8. 인터넷 보안연계 키관리 프로토콜

담당교수: 차 영욱
ywcha@andong.ac.kr

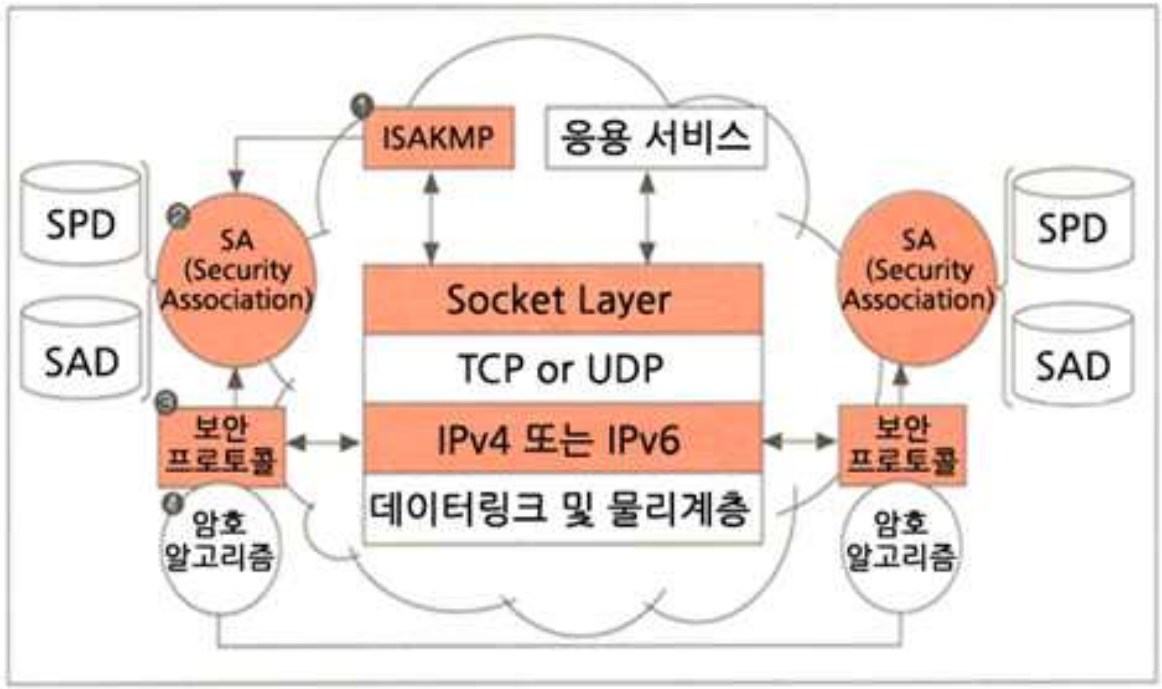
안동대학교
ANDONG NATIONAL UNIVERSITY

목 차

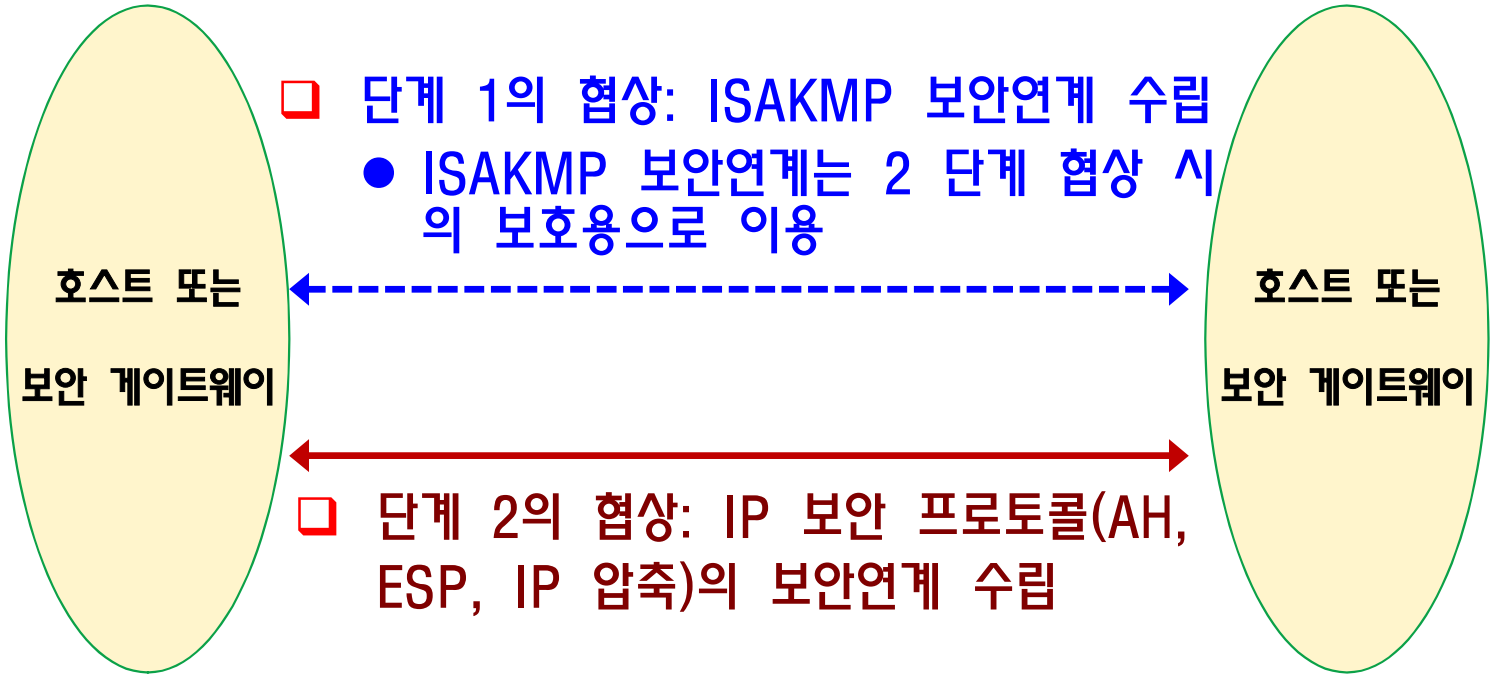
- IP 보안 프로토콜 구조
- 인터넷 보안연계 키관리 프로토콜(ISAKMP)
- ISAKMP 협상단계
- ISAKMP 메시지 헤더와 페이로드
- 인터넷 키교환 프로토콜(IKE)
  - 메인 모드
  - 어그레시브 모드
  - 퀵 모드

인터넷 보안연계 키관리 프로토콜의 개요

- 보안연계의 협상, 수립, 수정 및 삭제를 위한 절차와 패킷 형식 정의
- 키 교환 방식에 독립적이 되도록 설계. 즉, 특정 키 교환 프로토콜과 암호 알고리즘 및 키 발생 기술에 종속되지 않음
- ISAKMP 표준규격(RFC 2408)
  - ISAKMP 메시지는 UDP 또는 TCP 프로토콜을 통해 전송
  - UDP와 TCP의 500번 포트



ISAKMP의 2 단계 협상



ISAKMP 메시지 형식 및 필드(1/2)

- ISAKMP 메시지 = 헤더 + 페이로드들
- 페이로드 단위로 정보 교환. 즉, 페이로드가 모여 ISAKMP 메시지 구성
- 다음 페이로드: ISAKMP 메시지의 첫 번째 페이로드 유형(보안연계, 제안, 트랜스폼 페이로드, …)을 식별
- 주 버전: 자신 보다 높은 주 버전이나 부 버전 값을 갖는 ISAKMP 메시지는 받아들이지 않음
- 부 버전: ISAKMP 프로토콜의 부 버전 번호
- 교환 유형: 단계 1과 단계 2의 협상에서 교환되는 페이로드의 유형과 순서를 규정
  - 메인 모드, 퀵 모드. 어그레시브 모드, …

