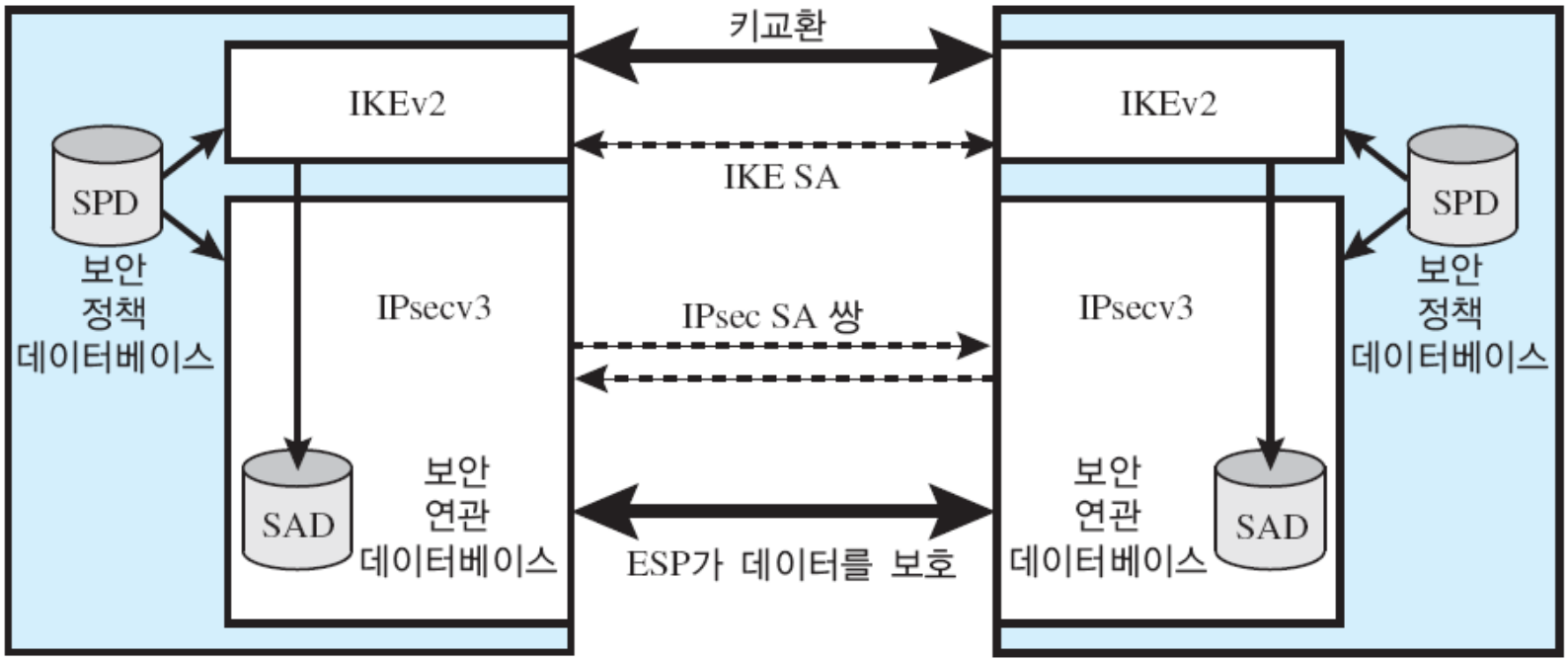
8.2 IP 보안정책

8장. IP 보안

개요

- 2개의 데이터베이스 상호 작용으로 결정
  - 보안 연관 데이터베이스(SAD: Security Association Database)
  - 보안 정책 데이터베이스(SPD: Security Policy Database)

IPSec 구조


키교환
IKEv2
IKEv2
IKE SA
SPD
SPD
보안
정책
데이터베이스
보안
정책
데이터베이스
IPsecv3
IPsecv3
IPsec SA 쌍
SAD
SAD
보안
연관
데이터베이스
보안
연관
데이터베이스
ESP가 데이터를 보호

보안 연관 (1)

- SA(security association)
- 연관이란?
  - 그 위에 실어 보내는 트래픽에 보안서비스를 제공하는 송신자와 수신자 사이의 일방향 관계
- 양방향 보안 교신을 위한 대등(peer) 관계가 필요시
  - 두 개의 보안 연관을 사용
- AH나 ESP를 사용(두 개 동시사용은 안 됨)하기 위해 SA에 보안 서비스를 제공

보안 연관 (2)

