What can a firewall do?**
  - A firewall can enforce security policy.
  - A firewall cna log activity effectively.
  - A firewall can limit your exposure to the untrusted network.
  - A firewall can be a focus for security decisions – a choke point.
- **What can't a firewall do?**
  - A firewall can't protect against malicious insiders.
  - A firewall can't protect against connections that don't go through it.
  - A firewall can't protect against completely new threats if the security strategy is different from "deny everything unless specifically permitted."

침입차단시스템(Firewall) 보안관리

1. **Preparation**
   1. risk assessment, training, etc → Security Policy
2. **Specification and Procurement**
   1. 보안정책을 준수하면서, 요구사항을 만족시킬수 있는 방화벽 하드웨어 및 소프트웨어의 선택단계
   2. “상용 방화벽 제품을 구매할 것인지, 직접 구현할 것인지?” 를 결정
      1. 주어진 요구사항과 예산에 따라 적절한 제품 및 서비스를 선택
3. **Installation**
   1. 설치 및 설치 후 테스트
4. **Maintenance**
   1. 주기적인 시스템 패치 및 업데이트
   2. 정기적으로 logging & auditing
   3. 네트워크 사용 환경의 변화에 따라 새로운 configuration 설정
5. **Re-evaluation**
   1. 새로운 보안위협요소 및 취약점에 대하여 신속한 대응
   2. Firewall 메일링 리스트 구독 및 보안 포털 사이트 모니터링

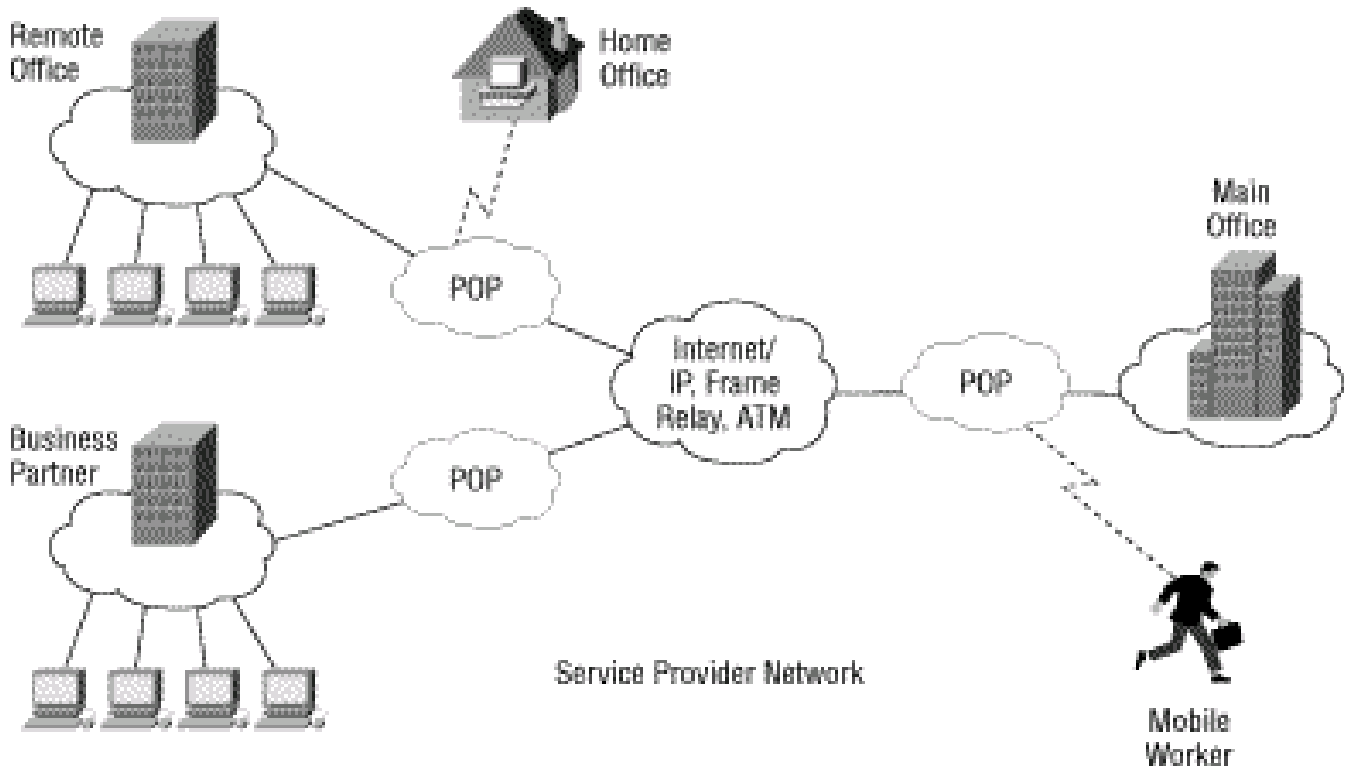
The Best Network Security

- **Tiered("layered") network security architecture provides the best security facilities.**



가상사설망(VPN)

- **VPN(Virtual Private Network)**이란?
  - 공중망(public network)을 통해 '안전하게' 통신할 수 있는 사설망으로 개개인과 사설망, 리모트 LAN과 사설망 사이에 위치



가상사설망(VPN)

- **VPN** 시스템의 기능
  - 암호화(Encryption)
  - 강력한 사용자 인증 및 메시지 인증(Strong Authentication)
  - mechanisms for hiding or masking information

- **VPN** 시스템의 종류 및 기능
  - Hardware-based VPN systems
    - encrypting routers,highest network throughput
  - Firewall-based VPNs
    - 내부 네트웍 접근제한을 비롯한 방화벽 보안메커니즘 이용
  - Standalone VPN application packages
    - VPN의 양단이 동일한 기관에 의해 통제되지 않는 상황에서 적합