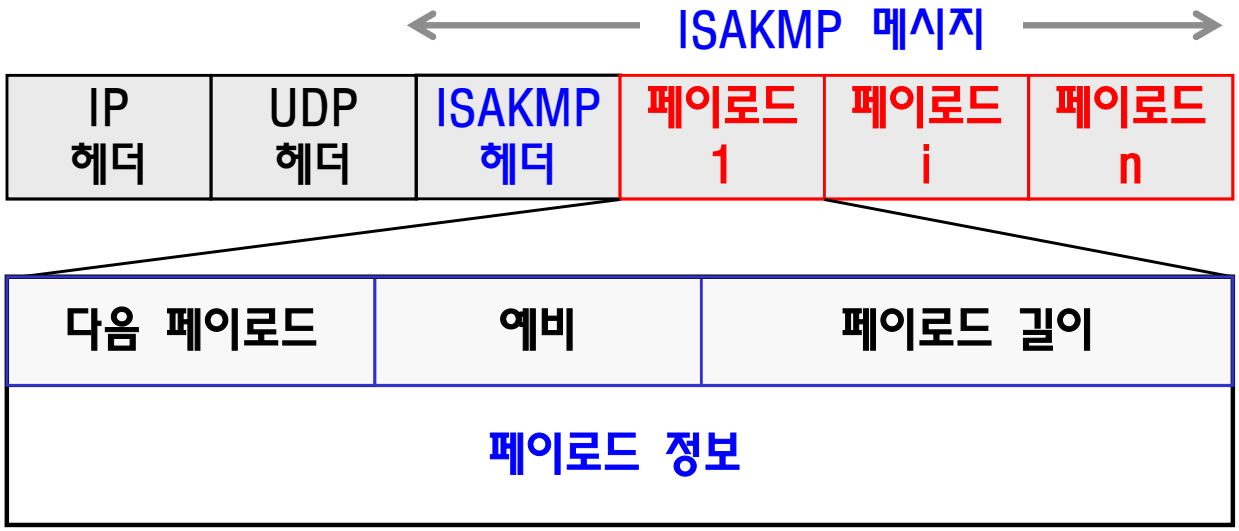
ISAKMP 메시지 형식 및 필드(2/2)

- 개시자 쿠키 및 응답자 쿠키
  - 개시자 및 응답자에 의해 발생되는 고유 비트 열
  - 서비스 거부 공격에 대한 보호용으로 사용: 상대방으로 부터 수신한 쿠키 값이 이전에 수신한 쿠키 값과 다른 경우에 수신한 메시지를 폐기
  - 쿠키를 발생시키는 방식은 ISAKMP의 구현에 따라 다름
    - 표준규격에 규정된 요구사항: 고유한 비밀 정보를 사용하여 쿠키를 발생시켜야 하며, 쿠키로부터 역으로 그 비밀 정보를 알아 낼 수 없어야 함
  - 쿠키의 생성 예:
    - 발신지와 목적지 IP 주소, 포트 번호, 그리고 비밀 난수와 현 날짜 시간 정보로 연결된 문자열에 해쉬 함수를 적용 → 생성된 메시지 다이제스트의 첫 8바이트를 쿠키로 사용

- 플래그: ISAKMP 메시지의 페이로드가 암호화 또는 인증되었음을 나타내는 플래그
- 메시지 식별자: 단계 2의 협상에서 개시자가 발생시킨 난수 값으로 키 생성에 사용
- 길이: 헤더와 페이로드를 포함한 전체 ISAKMP 메시지 길이

ISAKMP 페이로드 형식

- 공통 헤더
  - 다음 페이로드: 다음에 나타나는 페이로드의 유형을 표시
  - 예비
  - 페이로드 길이: 현재 페이로드의 길이
- 페이로드 정보: 페이로드 유형별로 정의된 정보 포함



페이로드 유형	값
보안연계	1
제안	2
트랜스폼	3
키교환	4
신분	5
인증서	6
인증서 요청	7
해쉬	8
서명	9
비표	10
통지	11
삭제	12
벤더 식별자	13

보안연계 페이로드

- 보안연계의 설정 및 협상이 발생하는 도메인을 표시
  - 인터넷에 적용되는 IP 보안 프로토콜 도메인은 한 예이며 ISAKMP는 다른 도메인에도 사용 될 수 있음

- 보안연계 페이로드와 제안 및 트랜스폼 페이로드의 관계
  - 하나의 보안연계 페이로드에 IP 보안 프로토콜을 나타내는 하나 이상의 제안 페이로드가 ISAKMP 메시지에 포함될 수 있음
  - 하나의 제안 페이로드에 보안 알고리즘을 나타내는 하나 이상의 트랜스폼 페이로드가 ISAKMP 메시지에 포함될 수 있음

보안연계의 협상 예(1/2)

- 제안 1: 트랜스폼 1로 SHA-1을 갖는 AH 프로토콜
- 제안 2: 트랜스폼 1로 SHA-1을 갖는 ESP 프로토콜
- 협상 결과: 제안 1(AH SHA-1) 또는 제안 2(ESP SHA-1)

보안 연계 페이로드 도메인=IPSec
제안 페이로드 제안 번호=1, AH 프로토콜, 트랜스폼 개수=1
트랜스폼 페이로드 트랜스폼 번호=1, SHA-1 트랜스폼
제안 페이로드 제안 번호=2, ESP 프로토콜, 트랜스폼 개수=1
트랜스폼 페이로드 트랜스폼 번호=1, SHA-1 트랜스폼

보안연계의 협상 예(2/2)

- 제안 1
  - 트랜스폼 1로 3중-DES, 트랜스폼 2로 DES를 갖는 ESP 프로토콜
  - 트랜스폼 1로 SHA를 갖는 AH 프로토콜
- 협상 결과: 3중-DES의 ESP와 SHA의 AH 또는 DES의 ESP와 SHA의 AH

보안연계 페이로드 도메인=IPSec
제안 페이로드 제안 번호=1, ESP 프로토콜, 트랜스폼 개수=2
트랜스폼 페이로드 트랜스폼 번호=1, 3중-DES 트랜스폼
트랜스폼 페이로드 트랜스폼 번호=2, DES 트랜스폼
제안 페이로드 제안 번호=1, AH 프로토콜, 트랜스폼 개수=1
트랜스폼 페이로드 트랜스폼 번호=1, SHA 트랜스폼

제안 페이로드(1/2)

- 보안연계에 대하여 선호하는 보안 프로토콜과, 해당 보안 프로토콜에 관련된 트랜스폼 페이로드의 개수를 상대방에게 제안

프로토콜 식별자	설명	값
PROTO_ISAKMP	ISAKMP 프로토콜의 식별자	1
PROTO_IPSEC_AH	AH 프로토콜의 식별자	2
PROTO_IPSEC_ESP	ESP 프로토콜의 식별자	3
PROTO_IPCOMP	IP압축 프로토콜의 식별자	4

제안 페이로드(2/2)

