IPsec

박승철교수

강의목표

- IPsec 구성
- IPsec 모드 : Transport, Tunnel
- 보안 연계(SA - Security Association)
- IKE(Internet Key Exchange)
- AH(Authentication Header) 프로토콜
- ESP(Encapsulating Security Payload) 프로토콜

IPsec 개요

IPsec 구성

- 보안 통신 당사자간의 키 관리 프로토콜(Key Management Protocol)인 IKE(Internet Key Exchange)
- 실제 보안 서비스를 제공하는 프로토콜인 AH(Authentication Header) 및 ESP(Encapsulating Security Payload)

IPsec의 대표적인 응용

- VPN(Virtual Private Network)
- 인터넷과 같이 공개된 네트워크 상에서 전용회선과 같이 보안이 유지되는 가상의 연결 서비스 제공
- 전용회선 대비 훨씬 싼 가격에 유사한 보안 수준의 연결 서비스 제공

IPsec 개요

❖ IPsec이 제공하는 보안 서비스

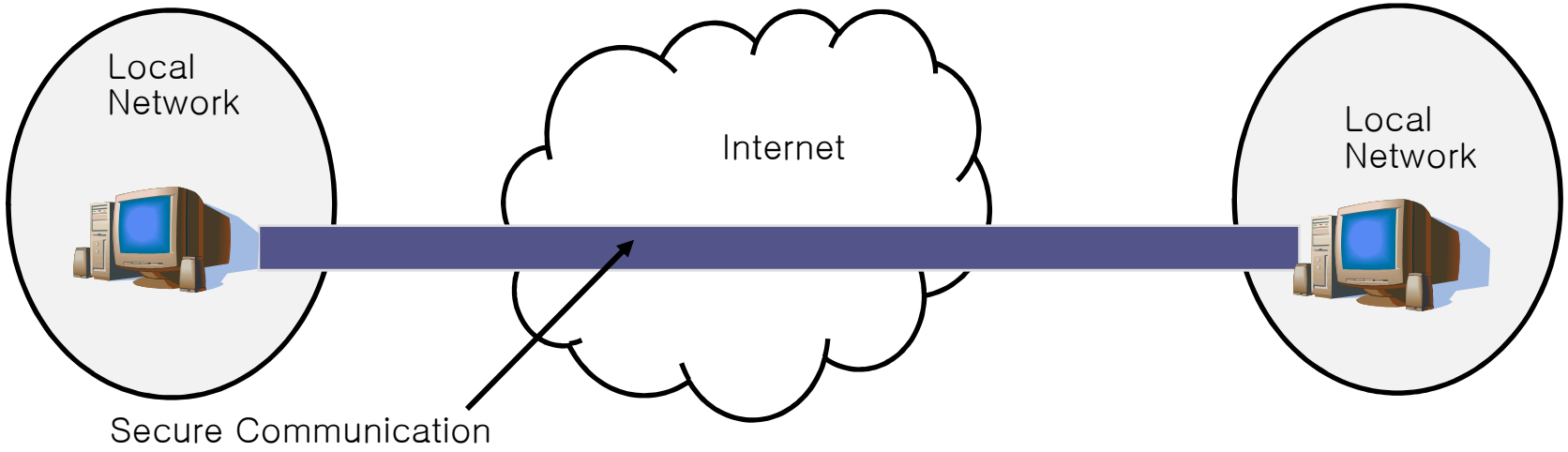
보안 서비스	AH 프로토콜	ESP 프로토콜
기밀성(Confidentiality)	X	O
출발지 인증(Source Authentication)	O	O
데이터 무결성(Data Integrity)	O	O
재현 공격 방지(Protection from Replay Attack)	O	O