VPN: pros and cons

- **Advantages**
  - the ability to securely connect high speed remote users over broadband technology
  - no administrative headache for managing direct access telephone lines
  - potential cost savings
- **Disadvantages**
  - potentially lower bandwidth avaiable to remote users
  - inconsistent remote access performance du to changes in Internet connectivity
  - No entrance in to the network if the Internet connection is broken

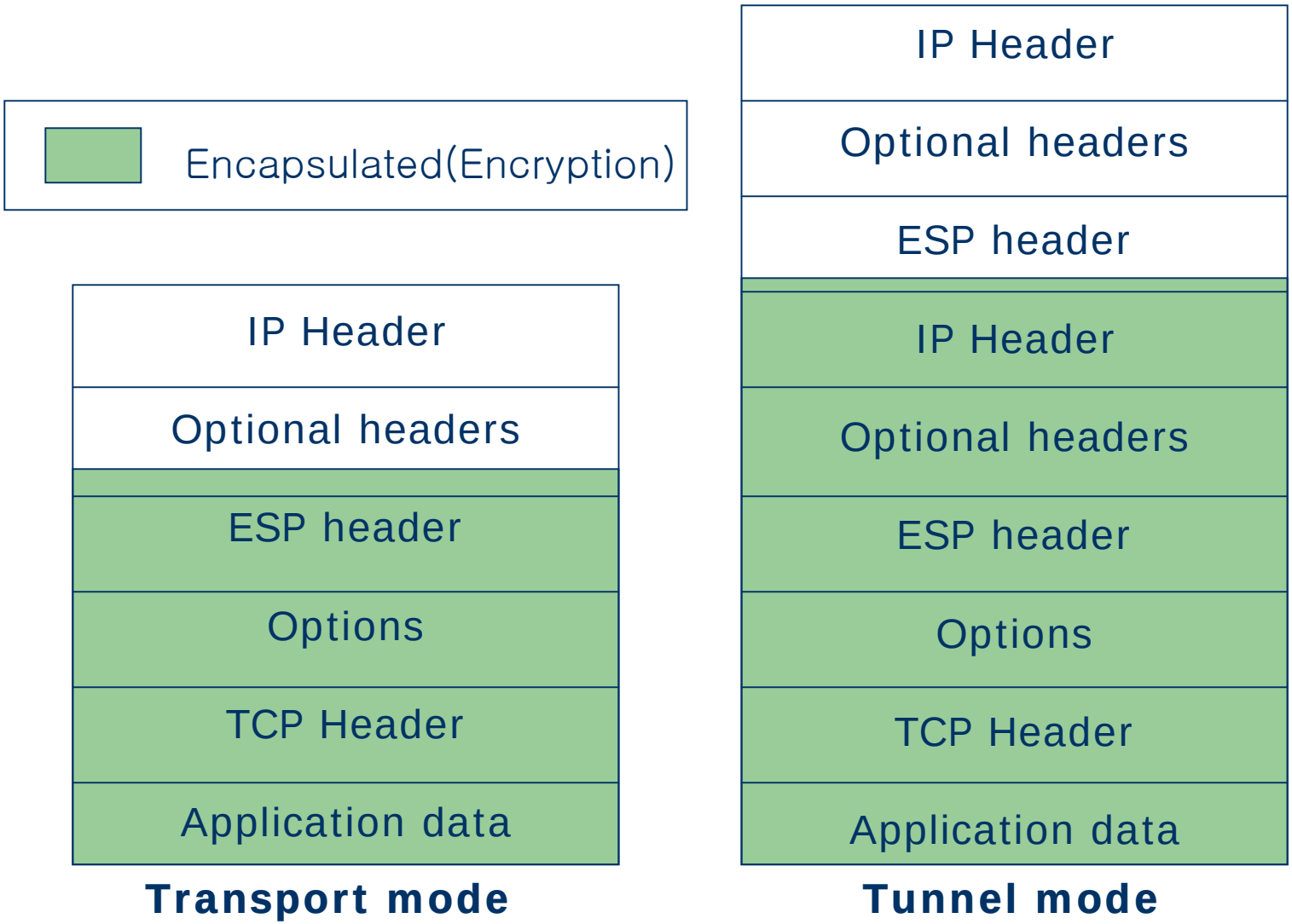
VPN Extentions

- **VPN Options**
  - SSL(Secure Socket Layer)
  - PKI(Public-Key Infrastructure)
    - A management structure of public keys
  - SSH(Secure SHell)
    - Secure replacement for the “r” utilities
    - Added security through public key encryption.
    - Ability to “tunnel” insecure services like POP and IMAP
  - IPSec(IP Security)
  - etc

IPSec(IP Security)

