A Top-Down Approach

chapter 8.7 ~8.9

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

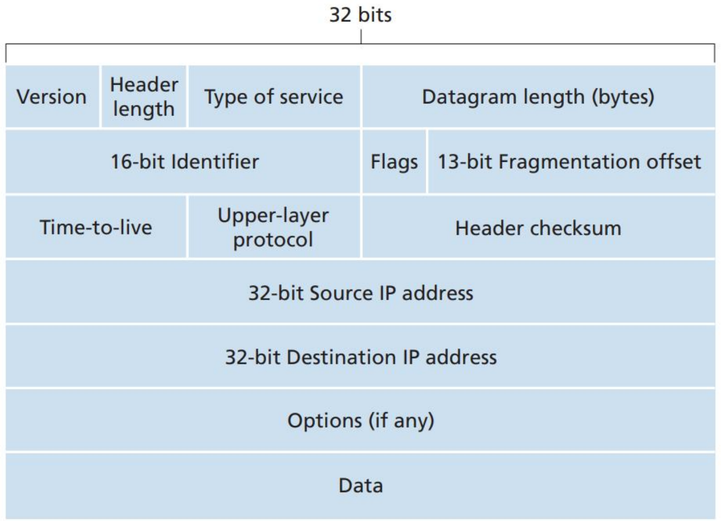
- Network layer에서 IP패킷을 암호화하고 인증하는 등의 보안을 위한 표준이다.
- **기업에서 사설 인터넷망으로 사용할 수 있는 VPN을 구현하는데 사용되는 프로토콜이다.**
- AH(Authentication Header)와 ESP(Encapsulating Security Payload)라는 두 가지 보안 프로토콜을 사용한다.

-2024 정처기 실기 2회차 일부

→ **IPsec**

발표자: 박지원

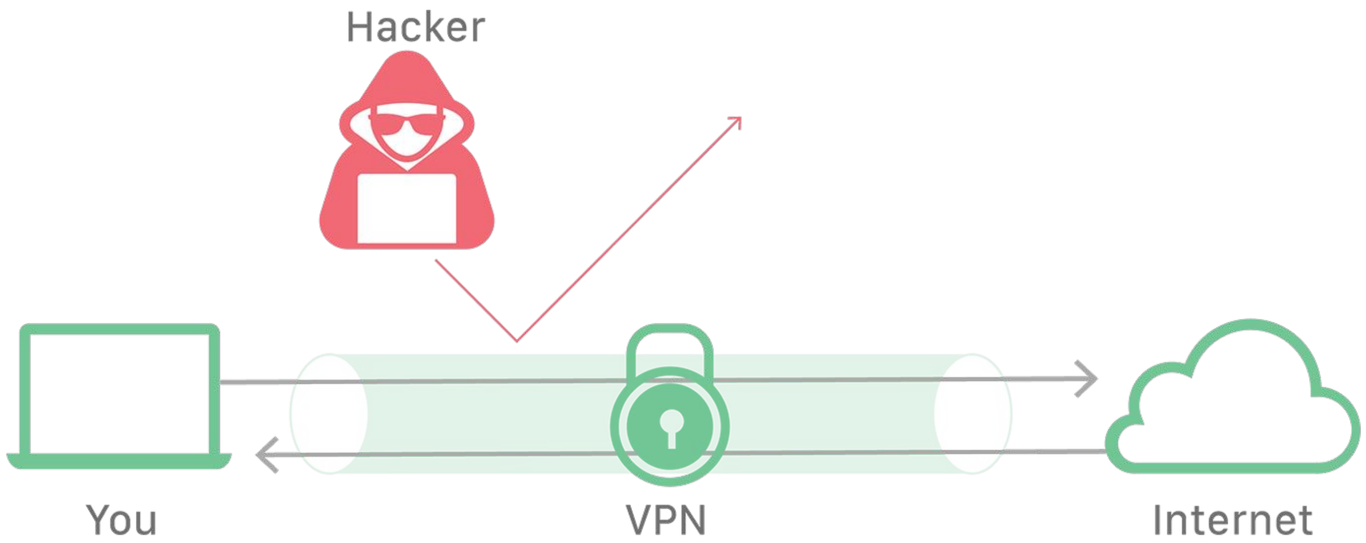
8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크



VPN은 IP를 우회하는 기법이다.
송신자의 IP를 조작한다.
IP와 checksum 이외에 조작할게 있을까?
datagram은 조작하지 않아도 무방할까?