- 보안 연관 식별 매개변수
  - 보안 매개변수 색인(SPI: Security Parameters Index):
    - SA에 할당된 비트열
  - IP 목적지 주소(IP Destination Address):
    - 유니캐스트 주소만 가능
  - 보안 프로토콜 식별자(Security Protocol Identifier):
    - IPv4나 IPv6 헤더 안의 목적지 주소와 그 안에 포함된 확장헤더(AH나 ESP) 속의 SPI를 가지고 유일하게 식별

보안 연관 데이터베이스 (1)

- Security Association Database
- IPSec 구현에서 각각의 SA에 연관된 매개변수를 정의한 명목상 DB
- SAD 매개변수
  - 보안 매개변수 색인(SPI: Security Parameter Index):
  - 순서 번호 카운터(Sequence Number Counter):
  - 순서 번호 오버플로우(Sequence Counter Overflow): 오버플로우 여부를 나타내는 플래그
  - 재전송 방지 윈도우(Anti-Replay Window):
  - AH 정보(AH Information): 인증 알고리즘, 키, 키 사용 주기 등

보안 연관 데이터베이스 (2)

- SAD 매개변수 (계속)
  - ESP 정보(ESP Information): 엄호화와 인증 알고리즘, 키, 초기 값 등
  - 보안 연관의 사용주기(Lifetime of this Security Association): 시간 또는 바이트 카운트 값
  - IPsec 프로토콜 모드(IPsec Protocol Mode): 전송, 터널 또는 와일드카드
  - 경로 MTU(Path MTU): Maximum Transmission Unit
- 키관리 메커니즘은 SPI를 통해서만 인증과 프라이버시 메커니즘에 연결
  - 인증과 프라이버시는 특정 키 관리 메커니즘과는 독립적으로 규정

보안 정책 데이터베이스 (1)

- Security Policy Database
- IP 트래픽을 특정 SA에 연관시키는 방법(단 IPsec을 우회하는 것이 허용된 트래픽의 경우에는 SA가 없음)을 정의하는 명목상 DB
  - 간단한 형식 SPD
    - IP 트래픽의 서브셋을 정의하는 각 엔트리와 트래픽을 위한 SA에 대해 포인트를 포함
  - 복잡한 환경의 SPD
    - 단일 SA에 관련된 다중 엔트리 또는 단일 SPD 엔트리와 연관된 다중 SA가 존재

보안 정책 데이터베이스 (2)

- 아웃바운드 IP 패킷 처리 절차
  1. 패킷에 들어 있는 해당 필드(selector 필드) 값에 대응되는 SPD 엔트리를 찾기 위해 SPD와 비교
     - 이때, 일치하는 SPD 엔트리는 0개 이상의 SA를 가리키게 됨
  2. 이들 패킷에 대한 SPD 엔트리와 연관된 SPI가 있다면 SA를 결정
  3. 필요한 IPSec 절차 처리
     - AH 또는 ESP 처리 절차

보안 정책 데이터베이스 (3)

- IP와 집합으로 정의되는 상위 계층의 프로토콜 필드 값으로 각 SPD 엔트리를 결정
- 아웃바운드 트래픽을 특정 SA에 대응시키기 위한 selector는 트래픽 필터링에 사용
- Selector
  - 원격 IP 주소(Remote IP Address):
  - 로컬 IP 주소(Local IP Address):
  - 다음 계층 프로토콜(Next Layer Protocol):
  - 이름(Name):
  - 로컬과 원격 포트(Local and Remote Ports):

보안 정책 데이터베이스 (4)