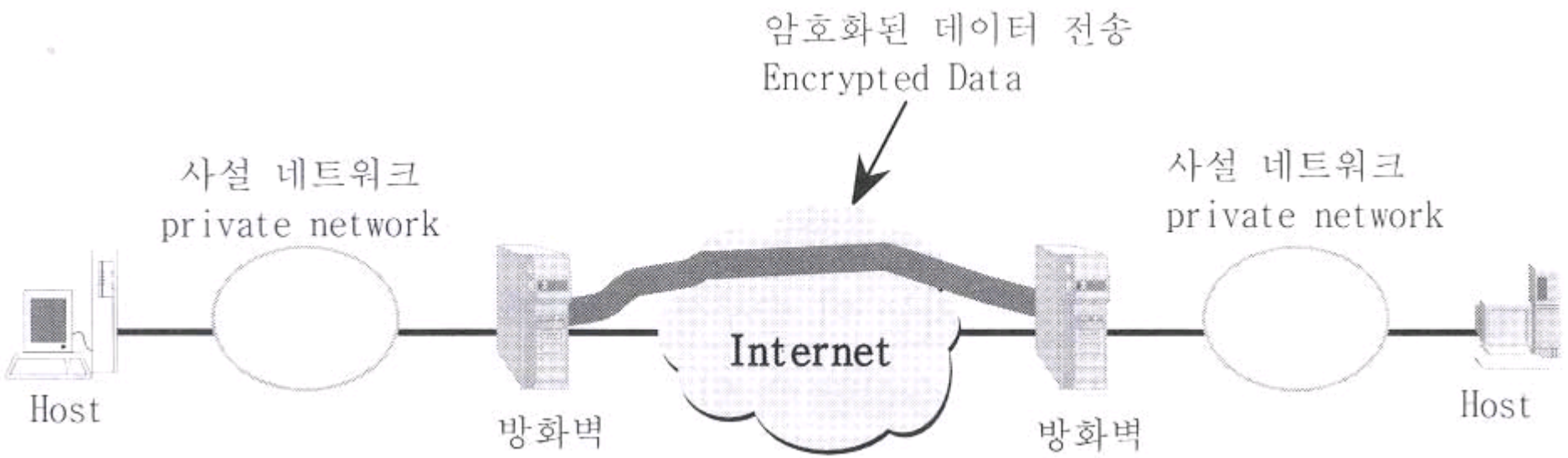
- **What is an IPSec?**
  - 인터넷(공중망)을 통해 안전한 통신을 제공하기 위한 표준 보안 프로토콜
- **IPv4**의 보안위협
  - Packet Header 정보(IP Address)의 spoofing
  - “man-in-the-middle” attacks
- **IPSec**
  - Authentication Header(AH)
    - Integrity (authenticate messages) by hash
    - i.e., IPv4 Packet: headers + payload(data)
  - Encapsulating Security Payload(ESP)
    - Confidentiality + Integrity by Secure hash & encryption

IPSec(IP ESP)



IP ESP(1)

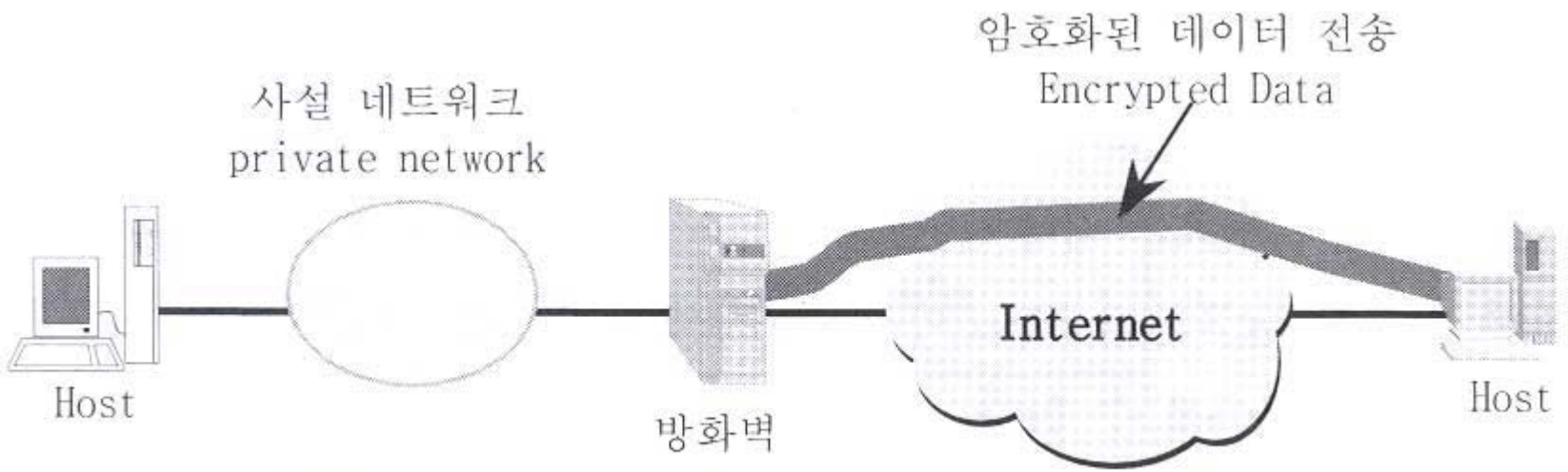
- 방화벽간에 구현되는 **IP ESP tunnel mode**



방화벽간에 구현되는 IP ESP tunnel mode

IP ESP(2)

