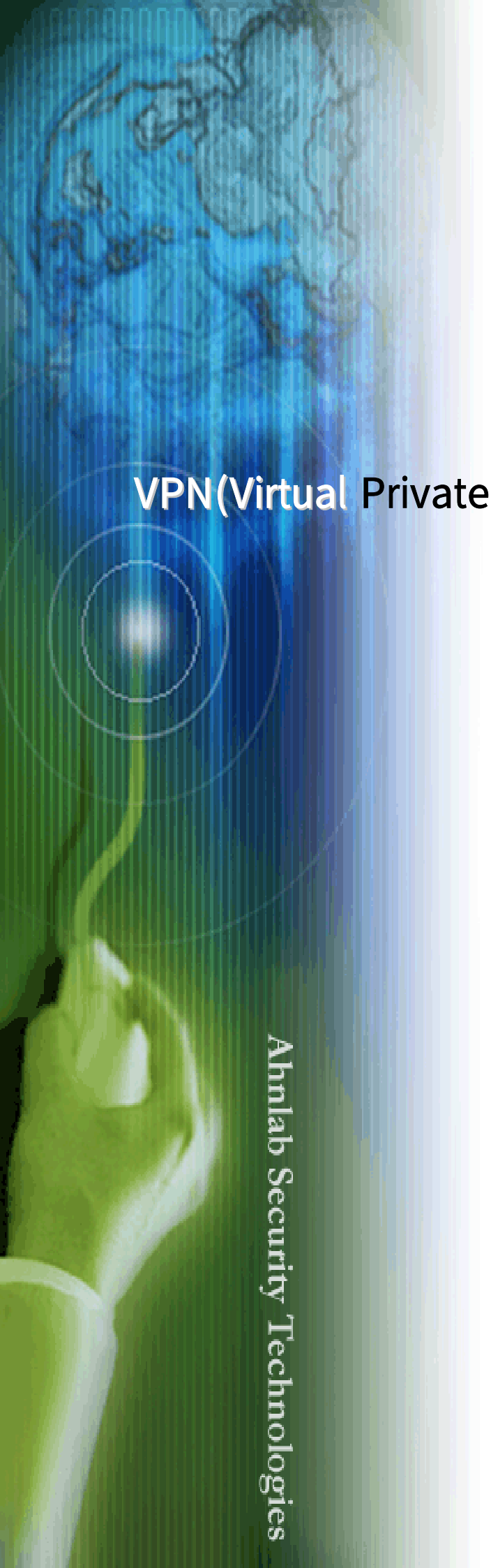


Technical Report

VPN(Virtual Private Network, 가상사설망)개요

강권학
안철수연구소 연구원

목 차

VPN은 인터넷의 폭발적인 확장과 사설망 유지비에 대한 부담으로 침입차단 시스템(방화벽, Internet Firewall)과 침입탐지 시스템(IDS, Intrusion Detection System) 이후 보안업계로부터 주목을 받고 있는 솔루션이다. 본 고에서는 VPN에 대한 이해를 돕기 위해 기본 개념에서 시작하여 VPN을 구현하는데 널리 쓰이는 IPsec(IP Security)프로토콜 및 공개 소프트웨어를 이용한 VPN 구축 방법에 대해 살펴보도록 하겠다.

VPN에 대한 개념을 이해하기 위해 우선 네트워크에서 제공할 수 있는 보안 서비스들을 살펴보는 것이 도움이 될 것이다. 그리고 VPN의 구축에 있어서 가장 널리 쓰이는 프로토콜인 IPsec, IPsec에서 사용할 키를 자동으로 교환하는 프로토콜인 IKE에 대해서도 알아보도록 하자.

1. 네트워크 상에서의 위협과 보안 서비스

네트워크 상에서의 공격은 크게 수동공격(passive attack)과 능동공격(active attack)으로 구분해 볼 수 있다. 이때 수동공격은 실제로 네트워크 트래픽을 생성하지 않는 반면, 능동공격은 공격자가 네트워크에서 패킷을 위조하거나 변조하는 공격 방법이다.