IPsec 모드

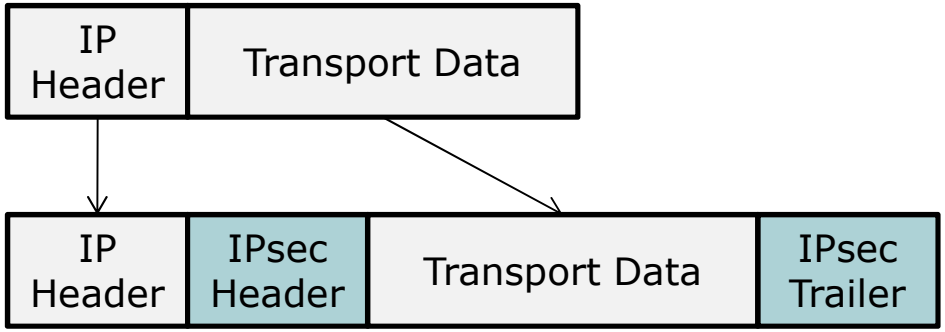
❖ 트랜스포트 모드(Transport Mode)

- 호스트와 호스트간의 통신을 보호하기 위해 사용
- IP 상위의 프로토콜 정보(주로 트랜스포트 프로토콜 정보)를 인터넷을 통해 안전하게 전달
- IP 헤더 다음에 IPsec 헤더 정보로 추가
- 관련 호스트들이 IPsec을 반드시 구현해야 함

트랜스포트 모드(Transport Mode)



(a) 트랜스포트 모드 개념

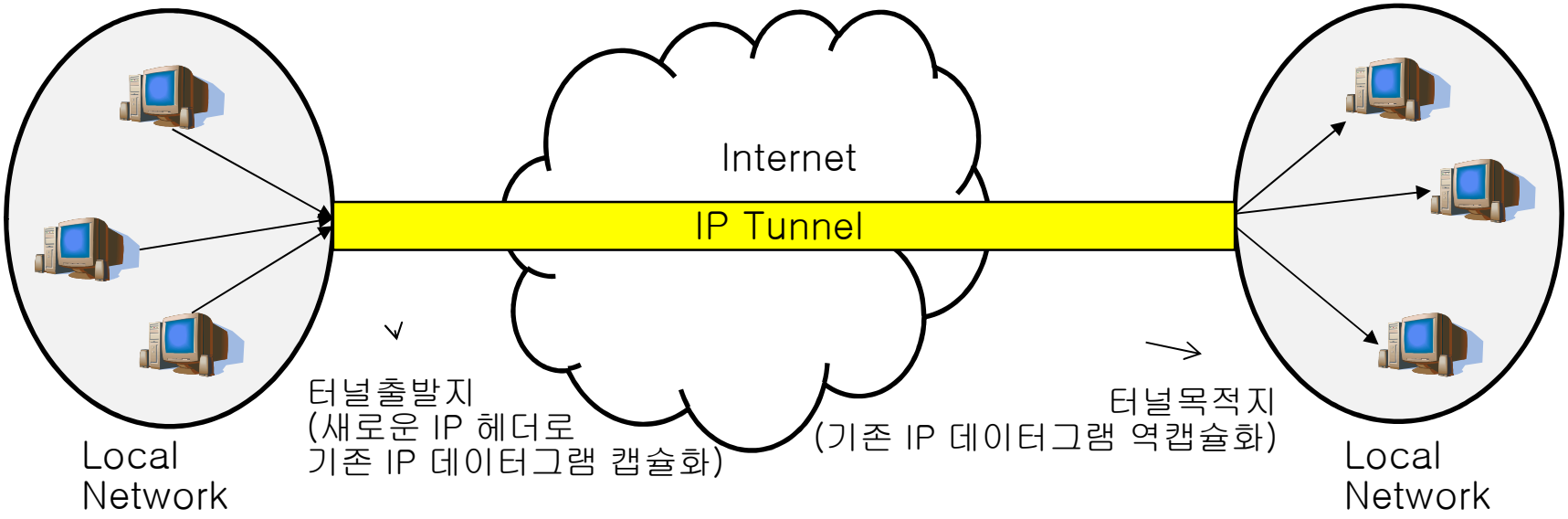


(b) 트랜스포트 모드 패킷 구조

IPsec 모드

❖ IP 터널

- IP 데이터그램들을 터널의 시작점에서 새로운 IP 데이터그램의 데이터로 캡슐화(encapsulation)하여 전송 → 원래 IP 데이터그램들을 한 묶음으로 처리
- 터널의 종점에서 원래의 IP 데이터그램을 복원하여 목적지로 전달하는 IP 계층의 가상 연결(Virtual Connection)

