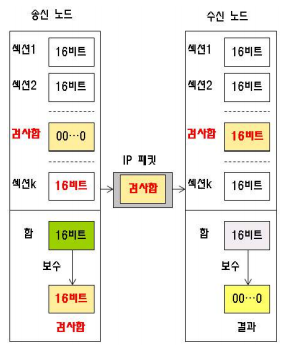
**인터넷 보안 프로토콜 (IPsec) 정리 - 20191072 박수빈**

**IPsec 프로토콜**

* 인터넷 프로토콜의 보안 취약성
  + 인터넷 프로토콜은 데이터의 신뢰성 있는 전달을 염두에 두고 설계함 🡪 **1970년대에는 보안이 중요한 고려 대상이 아니었음**
  + IP 프로토콜의 보안 취약성
    - IP 주소 및 패킷 내용의 변조 🡪 헤더 검사함 재계산
    - 패킷의 재전송, 패킷 내용의 훔쳐보기, …

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 버전  4비트 | 헤더길이  4비트 | 서비스유형  8비트 | 전체길이  16비트 | |
| 식별자  16비트 | | | 플래그  3비트 | 분할 오프셋  13비트 |
| 수명필드  8비트 | | 프로토콜  8비트 | 헤더검사합  16비트 | |
| 발신지 IP 주소 (32비트) | | | | |
| 목적지 IP 주소 (32비트) | | | | |
| IP 옵션들 (최대 40바이트) | | | | |

* + - 헤더 검사 합 필드
      * IP 헤더의 손상 여부를 검사
      * **계산의 용이성**: 16비트의 덧셈 및 보수 계산 (각 비트의 1은 0, 0은 1로 변환)



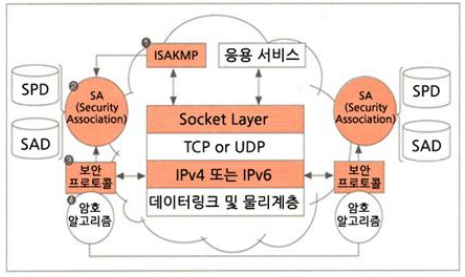
* + - 인터넷 프로토콜의 보안 취약성
      * 공격자는 영심이가 생성한 IP 패킷 (목적지: 경태)을 중간에서 캡쳐
      * IP 헤더의 필드 (ex, 발신지 IP 주소)를 변조 후 헤더 검사 합을 다시 계산하여 경태에게 전송
      * 경태는 변조된 IP 패킷을 정상적인 것으로 잘못 검증 후 응답 IP 패킷을 전송
      * 응답 패킷은 변조된 IP 패킷의 발신지 주소를 목적지 주소로 사용
      * 공격자가 발신지 IP 주소를 변조한 경우 경태가 생성한 IP 패킷은 목적지가 없으므로 네트워크에서 순환하다가 없어짐

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 영심 | 🡪 | IP 패킷 | 🡪 | IP 헤더 변조 및 검사 합 재 계산 | 🡪 | IP 패킷 | 🡪 | 경태 |
|  | | | 🡨 | IP 패킷 | 🡨 |

* 인터넷 보안 프로토콜
  + 인터넷 프로토콜의 취약성을 해결하기 위하여 **보안 프로토콜 개발**
  + **IP 보안 (IPsec)**은 IPv6와 연계하여 개발이 진행되었으며, 1995년 8월에 표준화된 **RFC 1825** (Security Architecture for the Internet Protocol)에 처음 정의됨
    - 인증 헤더 (AH), 캡슐화 보안 페이로드 (ESP), 키 관리 (ISAKMP) 및 압축 프로토콜
  + **SSL (Secure Socket layer) / TLS (Transport Layer Security)**
    - 1993년 웹 서버와 브라우저 사이의 안전한 통신을 위하여 Netscape 사에서 개발
    - 주요 기능: 서버/클라이언트 인증, 기밀성 보장
    - 지원 프로토콜: **HTTPS (443), TELNETS (992), POPS (995) 등**
    - TLS는 SSL을 기반으로 1996년 IETF가 TLS 표준화 (SSL3.1)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | IPsec 호환성 시험 | | | | |  |  |  |
|  | Starting IP Security In IETF |  | SSL | |  |  |  | TLS RFC  TLS RFC | |  | Security Area 22개 워킹 그룹 |
| 1990 | 🡪 | 1992 | 🡪 | 1993 | | 🡪 | 1995 | 🡪 | 1996 | | 🡪 | 2019 |