발표자: 박지원

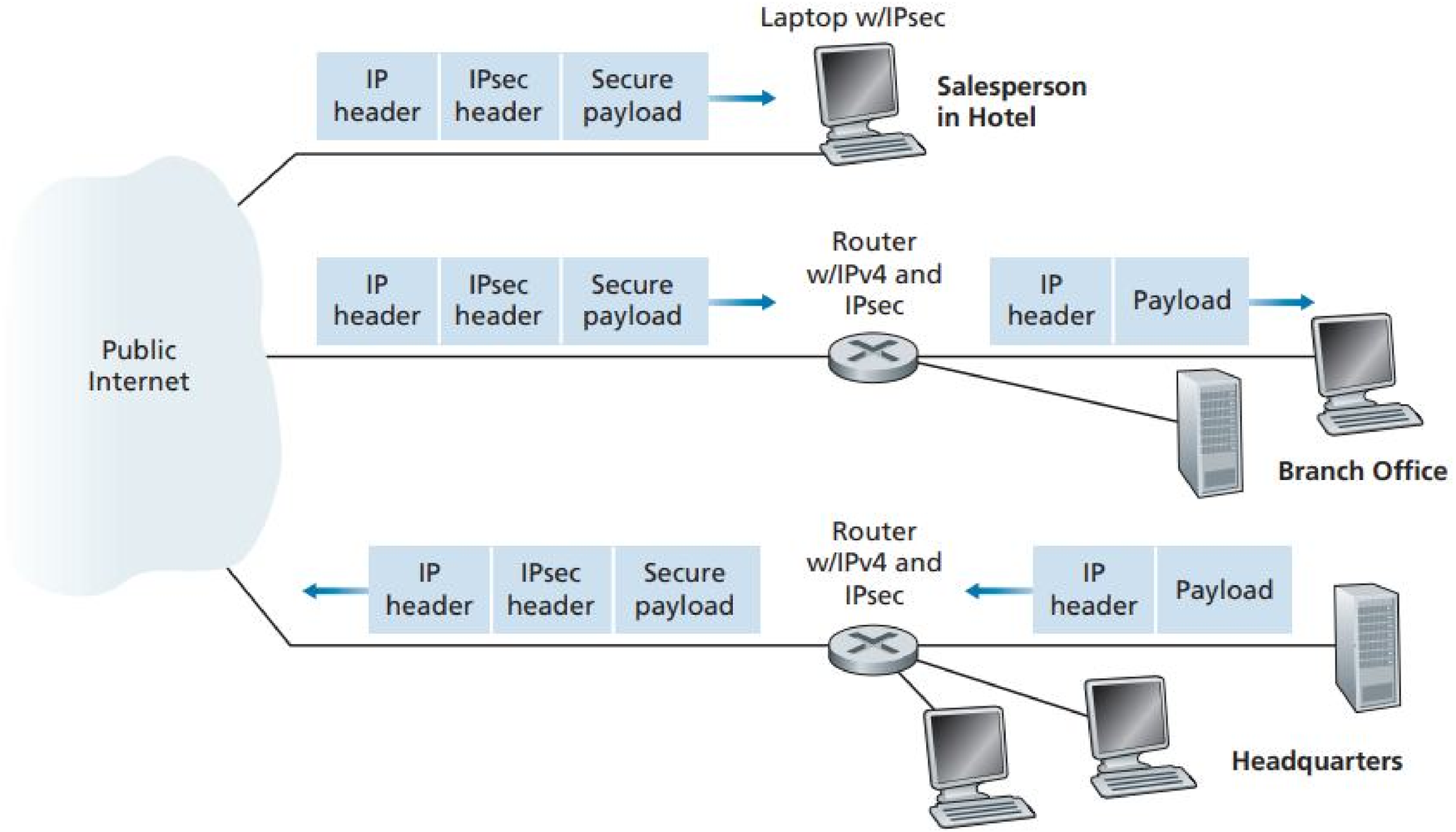
8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크



VPN과 IPsec는 다른 영역이다. VPN을 위해 IPsec를 사용한다 정도
ip 주소 변경 이외에도 datagram을 암호화한다.
굳이 datagram을 암호화해야할까? (TLS를 했다면 header 말고 암호화 되었을 텐데?)

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크



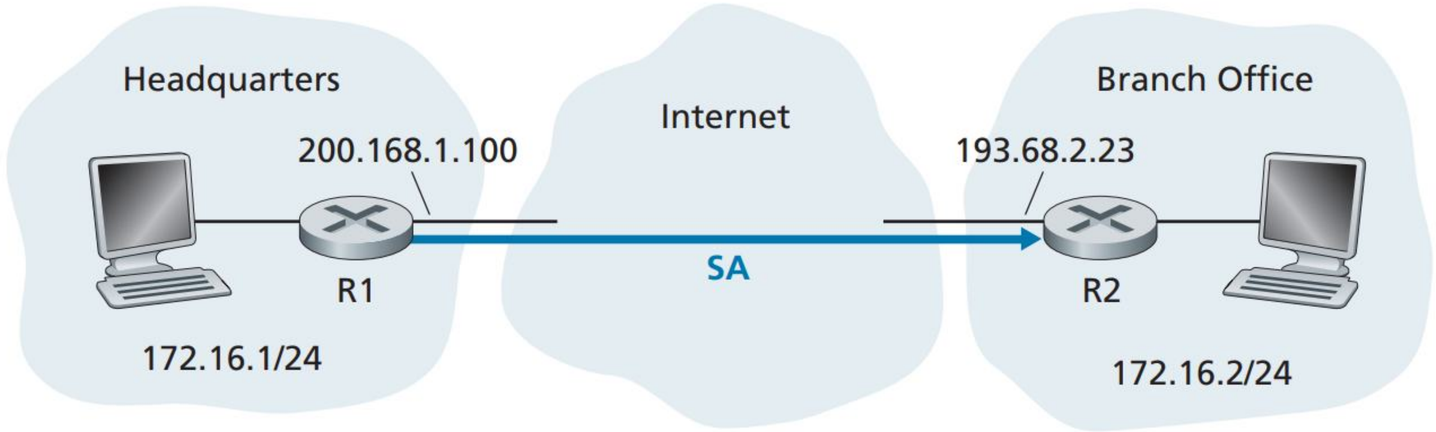
라우터가 IPsec datagram으로 변환

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

AH(Authentication header): 출발지 인증 O, 데이터 무결성 O, 기밀성 X
ESP(Encapsulation Security Payload): 출발지 인증 O, 데이터 무결성 O, 기밀성 O

SA(security association): 네트워크 계층에서 논리적 연결 (2n+2)