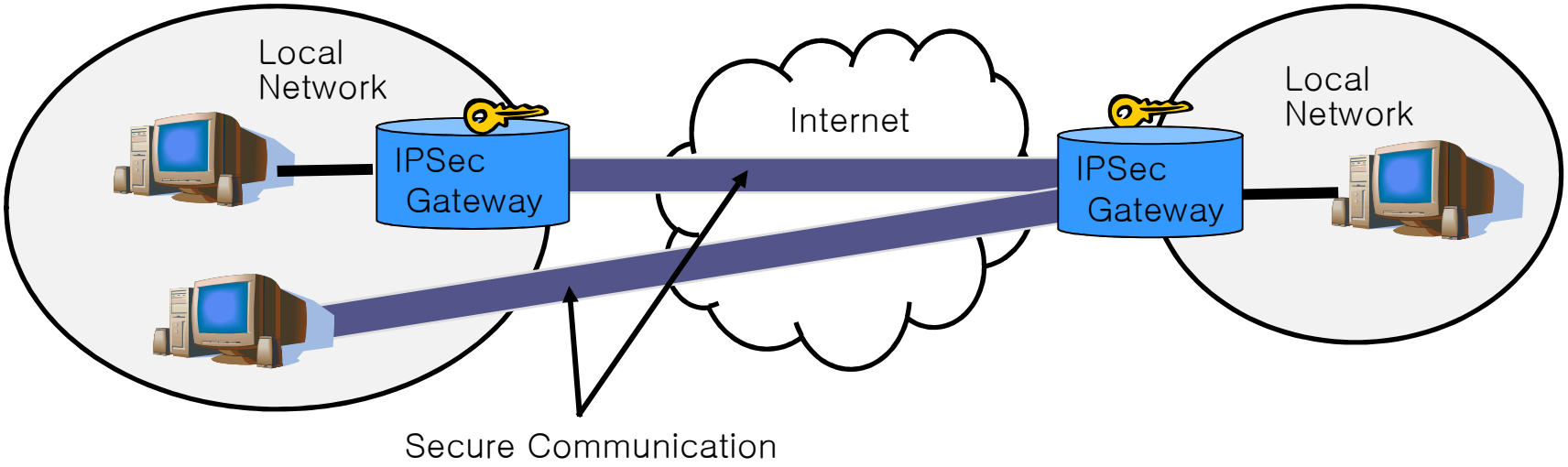


IPsec 모드

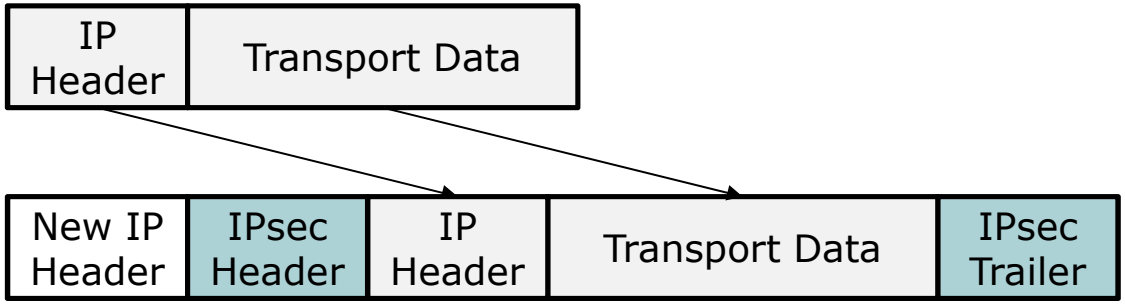
❖ 터널 모드(Tunnel Mode)

