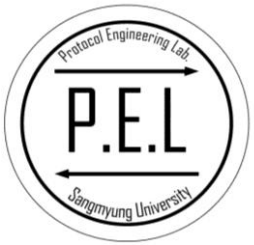


네트워크 보안 에센셜

8장 IPSec

Ji-Yeon Moon (jiyeon@pel.smuc.ac.kr)
Protocol **E**ngineering **L**ab., **Sangmyung** University

목차

- IPSec 개요
- IPSec 프로토콜
- IPSec 운용 모드
- 보안 연관
- 보안 정책
- IP 패킷 처리

IPSec 개요

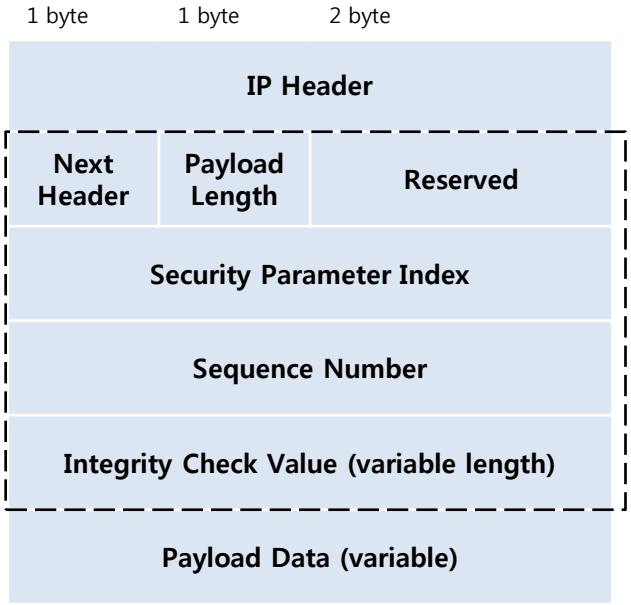
- **IPSec(IP Security)**
  - IP 계층에서 패킷에 대한 보안을 제공하기 위해 설계된 프로토콜
  - 1995년 IETF RFC 4301로 채택 (RFC 2401 업데이트)

IPSec 개요

- **IPSec 서비스**
  - 접근 제어(Access control)
  - 메시지 무결성(Message integrity)
  - 데이터 송신지 인증(Data source authentication)
  - 재전송 패킷 거부(Rejection of replayed packets)
  - 기밀성(Confidentiality)

IPSec 프로토콜

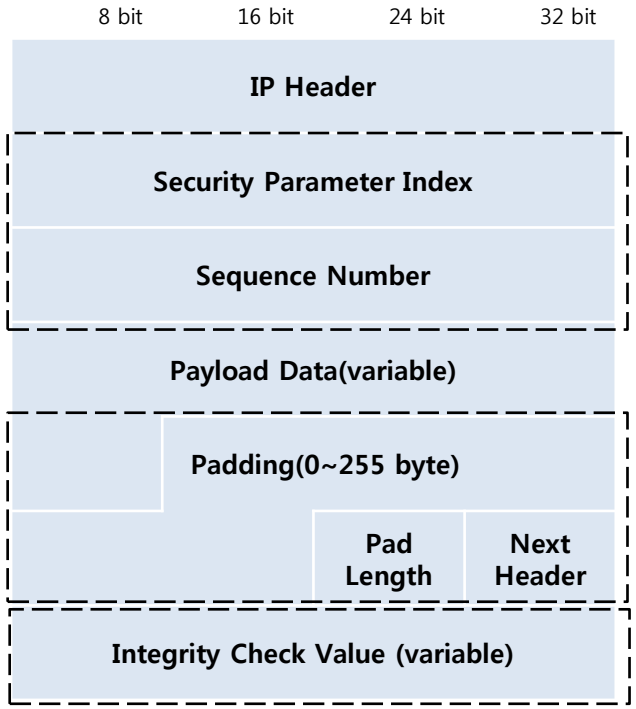
- **인증 헤더(AH: Authentication Header)**
  - IP 패킷의 무결성을 제공하는 헤더
  - 해시 알고리즘으로 HMAC-SHA1 등을 사용
  - RFC 4302, RFC 2402



