2017/01/17, 2017 보안 기초 세미나

Network Security Essentials

- Chapter_8 IP 보안 (1) -

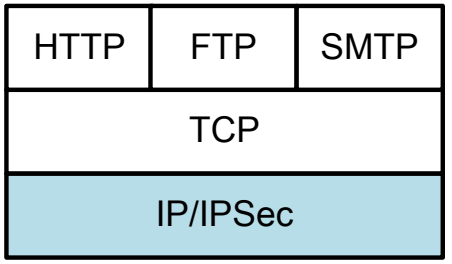
임연주(yeonjoo@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

IPsec 개요

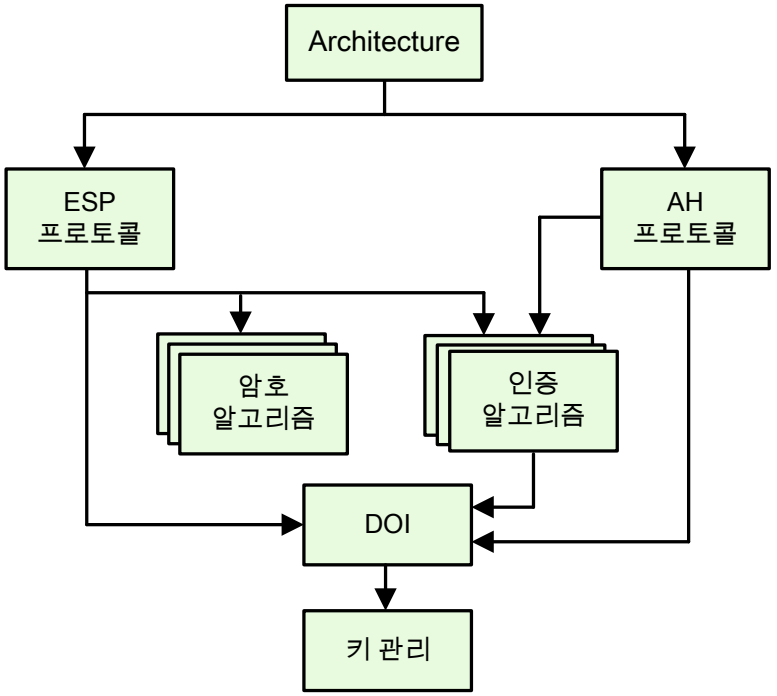
- 정의
  - Internet Protocol Security의 약자
  - IP 통신 보안을 위해 설계된 프로토콜 슈트



- 설계 목표
  - IP 계층 또는 그 상위 계층 프로토콜을 보호
    - 기밀성
    - 데이터 출처 인증
    - 비연결형 무결성
    - 재전송 공격 방지
    - 제한된 트래픽 흐름 기밀성
    - 접근 제어

IPsec 개요

- 특징
  - 여러 가지 응용을 지원할 수 있음
  - 모든 트래픽에 대한 암호화와 인증을 수행
  - 구현 구조에 따른 두 가지 동작모드가 있음
    - 터널모드, 전송모드
- 구조 그림



IPsec 개요

- 서비스
  - IP 계층에 필요한 보안 서비스 제공
    - 시스템이 필요한 보안 프로토콜 선택
      - 인증 프로토콜
        - 인증 헤더(AH, Authentication Header)
      - 보안 페이로드 캡슐화(ESP, Encapsulation Security Payload)
    - 서비스에 필요한 트래픽 처리 및 알고리즘 결정
      - 보안 정책(Security Policy)
      - 보안 연관(Security Association)
    - 요구된 서비스에 필요한 암호화 키 제공
      - 인터넷 키 교환(IKE, Internet Key Exchange)

