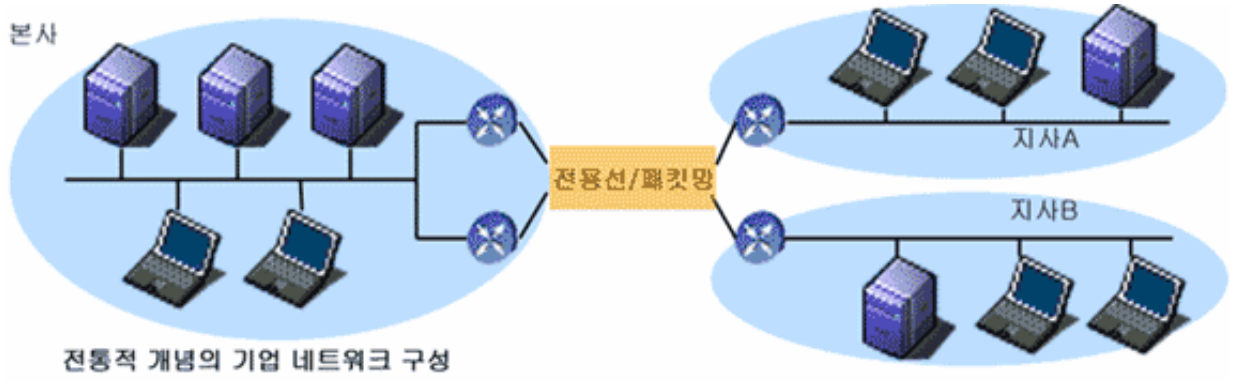
Part 7. IPSec

Virtual Private Network(VPN)

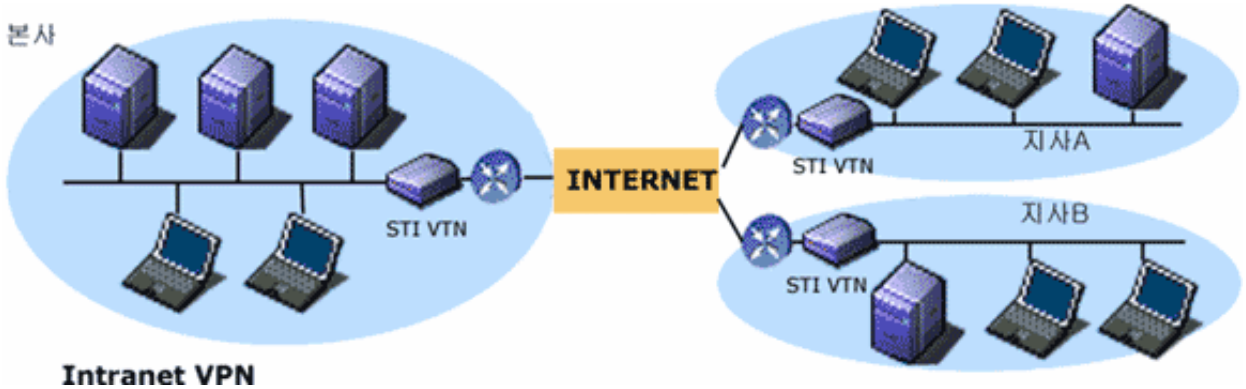
VPN 출현 배경

- 작업환경의 변화
  - 사용자 정보의 공유를 위한 네트워크 확장
  - 작업환경의 이동성/휴대용 PC, 재택 근무용 PC
  - 통제 불가능한 사용자 증가
- 네트워크 확장 요구
  - 전용회선 사용 증가로 인한 비용 증가
  - PSTN을 이용한 원격 접속에 따른 비용 증가
  - 독자적인 사설망 구축 및 관리 비용 증가
- 인터넷 기술 활용
  - 값싼 인터넷 기술 활용
  - Local ISP를 이용한 가상 사설망 설치의 용이성
- 강력한 네트워크 보안 요구