- 터널 구간을 통과하는 모든 IP 트래픽 보호
- 지역망내의 모든 호스트들의 터널 구간 IP 통신 보호
- 터널 시작점에서 추가되는 새로운 IP 헤더 다음에 IPsec 헤더로 추가
- 터널 시작점과 종점에 IPsec Gateway 설치
- 기존 호스트의 변경 없이 투명하게(Transparent) 보안 서비스를 제공

터널 모드(Tunnel Mode)



(a) 터널 모드 개념



(b) 터널 모드 패킷 구조

보안 연계(Security Association) 설정

❖ 보안 연계(SA - Security Association)

- IPsec 장치간에 보안 통신 방식에 대한 합의 → IPsec 장치간의 보안 서비스 매개변수들의 설정
- 보안 매개변수 : 보안 프로토콜 종류, 메시지 인증 알고리즘, 메시지 인증 키, 암호화 알고리즘, 암호화 키, 순서번호 등
- 양방향 통신을 보호하기 위해서는 두 개의 SA 설정
- 필요에 따라 다수의 SA를 설정하고 동적으로 SA 변경

→ SA 확립을 위해 보안 매개변수들을 안전하게 상호 합의할 수단 필요 : 수작업 또는 통신 프로토콜

보안 연계(Security Association) 설정

❖ 설정 방법

- 수작업 키 관리(Manual Key Management)로 설정
  → 확장성 결여
- IKE(Internet Key Exchange) 프로토콜을 통한 설정
  → 초기 보안 채널(암호화 키 교환) 설정 필요

❖ ISAKMP(Internet Security Association and Key Management Protocol)

- Diffie-Hellman을 개선한 Oakley 기법 기반의 IKE 프로토콜
- 1단계로 IKE 보안 채널 설정 후 2단계로 IPsec SA 설정

IKE(Internet Key Exchange)

❖ IKE 보안 채널(IKE SA)

- IPsec 장치간에 SA 설정을 위한 메시지들을 대칭키 암호화 기법으로 안전하게 전달할 수 있는 보안 채널
- Diffie-Hellman 기법을 개선한 Oakley 기법으로 설정 (안전하게 암호화 키 교환)

❖ IPsec SA 설정

- IKE 보안 채널을 통해 IPsec 단말간에 IPsec SA 설정을 위한 메시지들을 안전하게 교환 → 단방향 SA 설정, 다수 SA 설정 가능
- 필요할 때마다 IPsec SA를 자유롭게 변경 가능

IKE 보안 채널 설정

❖ Diffie-Hellman 키 교환의 문제점

- 방해 공격(Clogging Attack)
  - 공격자가 IP 주소를 위조하여 특정 통신 장치에 대해 DH 기법으로 계산이 복잡한 많은 수의 비밀 세션키를 만들도록 시도
    → DoS 공격

- 중간자 공격(Man-In-The-Middle Attack) :
  - 공격자가 공개키인 반키(Hlaf-Key) 가로채고 자신의 반키 제공

- 재현 공격(Replay Attack) :
  - 반키(Half-Key) 정보를 가로챈 제3자가 재사용하여 합법적인 사용자인 것처럼 비밀 키 생성 시도

IKE의 Oakley 기법

❖ DoS 공격 방어 : 쿠키(Cookie)

- 쿠키를 수신한 사용자간 세션키 생성만 가능

- 쿠키 : 출발지 IP 주소, 목적지 IP 주소, 출발지 포트 번호, 목적지 포트 번호, 쿠키 생성자의 비밀 랜덤 번호, 그리고 타임 스탬프(Timestamp)를 해시 함수(예, MD-5)로 해싱한 값
  → 공격자는 쿠키 추론 불가

- DH 기법에서 공개키인 반키(half-Key) 교환 전에 비밀 키를 생성하고자 하는 통신 장치간에 쿠키를 먼저 교환

- 메시지 교환 시(예, 반키 등)에 반드시 자신의 쿠키와 함께 상대방의 쿠키 정보를 함께 전달
  → 쿠키를 수신하지 못한 공격자(IP 스푸핑)는 반키 전송 불가 (세션키 생성 요청 불가) → IP 스푸핑 기반의 DoS 공격 방지