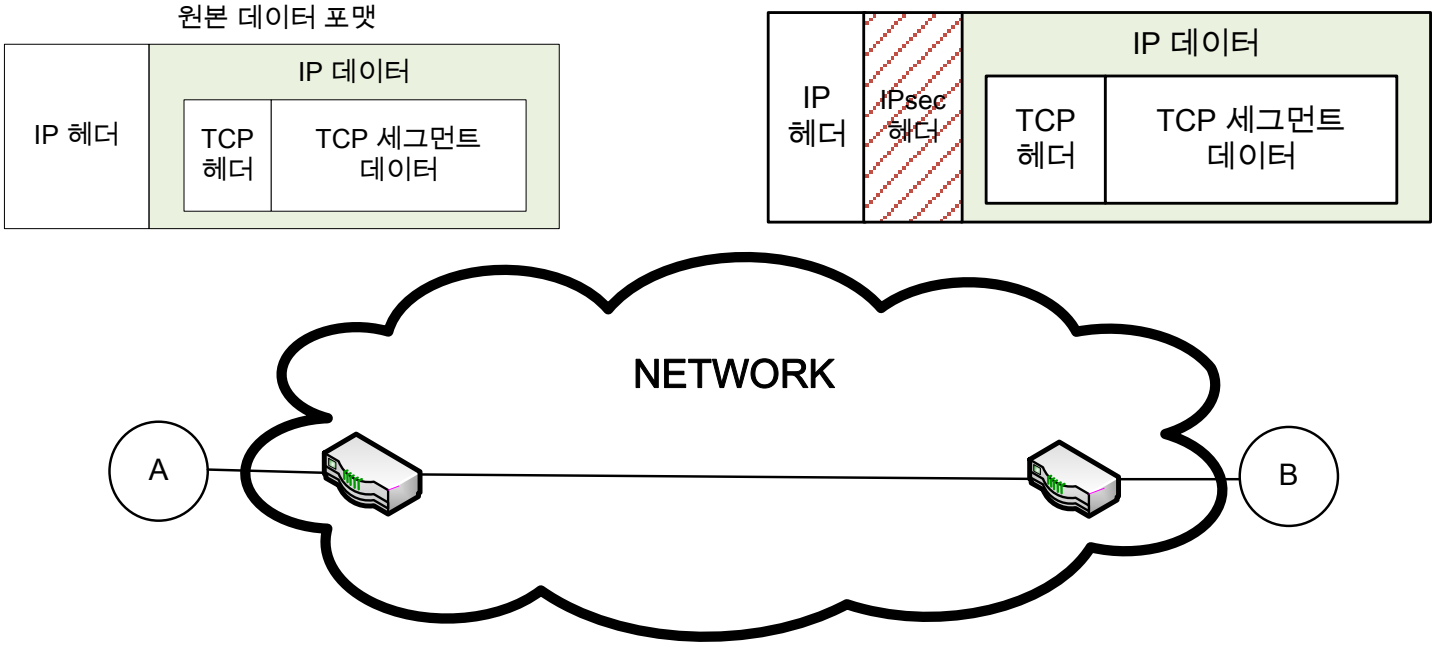
IPsec 개요

- 서비스
  - 제공되는 보안 서비스 정리 표

	AH	ESP
접근제어 (Access Control)	Y	Y
데이터 기밀성 (Confidentiality)		Y
데이터 출처 인증 (Data Origin Authentication)	Y	
재생공격 방지 (Replay Attack Protection)	Y	Y
비연결형 무결성 (Connectionless Integrity)	Y	
개체 인증 (Peer Authentication)	Y	Y

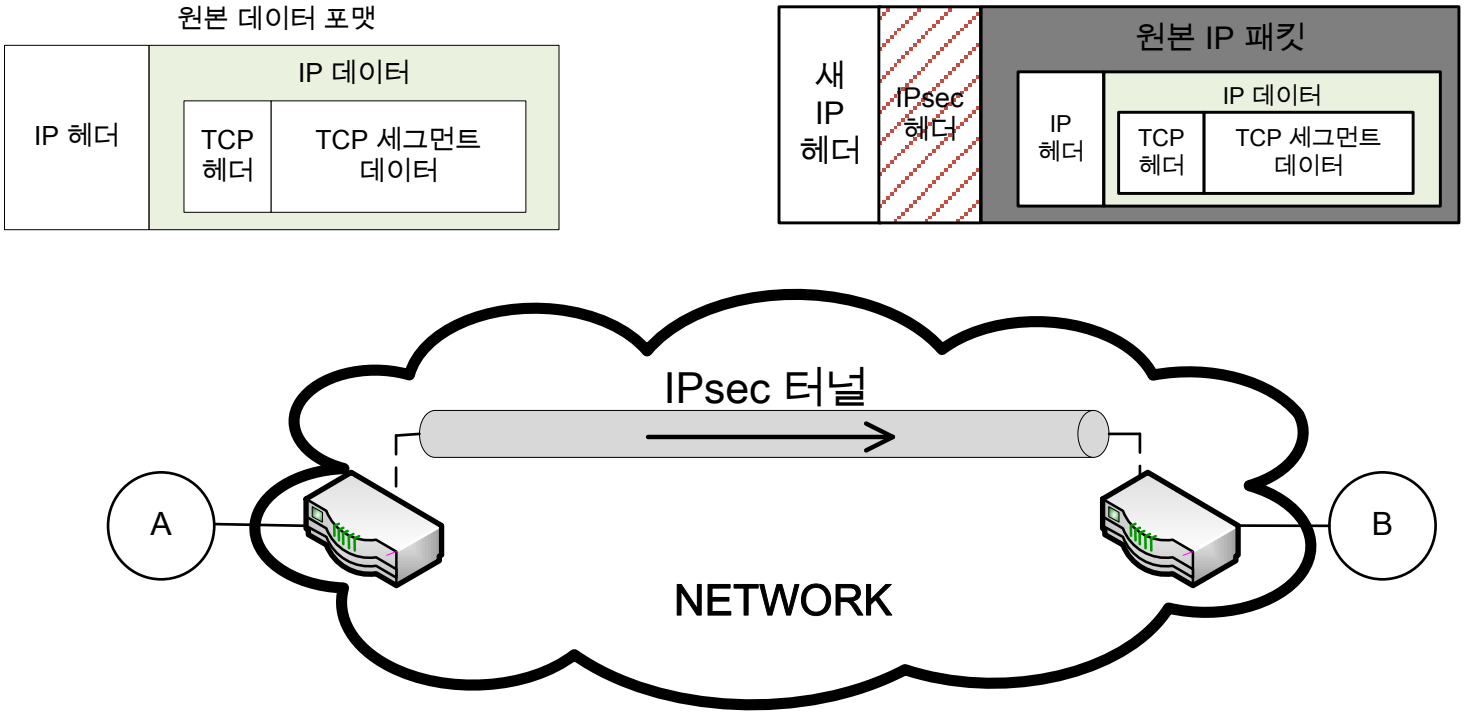
IPsec 개요

- IPsec 동작 모드
  - 전송 모드
    - IP헤더는 보호되지 않고 IP 페이로드까지만 보호
    - 종단-대-종단 구현을 필요로 할 때 적합
    - 상위 계층의 페이로드만 보호