수동공격에는 스니핑(sniffing, 냄새맡기), 트래픽 엔지니어링(traffic engineering) 등의 공격방법이 있고, 능동공격에는 스푸핑(spoofing, 패킷위조), MITM(Man-in-the-Middle, 중간자)등의 공격방법이 있다.

스니핑은 단지 통신하는 내용을 훔쳐보는 것이고, 트래픽 엔지니어링은 스니핑과 같이 훔쳐보는 것에 기반하여 내용들을 분석한 후 네트워크의 구성이나 서버의 서비스 내용 등을 분석해 내는 기법이다. 이에 비해 스푸핑은 공격자가 원하는 결과를 얻기 위해서 직접 패킷을 생성해서 보내는 공격 방법으로, 이 기법을 사용하면 서비스 거부 공격(Denial-of-Service Attack) 등이 가능하다.

MITM은 A와 B양자가 통신하는 중간에 끼어 들어서 A에게는 자신이 B처럼 보이게 하고, B에게는 자신이 A처럼 보임으로써 공격자가 A와 B를 동시에 속이는 공격법이다.

이런 공격으로부터 정보를 보호하기 위해 제공되는 3대 보안 서비스들은 다음과 같다.

- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)

이 외에 부인방지 서비스도 전자 상거래에 있어서 매우 중요한 서비스이다.

기밀성은 전달하고자 하는 내용을 수신자만이 풀 수 있는 키로 암호화하는 서비스로, 적절히 암호화되었다면 정당한 수신자만이 그 내용을 풀어서 볼 수 있게 된다. 무결성은 전달하고자 하는 내용이 도중에 변경되었는지 확인할 수 있는 서비스로, 주로 비밀키가 들어있는(keyed) 해시(hash)값을 이용하며, 이는 전송 경로에 있는 공격자가 내용을 변경하고자 해도 키를 모르기 때문에 정당한 해시를 생성할 수 없기 때문이다. 다음으로 가용성은 적절한 사용자에게 미리 정의된 수준의 서비스가 가능하게 하는 성질을 말하며, 부인방지 기능은 송신자 또는 수신자가 송신한 사실 또는 수신한 사실을 나중에 거부하지 못하도록 하는 서비스이다. 이것은 네트워크 공증(Notarization)서비스를 통해서 어느 정도 지원될 수는 있지만 완전하지는 않다.

이상과 같이 네트워크상에서의 위협과 이러한 위협으로부터 보호하기 위한 서비스들에 대해서 간략히 살펴보았다. 이제부터 VPN에 대해서 구체적으로 살펴보도록 하자.

2. VPN 개요

기존에는 보안이나 서비스 품질이 절대적으로 중요한 네트워크들(국방망 및 각종 국가기간전산망 외에도 기업 자체적인 망들이 이에 속할 수 있다.)을 구축하기 위해 전용선을 기반으로 한 물리적인 사설망을 구축하는 것이 일반적이었다. 그러나 이런 사설망의 지리적인 범위가 커지게 되면, 회선 비용은 상당히 비싸지게 된다.(사실 우리나라처럼 면적이 적은 나라는 문제가 그리 크지 않으나, 미국 등과 같이 면적이 넓은 나라일 경우에는 이런 문제가 더욱 커지게 된다.)

이에 비해 VPN은 Internet과 같은 저렴한 통신 매체를 기반으로 하지만 궁극적으로는 사설망과 같이 안전하고(Secure), 통신의 품질이 보장되는(QoS, Quality of Service)네트워크를 구축하는 것이다. 그러나 Internet은 기본적으로 통제가 되지 않는 신뢰할 수 없는 네트워크들의 모임이기 때문에 안전 및 품질을 보장하기 위한 대가를 치루어야 한다. 본 고에서는 QoS를 제공하기 위한 VPN에 대해서는 다루지 않고 높은 수준의 보안을 제공하는 VPN에 대해서 다루도록 한다.