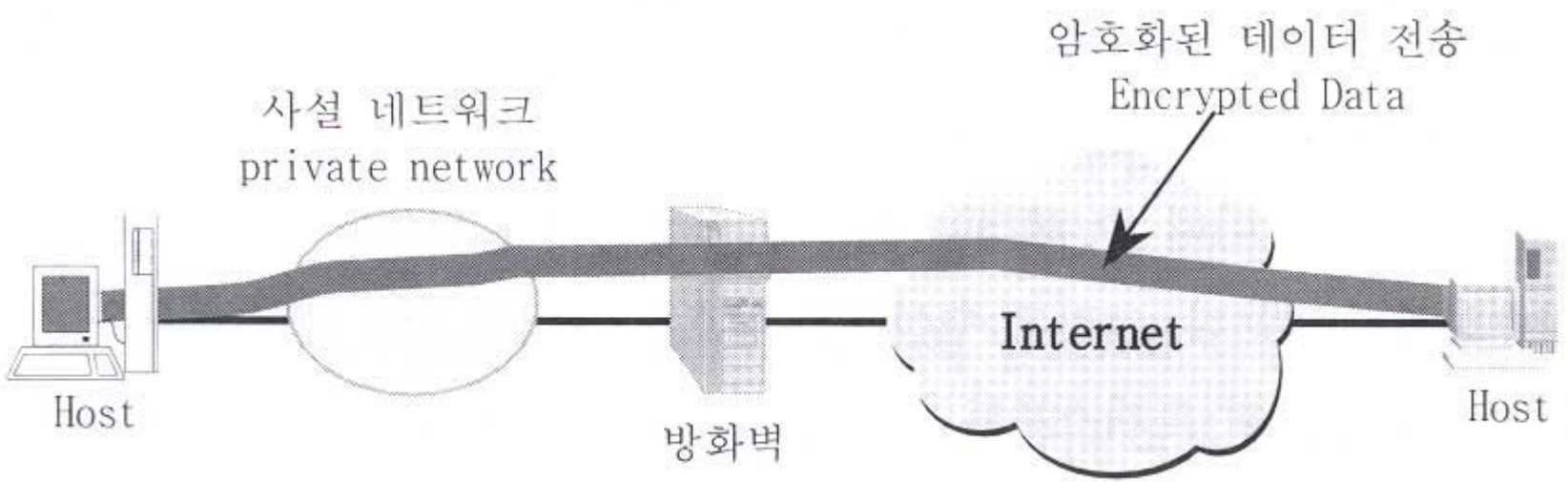
- 방화벽과 인터넷상의 호스트간의 **IP ESP tunnel mode**



방화벽과 인터넷상의 호스트간의 IP ESP tunnel mode

IP ESP(3)

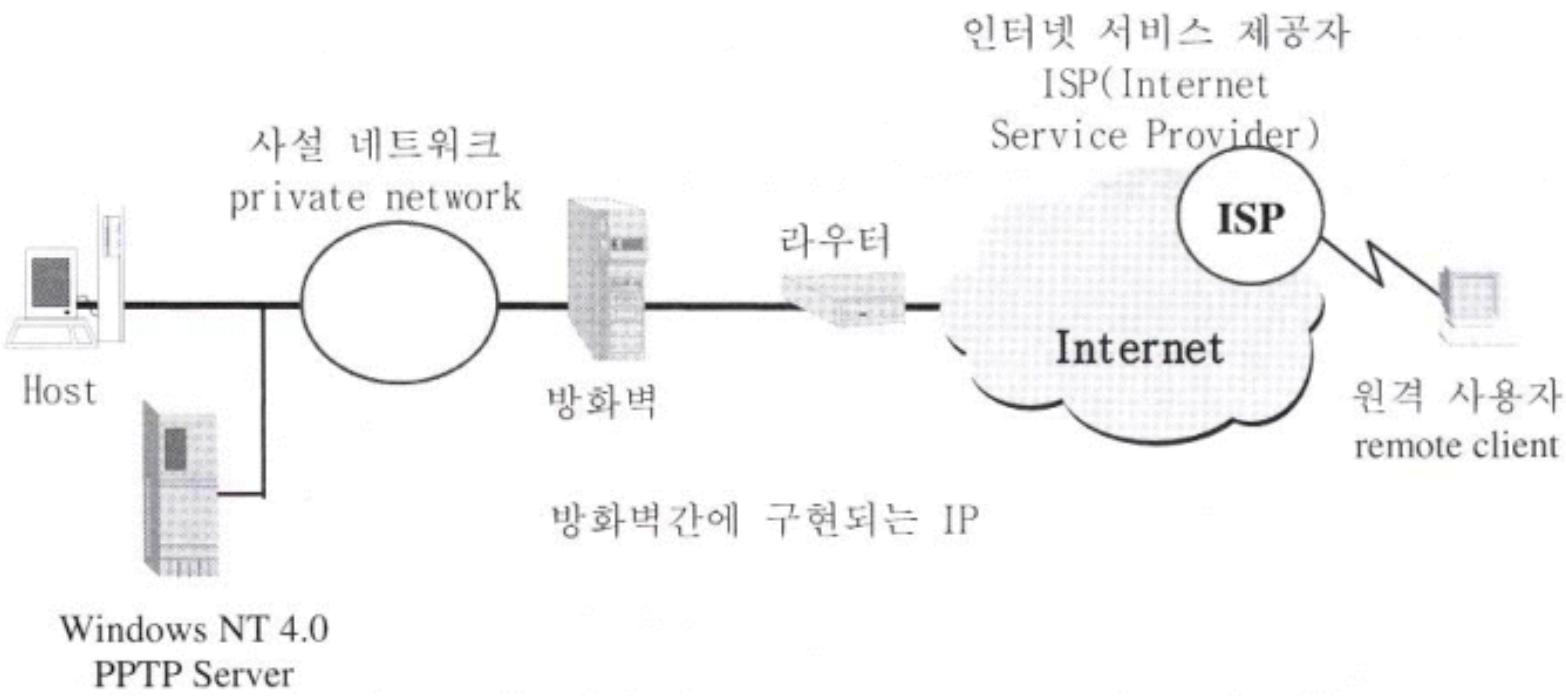
- 사설 네트워크상의 호스트와 인터넷상의 호스트간의 **IP ESP tunnel**