IPsec 개요

- IPsec 동작 모드
  - 터널 모드
    - 원본 IP 패킷 전체를 보호
    - 추가적인 캡슐화를 진행



AH 프로토콜

- IPsec 인증 헤더(AH)
  - 메시지 인증을 제공하는 확장 헤더
  - ESP에서도 메시지 인증이 제공되기 때문에 단독으로 사용은 권장하지 않음

  - 특징
    - 데이터 무결성(Integrity) 보장
    - 개체 인증(Authentication)
    - 재전송 공격에 대한 보호기능 제공
    - 인증 데이터를 만들기 위해 해시 알고리즘 사용
      - e.g., MD5, SHA-1

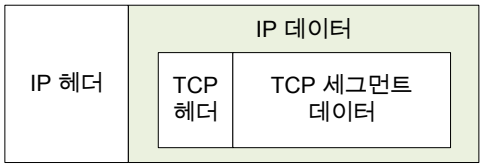
AH 프로토콜

- IPsec 인증 헤더(AH)
  - AH를 포함하는 패킷 포맷 그림

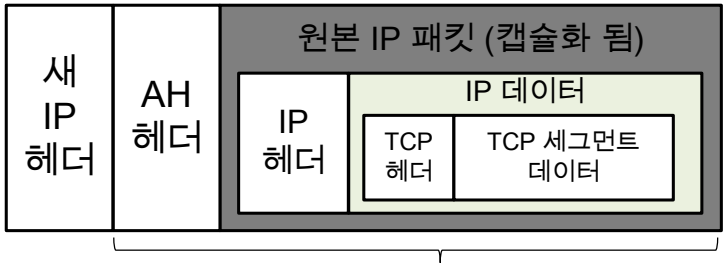
AH 프로토콜

- IPsec 보안 적용 모드
  - 전송모드와 터널모드 구현 그림

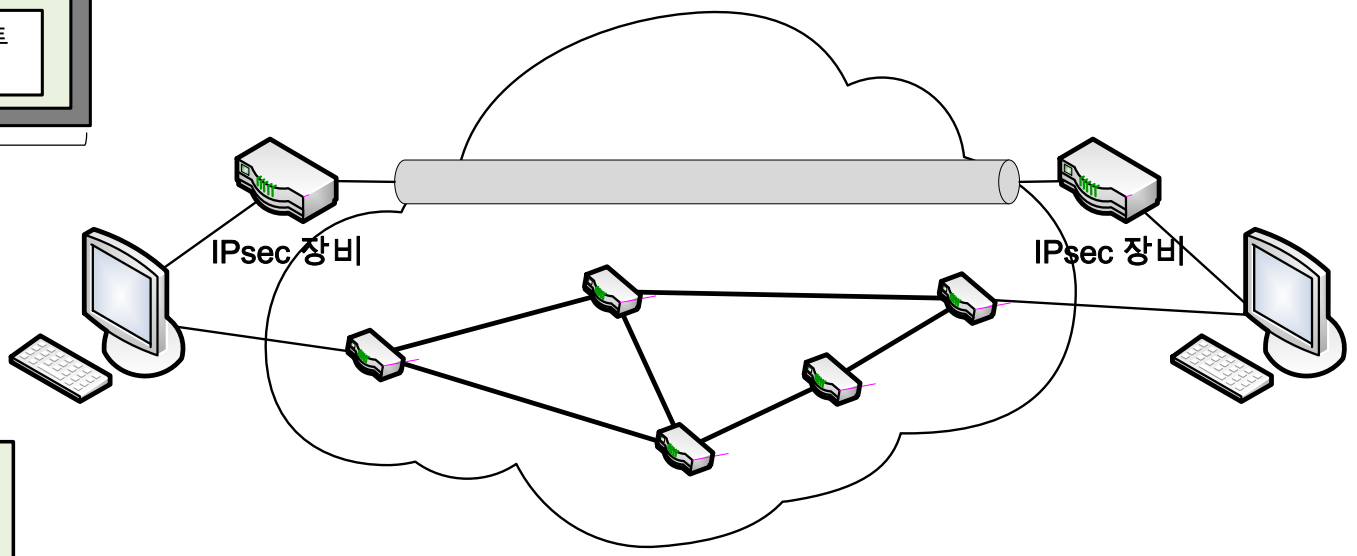
원본 데이터 포맷



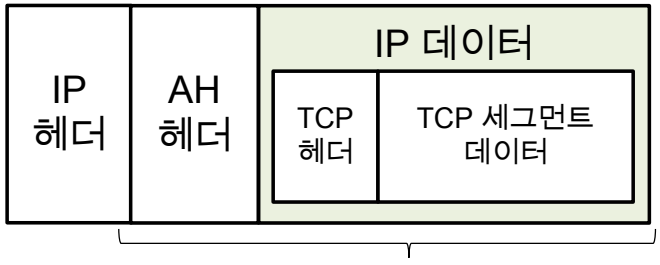
IPsec AH 터널모드 패킷 포맷



터널 모드 구현



IPsec AH 전송모드 패킷 포맷



전송 모드 구현

ESP 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - 암호화 또는 암호화/인증의 결합을 제공하기 위해 사용
  - 캡슐화 헤드와 트레일러로 구성