VPN을 구현하기 위해 사용되는 주요 기술로는 터널링(Tunneling), 암호화/인증 (Encryption/ Authentication), 그리고 접근 제어(Access Control)기술 등이 있다. 각각에 대한 간단한 개념을 살펴보면 다음과 같다.

- 터널링 : 두 Tunneling-End 포인트에게 가상 경로를 설정해 준다. 이때 터널 외부의 환경은 내부에 있는 프로토콜에게 보이지 않게 된다. 차를 타고 터널을 지날 때를 생각해보라. 터널 밖에 산이 있을 수도 있고, 해저 터널인 경우에는 바다가 있을 수도 있지만 터널 내부에 있는 차들에게는 같은 통로를 제공하는 것과 같은 원리이다.

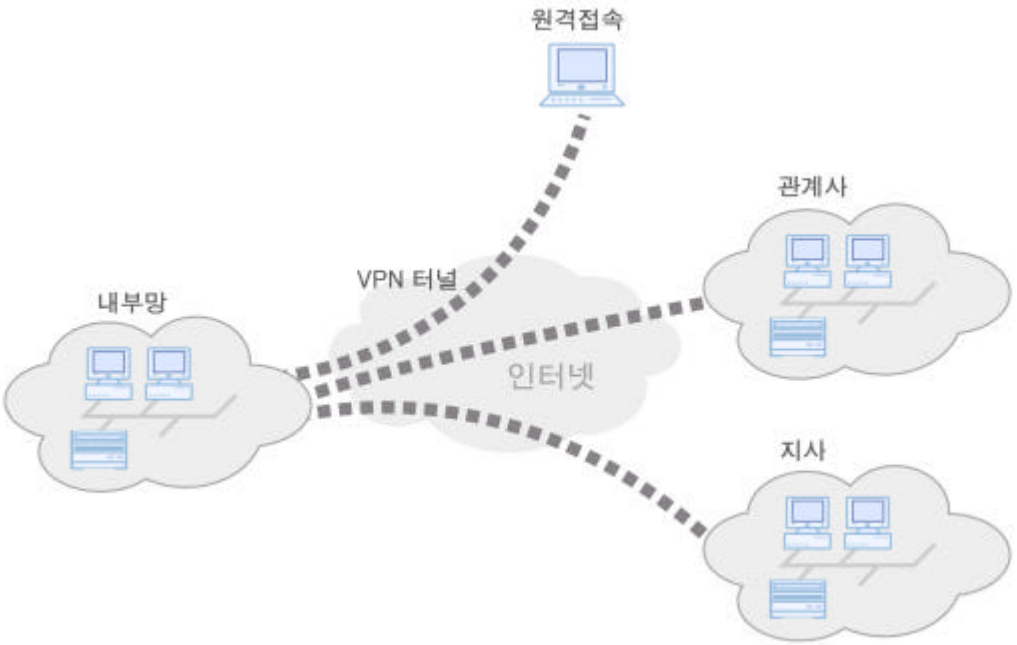
[터널링은 VPN 구현을 위한 주요 기술이다]

- 암호화/인증: 암호화 및 인증은 각 터널을 안전하게 분리하는 역할을 한다. 단순한 터널링만으로는 그 안에 들어가는 데이터를 안전하게 보호할 수 없기 때문이다.
- 접근 제어: VPN 내부의 자원에 대해서 접근 제어기능을 제공할 수 있다.

3. VPN의 분류

VPN은 연결 시나리오에 따라 다음과 같이 세가지로 분류하고, 경우에 따라 서로 다른 보안 정책(Security Protocol)및 구현 기술이 적용될 수 있다.