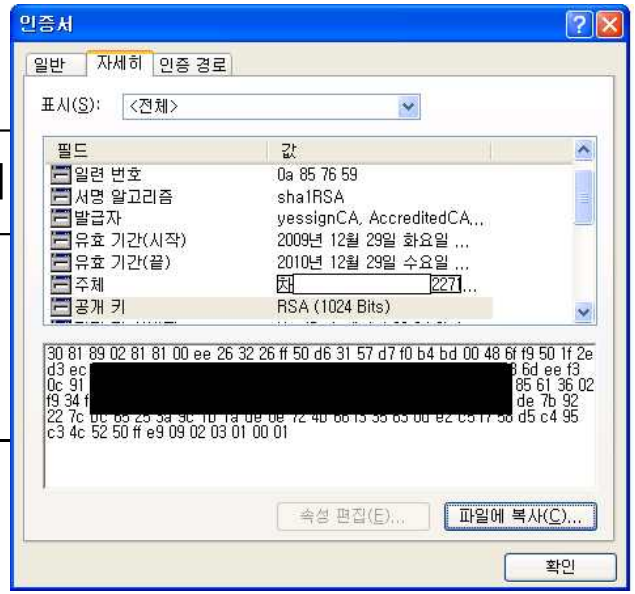
- ❑ 제안 번호
  - 제안 페이로드의 식별 번호
  - 3중-DES ESP 암호와 HMAC-SHA-1 AH 인증이 결합된 보안을 희망
    - 개시자는 동일한 제안 번호를 갖는 두 개의 제안 페이로드를 전송
  - HMAC-MD5 ESP 인증이나 HMAC-SHA-1 AH 인증 중에 하나를 요구
    - 개시자는 단조 증가하는 제안 번호를 갖는 두 개의 제안 페이로드를 전송
    - 제안 선호도가 클수록 제안 번호는 작은 값 할당
- ❑ 트랜스폼 개수
  - 제안 페이로드와 연관되는 트랜스폼 페이로드의 개수를 표시
- ❑ 보안파라미터 인덱스(SPI: Security Parameter Index)
  - 패킷의 수신 시에 목적지 IP 주소와 함께 보안연계 데이터베이스의 보안연계를 구분하는 인덱스

트랜스폼 페이로드

- **트랜스폼 번호:** 트랜스폼 페이로드의 식별 번호
  - 제안된 IPSec에 대해 하나 이상의 트랜스폼이 있으면, 가장 선호되는 트랜스폼에 가장 낮은 트랜스폼 번호 할당
- **트랜스폼 식별자**
  - AH 트랜스폼 식별자: MD5, SHA, RIPEMD, …
  - ESP 트랜스폼 식별자: DES, 3중-DES, AES, …
  - IPComp 트랜스폼 식별자: DEFLATE, LZS, …
- **보안연계 속성:** 상대에게 다음과 같은 부가 정보를 전달하는데 사용
  - 프로토콜 동작 모드: 터널 또는 트랜스포트 모드
  - 보안연계의 생명 유형: 경과시간(Seconds) 또는 보안연계가 적용된 총 바이트의 수(Kilobytes)
  - 보안연계의 생명 기간: 보안연계의 생명 주기를 결정하는 변수

ISAKMP 기타 페이로드(1/2)

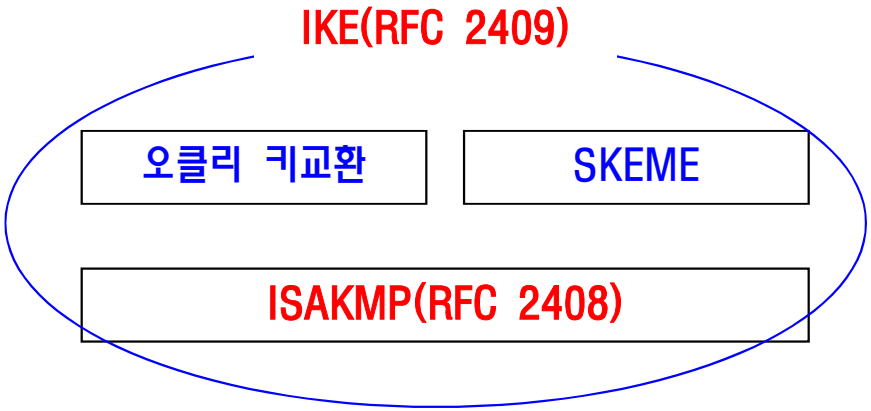
- 키교환 페이로드: 키를 생성하는데 필요한 키교환 데이터의 전달에 사용
- 신분 페이로드: 통신 동배간 신분 정보의 교환에 사용
- 벤더 식별자 페이로드
  - 특정 벤더의 제품을 식별 및 인식하기 위하여 사용하거나
  - 벤더가 원격에 있는 제품의 유지 보수를 위하여 사용할 수 있는 식별자
- 인증서 요청 페이로드: 상대방에 인증서를 요청하기 위한 페이로드
- 인증서 페이로드: 통신 동배간 인증서나 인증서 관련 자료를 교환하는데 사용



ISAKMP 기타 페이로드(2/2)

- 해쉬 페이로드: 보안연계 협상 시 선택된 해쉬 함수에 의해 발생된 메시지 다이제스트를 포함
- 서명 페이로드: 보안연계에서 협상된 서명 함수에 의해 생성된 서명을 포함
- 비표 페이로드: 사용되는 키 교환 메커니즘에 따라 키 생성의 재료로 이용되는 비표 데이터를 포함
- 통지 페이로드: 상대에게 ISAKMP 통신의 오류 상황을 통보하는 페이로드
  - 부적절한 페이로드 유형, 부적절한 쿠키,
  - 부적절한 버전, 부적절한 교환유형,
  - 부적절한 SPI, 부적절한 트랜스폼 식별자,
  - 부적절한 해쉬정보,
  - 부적절한 서명, …
- 삭제 페이로드: IP 보안 프로토콜에 대한 특정 보안연계가 SAD에서 제거되었음을 상대에게 통보하는 페이로드

인터넷 키교환 프로토콜(IKE)의 개요

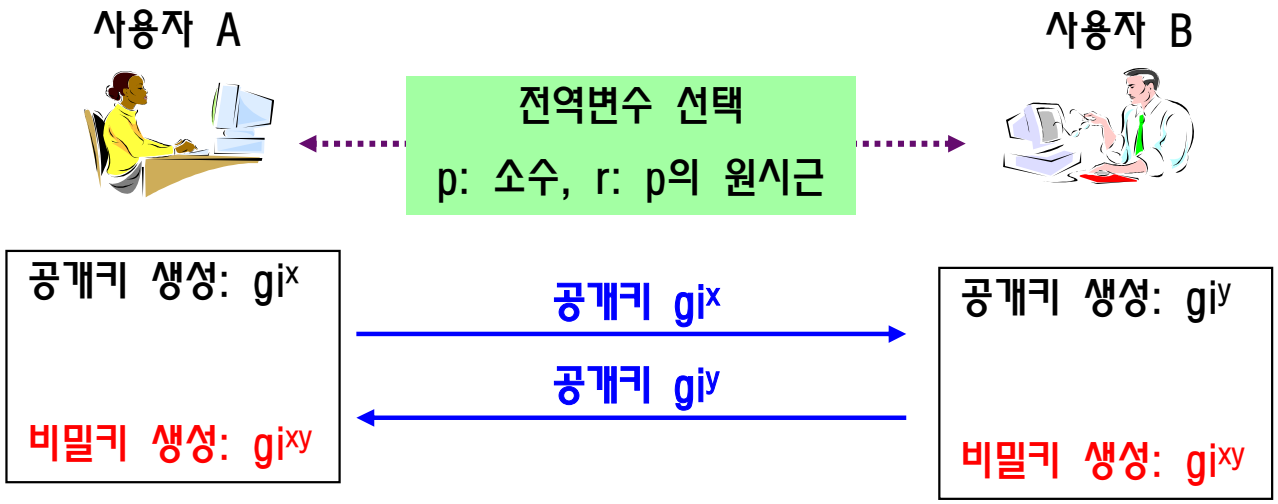


IKE: Internet Key Exchange
ISAKMP: Internet Security Association and Key Management Protocol
SKEME: Secure Key Exchange Mechanism for Internet