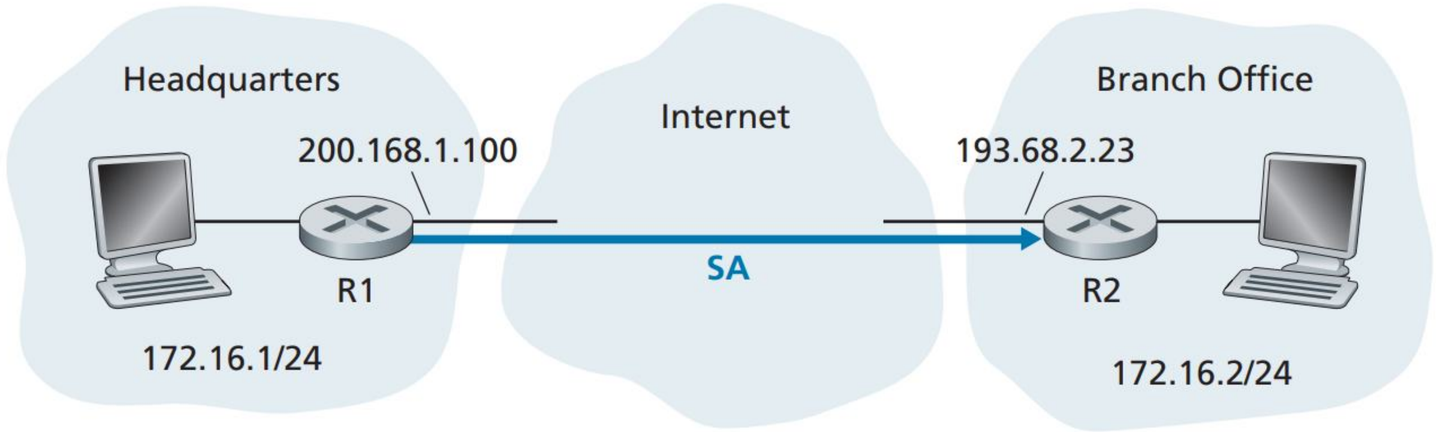


SPI(Security Parameter Index): SA 식별자
origin interface: 200.168.1.100, dst interface: 193.68.2.23
encryption type: 3DES, encryption key
integrity check(HMAC), key

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

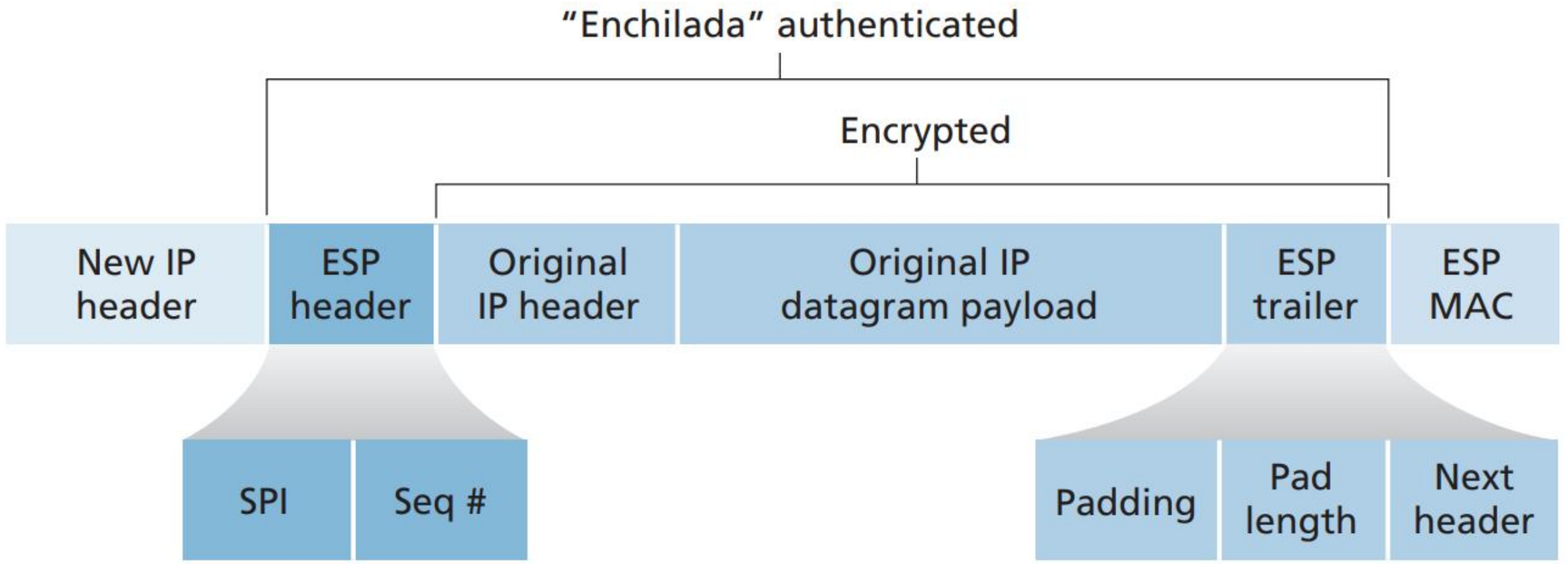
SAD(Security Association Database) → 라우터 소유
key와 type을 어떻게 dst에게 전달하죠? → IKE