* 인터넷 보안 프로토콜의 구조



* IP 보안 프로토콜의 서비스와 구현
  + IP 보안 프로토콜 (IPsec)이 제공하는 보안 서비스
    - 인증 코드를 이용한 IP 패킷의 **무결성과 인증** 기능 제공 🡪 IP 주소 및 패킷의 위조 방지
    - 암호화를 통한 IP 패킷의 **기밀성** 제공
    - **재전송되어 수신된** IP 패킷의 감지 및 폐기
  + 네트워크 계층에서 제공되므로 **전송 계층 및 모든 응용 서비스들이 IP 보안 프로토콜의 보안 서비스를 사용**할 수 있음
  + IP 보안 프로토콜의 구현
    - IP 버전 4: 기존 IP 계층에 IPsec을 추가적으로 구현하여 보안 기능 제공
    - IP 버전 6: 인터넷의 보안 문제를 근본적으로 해결하기 위하여 IP 계층의 확장 헤더에 보안 기능 구현
      * **인증 헤더: 인터넷 보안 프로토콜의 인증 기능**
      * **ESP 헤더: 인터넷 보안 프로토콜의 암호화 기능**
* IP 보안 프로토콜의 개요
  + **키 관리 프로토콜 (ISAKMP)**
  + **AH 및 ESP 프로토콜**
    - AH: 패킷의 근원에 대한 인증과 전송 중에 변조되지 않았음을 보장하는 무결성 서비스 제공
    - ESP: IP 패킷의 기밀성 제공을 위한 암호화 기능과 무결성 및 인증 기능 제공
    - 보안 알고리즘
      * **인증 및 무결성 서비스: HMAC-MD5, HMAC-SHA-256**
      * **기밀성 서비스: 3DES-CBC, AES-CBC**
  + **IP 압축 (IPComp) 프로토콜**
* 보안 연계 (SA: Security Association)
  + **SA**: IP 보안 프로토콜, 프로토콜의 운용 모드, 보안 알고리즘, 보안 키와 키의 수명 등에 대한 쌍방 간의 합의
  + ISAKMP 보안 연계의 설정 및 해제 기능 담당
  + 각 호스트는 **송신과 수신 트래픽을 위하여 별도의 보안 연계 설정**
  + 보안 연계의 종류: AH 보안 연계, ESP 보안 연계, IPComp 보안 연계

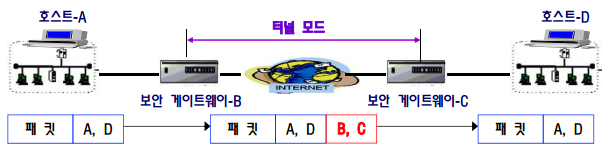


* 보안 연계의 운영 모드
  + **트랜스포트 모드** 
    - 호스트와 호스트 간의 보안 연계
    - 원래 IP 헤더의 발신지 및 목적지 주소를 그대로 유지

텍스트이(가) 표시된 사진

자동 생성된 설명

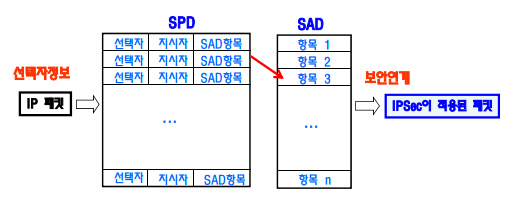
* + **터널 모드**
    - 적용구간: 보안 게이트웨이와 보안 게이트웨이 사이 또는 호스트와 보안 게이트웨이 사이
    - 로컬 네트워크의 호스트들을 대신하여 보안 게이트웨이에 IPsec 프로토콜 구현
    - **새로운 IP 헤더를 만들어 원래의 IP 패킷을 모두 페이로드화** 함
  + 보안 게이트웨이와 보안 게이트웨이 사이의 터널