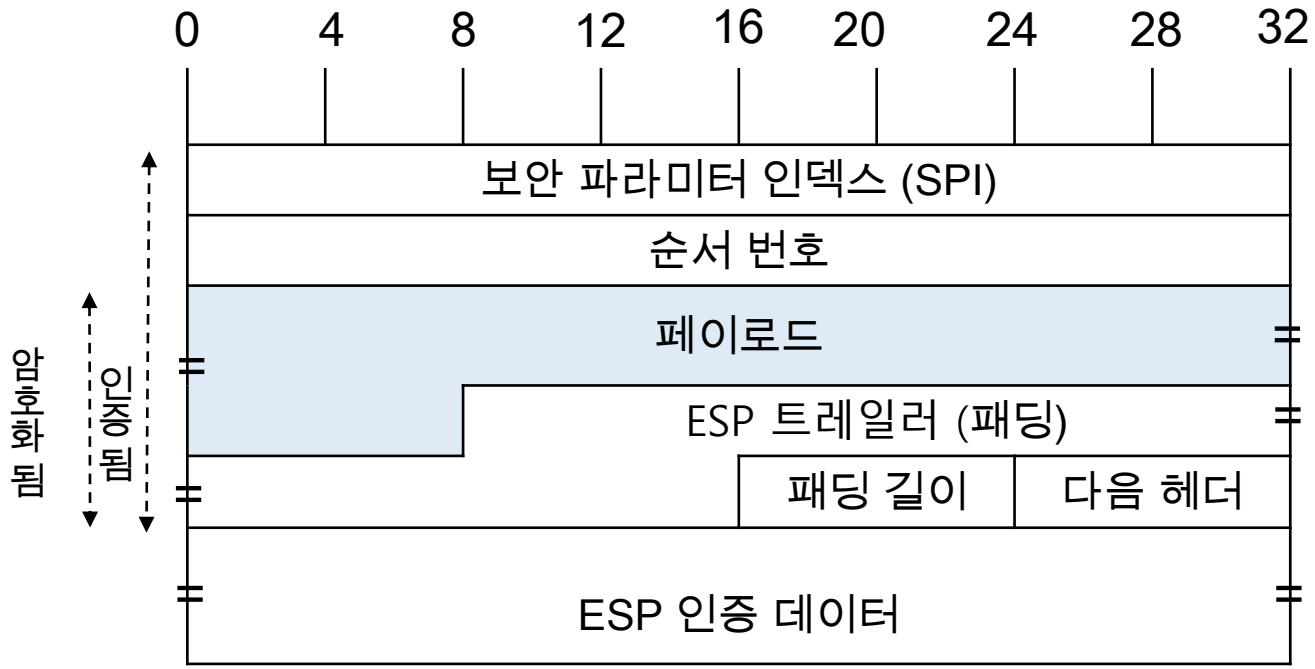
  - 특징
    - 데이터 무결성(Integrity) 보장
    - 개체 인증(Authentication)
    - 데이터 기밀성 제공
      - 수신 측에는 인터넷 키 교환 (IKE, Internet Key Exchange)로 미리 교환한 Key 값을 이용하여 데이터를 암/복호화
      - 사용되는 암호 알고리즘: DES, 3DES 등

ESP 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - 구성 요소
    - ESP 헤더
      - 두 가지 동작 모드에 따라 붙는 위치가 다름
      - 암호화 되지 않음
    - ESP 트레일러
      - 암호화 알고리즘으로 인해 패딩이 필요한 경우, 패딩을 한 뒤 암호화 수행
    - ESP 인증 데이터 필드
      - 인증 서비스 제공