터널 모드(tunnel mode):
전송 모드(transport mode): 다루지 않는다

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

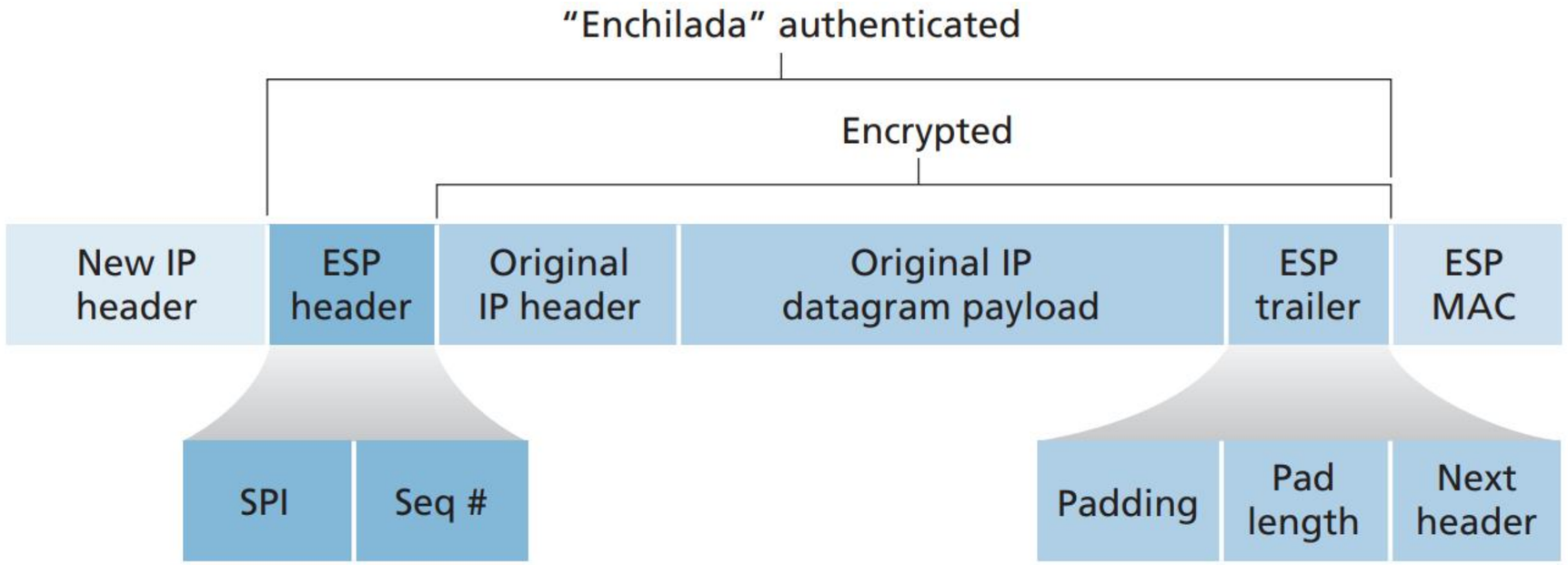


상황: 라우터 R1가 172.16.1.17 으로 부터 172.16.2.48에게 보내는 IPv4 데이터 그램을 받았다.

1. **ESP trailer 추가(padding, pad length, next header) 왜 next header가 필요?**
2. **SA에 의해 암호화**
3. **ESP header 추가 (enchilada)**

발표자: 박지원

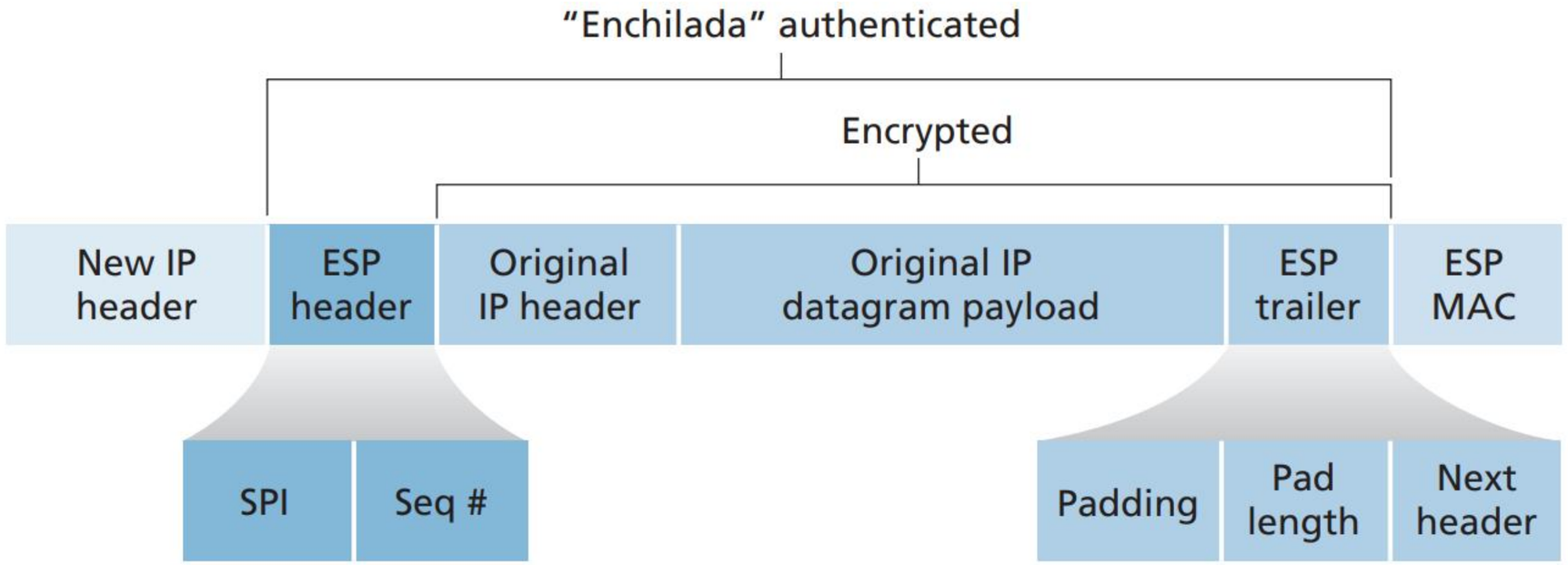
8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크