사설 네트워크상의 호스트와 인터넷상의 호스트간 IP ESP tunnel

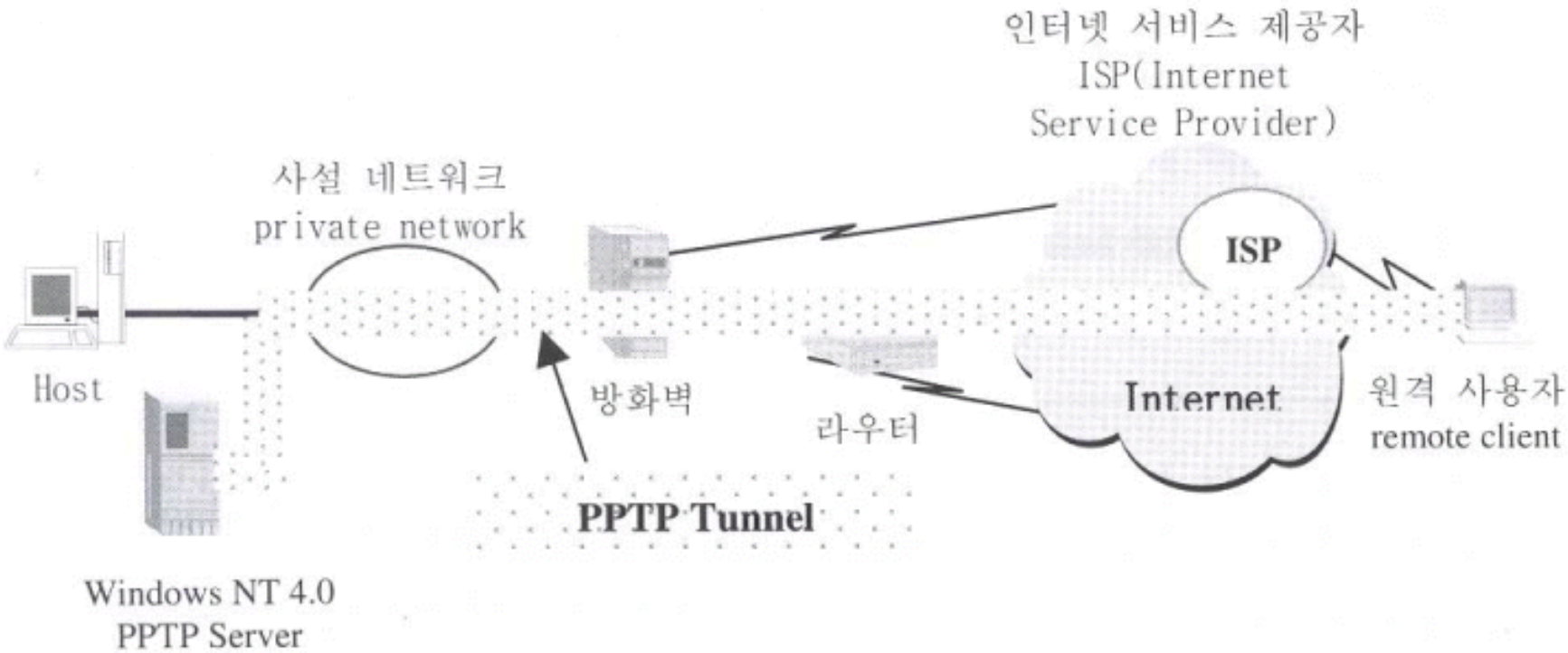
Example: PPTP(1)

1. Establish PPP connection between PC client and ISP



Example: PPTP(2)

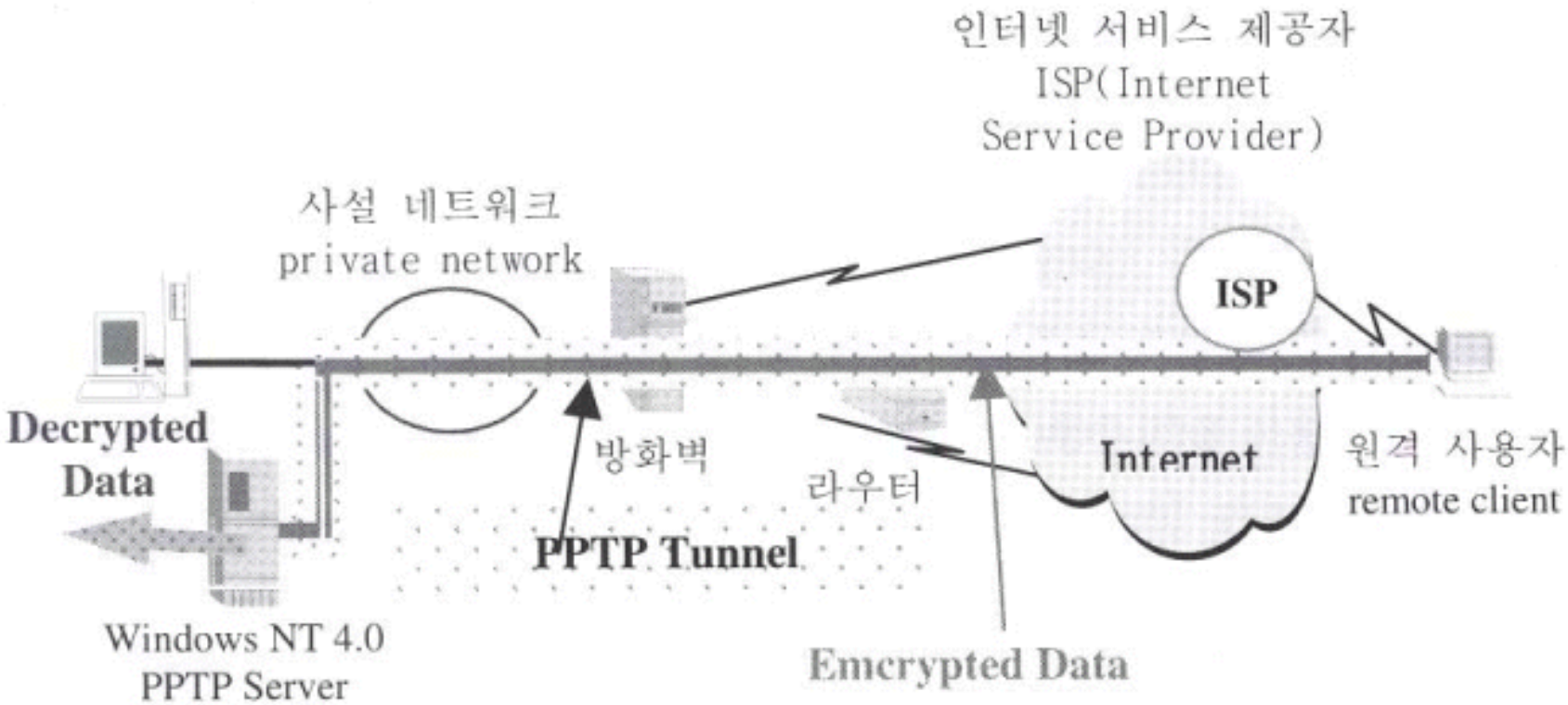
2. Establish PPTP control connection via TCP/1723