- **다음 헤더(Next Header):** IP 패킷에 의해 전달되는 페이로드 유형을 정의 (ex TCP, UDP 등)
- **페이로드 길이(Payload Length)**
- **예약(Reserved)**
- **보안 매개변수 색인(SPI: Security Parameter Index):** SA 식별
- **순서 번호(Sequence Number):** 재전송 방지 기능 제공
- **무결성 확인 값(ICV: Integrity Check Value):** IP 패킷에 대한 무결성 확인 값을 포함하는 필드

IPSec 프로토콜

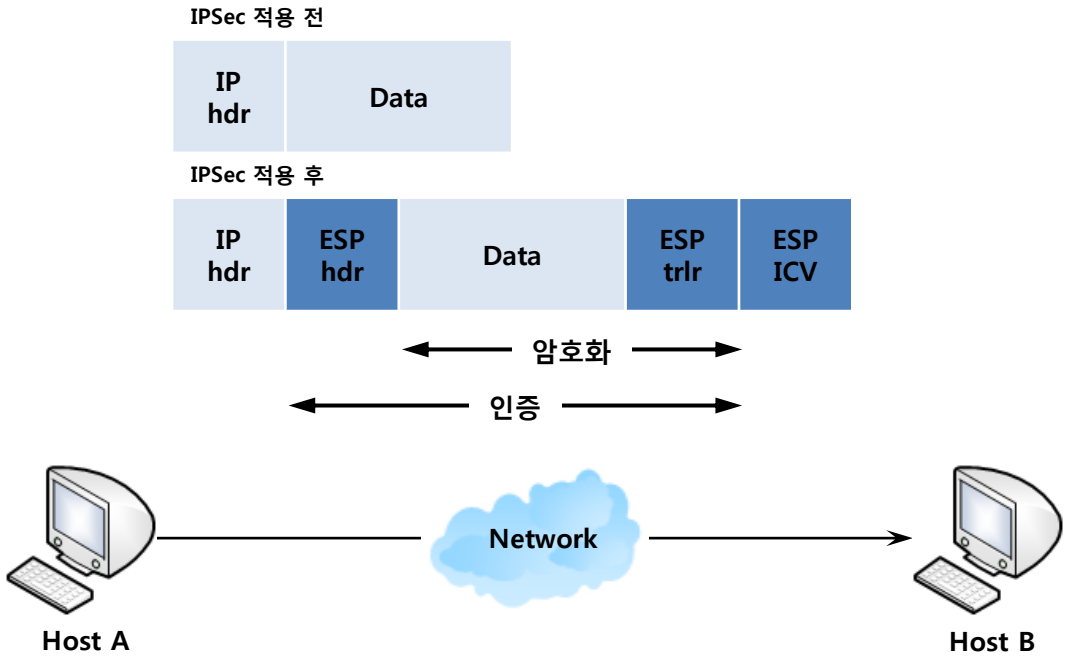
- **캡슐화 보안 페이로드(ESP: Encapsulating Security Payload)**
  - IP 패킷의 무결성과 기밀성을 제공하는 헤더
  - 암호화 알고리즘으로 3DES-CBC 등을 사용
  - RFC 4303, RFC 2406



- **보안 매개변수 색인(SPI: Security Parameter Index):** SA 식별
- **순서 번호(Sequence Number):** 재전송 방지 기능 제공
- **패딩(Padding):** 길이는 0~255 byte
- **패드 길이(Pad Length):** 패드 바이트 수
- **다음 헤더(Next Header):** IP 패킷에 의해 전달되는 페이로드 유형을 정의 (ex TCP, UDP, ICMP 등)
- **무결성 확인 값(ICV: Integrity Check Value):** ESP 패킷에 대한 무결성 확인 값을 포함하는 필드