4. Enchilada 인증 mac 생성 → 페이로드
5. ip header 추가(프로토콜, ip 주소 변경)

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

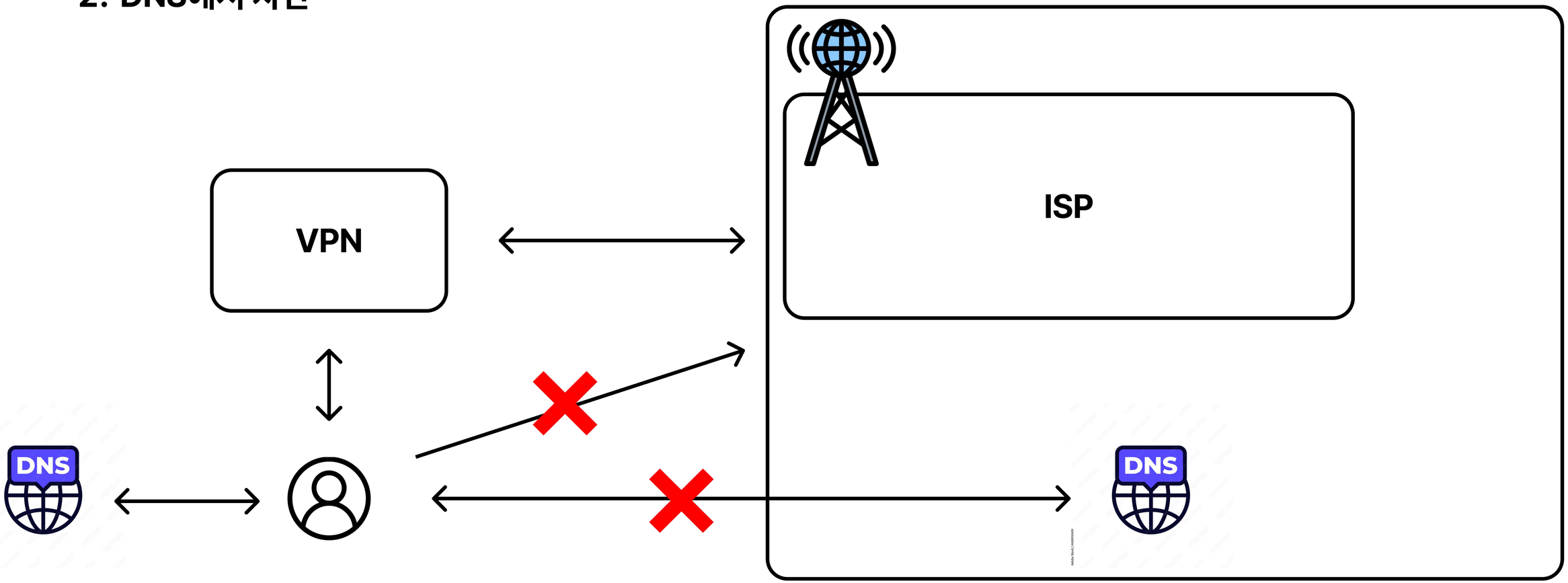


1. 상위 프로토콜 확인 50 → IPsec
2. SPI를 통해 SA 확인
3. MAC 계산 (무결성 확인)
4. seq 확인
5. 복호화

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

1. ISP에서 차단
2. DNS에서 차단

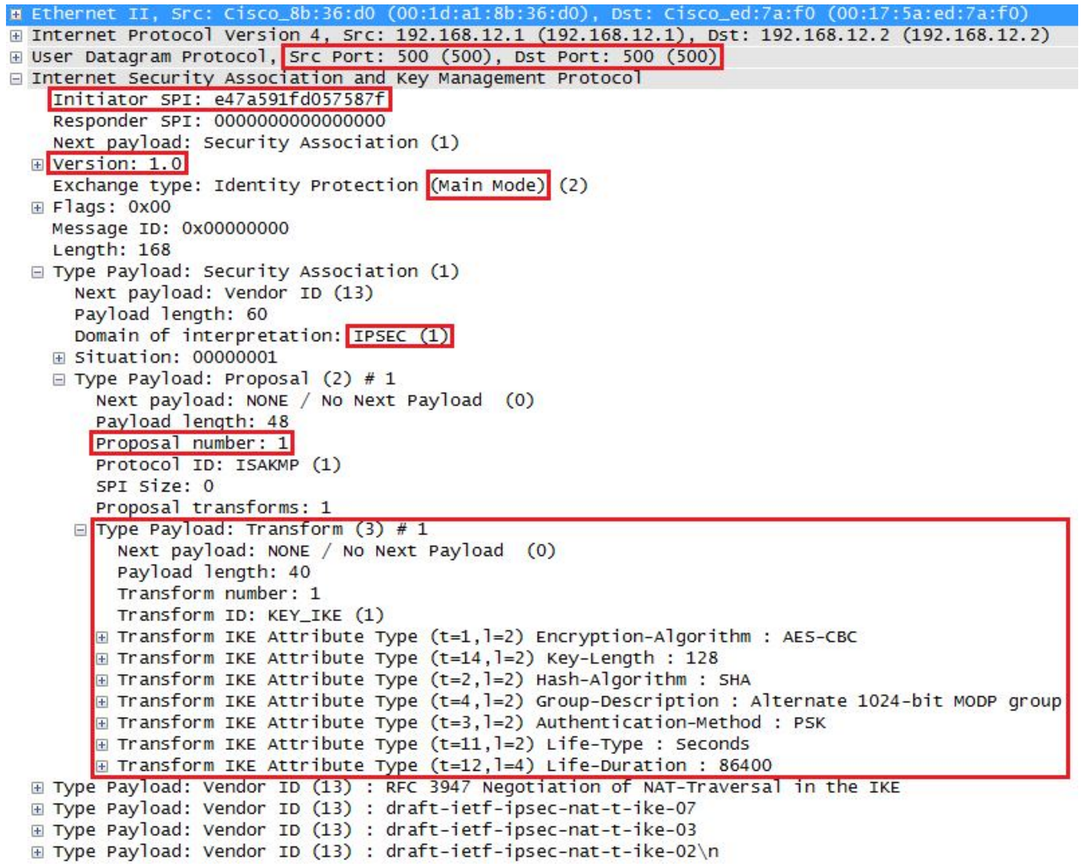


발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

IKE(Internet Key Exchange): SA를 결정하고, 교환한다. (version 1)

1. 정책 결정
2. 암호화 데이터 송수신



SA는 누가 결정하는데?
결정과정에서 데이터가 노출될 위험은 없을까?

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

1 Step

1. **default mode**
2. **aggressive mode**

제안 1: AES(암호화 알고리즘) + SHA(해시 알고리즘) + Diffie-Hellman Group 2 + 프리셰어드 키(인증) + SA 수명 1시간.
제안 2: 3DES(암호화 알고리즘) + MD5(해시 알고리즘) + Diffie-Hellman Group 5 + 디지털 인증서(인증) + SA 수명 2시간
2번 선택

발표자: 박지원

8.7 네트워크 계층 보안 IPsec과 가상 사설 네트워크