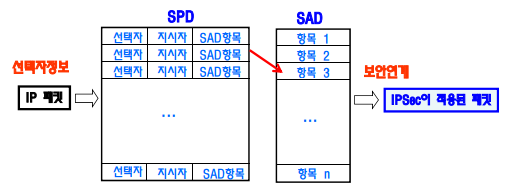
* + 호스트와 보안 게이트웨이 사이의 터널



* 보안 데이터베이스
  + **보안 정책 데이터베이스 (SPD)**
    - IP 패킷에 IPsec의 적용 여부를 결정하기 위하여 하나 이상의 선택자 정보를 이용
    - **지시자**: 선택자들과 일치하는 IP 패킷의 **폐기, 통과** 또는 **IPsec 처리**를 지시
    - IPsec 처리가 요구되는 경우 보안 연계 데이터베이스의 관련 항목을 지정



* + **보안 연계 데이터베이스 (SAD)**
    - 각 항목은 IPsec에 적용할 보안 연계를 나타냄
    - 보안 연계 데이터베이스 항목의 인덱스: 보안 파라미터 인덱스, 목적지 IP주소, IPsec 프로토콜 식별자 (AH또는 ESP)



* IP 보안 프로토콜의 송신 및 수신 처리

|  |  |
| --- | --- |
| IP 보안 프로토콜의 송신 처리 | IP 보안 프로토콜의 수신 처리 |
|  |  |

**인증 헤더 (AH) 프로토콜**

* 인증 헤더 프로토콜 개요
  + AH 프로토콜의 보안 서비스
    - IP 헤더 및 패킷 내용의 변조 여부를 확인할 수 있는 무결성 서비스
    - 데이터의 근원지를 식별하는 인증 서비스
    - 공격자에 의한 재전송 패킷의 감지 및 폐기
  + 인증 헤더 프로토콜은 IP 버전 4의 보안 취약성을 개선하기 위하여 메시지 인증코드 사용
* AH의 메시지 형식
  + **다음 헤더**: 인증 헤더 다음에 오는 페이로드의 유형 식별
  + **페이로드의 길이**: 인증 프로토콜의 메시지 길이
  + **예비 필드**: 0으로 설정
  + **보안 파라미터 인덱스 (SPI)**
    - 목적지 IP 주소와 함께 보안 연계 데이터베이스의 **보안 연계를 구분하는 인덱스**

|  |  |  |
| --- | --- | --- |
| 다음 헤더 (0 ~ 7) | 페이로드의 길이 (~ 15) | 예비 필드 (~ 31) |
| 보안 파라미터 인덱스 (SPI) | | |
| 순서 번호 | | |
| 인증 데이터 (가변 길이) | | |

* + **순서 번호**
    - 송신측과 수신측은 보안 연계 설정 시에 순서 번호를 0으로 초기화
    - 패킷의 송신 시에 순서 번호를 1씩 증가
    - **IP 패킷의 헤더에는 순서 번호가 없음**
  + **인증 데이터**
    - **무결성 검사 값 (ICV)** 포함
    - IC의 생성에 이용되는 알고리즘은 보안 연계에 정의되어 있음
    - AH의 필수적인 메시지인증 알고리즘: **HMAC-MD5와 HMAC-SHA-1, AES-XCBC- MAC**
* 인증 데이터의 생성 및 검증

|  |  |
| --- | --- |
|  | 1. 송신자는 인증키를 메시지에 추가하여 HMAC 알고리즘의 수행 결과로 생성된 무결성 검사 값을 AH 헤더의 ICV 필드에 세팅 2. 생성된 AH를 포함하는 메시지 전송 3. 수신자는 수신된 메시지에 인증키를 추가하여 HMAC 알고리즘 수행 4. 생성된 무결성 검사 값과 AH 헤더의 ICV 필드에서 수신한 무결성 검사 값이 일치 |

* IPv4에서의AH 위치
  + IPv4의 패킷 형태
    - 헤더 부분: 20바이트 고정 부분과 가변 길이의 선택사항 부분
    - 데이터 부분: 전송계층(TCP 또는 UDP), ICMP, IGMP, OSPF 메시지