VPN 구성도



전통적 개념의 기업 네트워크 구성



Intranet VPN

VPN 특징

- 공중통신망을 활용한 독자적인 망 구축
  - 동일한 네트워크를 사용하여 다수의 독립망 구성
  - 인터넷의 개발적, 분산된 하부구조 활용
- 특정 그룹 및 사용자간의 통제된 네트워크 접속
- 원격 사용자 그룹을 포함한 독자적 보안망 구축
  - ISP에 POP(Points of Presence)으로 연결
- 서비스 품질 보장
- 차별화된 보안 등급 구분
  - 차별화된 인증 기능
  - 다양한 데이터 암호/복호화

Chapter 21. IPSec 개요

- 설계목표
  - IP 계층 또는 그 상위 계층 프로토콜 보호
    - 기밀성
    - 데이터 근원 인증
    - 비연결형 무결성
    - 재전송 공격 방지
    - 제한된 트래픽 흐름 기밀성
    - 접근 제어
- 보안 메커니즘
  - AH(인증헤더; Authentication Header)
  - ESP(캡슐화 보안 페이로드; Encapsulating Security Payload)
  - 키 관리 절차
    - 수동식
    - 자동식: IKE(Internet Key Exchange), KINX, ...

IPSec

- Internet Protocol Security Protocol
- IETF IPSec working group 제안
- 계층 2/3, 3에서 동작
  - IPv4, IPv6에서 수용
- 정보보호 서비스
  - AH(Authentication Header), ESP(Encapsulation Security Payload)
    - SA: Security Parameter Negotiation 통해 서비스

    - 기밀성
    - 사용자 인증
    - 무결성
    - 접근제어 Packet Filtering
- Host-to-Host, Host-to-GW, GW-to-GW Security 지원
    - 양방향 tunnel 형성
- PKI 기반의 키 교환 메커니즘 이용

IPSec의 작동 위치

- IPSec은 IP 수준에서 작동, 모든 IP 데이터그램을 처리
    - 모든 응용 프로그램을 투명하게 보호
    - 네트워크를 사용하는 모든 장치에 구현 가능
    - 종단간 또는 연결부의 보안 제공
- IPv6에서는 필수사항
- IPv4에서는 선택 사항이므로 IPSec을 구현한 제품 필요

IPSec의 두 부분

- Part1: User Authentication, *SA*협상과 세션키 교환*(IKE* 사용*)*
- Part2: 전송되는 데이터의 기밀성*(*세션키를 이용하여 암호화*)*과 무결성을 위해 를 제공**(AH, ESP)**

SA(Security Association)

- 데이터 교환전에 통일되야 할 보안요소들의 정의
- IPSec 서비스를 제공하는 송신자와 수신자 사이에서 협상
    - 보안 서비스와 메커니즘을 정의하는 파라미터들의 집합
        - 보안 서비스 종류(AH or ESP)
        - 암호 알고리즘
        - 세션키 교환방법
        - 세션키 교환 주기(세션키 수명) 등
- 트래픽에 보안 서비스를 제공하는 일방향 연결
    - 보안 서비스는 ESP나 AH 중 하나
        - 두 가지 서비스를 모두 받기 위해선 두 개의 SA가 필요
    - 양 방향 통신에선 각 방향별로 SA 필요(두 SA의 내용이 다를 수 있음)

SA 협상 및 키의 관리

- 수동식

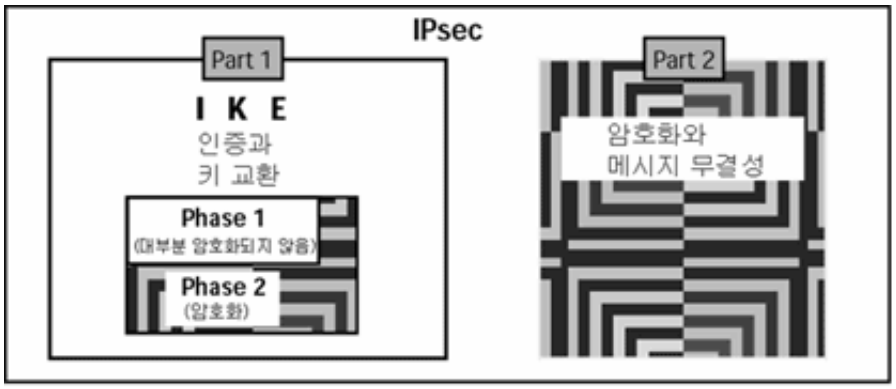
    - 소규모의 정적인 환경에 적합
    - 일반적으로 대칭 키를 사용
- 자동식
    - 대규모의 동적인 환경 지원
    - 재전송 공격 방지, 사용자별/세션별 키 제공 등에 필요
    - 기본 프로토콜: IKE