- 예

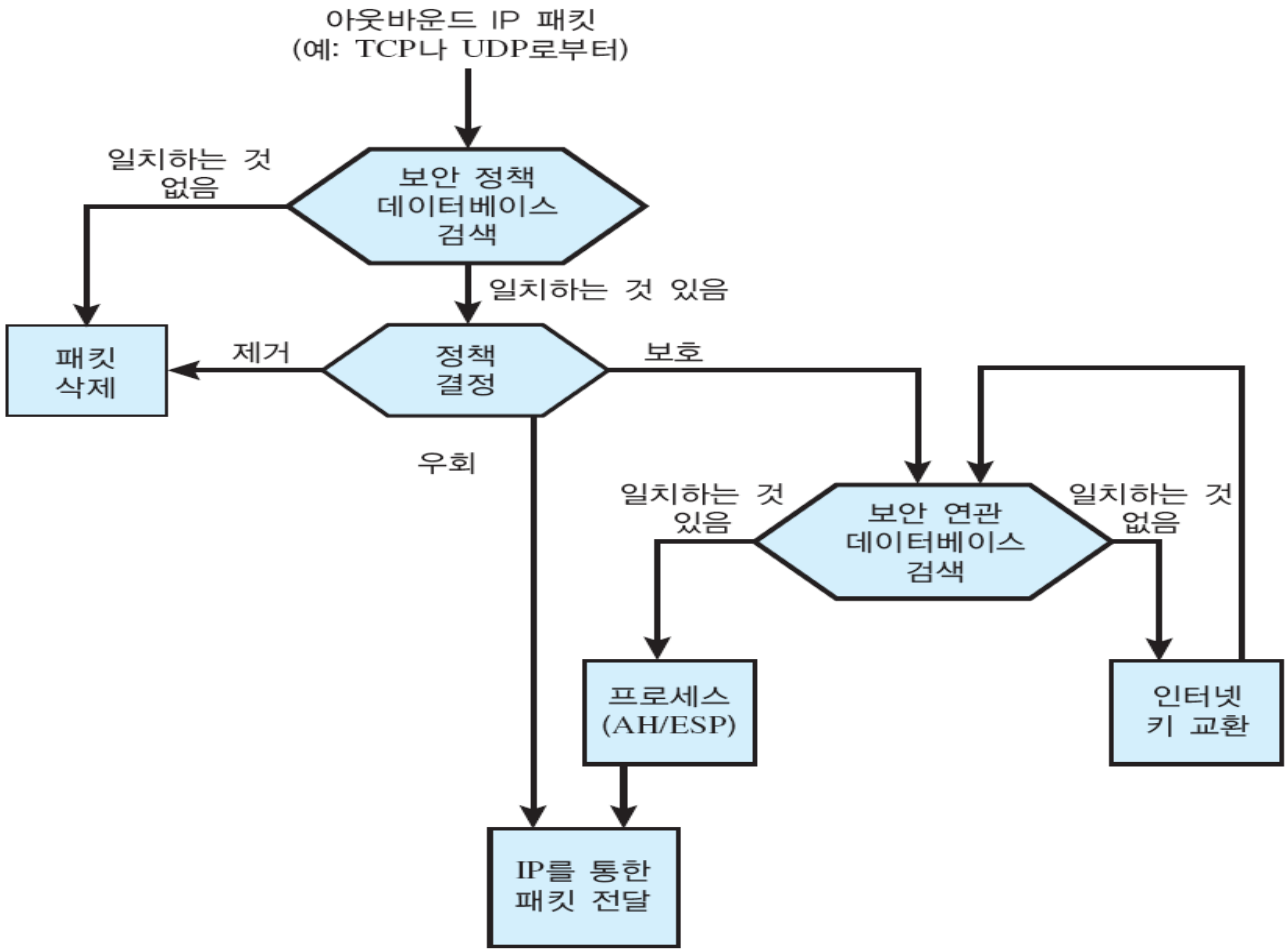
프로토콜	로컬 IP	포트	원격 IP	포트	동작	설명
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error message
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT:ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT:ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

IP 트래픽 처리 (1)

- IPSec은 개별 패킷 기반으로 처리
  - 아웃바운드 패킷
    - 아웃바운드 IP 패킷은 전송되기 전에 IPSec 로직에 의해 처리
  - 인바운드 패킷
    - 인바운드 패킷이 수신되면 다음 상위계층(예를 들면 TCP 또는 UDP)으로 패킷 내용을 전달하기 전에 IPSec 로직에 의해 처리

IP 트래픽 처리 (2)