- IKE는 오클리 및 SKEME 키교환 기술을 ISAKMP 프레임워크 내에서 구현한 합성 프로토콜
  - IP 보안 프로토콜을 위한 보안연계 협상
  - IP 보안 프로토콜 동배들로 하여금 암호 키와 인증 키를 생성시킬 수 있도록 키 생성 자료를 교환

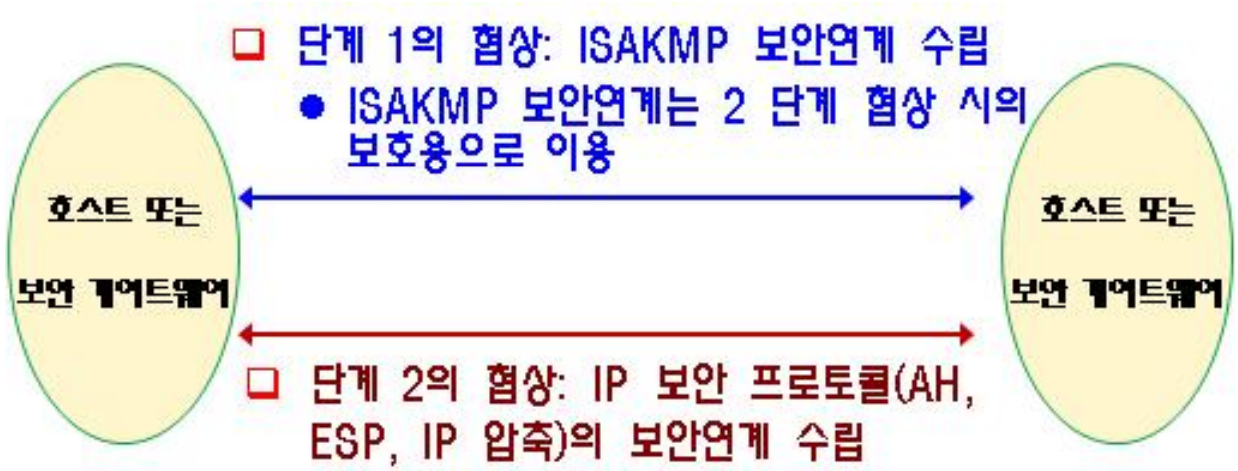
오클리 키교환 프로토콜

- Diffie-Hellman의 장점을 유지하며, 취약성을 개선한 프로토콜
  - Diffie-Hellman의 장점: 보안키는 필요할 때만 생성하며, 키의 교환은 전역 변수 (p와 r)들의 합의 이외에는 특별한 요구사항이 없다.
  - Diffie-Hellman의 취약성: 송신 및 수신자의 신분정보를 제공하지 않으며, 중간자 공격을 받기 쉽다.

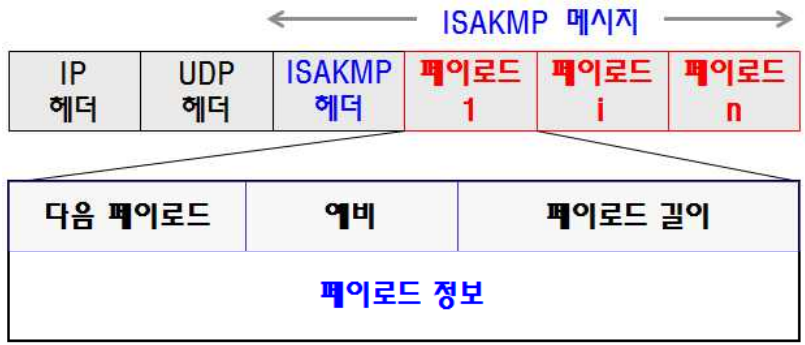


교환 모드

- 교환 모드: 단계 1과 2의 협상에서 교환되는 페이로드의 유형과 순서를 규정
- IKE에서 정의한 네 가지 교환 모드
  - 단계 1의 협상: ISAKMP 프로토콜의 보안연계 협상
    - 메인 모드
    - 어그레시브(aggressive) 모드
  - 단계 2의 협상: IP 보안 프로토콜(AH, ESP, IP 압축)의 보안연계 협상
    - 퀵 모드, 뉴 그룹 모드