IKE의 Oakley 기법

❖ 중간자 공격 방어 : 메시지 인증

- DH 기법의 중간자 공격을 방지하기 위해 통신 장치간에 교환되는 모든 메시지 인증(Message Authentication Code)

❖ 재현공격 방어 : 넌스(Nonce)

- 반키(Half-Key)를 교환할 때 임의의 임시 번호인 넌스를 포함하여 전달
- 다음에 부여할 넌스를 알 수 없는 제3의 사용자에 의한 반키 재사용을 통한 재현 공격(Replay Attack) 방지

IKE의 메시지 인증 기법

1. 비밀 키 사전 공유 기법(Pre-shared Secret Key Method) :

- 2개의 IPsec 장치가 비밀 키(Secret Key)를 사전에 공유
- IKE 메시지를 전송하는 장치는 자신이 전송하는 메시지에 대한 무결성 보장을 위한 해시 함수 계산에 비밀 키를 포함하여 계산

IKE의 메시지 인증 기법

2. 공개키 암호화 기법(Public-key Encryption Method):

- IPsec 장치 A가 먼저 임의의 번호인 넌스 값을 사전에 알려진 상대방 IPsec 장치 B의 공개키로 암호화 하여 전송
- IPsec 장치 B는 자신의 개인키(Private Key)로 A로부터 수신한 넌스 값을 복호화한 후, 넌스 값이 포함된 IKE 메시지의 해시 함수 결과 값을 IKE 메시지와 함께 IPsec 장치 A에게 전송
- IPsec 장치 A는 자신이 전송한 원래의 넌스 값을 포함시켜 수신된 IKE 메시지에 대한 해시 함수 결과 값을 생성하여 수신된 해시 함수 결과 값과 비교
- 상대방이 정상적으로 넌스 값 복호화 여부 확인

IKE의 메시지 인증 기법

3. 디지털 서명 공개키 기법(Digital Signature Public Key Method):

- 송신 IKE 장치가 메시지에 디지털 서명 정보를 포함하여 전송함으로써 수신 IKE 장치는 메시지 송신자를 인증하고 위조되지 않았음을 확인
- 송신자의 공인 인증서(certificate)와 함께 전송됨으로써 송신자의 공개키가 수신자에게 전달되어 수신자가 서명 정보 확인

IKE SA와 IPsec SA

IKE SA

- 개선된 DH 기법인 Oakley 기법 기반의 ISAKMP에 의해 설정되는 보안 연계
- 1단계 SA

IPsec SA

- IKE SA를 통해 송신자와 수신자는 메시지 교환을 안전하게 수행하여 IPsec SA 설정
- 송신자와 수신자는 AH 또는 ESP가 필요로 하는 인증 알고리즘과 인증 키, 암호화 알고리즘과 암호화 키를 포함하는 모든 보안 매개변수들을 동기화