- 아웃바운드 패킷 처리 모델

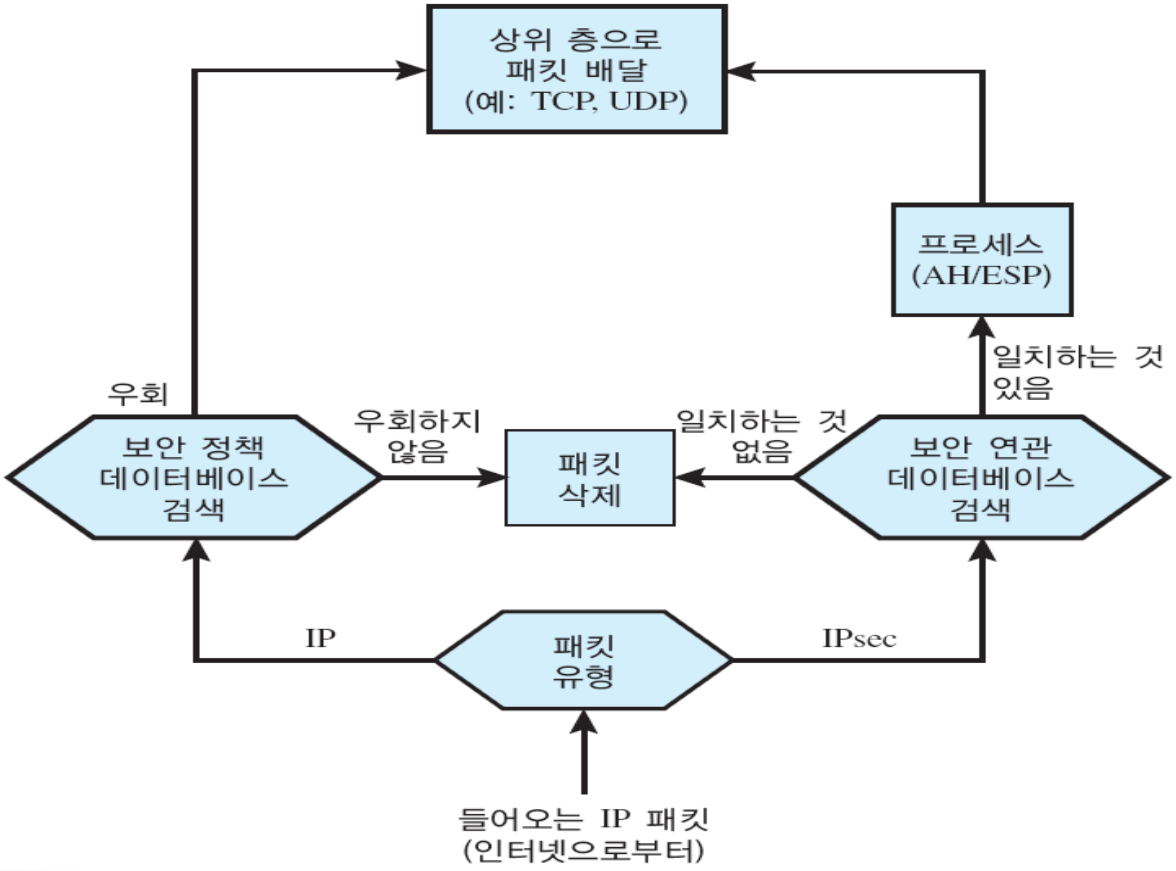


IP 트래픽 처리 (3)

- 아웃바운드 패킷 처리
  1. IP 패킷에 일치되는 SPD를 검색
  2. 일치되는 것이 없을 때
     - 패킷은 폐기되고 오류 메시지 생성
  3. 일치되는 것 발견
     - SPD에서 처음 일치되는 엔트리에 의해 추가 처리
     - 정책이 DISCARD이면 패킷은 폐기
     - 정책이 BYPASS이면 더 이상 IPSec 처리 안 함
     - 패킷은 전송을 위해 네트워크로 발송
  4. 정책이 PROTECT이면
     - 일치되는 엔트리를 찾기 위해 SAD를 검색
     - 일치하는 엔트리가 없다면, 적절한 키를 가진 SA를 생성하기 위해 IKE수행되며 엔트리는 SA로 구성
  5. SAD에서 일치하는 엔트리가 패킷에 대한 처리를 결정
     - 암호화나 인증, 또는 두 가지 중 하나 수행
     - 전송 또는 터널 모드 중 하나 사용
     - 이후에 패킷은 전송을 위해 네트워크로 발송

IP 트래픽 처리 (4)

- 인바운드 패킷 처리 모델



IP 트래픽 처리 (5)

- 인바운드 패킷 처리
  1. IP Protocol 필드(IPv4) 또는 Next Header 필드(IPv6)를 조사하여 보호되지 않은 IP 패킷인지 또는 ESP나 AH 헤더/트레일러를 가진 패킷인지 판단
  2. 패킷이 보호되어 있지 않다면, IPsec은 이러한 패킷에 대해 일치하는 정책을 찾기 위해 SPD를 검색
     - 첫 번째 일치하는 엔트리가 BYPASS의 정책에 해당되면
       - IP 헤더를 처리해 벗겨지고, 패킷의 몸체는 상위 계층 TCP로 전달
     - 첫 번째 일치하는 엔트리가 PROTECT 또는 DISCARD의 정책에 해당 되거나 일치하는 엔트리가 없으면
       - 패킷은 폐기
  3. 보호된 패킷에 대해서는 IPSec이 SAD를 검색
     - 일치하는 엔트리 없으면
       - 패킷은 폐기
     - 일치하는 엔트리가 있으면
       - IPSec은 적절한 ESP나 AH 처리
       - IP 헤더를 처리하여 제거
       - 패킷의 몸체는 다음 상위 계층으로 전달