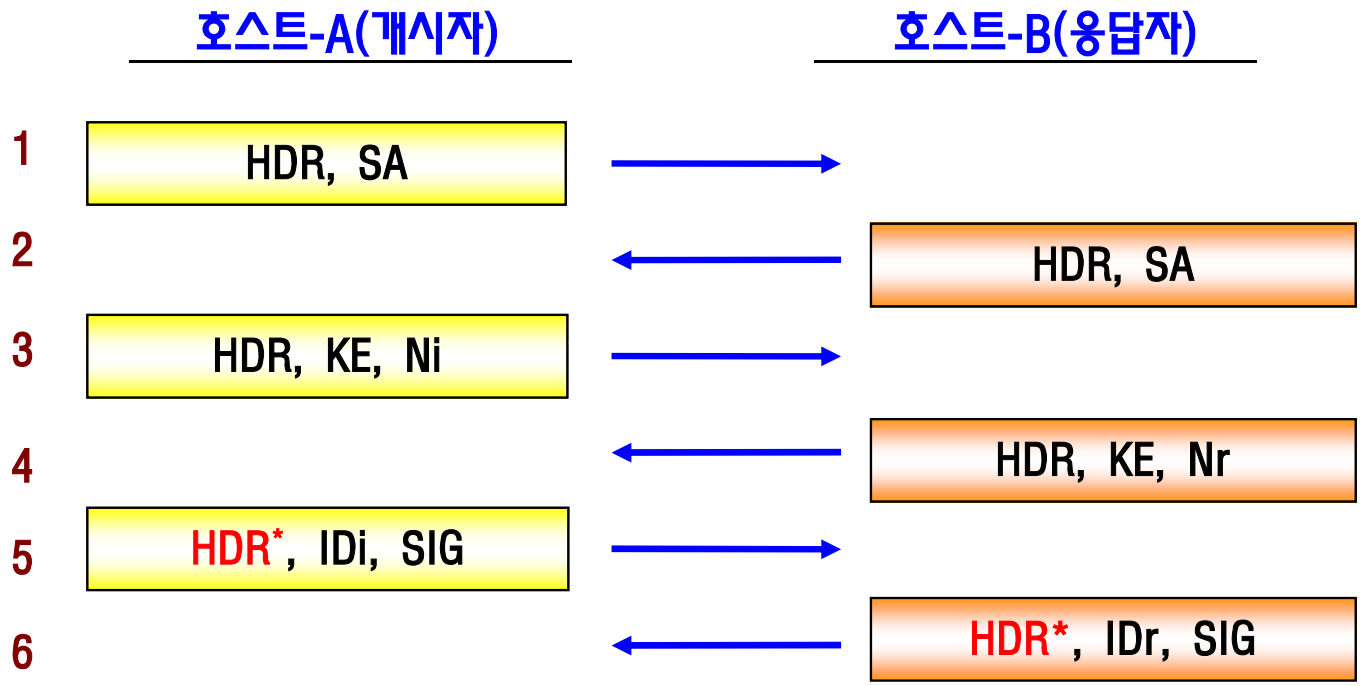
기호



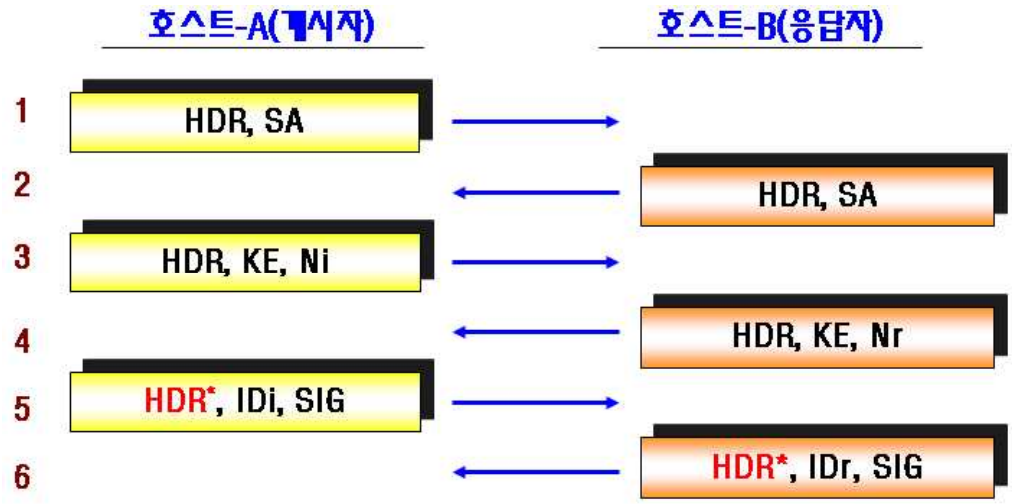
- i: ISAKMP 개시자, r: ISAKMP 응답자
- HDR: ISAKMP 메시지의 헤더
- HDR*: ISAKMP 헤더 뒤의 페이로드들이 암호화 됨
- SA: 보안연계 페이로드(제안 페이로드와 트랜스폼 페이로드 포함)
- KE: 키교환 페이로드
- IDi, IDr: 개시자 및 응답자의 신분 페이로드
- HASH: 해쉬 페이로드
- SIG: 서명 페이로드
- Ni, Nr: 개시자 및 응답자의 비표 페이로드
- <P>_b: 페이로드의 공통 헤더를 제외한 페이로드 부분
- CKi, CKr: ISAKMP 헤더의 개시자 쿠키 및 응답자 쿠키
- g^{i^x}, g^{r^x}: 개시자 및 응답자의 Diffie-Hellman 공개키 값
- xIy: x와 y를 연결함

메인 모드(1/4)

- ISAKMP 보안연계의 협상
  - 메시지 1, 2: 보안방법에 관해서 협상
  - 메시지 3, 4: 키 정보 교환
  - 메시지 5, 6: 신분정보와 서명을 교환 함으로 상호인증



메인 모드(2/4)



- 메시지 1
  - 호스트 A는 쿠기를 생성한 후 평문의 ISAKMP 메시지를 호스트 B에게 전송
  - ISAKMP 교환의 보호를 위해 하나 이상의 보안 방법을 제안
  - ISAKMP 메시지: 헤더, 보안연계 페이로드, 제안 페이로드(ISAKMP), 트랜스폼 페이로드(오클리 키 교환)
- 메시지 2
  - 호스트 B는 쿠기를 생성한 후 평문의 ISAKMP 메시지를 호스트 A에게 전송
  - 호스트 A의 제안에 대하여 B가 어떠한 보안 방법을 제공하는지 응답
  - ISAKMP 메시지: 헤더, 보안연계 페이로드, 제안 페이로드, 트랜스폼 페이로드

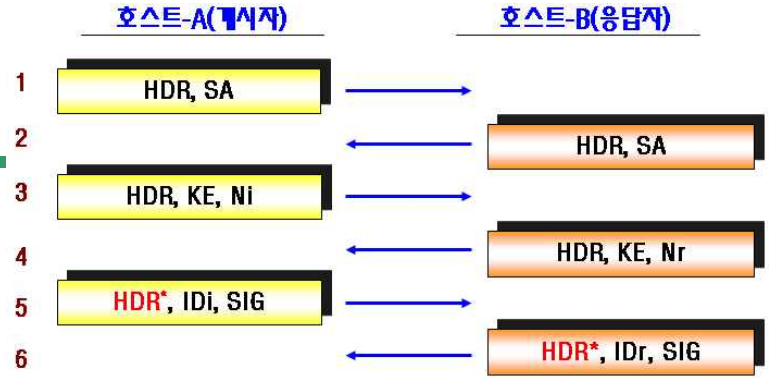
메인 모드(3/4)

- 메시지 3
  - 키를 생성하는데 필요한 자료를 포함하는 키 교환 페이로드와 비표 페이로드를 평문 메시지로 전송
  - 키교환 페이로드: Diffie-Hellman 공개키 값, g^{i^x}
  - 비표 페이로드: 비표 값
- 메시지 4
  - 호스트 B는 자신의 Diffie-Hellman 공개키 값(g^{r^y})과 비표 값을 호스트 A로 전송

- 메시지 3, 4의 교환 후 각 호스트는 키 생성을 위한 키 자료 계산

  - SKEYSTR: 쿠키, 비표 값 및 비밀 키 자료로 부터 추출된 키 스트링
  - SKEYSTR_2: 단계 2 협상의 보안연계를 위한 키 생성에 사용
  - SKEYSTR_a: 단계 2의 ISAKMP 메시지 인증을 위해 사용하는 키 자료
  - SKEYSTR_e: 단계 2의 ISAKMP 메시지의 암호화를 위해 사용하는 키 자료

메인 모드(4/4)



- 메시지 5: 헤더, 신분 페이로드, 서명 페이로드
  - ISAKMP의 모든 페이로드는 암호화
    - 메시지 1과 2에서 협정한 암호 알고리즘과 메시지 3과 4의 정보로 부터 생성한 키를 사용해서 암호화
    - 신분 페이로드의 정보는 보호 됨
  - 개시자는 ISAKMP 메시지 자체가 아닌 호스트 A와 B에서 사용하는 정보에 대하여 디지털 서명 알고리즘을 실행한 결과를 서명 페이로드에 저장

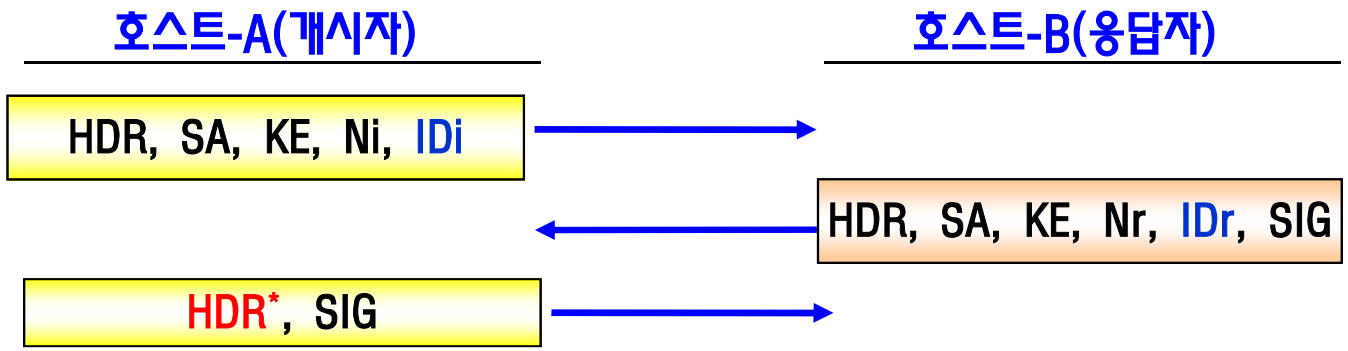
SIG = HMAC-SHA-1(SKEYSTR, g^{xi} g^{xr} CKi CKr SAi_b IDi_b)

- 메시지 6: 헤더, 신분 페이로드, 서명 페이로드
  - 호스트 B는 메시지 5의 디지털 서명을 검증함으로 호스트 A의 신분을 확인
  - 상호 인증하기 위하여 호스트 B의 신분과 서명을 호스트 A에게 전송
  - ISAKMP의 모든 페이로드는 암호화
  - 응답자는 다음의 서명 값을 생성하여 서명 페이로드에 저장