IKE SA와 IPsec SA

IPsec SA 구별

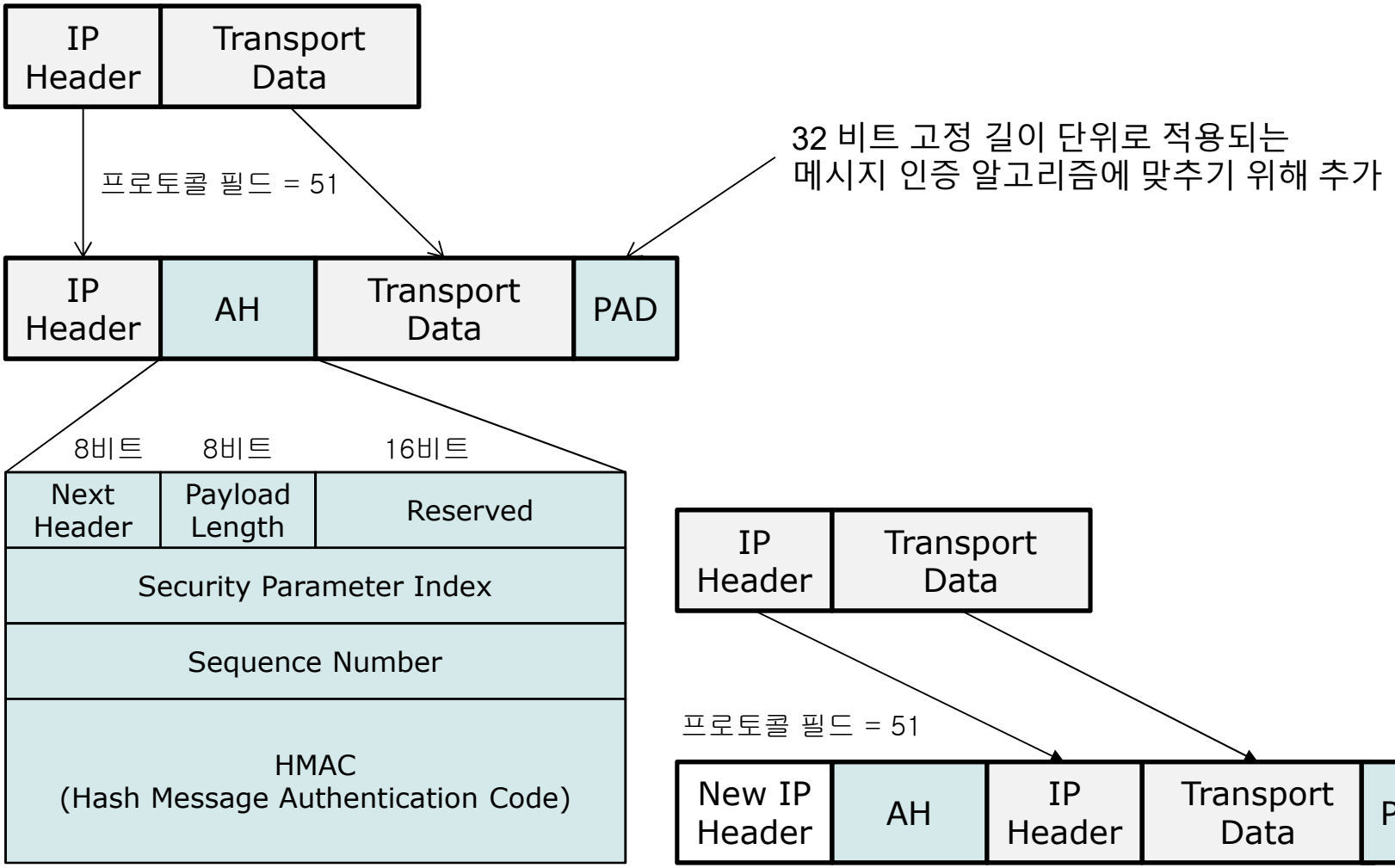
- 사용할 보안 프로토콜(AH 또는 ESP) 식별자
- 관련 SA의 출발지 주소
- SA에서 사용할 보안 매개 변수들의 집합에 대한 인덱스(SPI – Security Parameter Index)

AH(Authentication Header) 프로토콜

AH:

- IP 데이터그램 무결성(Data Integrity)을 보장하고, 출발지 호스트를 인증(Source Authentication)하며, 재현 공격(Replay Attack)을 방지
- HMAC : 무결성 보장, 출발지 인증
- 순서 번호 : 재현 공격 방지
- 메시지 인증 알고리즘과 키는 IPsec SA 설정 과정에서 결정