PPTP Control Connection

Example: PPTP(3)

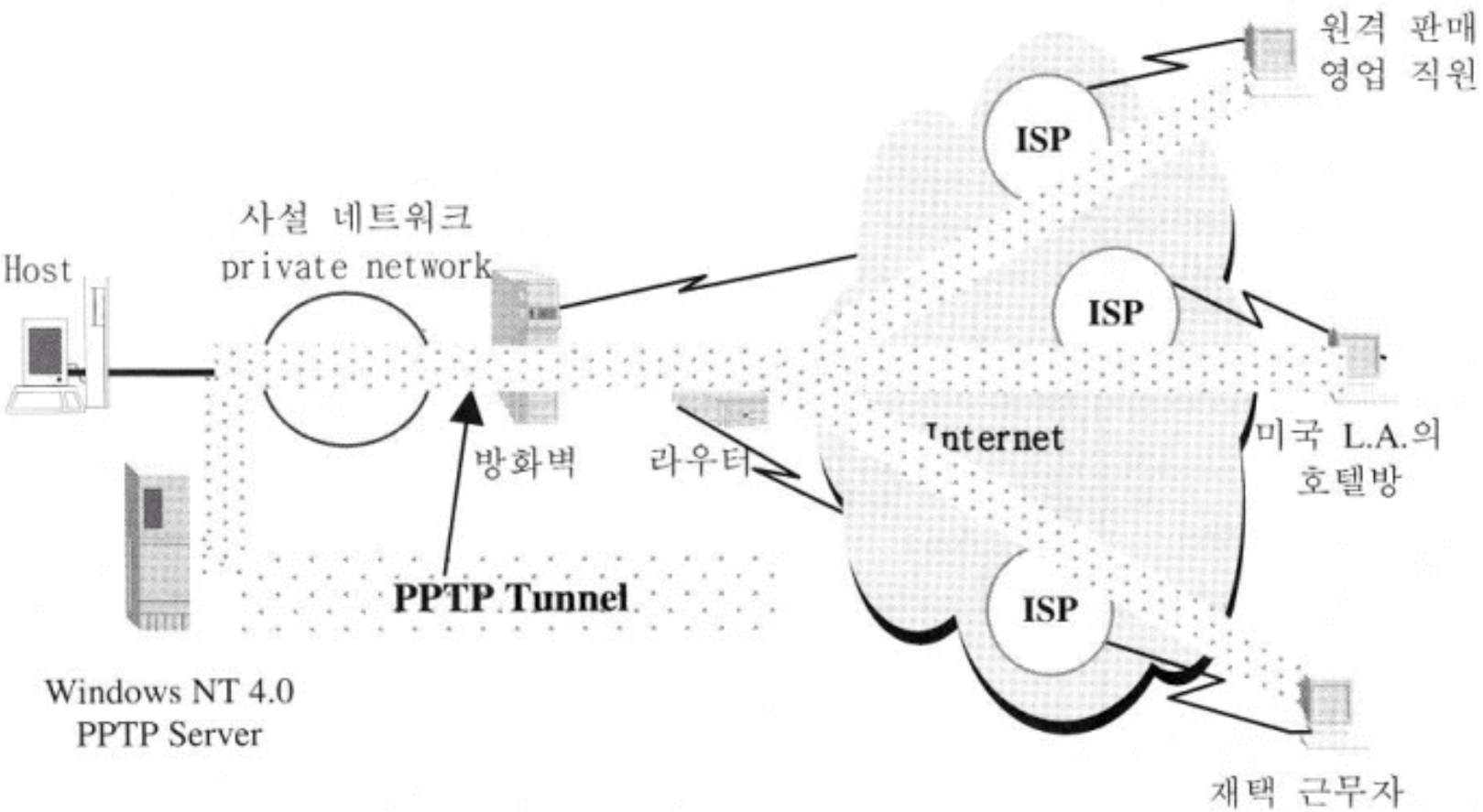
3. Encapsulate data and transfer to PPTP Server via IP Protocol 47(Generic Routing Encapsulation)



PPTP Data Connection

Example: PPTP

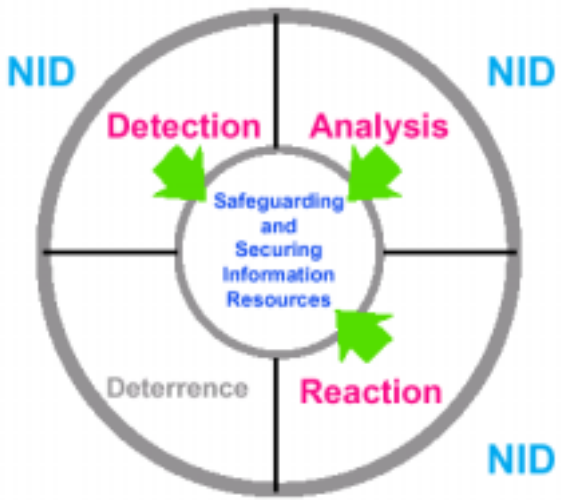
- **VPN 응용**



침입탐지시스템(IDS)