SIG = HMAC-SHA-1(SKEYSTR, g^{xi} g^{xr} CKr CKi SAi_b IDr_b)

어그레시브 모드

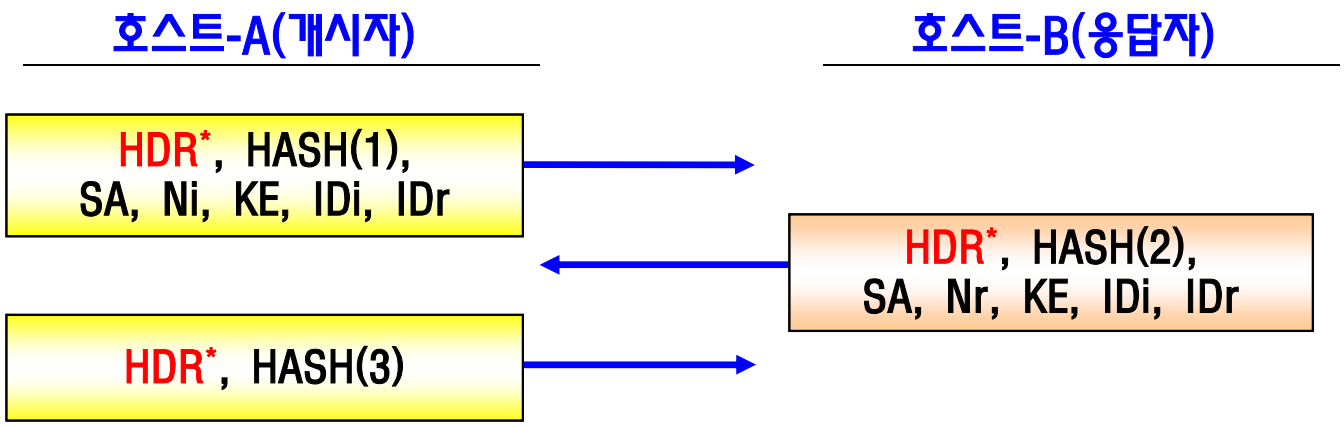
- 신분정보의 보호가 요구되지 않는 환경에서 ISAKMP 보안연계를 협상
- 메시지 1: 헤더, 보안연계, 키교환, 비표, 신분 페이로드
  - 보안연계 페이로드: 하나의 제안 및 하나의 트랜스폼 페이로드 만을 포함
  - 응답자: 개시자의 제안을 수락하거나 거절
- 메시지 2: 헤더, 보안연계, 키교환, 비표, 신분, 서명 페이로드
- 메시지 3: 헤더, 서명 페이로드
  - 메시지 1과 2에서 교환된 키 자료에서 생성된 키로 메시지 3을 암호화
- 메시지 2와 3은 상호 합의한 인증 기능으로 생성된 서명 값을 서명 페이로드로 전송



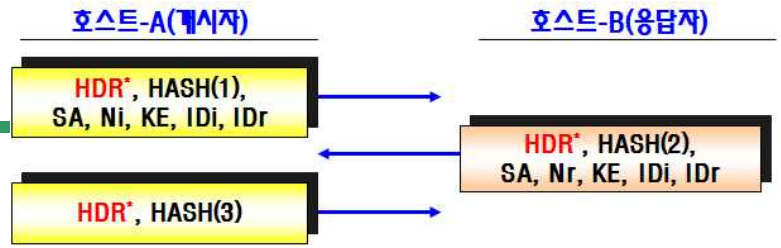
퀵 모드(1/3)

- 단계 1에서 협상된 ISAKMP 보안연계의 보호 아래 단계 2인 IP 보안 프로토콜의 보안연계 협상
  - 단계 2 협상은 일반적으로 단계 1 보다 자주 발생
  - 단계 2 협상의 대표적인 응용은 2, 3 분마다 암호 키를 갱신

- 퀵 모드에서 교환되는 모든 페이로드는 암호화
  - 메시지 1, 2: 보안방법 협상 및 키 생성을 위한 정보 교환
  - 메시지 3: 호스트 A의 존재 증명



퀵 모드(2/3)



- ❑ 메시지 1: 헤더, 해쉬, 보안연계, 제안, 트랜스폼, 비표, 키교환, 개시자 및 응답자의 신분 페이로드
  - ● 해쉬 페이로드의 메시지 다이제스트
    - ▪ HMAC-SHA-1은 단계 1에서 협상된 인증 알고리즘
    - ▪ SKEYSTR_a는 단계 1에서 인증을 위하여 생성된 키 자료
    - ▪ ISAKMP 헤더의 메시지 식별자(MsgID)와 전체 페이로드들을 연결하여 메시지 인증 알고리즘에 적용

HASH(1) = HMAC-SHA-1(SKEYSTR_a, MsgID |SA |Ni |KE |IDi |IDr)

- ❑ 메시지 2: 호스트 B는 수신한 메시지 1의 HASH(1)을 사용하여 호스트 A를 인증한 후에 메시지 2로 응답
  - ● HASH(2)의 메시지 다이제스트는 HASH(1)과 유사하나 헤더를 제외한 개시자 비표 페이로드 Ni가 MsgID 다음과 전체 페이로드 앞에 삽입

HASH(2) = HMAC-SHA-1(SKEYSTR_a, MsgID |Ni_b |SA |Nr |KE |IDi |IDr)

퀵 모드(3/3)

- 메시지 3: 메시지 1과 2를 교환함으로 호스트 A와 호스트 B는 키 자료를 생성하기 위한 모든 정보를 교환
  - 호스트 A의 존재를 증명하기 위하여 메시지 3을 전송
    - ISAKMP 헤더와 해쉬 페이로드로 구성
  - HASH(3)의 메시지 다이제스트