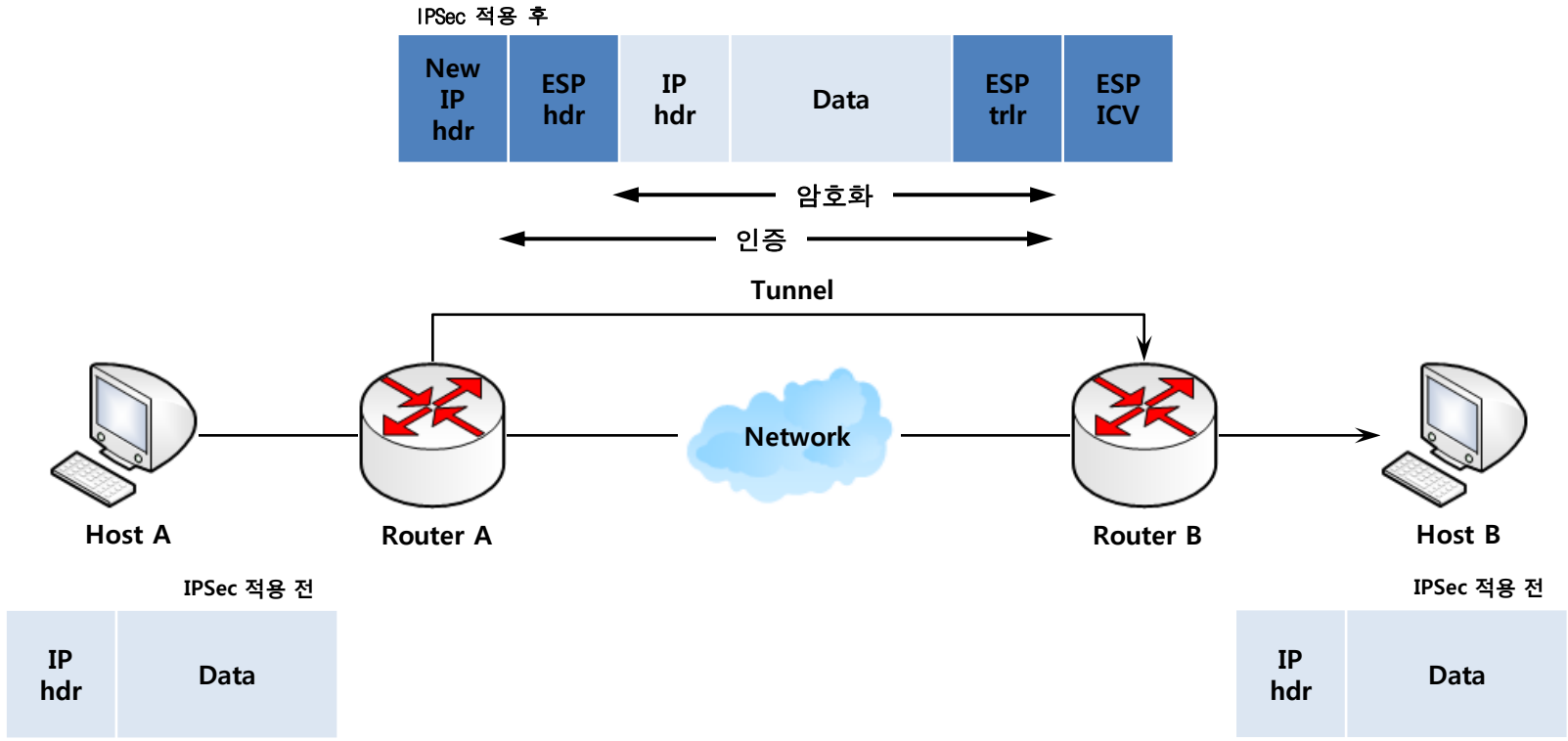
IPSec 운용 모드

- **전송 모드(Transport mode)**
  - IP 헤더를 제외한 IP 패킷의 페이로드만 암호화하는 방식
  - 호스트 간 통신에 사용



IPSec 운용 모드

- **터널 모드(Tunnel mode)**
  - IP 패킷 전체를 암호화하며 새로운 IP 헤더를 추가하는 방식
  - 호스트-라우터 간 또는 라우터 간 통신에 사용



보안 연관

- **보안 연관(SA: Security Association)**
  - 송/수신자 간 데이터 통신에 보안 서비스를 제공하기 위해 사전에 합의되어야 할 요소

- **보안 연관을 식별하기 위한 매개변수**
  - **보안 매개변수 색인(SPI: Security Parameters Index):** IP 패킷을 처리하기 위해 필요한 SA
  - **IP 목적지 주소(IP Destination Address):** 최종 목적지 주소
  - **보안 프로토콜 식별자(Security Protocol Identifier):** AH/ESP 보안 연관 식별

보안 연관

- **보안 연관 데이터베이스(SAD: Security Association Database)**
  - IPsec에서 각 SA에 연관된 요소들을 정의한 데이터베이스