테이블이(가) 표시된 사진

자동 생성된 설명

* + 트랜스포트 모드에서의 AH 위치

|  |  |
| --- | --- |
|  | * IP 헤더의 뒤 * 다른 IPsec 프로토콜 및 전송 계층 프로토콜의 앞 * 전체 IP 패킷을 인증 |

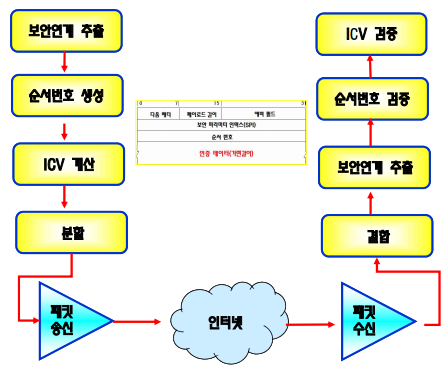
* + 터널 모드에서의 AH 위치

|  |  |
| --- | --- |
|  | * AH는 원래 IP 헤더와 새로운 IP 헤더 사이에 위치 * 새로운 IP 헤더를 포함하여 전체 IP 패킷을 인증 |

* 무결성 검사 값 계산
  + IP 패킷의 인증 및 무결성 확인을 위해 **IP 헤더, AH 헤더 및 페이로드에 대해 ICV 계산**
  + 목적지로 향하는 중간 라우터에서 변경 가능성 있는 **가변 필드**들은 ICV 계산에 앞서 **0으로 설정**
  + IP 헤더, AH 헤더 및 페이로드들을 인증키와 함께 HMAC 절차에 입력
  + 생성된 무결성 검사 값을 AH 헤더의 ICV 필드에 세팅
* IPv4 헤더의 불변 및 가변 필드

|  |  |
| --- | --- |
| 불변 필드 | 가변 필드 |
| * 버전, 헤더 길이, 전체 길이, 식별자, 프로토콜 * 발신지 IP 주소, 목적지 IP 주소, 데이터 (전송 계층 메시지) | * 서비스 유형 * 플래그 * 분할 오프셋 * 수명 * 헤더 검사 합 * 선택 사항 헤더 |

* 인증 헤더 프로토콜의 처리



* AH 프로토콜의 송신 처리

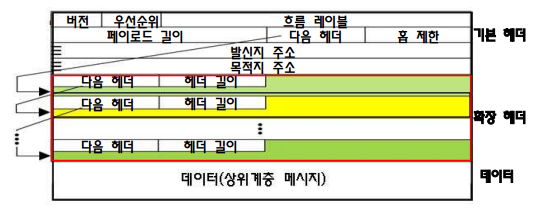
|  |  |
| --- | --- |
|  | * 송신할 IP 패킷의 수신지 IP 주소, 포트, 전송 프로토콜 등의 선택자를 사용하여 보안 정책 데이터베이스 검색 * 검색된 보안 정책 데이터베이스의 항은 출발용 보안연계 데이터베이스에 있는 보안 연계를 지정 * 보안연계가 확립되어 있지 않을 경우, 인터넷 키 교환 프로토콜을 호출하여 보안연계를 협상하고 보안 정책 데이터 베이스에 연결 * 보안 연계를 다은과 같이 인증 헤더 프로토콜 처리에 사용  1. 순서 번호 값을 1만큼 증가 2. 무결성 검사 값 (ICV) 계산 3. 필요하다면 분할하여 패킷을 목적지로 전송 |

* AH 프로토콜의 수신 처리

|  |  |
| --- | --- |
|  | * 분할 된 IP 패킷들의 재 조립 후 IP 보안 프로토콜 처리 * **보안 파라미터 인덱스, 수신지 IP 주소를** 사용하여 보안 연계 데이터서비스에서 해당 패킷이 연계된 보안 연계 검색 * 순서 번호를 사용하여 **패킷의 재전송 여부 확인** * 보안 연계에 규정된 메시지 인증 알고리즘을 사용하여 무결성 검사 값을 계산하고, 인증 데이터 필드에 저장되어 있는 값과 비교 * **호스트의 경우는 패킷을 상위 계층으로 전달하며, 보안 게이트웨이인 경우에는 지정된 노드로 전달** |