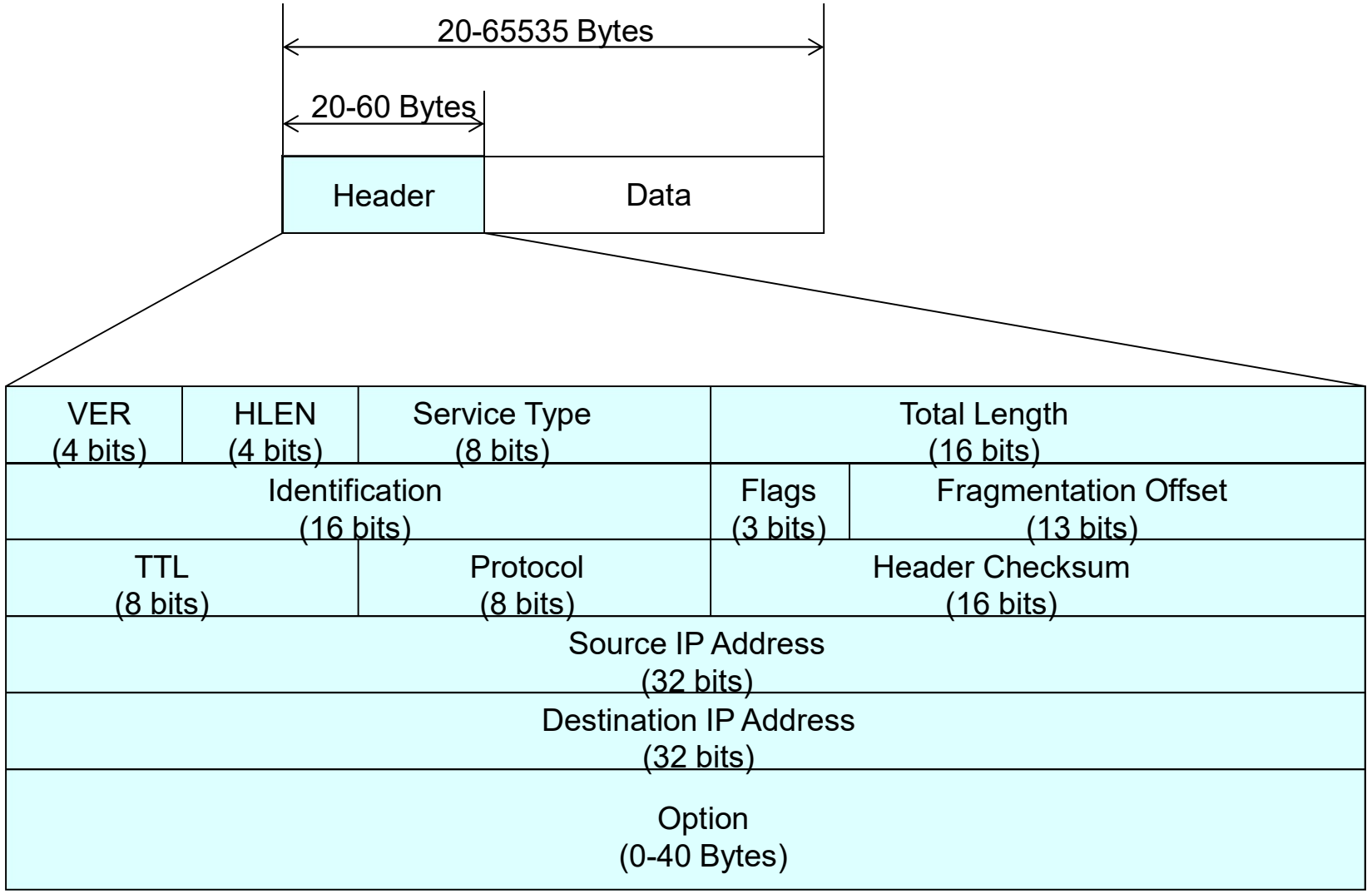
AH 프로토콜의 헤더의 위치와 구조



(a) 트랜스포트 모드

(b) 터널 모드

IP 데이터그램

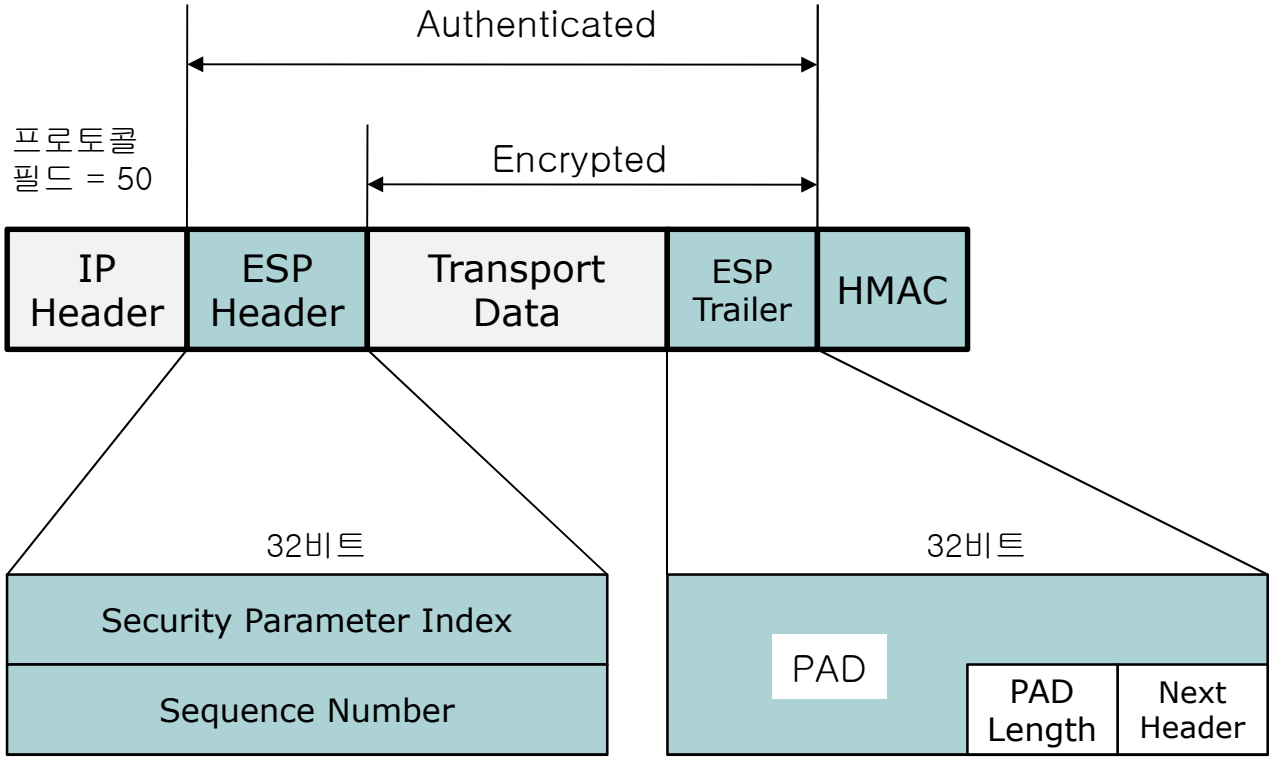

20-65535 Bytes
20-60 Bytes
Header
Data
VER (4 bits)
HLEN (4 bits)
Service Type (8 bits)
Total Length (16 bits)
Identification (16 bits)
Flags (3 bits)
Fragmentation Offset (13 bits)
TTL (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
Source IP Address (32 bits)
Destination IP Address (32 bits)
Option (0-40 Bytes)

ESP(Encapsulating Security Payload) 프로토콜

ESP:

- IP 데이터그램 무결성(Data Integrity)을 보장하고, 출발지 호스트를 인증(Source Authentication)하며, 재현 공격(Replay Attack)을 방지하고, 기밀성(Confidentiality) 서비스를 제공
- HMAC : 무결성 보장, 출발지 인증
- 순서 번호 : 재현 공격 방지
- 대칭키 암호화 : 기밀성 보장
- 메시지 인증 알고리즘과 키, 암호화 알고리즘과 키는 IPsec SA 설정 과정에서 결정

ESP 프로토콜의 헤더의 위치와 구조



(a) 트랜스포트 모드

(b) 터널 모드