  - **요소**
    - **보안 매개변수 색인(SPI: Security Parameter Index):** SA를 식별하도록 수신자가 선택한 32 bit 값
    - **순서 번호 카운터(Sequence Number Counter):** 순서 번호 필드를 위해 생성되는 32 bit 값
    - **순서 계수기 오버플로우(Sequence Counter Overflow):** 순서 번호 카운터의 오버플로우에 대한 유무를 가리키는 플래그
    - **재전송 방지 윈도우(Anti-Replay Window):** 패킷의 재전송 여부를 판별
    - **AH 정보(AH Information):** AH와 함께 사용되는 인증 알고리즘, 키, 키 사용 주기 그리고 관련 매개변수의 정보를 포함
    - **ESP 정보(ESP Information):** ESP와 함께 사용되는 암호화 및 인증 알고리즘, 키, 초기 값, 키 사용 주기 그리고 관련 매개변수의 정보를 포함
    - **보안 연관 사용주기(Lifetime of this Security Association):** 하나의 SA가 새로운 SA로 교체/종료되는 시간 간격 또는 바이트 카운트 값
    - **IPsec 프로토콜 모드(IPsec Protocol Mode):** 터널/전송 모드
    - **경로 MTU(Path MTU)**

보안 정책

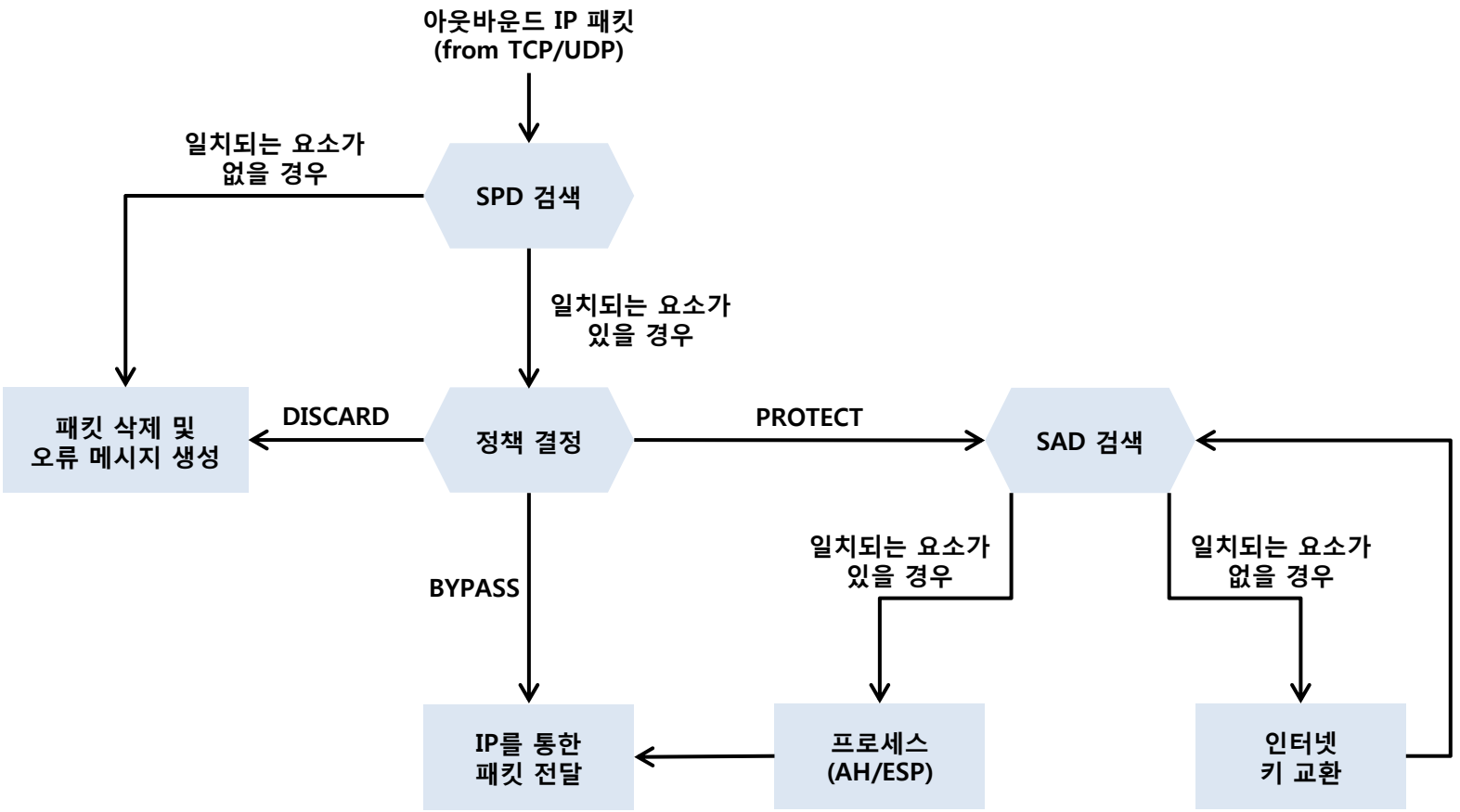
- **보안 정책(SP: Security Policy)**
  - 패킷이 송/수신될 때 적용되는 보안 유형을 정의