**IPv6에서 인증 헤더의 위치와 불변 및 가변 필드**

* IPv6의 패킷 형태: 기본 헤더, 선택적인 확장 헤더 그리고 데이터로 구성
* 확장 헤더
  + AH 확장 헤더는 종단에 있는 호스트에서 사용
  + 중간의 라우터들은 경로를 결정하기 위하여 홉대홉 및 발신지 라우팅의 확장 헤더 정보를 이용
  + 분할 헤더를 이용하여 분할은 발신지, 결합은 목적지 호스트레서 수행



* + 트랜스포트 모드에서의 AH 위치

테이블이(가) 표시된 사진

자동 생성된 설명

* + 터널 모드에서의 AH 위치

테이블이(가) 표시된 사진

자동 생성된 설명

* + 불변 필드 & 가변 필드

|  |  |
| --- | --- |
| 불변 필드 | 가변 필드 |
| * 버전, 페이로드 길이, 다음 헤더 * 발신지 주소, 목적지 주소 | * 우선 순위 * 흐름 레이블 * 홉 제한 * 홉 별 확장 헤더와 수신지 옵션 확장 헤더 * 분할 확장 헤더 |

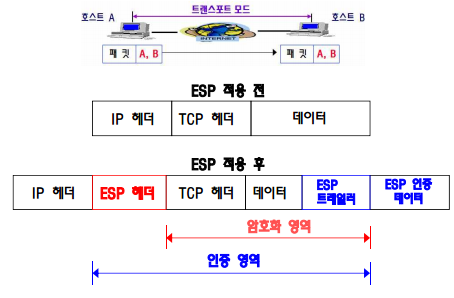
**캡슐화 보안 페이로드 (ESP) 프로토콜**

* ESP 프로토콜의 개요
  + ESP (Encapsulating Security Payload) 프로토콜의 보한 서비스
    - 기밀성 서비스, 인증 서비스, 무결성 서비스, 재전송 패킷의 감지 및 폐기
  + 기밀성 서비스를 위하여 암호화에 대칭 키 암호 알고리즘 사용

텍스트, 시계, 장치이(가) 표시된 사진

자동 생성된 설명

* ESP의 보안 알고리즘
  + **표준화 문서 (RFC 4835, 2007)**: ESP와 AH를 위한 암호 알고리즘의 구현 요구사항
  + 상호 운용성을 보장하기 위해 규정한 **필수 구현 암호와 알고리즘**
  + 인증 및 무결성 서비스를 위하여 규정한 **필수 구현 인증 알고리즘**
  + **NULL 암호화 알고리즘과 NULL 인증 알고리즘은 동시에 이용될 수 없음**
* ESP 메시지 형식 및 필드
  + **ESP 헤더**
    - 보안 파라미터 인덱스 (SPI): 목적지 IP 주소와 함께 보안연계 데이터베이스의 보안연계를 구분하는 인덱스
    - 순서 번호
      * 송신측과 수신측은 보안 연계 설정 시에 순서 번호를 0으로 초기화
      * 패킷의 송신 시에 순서 번호를 1씩 증가
      * 수신자는 순서 번호를 체크함으로 공격자에 의한 재전송 패킷 감지
  + **페이로드 데이터**
    - 상위 계층의 메시지
    - 기밀성 서비스가 협상된 경우 **페이로드는 암호화됨**
  + **ESP 트레일러**
    - 패딩: 암호화 알고리즘이 블록 단위의 평문을 요구하는 경우, 페이로드 데이터를 블록 길이의 배수가 되도록 확장하기 위하여 사용
    - 패딩 길이: 패딩 필드의 바이트 길이를 나타내는 필드
    - 다음 헤더: 페이로드 데이터 필드에 포함되어 있는 데이터의 유형을 식별하는 필드로 전송 계층 프로토콜 또는 IPv6 확장 헤더를 표시
  + **인증 데이터**
    - 무결성 검사 값을 포함
    - ESP 메시지 전체에서 인증 데이터 필드를 제외한 부분에 대해 무결성 검사 값 계산
* IPv4에서의 ESP위치
  + **트랜스포트 모드에서의 ESP 위치**
    - ESP 헤더: IP 헤더 뒤
    - ESP 트레일러: 전송 계층 프로토콜의 메시지가 뒤