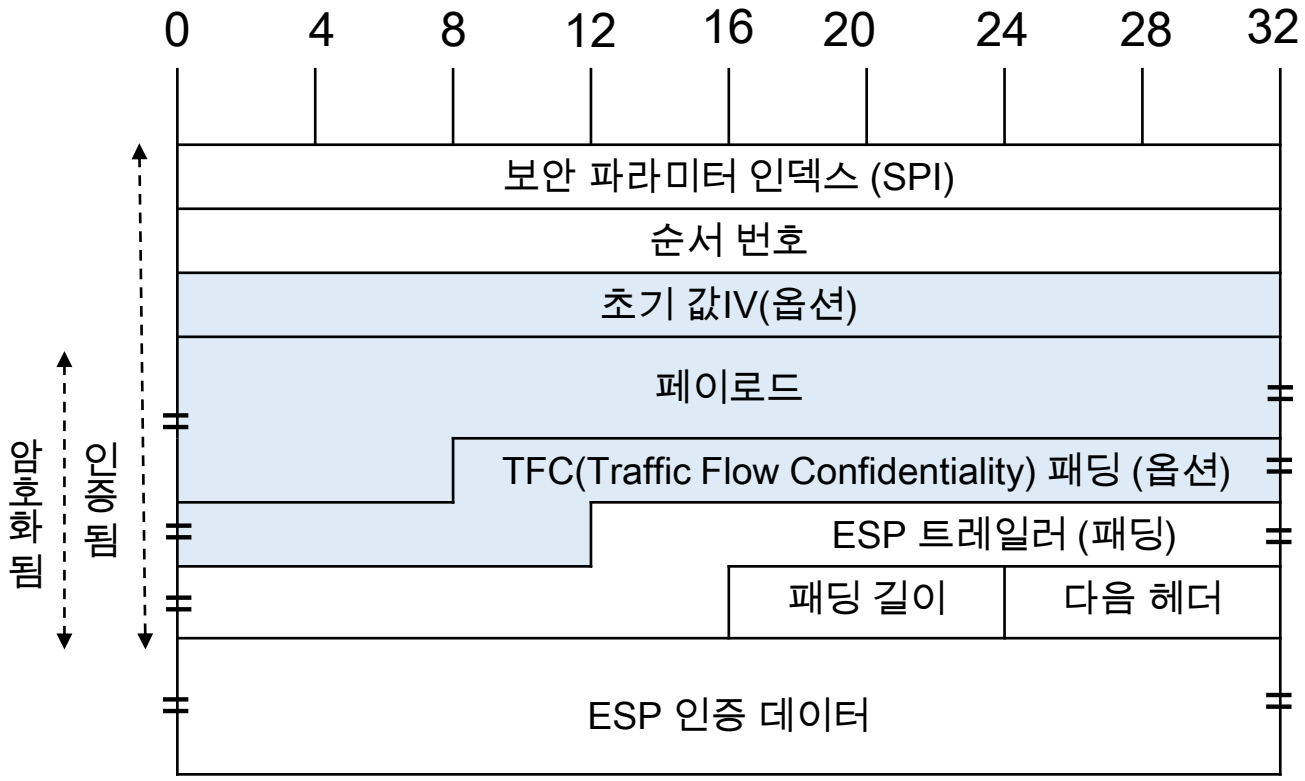
ESP 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - ESP를 포함하는 패킷 포맷



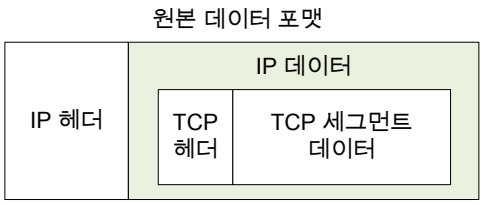
ESP 프로토콜

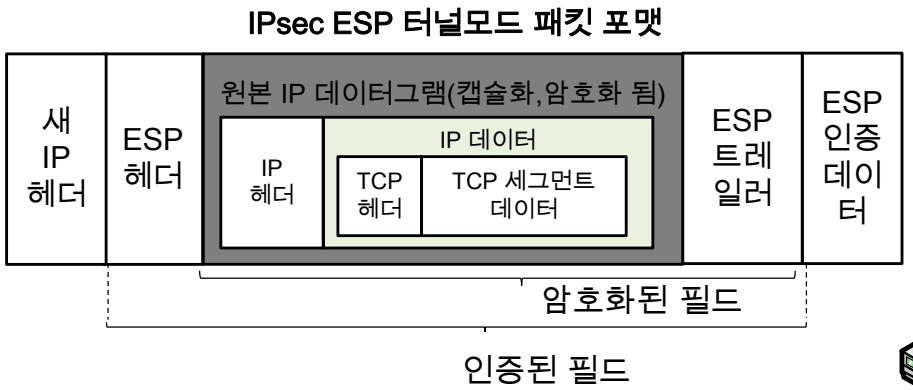
- IPsec 보안 페이로드 캡슐화(ESP)
  - ESP 페이로드 서브 구조 포맷