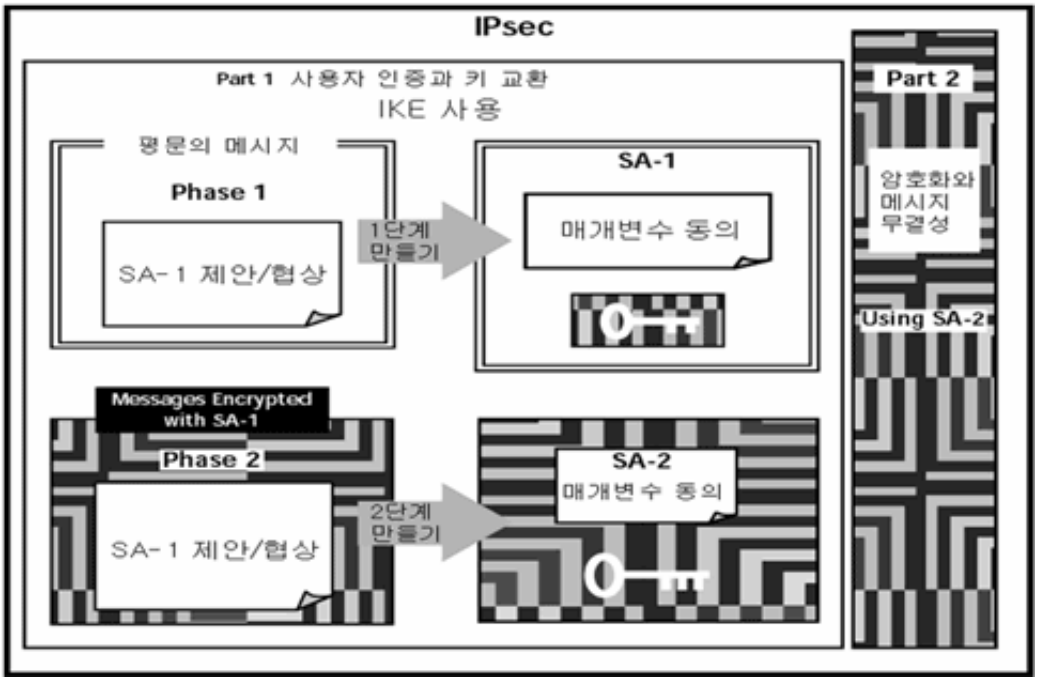
IPSec Part 1: IKE

- 자동식으로 SA 협상과 키 교환 이루어짐
- P2P 방식: 서버 없어도 됨
- ISAKMP 프레임워크 + Oakley 키 교환 절차
- DoS에 대한 제한적 방어
- Man-in-the-middle 공격 방지
- 협상항목
    - Encryption / Authentication / Hash Algorithms
    - Diffie-Hellman 그룹
    - 키 재료