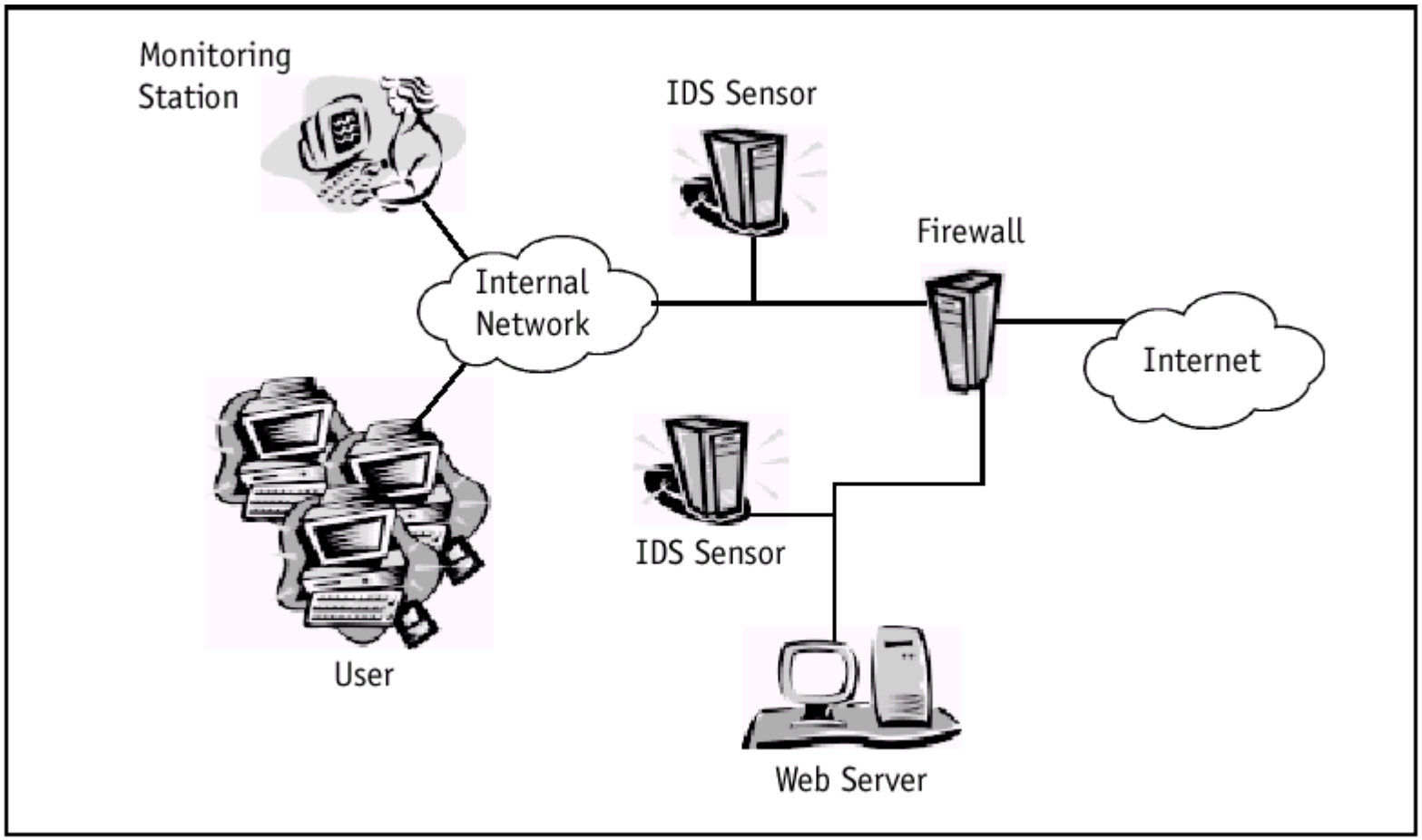
- 침입탐지시스템(IDS)이란?
  - 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 탐지

- **How are intrusions detected ?**
  - Anomaly Detection
    - *identify abnormal unusual behaviors(anomalies)*
  - Misuse Detection
    - *analyze system activity*
    - called “state-based analysis”
    - called “signature-based detection”



침입탐지시스템(IDS)

- 침입탐지시스템(NIDS)의 구성



침입탐지시스템(IDS)

- **Major types of IDSs**
  - Netwok-based IDS
  - Host-based IDS
  - Application-based IDS

- **What are the limitations of NIDS?**
  - Switched network(inherent limitation)
  - Resource limitations
  - Attacks agains the NIDS
  - Simple evasion
  - Complex evasion

침입탐지시스템(IDS)

- **What kind of attacks does IDS detect?**
  - Scanning Attacks
  - Denial-of-service
  - Pentration Attack
  - Remote vs Local Attack

- **complement IDS tools**
  - Vulnerability analysis & assessment tools
  - File Integrity Checking
  - Honey Pots and Padded Cells

Honey Pots

- **What is Honeypot?**
  - 쉽게 침입할 수 있을 것처럼 꾸며 놓은 시스템으로, 침입자를 엉뚱한 시스템으로 유도하기 위한 시스템
  - e.g. Installing an older unpatched operating system on a machine.