- **보안 정책 데이터베이스(SPD: Security Policy Database)**
  - IP 패킷을 SA에 연관시키는 방법을 정의한 데이터베이스

  - **요소**
    - **원격 IP 주소(Remote IP Address)**
    - **로컬 IP 주소(Local IP Address)**
    - **로컬과 원격 포트(Local and Remote Ports)**
    - **다음 계층 프로토콜(Next Layer Protocol)**
    - **동작(Action)**

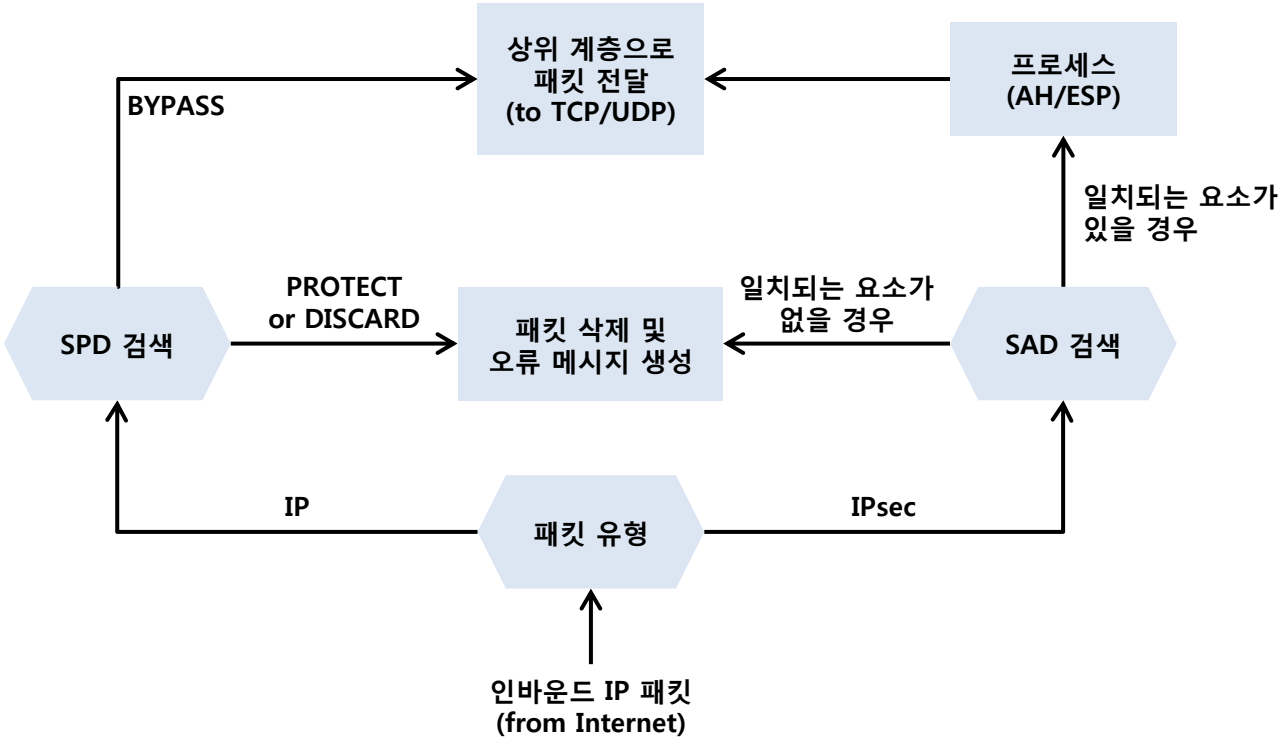
IP 패킷 처리

- 아웃바운드 패킷 처리



IP 패킷 처리

- 인바운드 패킷 처리



네트워크 보안 에센셜

끝!