2 step: SA 내부 값 결정

```
crypto ipsec transform-set myset esp-aes esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set myset
 match address 100
!
RouterA#
*Mar  1 02:43:19.259: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed wit

RouterA#ping 172.16.2.1 sour 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.2
.....
Success rate is 0 percent (0/5)
RouterA#sho crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        MM_NO_STATE          1    0 ACTIVE (deleted)
10.0.0.2        172.16.1.1      MM_NO_STATE          2    0 ACTIVE (deleted)
```

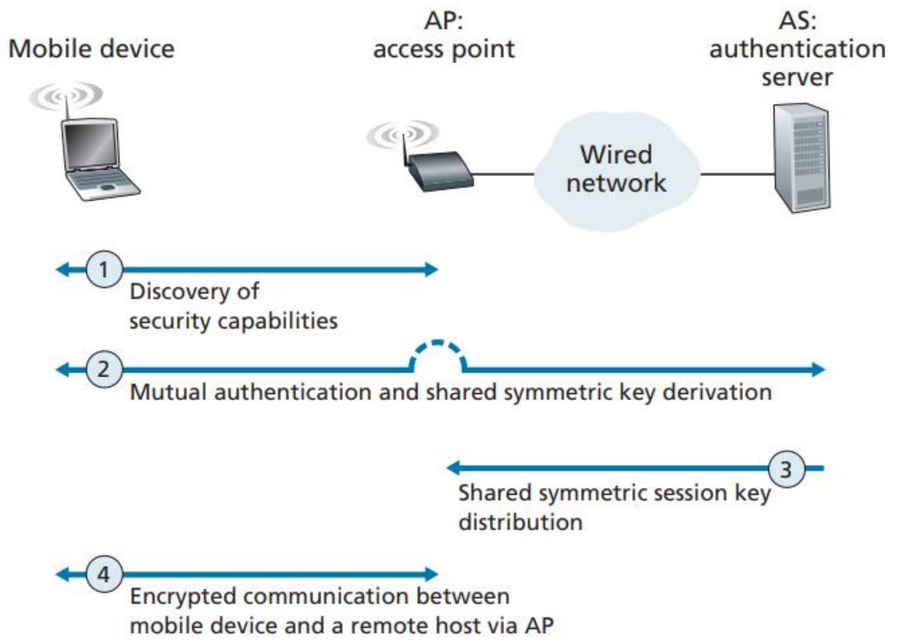
서로를 가리키는 SA는 서로다른 SPI를 가지는데 어떻게 찾을 수 있을까?
변경될 여지는 없는가

https://jaychoi-us-life.tistory.com/175
https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security#Message_1

발표자: 박지원

8.8 무선 랜과 4G/5G 셀룰러 네트워크 보선 랜과 4G/5G 셀룰러 네트워크 보안

상호 인증: 이동 장치와 네트워크 간의 인증
암호화:

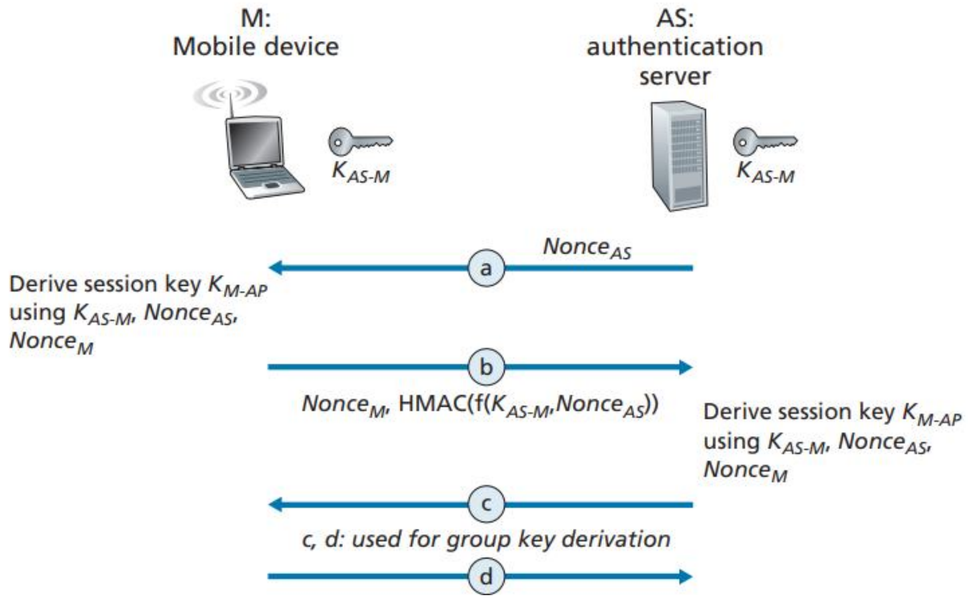


1. 보안 능력 발견(discovery)
2. 상호 인증과 공유 대칭키 생성
3. 공유 대칭 세션키 분배(AP에게 세션키-대칭키를 알려준다?)
4. AP를 통한 이동 장치와 원격 호스트 간의 암호 통신

발표자: 박지원

8.8 무선 랜과 4G/5G 셀룰러 네트워크 보선 랜과 4G/5G 셀룰러 네트워크 보안

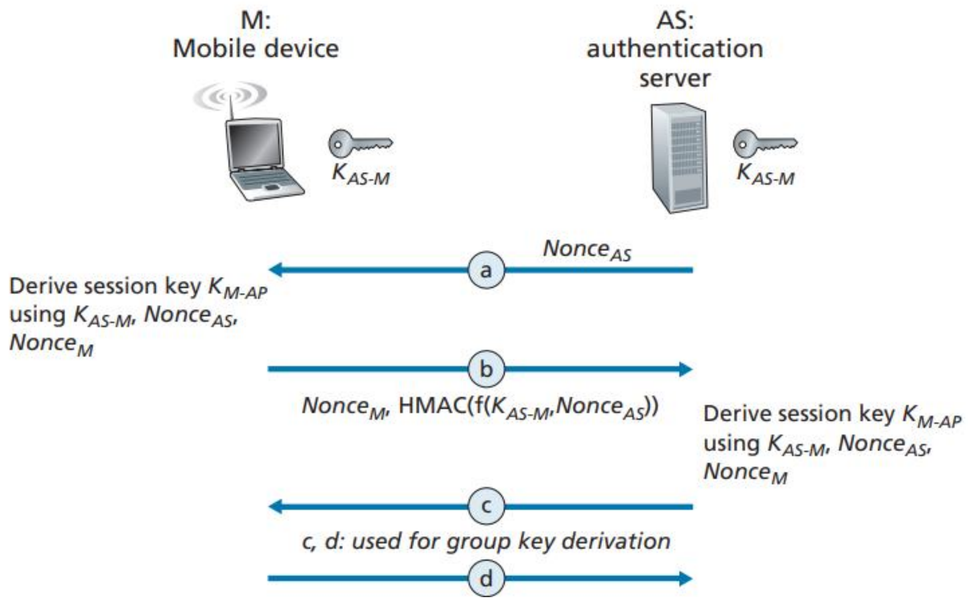
가정: 이동 장치와 인증 서버(AS)가 공유 비밀키를 알고 있다.(K_AS_M)



1. **AS: Nonce_AS 생성후 전달**
2. **M: Nonce_M 생성후 (Nonce_AS + K_AS_M(공유 비밀키) + M_mac주소 + AS_mac주소)**
   → K_M_AP(공유 대칭키 생성)
3. **Nonce_M + HMAC(Nonce_AS + K_AS_M) 전달**