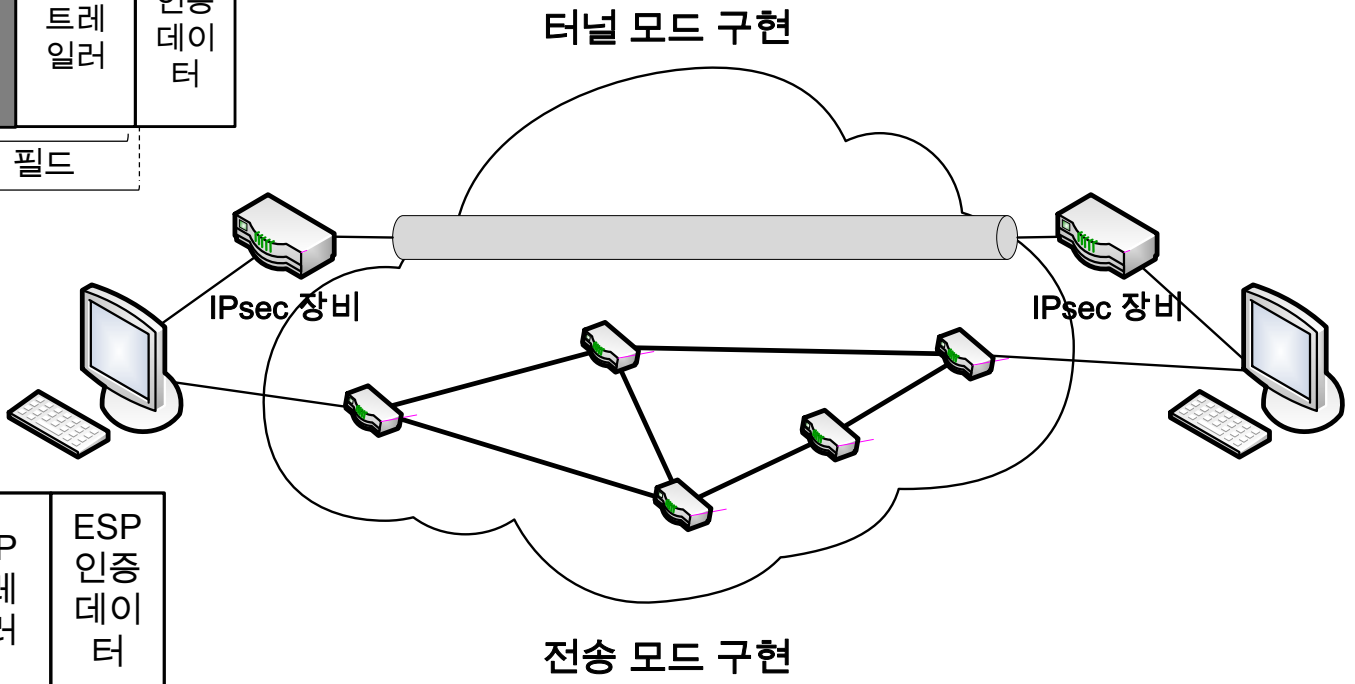


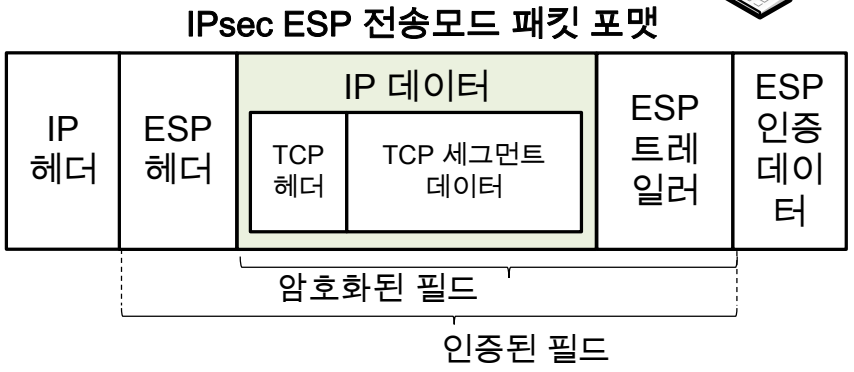
ESP 프로토콜

- IPsec 보안 적용 모드
  - 전송모드와 터널모드 구현 그림









SA와 SP

- 지원 구성 요소
  - 보안 정책(SP, Security Policy)
    - IP 트래픽의 보안 적용 여부와 보안 적용 시 어떤 보안을 적용하는지 보안 연관(SA) 유형을 정의
    - 보안 적용 여부(Discard, Bypass, Protect) 판단
    - 보안 정책 데이터베이스(SPD)에 저장될 요소
      - 목적지 IP 주소
      - 출발지 IP 주소
      - 출발지/목적지 포트 번호
      - 다음 계층 프로토콜