IKE의 두 단계 프로토콜

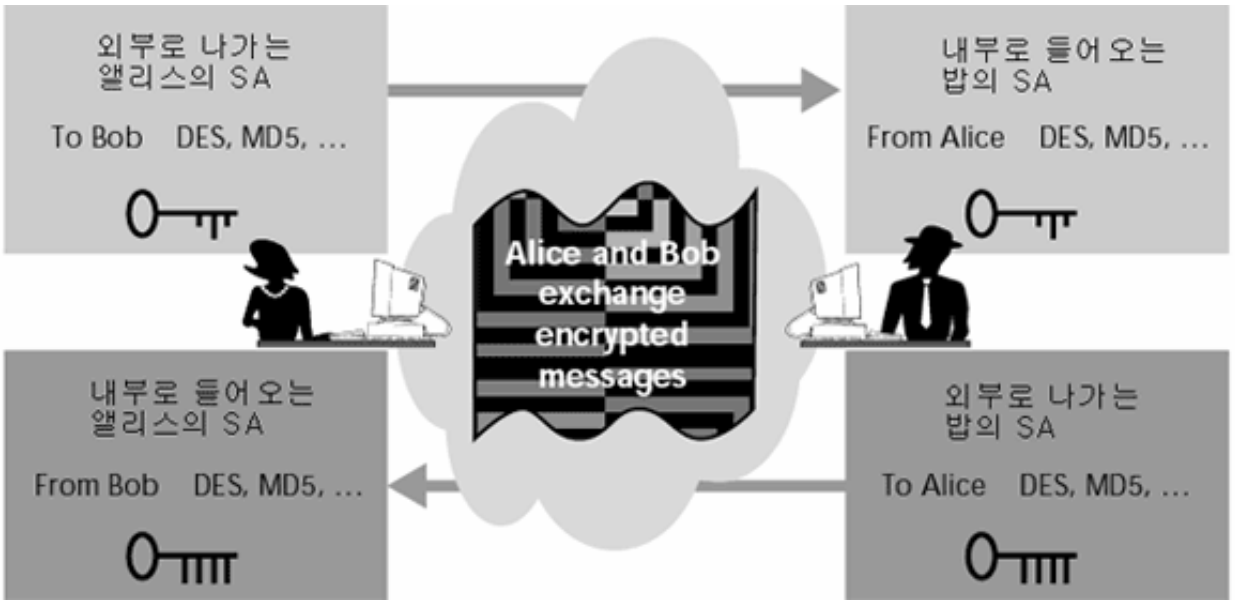
- Phase 1:
    - IKE의 Phase 2를 위한 SA-1(암호화 매개변수) 협상
        - Phase 2에서 사용할 암호화 키 및 인증 키 발생
        - Phase 2를 안전하게 만들기 위한 암호화 매개변수(SA-1) 교환
- Phase 2:
    - 실제 데이터 전송시(part2)에서 데이터 보호를 위한 SA-2 협상
        - SA-2: AH와 ESP를 위한 SA임
    - 세션키 협상