발표자: 박지원

8.8 무선 랜과 4G/5G 셀룰러 네트워크 보선 랜과 4G/5G 셀룰러 네트워크 보안

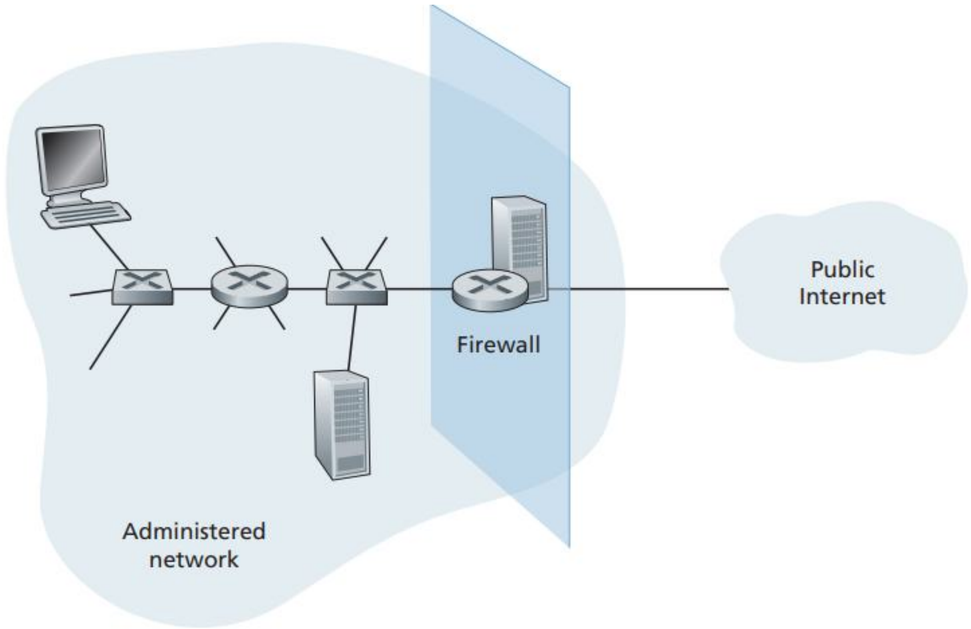


1. AS: Nonce_AC와 HMAC-signed 버전으로 이동장치 활성 상태 파악
2. AS: M과 동일하게 K_M_AP 생성
3. K_M_AP를 AP에게 전달

발표자: 박지원

8.9 운영 보안: 방화벽과 침입 탐지 시스템

방화벽: 패킷을 필터링한다. 네트워크를 분리할 수 있다.



- **외부와 내부를 오가는 모든 트래픽은 방화벽을 거친다.**
- **로컬 보안 정책에 정의된 대로 승인된 트래픽만이 통과가 허용된다.**
- **방화벽 자체가 침입 시도에 안전해야 한다.**

발표자: 박지원

8.9 운영 보안: 방화벽과 침입 탐지 시스템

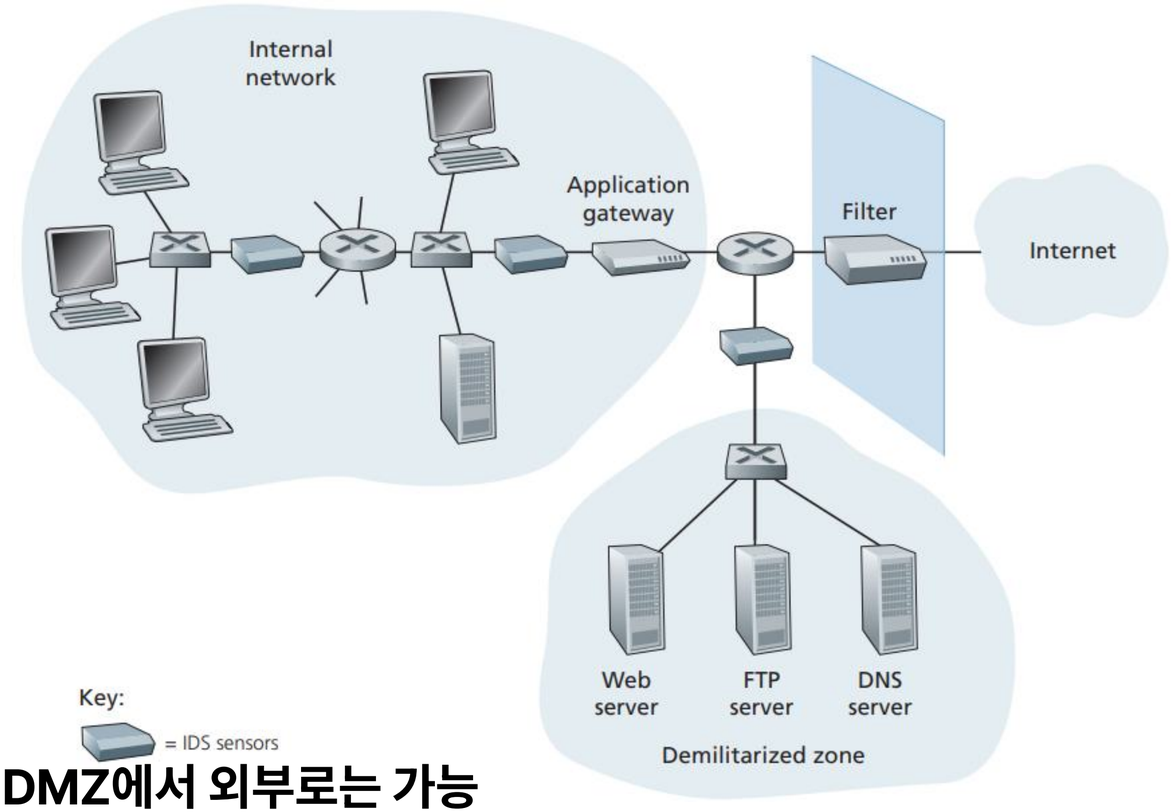
패킷 필터링

- **IP 출발지 또는 목적지 주소**
  - **불행히 출발지 주소를 위장한 데이터그램을 막을 수 없다.**
- **IP 데이터그램 내의 프로토콜 타입 : TCP,UDP OSPF 등**
- **TCP 또는 UDP 출발지와 목적지 포트**
- **TCP 플래그 비트 : SYN, ACK**
  - **ACK 비트가 0인 입력 세그먼트를 거른다면 외부에서 오는 모든 TCP 연결은 거부하고, 내부에서 나가는 건 허락한다.**
- **ICMP 메시지 타입**
- **네트워크에서 나가는 데이터그램과 들어오는 데이터그램에 대한 서로 다른 규칙들**
- **서로 다른 라우터 인터페이스에 대한 서로 다른 규칙들**

발표자: 박지원

8.9 운영 보안: 방화벽과 침입 탐지 시스템

침입 탐지 시스템



DMZ 서버: 내부로 접근이 불가하지만 DMZ에서 외부로는 가능
회사 개인 서버가 DMZ가 되지 않을까...

발표자: 박지원