SA와 SP

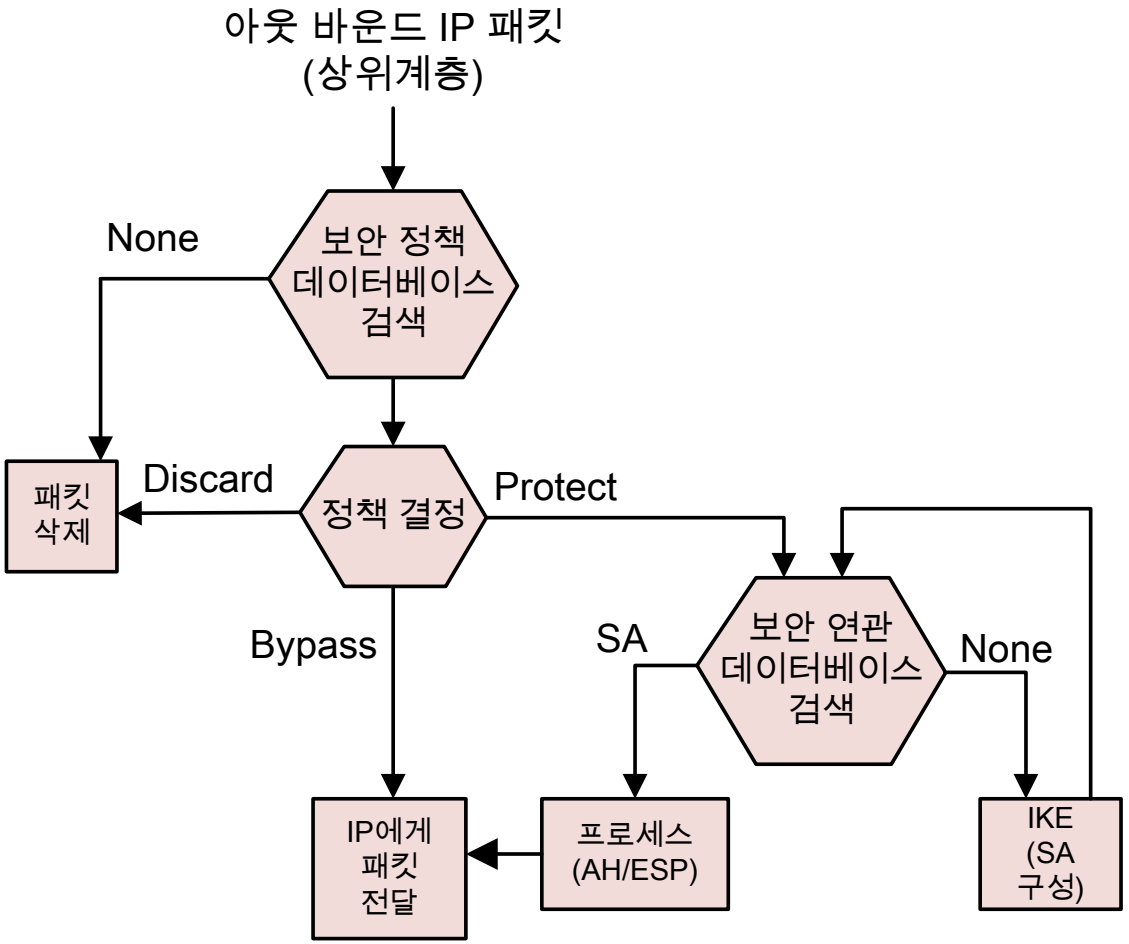
- 지원 구성 요소
  - 보안 연관(SA, Security Association)
    - 송/수신자간 보안 서비스를 제공하기 위해 정의된 요소
      - 보안 연관 데이터베이스(SAD)에 저장
    - 보안 연관을 식별하기 위한 파라미터(트리플)
      - 보안 인자 색인(SPI, Security Parameters Index)
        - SA를 식별하도록 수신자가 선택한 32 bit 값
      - IP 목적지주소
        - 최종 목적지 주소
      - 보안 프로토콜 식별자
        - AH/ESP 보안 연관 식별
          - 둘 다 사용하는 경우 각각 별도의 SA를 지정

SA와 SP

- 지원 구성 요소
  - 보안 연관(SA, Security Association)
    - 보안 연관 데이터베이스(SAD)에 저장될 요소
      - SPI: SA 식별
      - 순서번호 카운터: 패킷의 순서번호
        - 재전송 공격 방지
      - 순서계수기 오버플로우: 순서번호 카운터의 오버플로우감지 플래그
      - AH 정보: 인증 알고리즘, 키, 키의 갱신 주기와 관련된 AH 파라미터들을 포함
      - ESP 정보: 암호화, 인증 알고리즘, 키, IV, 키의 갱신주기와 관련된 ESP 파라미터들을 포함
      - 보안 연관 사용주기: SA의 갱신에 대한 정보, 주기, 갱신 지시 등을 포함
      - IPsec 프로토콜 모드: 터널/전송을 구분
      - 경로 MTU: 패킷 단편화를 하지 않기 위한 정보를 담은 값