- 인트라넷(Intranet): 회사 내부망과 이 회사의 지사들과의 VPN 연결
- 원격 접속(Remote Access): 회사 내부망과 원격지에서 접속하는 직원과의 VPN 연결
- 익스트라넷(Extranet): 회사 내부망과 사업관계자 또는 투자자들 등과의 VPN 연결



[연결 시나리오에 따른 VPN 분류]

3.1. 인트라넷 VPN

인트라넷 VPN은 망-대-망으로 연결된 거의 반 영구적인 사설망이며, 회사의 입장에서 보면 지사는 일반적으로 신뢰할 수 있는 것으로 보기 때문에 보안상의 위협은 그렇게 크다고 보지는 않는다. 그러나 서브 네트워크들 사이를 연결하는 만큼 대용량의 통신이 일어날 수 있으므로 성능이 보다 중요한 요소가 될 수 있다. 대부분의 경우 라우터나 방화벽 혹은 전용 VPN 장비를 이용하여 망-대-망의 암호화 / 인증에 의해 구성된다.

그러나 많은 경우 보안상의 위협요소는 외부보다는 내부에 더 많이 존재한다. FBI와 CSI(Computer Security Institute)의 공동 조사에 따르면 실제로 보안침해의 반 이상이 내부에서 일어난다고 한다. 따라서 고의든 실수든 내부인에 의한 정보누출이 더 심각하다고 판단되거나, 혹은 개인이나 부서에 따라 서로 다른 신뢰를 둘 필요가 있다면, 망-대-망의 VPN보다는 개별 사용자에게 서로 다른 보안정책을 적용하고 종단간(end-to-end)보안을 보장해야 할 것이다. 이런 경우는 내부자원의 접근제한을 개인이나 부서에 따라 두어야 하므로 종단간 암호화(end-to-end encryption)및 사용자별 인증에 의한 보다 정교한 접근제어가 필요할 것이다.

3.2. 원격 접속(Dial-up)VPN

기존에 직접 전화접속을 해야 했던 네트워크를 위해서 많은 회사들이 모뎀 풀(modem pool)을 유지하고 장거리 전화 비용을 부담해야 했으나, 이 경우에도 Internet을 백본으로 이용함으로써 보다 저렴하고 구현 및 관리가 쉬운 원격 접속 VPN을 구성할 수 있다. 원격 접속 VPN 시나리오는 이동 사용자-대-LAN 연결로서, 그 기본 기능은 이동 사용자로 하여금 사내의 자원에 대한 안전한 접근을 허용하여 업무의 능률을 높이고자 하는 것이다.

따라서 이 경우는 대부분의 응용에서 사용이나 관리상의 용이성(ease of use/management)이 보다 중요한 고려사항이 될 수 있다. 이동 단말의 특성상, 클라이언트는 사용하기 쉽고(특히 VPN 클라이언트 설정)사용자에게 투명(user-transparent)하게 동작해야 하며, 서버의 입장에서는 쉽고 중앙집중적인 관리가 필수적이다. 전화접속 연결의 특성상 과금(billing)과 관련하여 사용자 인증을 기본적으로 제공해야 하므로 기본적인 데이터 암호/인증뿐만 아니라, 과금과 관련된 각종 통계자료의 중앙 집중적 관리가 필요하다. 이러한 목적으로 인터넷 표준인 RADIUS(Remote Authentication in Dial-In User Service)가 가장 널리 사용된다.

갈수록 재택 근무자나 SOHO, 이동 사용자(판매원, 출장 사원들) 등 이동 단말을 사용하는 인구가 증가하고 있으므로 이들이 사내의 자원(email/web server, database 등)을 안전하게 공유할 수 있게 하는 것은 업무의 능률, 곧 회사의 경쟁력을 향상시키는데 필수적이다. 따라서 현재 VPN 시장에서 원격 접속 VPN이 차지하는 비중이 급속히 증가하고 있는 추세이다.

3.3. 익스트라넷 VPN

익스트라넷 VPN은 보안 정책이 서로 다른 이질적인 서브넷들을 상호 연결시켜 주는 업체-대-업체(business-to-business)VPN인 만큼, 인트라넷에 비해 보안 위험도가 높고 보다 정교한 접근 제어와 함께 상호운용성을 고려해야 하는 등 가장 구성하기 어려운 VPN이라 할 수 있다. 비록 상호 연결되어 자원을 공유한다 하더라도 꼭 필요한 자원에 대해서만 접근을 허용해야 하고 상대방은 항상 잠재적인 공격자가 될 수 있으므로 모든 가능한 경우를 대비한 총체적인 보안 솔루션이 요구된다.