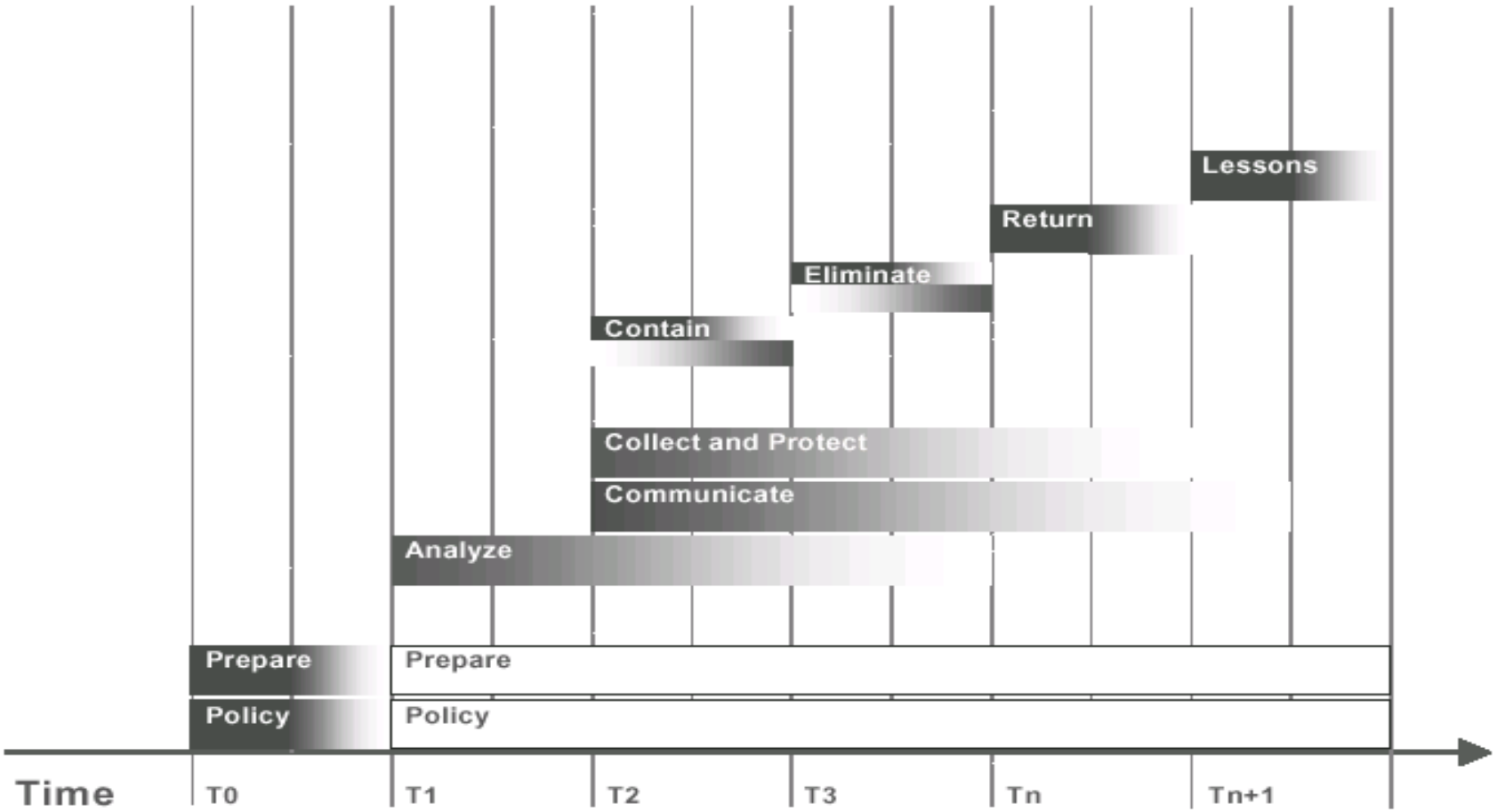
- **What are the types of honeypots?**
  - Port monitors
  - Deception systems
  - Multi-protocol deception systems
  - Full systems
  - Full systems plus NIDS (c.f. *Padded cells*)

Incident Handling

1. **Preparation**
   - 침입사고 발생전에 취해져야할 일련의 조치사항, 나머지 단계의 성공적인 수행을 위해서 필수적이다.
   - Policy(People, H/W, S/W, Network, Documentation, etc)
2. **Identification**
   - Reactive / Proactive identification
3. **Containment(견제, 억제, 봉쇄)**
   - 침입차단, 침입탐지 등 지속적인 시스템관리(PT,보안패치)
4. **Eradication(근절,박멸,소거)**
   - Sanitizing(기밀삭제), Self Sanitizing, Backup and Degauss
5. **Recovery**
6. **Follow-up**

Incident Handling

- **Practice Steps**



Disaster Recovery

- **Basic Steps in disaster recovery plan**
  1. Identify the mission or business critical functions.
  2. Identify the resources that support the critical functions.
  3. Anticipate potential contingencies or disasters.
  4. Select contingency planning strategies.
  5. Implement the contingency strategies.
  6. Test and revise the strategy.

네트웍 보안 강화대책

- **Planning deployment**
  - Develop a computer deployment plan that includes security issues.
  - Include explicit security requirements when selecting servers.
- **Configuring servers**
  - Keep operating systems and applications software up to date.
  - Offer only essential network services and operating system services on the server host machine.
  - Configure computers for user authentication.
  - Configure computer operating systems with appropriate object, device, and file access controls.
  - Identify data that characterize systems and aid in detecting signs of suspicious behavior.
  - Manage logging and other data collection mechanisms.
  - Configure computers for file backups.
- **Maintaining server integrity**
  - Protect computers from viruses and similar programmed threats.
  - Configure computers for secure remote administration.
  - Allow only appropriate physical access to computer.

결론

- 네트웍 보안위협
  - 네트웍 환경의 변화
  - 다양한 공격툴
  - 네트웍 공격기법의 고도화
- 네트웍 보안대책
  - 보안 도구의 대중화
  - 보안 솔루션의 다양화
  - 기반기술/표준

지속적인 보안관리가 필요
보안컨설팅(위험분석)
보안솔루션(보안대책)
침입대응/침입예방