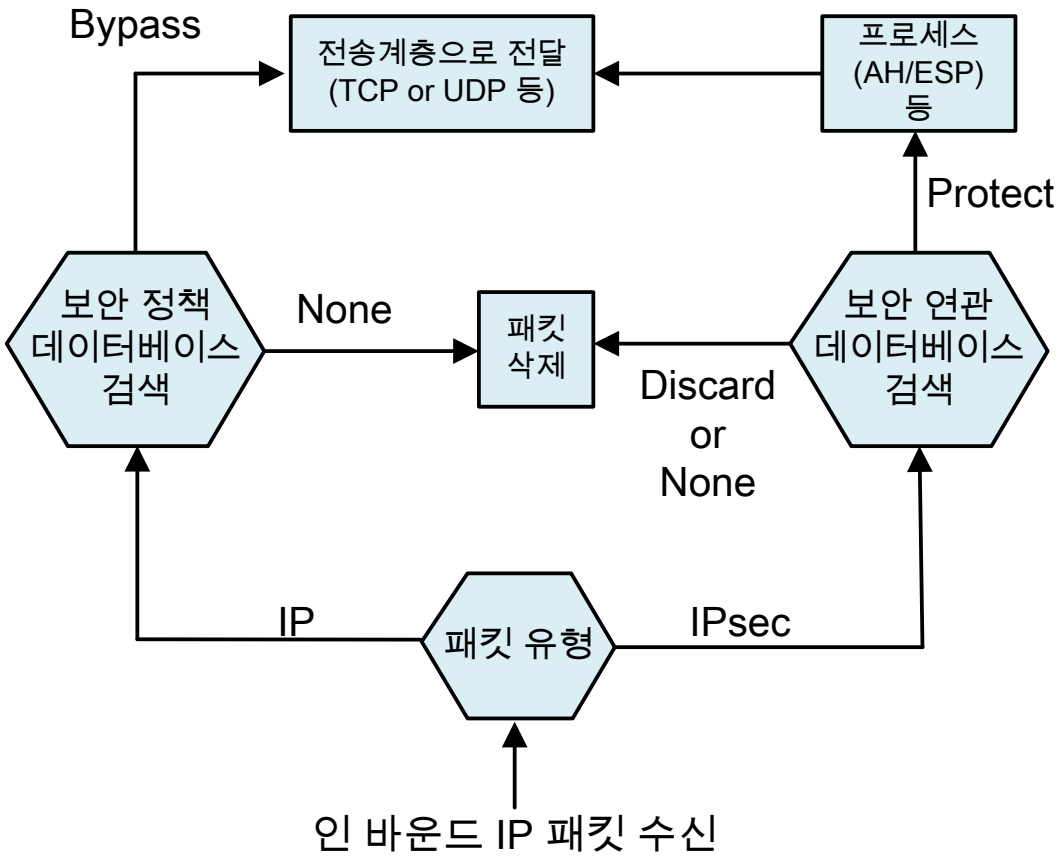
IPsec 동작

- IPsec 트래픽 처리
  - 아웃바운드 처리 모델 그림



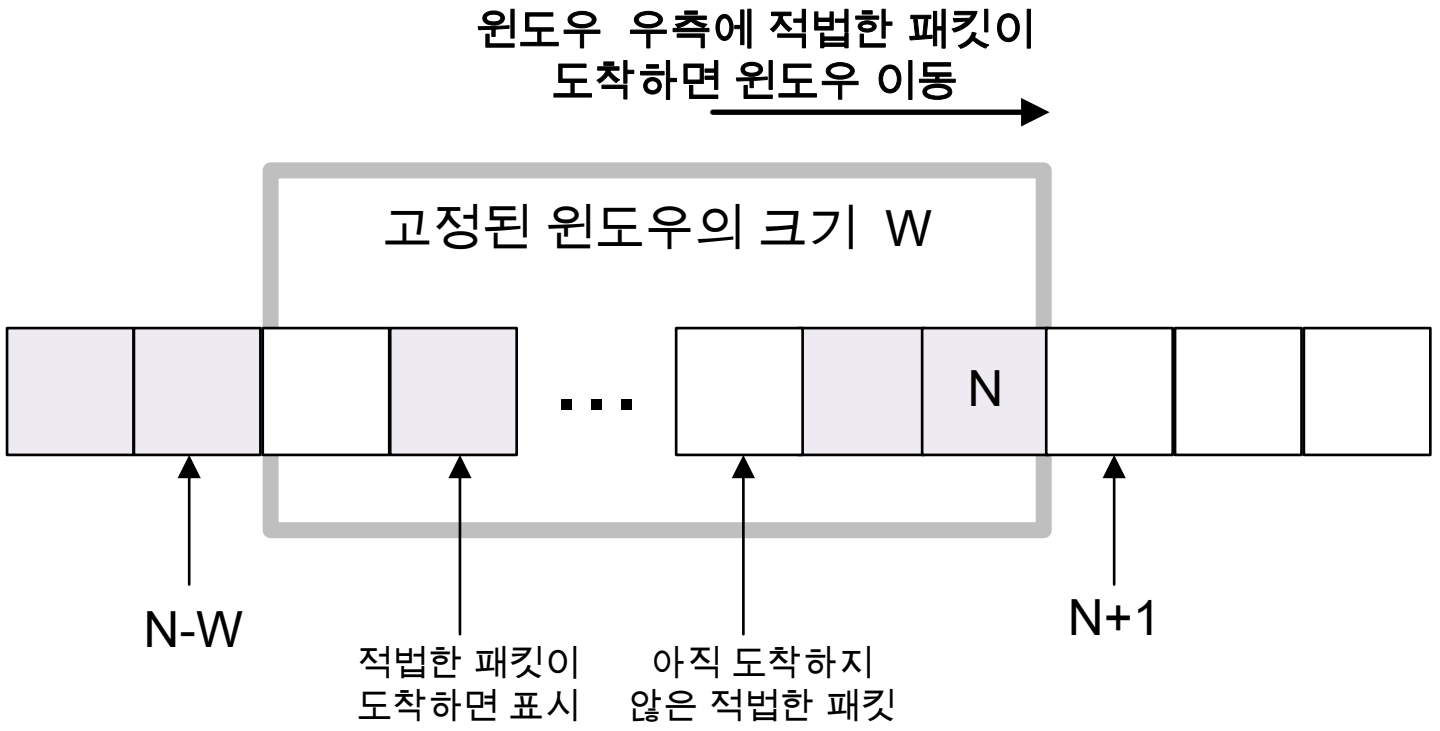
IPsec 동작

- IPsec 트래픽 처리
  - 인바운드 처리 모델 그림



IPsec 동작

- 재전송 공격 방지
  - IPsec 패킷에 대한 윈도우를 구현
  - 윈도우가 지나간 순서의 패킷은 Discard 처리



감사합니다!