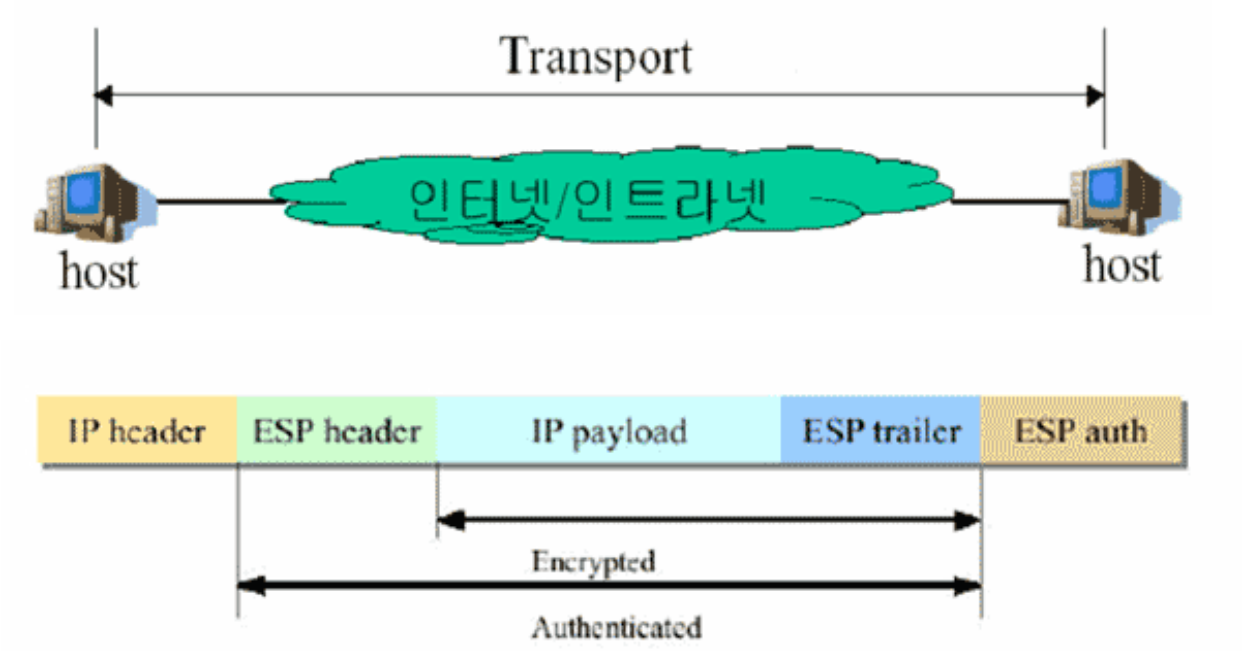
IPSec Part2: AH, ESP

- 실제 전송하려는 데이터가 암호화, 인증되는 부분
- 양방향 각각의 보안을 위하여 SA를 각 방향당 하나씩 설정
  - 1쌍의 SA 필요
  - A → B 위한 SA, B → A 위한 SA



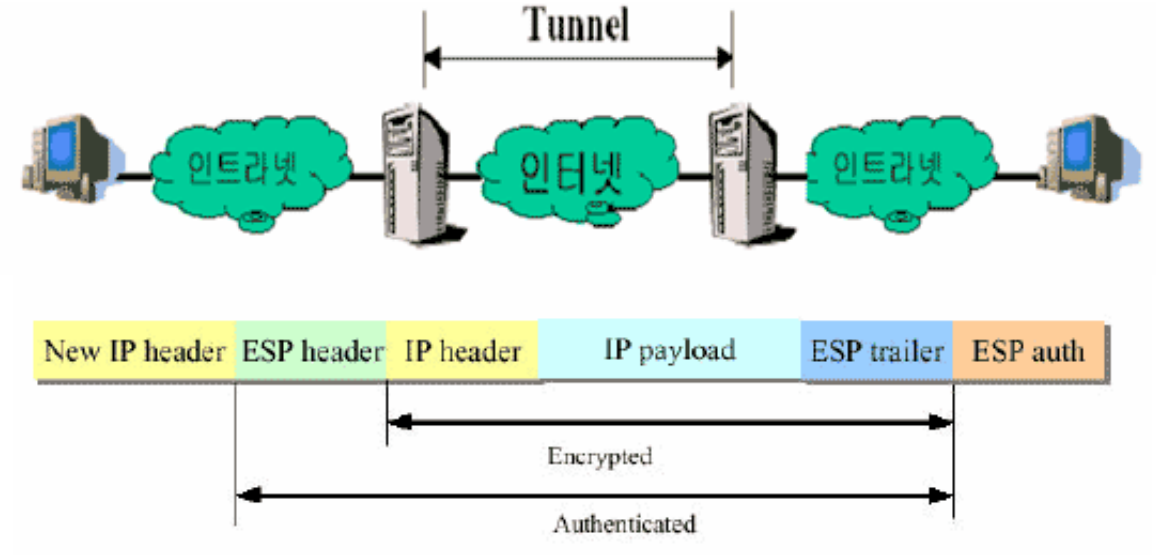
보호모드(Security Mode)

- Transport Mode
  - 데이터그램의 내용만 보호
  - 터미널 장비에만 사용
  - Host 마다 IPsec이 구현



- Tunnel Mode
  - 원본 패킷을 새로운 패킷으로 캡슐화
  - Routing문제로 인해 Gateway에서 필수(터미널 장비에서도 사용가능)
  - 패킷이 Gateway를 통과할 수 있도록 외부 헤더의 주소를 Gateway 주소로 대치
  - 통신자들의 IP 주소 은폐