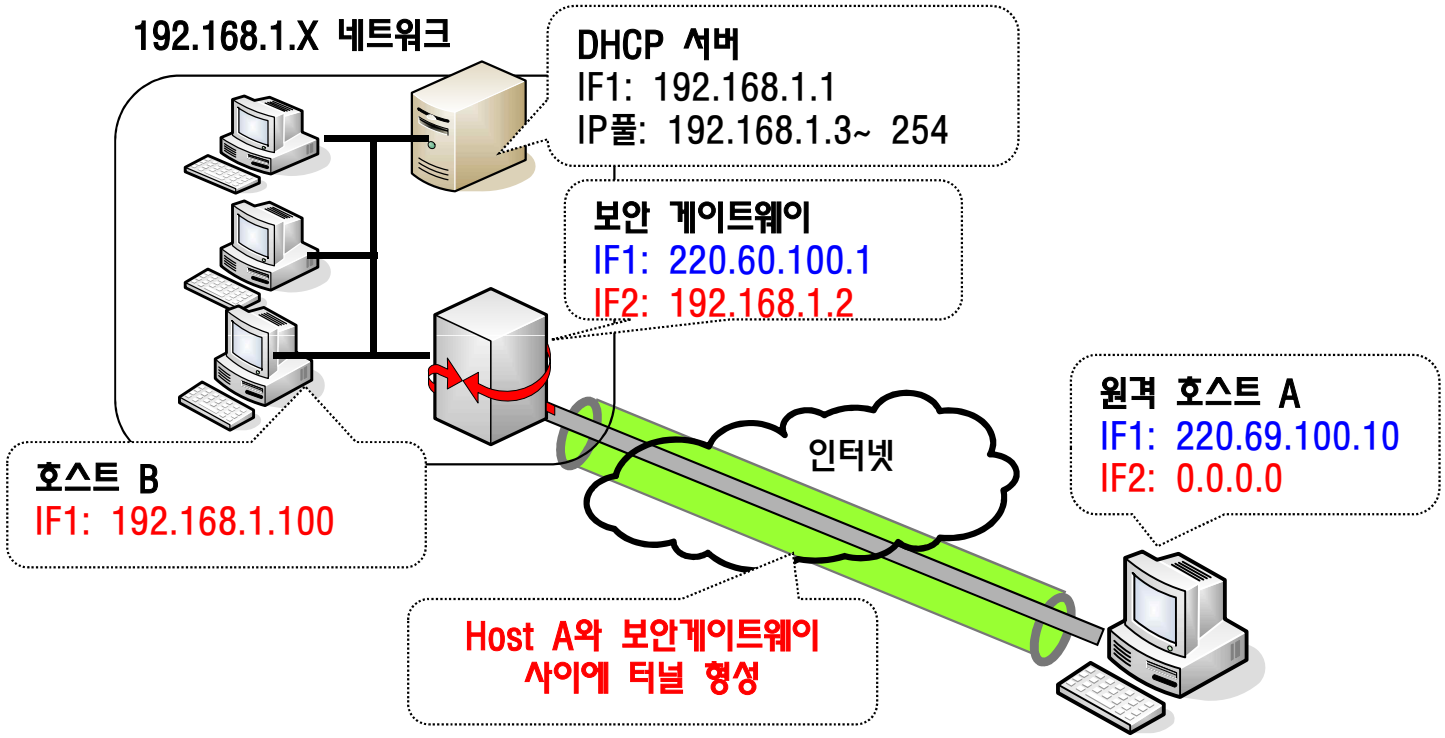
$$HASH(3) = HMAC\text{-}SHA\text{-}1(SKEYSTR\_a, 0 \mid MsgID \mid Ni\_b \mid Nr\_b)$$

- 호스트 A와 B 사이의 새로운 키 자료 NewKEYSTR
  - SKEYSTR_2: 단계 1 협상에서 생성된 키 자료
  - g^{xy}: 메시지 1과 2에서 교환된 Diffie-Hellman 비밀키 값
  - protocol: 제안 페이로드 내의 프로토콜 식별자
  - SPI: 보안 파라미터 인덱스

$$NewKEYSTR = HMAC\text{-}SHA\text{-}1(SKEYSTR\_2, g^{xy} \mid protocol \mid SPI \mid Ni\_b \mid Nr\_b)$$

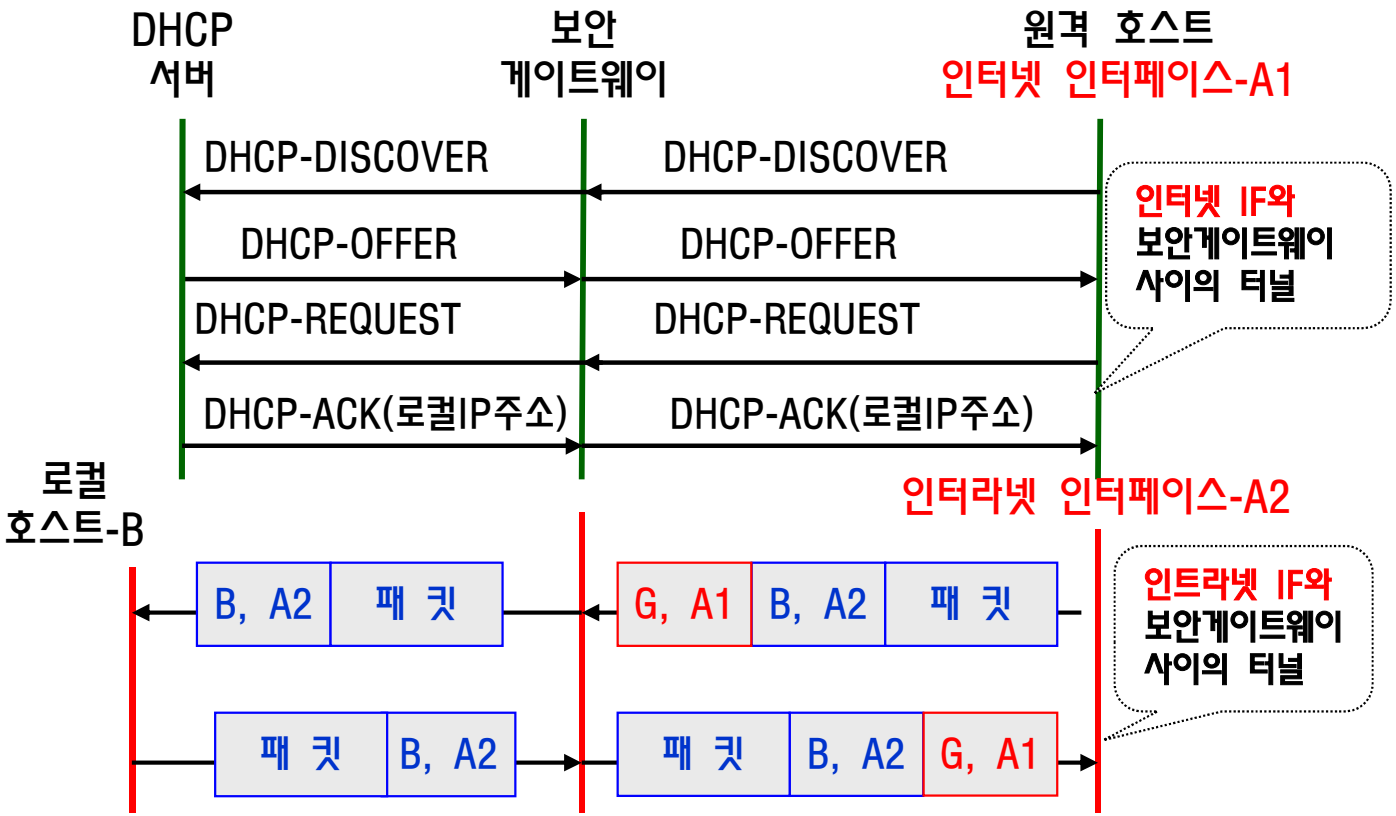
인트라넷 인터페이스 구성(1/2)

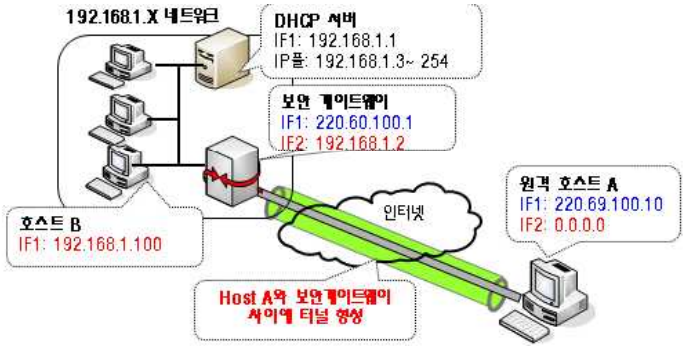
- 대부분의 네트워크 및 보안 관리자는 보안상의 이유로 그들이 관리하는 시스템에 대하여 로컬 IP 주소를 갖는 호스트만이 접근할 수 있도록 구성하여 운영
- 원격의 호스트에 대하여 IPSec 터널 모드와 DHCP를 이용하여 마치 사내망(인트라넷)에 존재하는 것처럼 구성
  - DHCP(Dynamic Host Configuration Protocol): IP 주소의 동적 할당을 위하여 사용