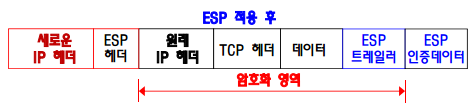


* + 터널 모드에서의 ESP 위치
    - ESP 헤더: 원래 IP 헤더와 새로운 IP 헤더 사이에 위치
    - ESP 트레일러: 전송 계층 프로토콜의 메시지 뒤

테이블이(가) 표시된 사진

자동 생성된 설명

* ESP 트랜스포트와 터널 모드 비교
  + **터널 모드의 보안 서비스**는 트랜스포트 모드에 비하여 **높은 보안성을 제공**
  + 보안 게이트웨이에 터널 모드의 기밀성 서비스가 구현될 경우

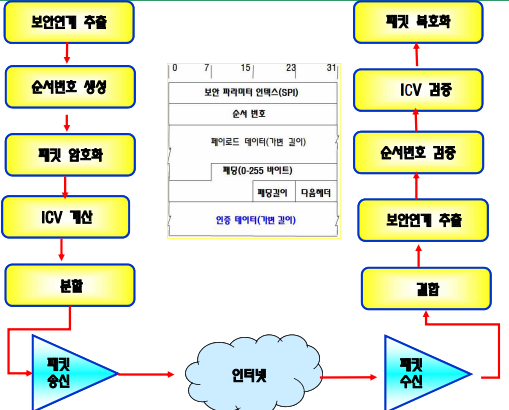


* AH와 ESP의 인증 서비스 비교
  + 인증 헤더는 IP 헤더를 포함한 전체 패킷에 대하여 인증 데이터 계산
  + ESP는 IP 헤더를 제외한 전체 패킷에 대하여 인증 데이터 계산
  + **높은 수준의 인증에 대한 보안성이 필요한 경우** IP 헤더를 포함한 전체 패킷을 인증하는 **AH 인증 서비스 이용**

테이블이(가) 표시된 사진

자동 생성된 설명.

* ESP 프로토콜의 처리



* ESP 프로토콜의 송신 처리

|  |  |
| --- | --- |
|  | * 송신할 IP 패킷의 수신지 IP 주소, 포트, 전송 계층 프로토콜 등의 선택자를 사용하여 SPD 검색 * 검색된 보안 정책 데이터베이스 항은 출발용 SAD의 보안 연계 지정 * 보안 연계가 확립되어 있지 않을 경우, 인터넷 키 교환 프로토콜을 호출하여 보안 연계를 생성하고 SPD에 연결 * 추출된 보안 연계를 이용하여 ESP 처리  1. 순서 번호 값을 1만큼 증가 2. 보안 연계가 기밀성 서비스를 요구하는 경우 암호화 3. SA가 무결성 서비스를 요구하는 경우에 ICV 계산 4. 필요하다면 패킷을 분할하여 수신지로 전송 |

* ESP 프로토콜의 수신 처리

|  |  |
| --- | --- |
|  | * 분할된 IP 패킷들을 재 조립한 후 IP 보안 프로토콜 처리 * 다음 각 단계의 처리에 실패할 경우 패킷을 폐기하고 해당 이벤트 기록 * SPI, 수신지 IP 주소를 사용하여 SAD에서 해당 패킷의 보안 연계 추출 * **순서 번호**를 사용하여 **패킷의 재 전송** 여부 확인 * **SA가 인증 서비스를 요구하는 경우**: 규정된 인증 알고리즘과 키를 사용하여 ICV를 계산하고, 인증 데이터 필드에 저장되어 있는 ICV 값과 비교하여 검증 * **SA가 기밀성 서비스를 요구하는 경우**: 규정된 알고리즘과 키를 사용하여 복호화 🡪 **일반적으로 복호화는 CPU 시간과 메모리를 많이 사용하므로 인증 후에 적용** * 호스트의 경우는 패킷을 상위 계층으로 전달하며, 보안 게이트웨이인 경우에는 지정된 노드로 전달 |