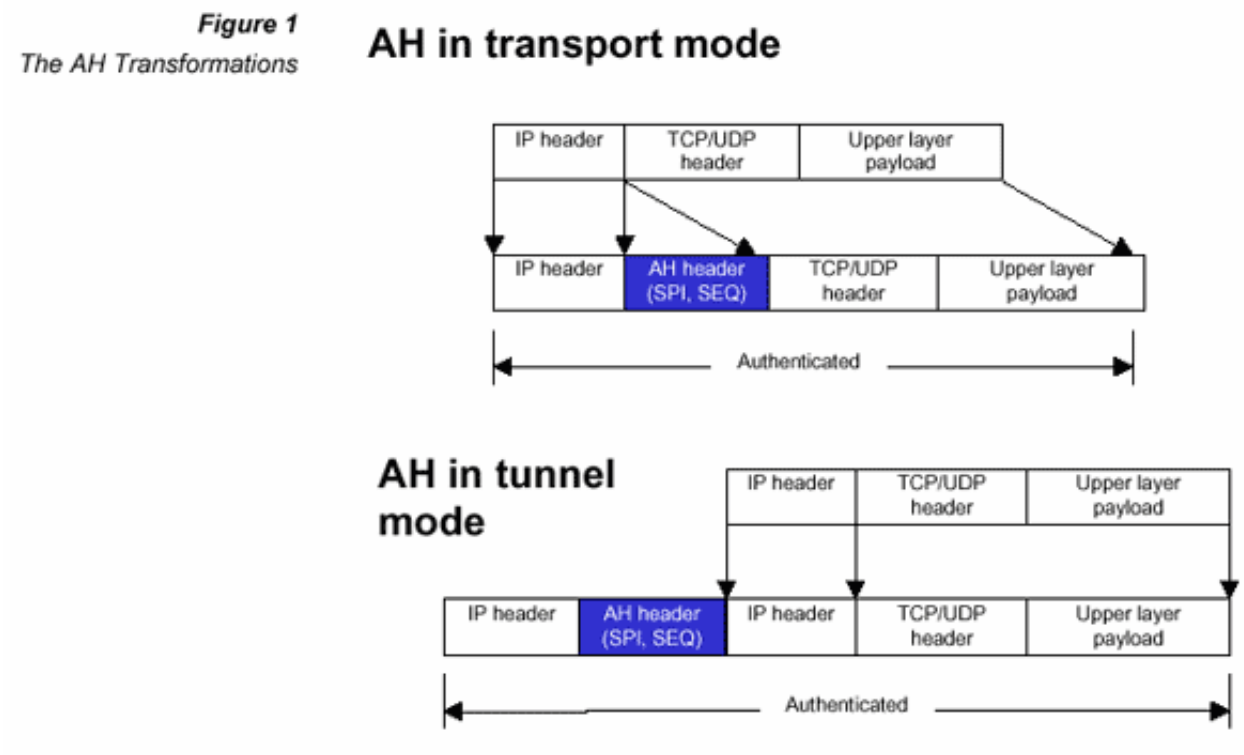
- 대부분의 경우 선호
- 보통 Router에 IPSec구현(내부에서 공격 위험)



- ESP 프로토콜이 가장 강력한 보안 제공
- VPN의 많은 벤더들이 IPSec 중 터널모드에서 ESP 프로토콜 사용
- Host-to-Gateway, Gateway-to-Gateway간 통신에 사용
- IP헤더부분에 대해서도 보안기능 제공

AH

- **인증(Authentication)** 제공
- 기밀성(Confidentiality)은 제공하지 않음
- Message Digest(MD5, SHA-1), MAC(Message Authentication Code) 사용



ESP

- 기밀성(Confidentiality) 제공
- 데이터 근원지 인증(Authentication)
- 메시지 인증(Integrity) 서비스
- 재전송 공격 방지(Anti-replay protection)