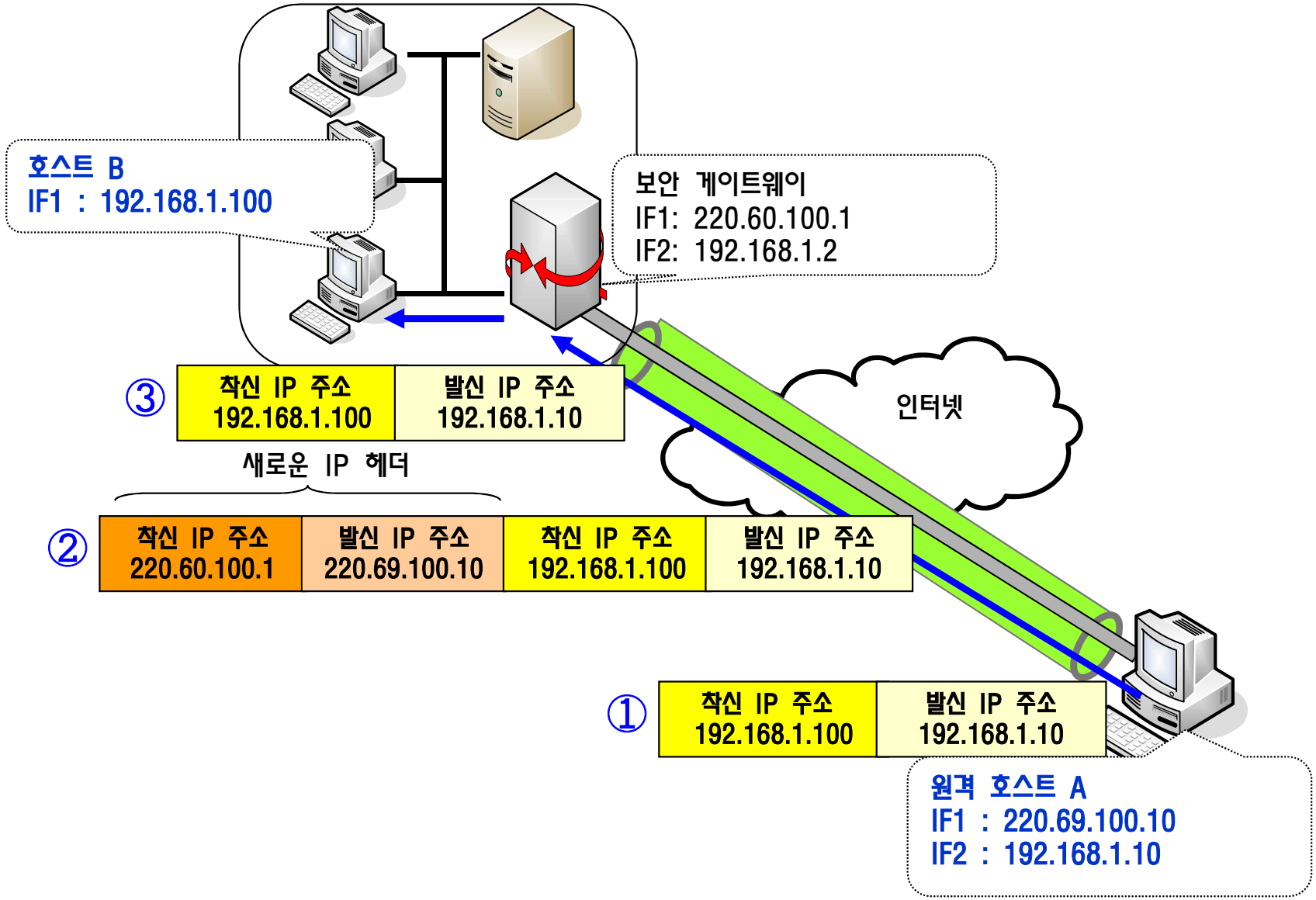
인트라넷 인터페이스 구성(2/2)

- IKE의 단계 1, 2를 통하여 원격 호스트와 보안 GW의 인터넷 인터페이스에 터널모드 수립
- DHCP를 이용하여 원격 호스트의 인트라넷 인터페이스 설정
- IKE의 단계 1, 2를 통하여 원격 호스트와 보안 GW의 인트라넷 인터페이스에 터널모드 수립





IPSec의 터널을 통한 인트라넷 통신



IPSec의 터널을 통한 인터넷 및 인트라넷 통신

① 원격 호스트 A와 보안 게이트웨이는 인터넷 인터페이스에 대하여 IPSec의 보안연계 수립

② 원격 호스트 A는 DHCP-DISCOVER 메시지를 생성하여 보안 게이트웨이로 전달

- 보안 게이트웨이는 이 메시지를 인트라넷 상의 DHCP 서버에 중계

③ DHCP 서버는 구성 변수를 포함하는 DHCP-OFFER 메시지를 보안 게이트웨이에 전송하며, 보안 게이트웨이는 이 메시지를 원격 호스트 A의 인터넷 인터페이스로 전달

④ 원격 호스트로 DHCP-OFFER 메시지가 수신되면 DHCP-REQUEST 메시지를 생성하여 보안 게이트웨이로 전달

⑤ 보안 게이트웨이는 이 메시지를 DHCP 서버로 중계하며, DHCP 서버는 DHCP-ACK로 응답

- 보안 게이트웨이는 이 응답을 원격 호스트 A의 인터넷 인터페이스로 전달

⑥ DHCP-ACK 메시지를 수신한 원격 호스트 A는 이 메시지에 있는 로컬 IP 주소를 이용하여 인트라넷 인터페이스 구성

⑦ 사내 망의 호스트들과의 통신을 위하여 인트라넷 인터페이스는 보안 게이트웨이와 새로운 IPSec 터널 모드의 보안연계를 수립

- 원격 호스트는 물리적으로는 원격지에 위치하지만, 사내 망에 있는 호스트 처럼 인식
- 원격 호스트와 보안 게이트웨이는 새로운 보안연계를 통해 메시지 교환

요약 정리(1/2)

- ISAKMP
  - 보안연계의 협상, 수립, 수정 및 삭제를 위한 절차와 패킷 형식 정의
  - 키 교환 방식에 독립적이 되도록 설계. 즉, 특정 키 교환 프로토콜과 암호 알고리즘 및 키 발생 기술에 종속되지 않음

- ISAKMP 협상 단계
  - 단계 1의 협상: 두 통신 동배의 ISAKMP 보안연계 수립
  - 단계 2의 협상: ISAKMP 보안연계 하에 IP 보안 프로토콜의 보안연계 수립

- ISAKMP 메시지는 헤더와 페이로드들로 구성
  - 보안 연계 페이로드, 제안 페이로드, 트랜스폼 페이로드
  - 키교환 페이로드, 신분 페이로드, 인증서 페이로드, 인증서 요청 페이로드
  - 해쉬 페이로드, 서명 페이로드, 비표 페이로드
  - 통지 페이로드, 삭제 페이로드, 벤더 식별자 페이로드

요점 정리(2/2)

- IKE는 오클리 및 SKEME 키교환 기술을 ISAKMP 프래임워크 내에서 구현한 합성 프로토콜
  - IP 보안 프로토콜 동배들로 하여금 암호 키와 인증 키를 생성시킬 수 있도록 키 자료를 교환
- IKE의 단계 1 협상: ISAKMP 프로토콜의 보안연계 협상
  - 메인 모드, 어그레시브 모드
- IKE의 단계 2 협상: IP 보안 프로토콜(AH, ESP, IP 압축)의 보안연계 협상
  - 퀵 모드, 뉴 그룹 모드
- IPv4에서 IPSec 터널 모드의 DHCP 구성
  - 원격에 있는 호스트에 대하여 IPSec 터널 모드와 DHCP를 이용하므로 마치 사내망(인트라넷)에 존재하는 것처럼 구성