이를 위해 종단간(End-to-end)보안 및 사용자별 접근 제어가 기본적으로 제공되어야 하고, 각 서브넷의 경계에는 가능한 직접 연결을 피하고 보다 정교한 접근 제어가 가능한 어플리케이션 프락시(application proxy)방화벽을 설치하여 서브넷들을 선택적으로 격리시키는 것이 바람직하다. 그리고 서로 다른 조직체를 연결시켜 주어야 하므로 상호운용성을 위한 표준에 기반한 보안 프로토콜을 사용해야 하며, 가능한 다양한 보안 메카니즘을 지원하는 제품이 유리할 것이다. 특히 익스트라넷 VPN은 한 서브넷에서의 보안 결함이 다른 서브넷의 보안에 영향을 미치지 않도록 단방향 보안 모델(unidirectional security model)을 기반으로 해야 한다.

VPN 기능은 통상 router나 firewall에 내장되거나 전용 VPN server로 구현되는데, VPN 구현에 가장 널리 사용되는 tunneling protocol로는 다음의 4가지가 있다.

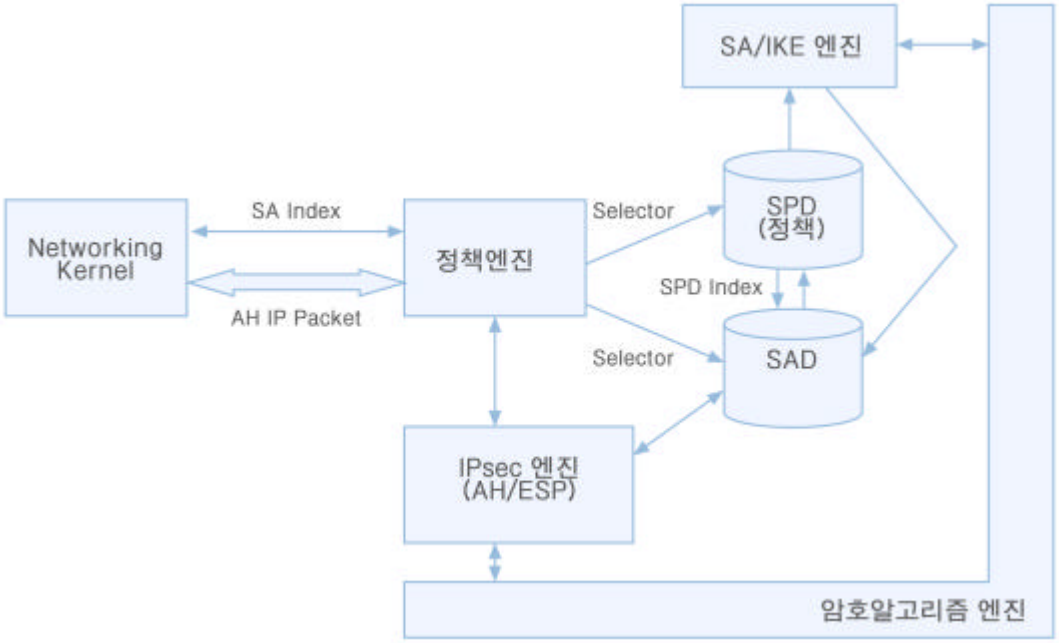
- PPTP(Point-to-Point Tunneling Protocol)/ L2TP(Layer 2 Tunneling Protocol: Layer 2 터널링)

  ; PPTP와 L2TP는 인터넷 기반의 접속 VPN을 구성하는데 가장 널리 사용되는 클라이언트/서버 방식의 터널링 프로토콜이다. PPTP는 Microsoft로부터, L2TP는 Cisco의 L2F(Layer 2 Forwarding)와 PPTP의 장점을 따서 만들어진 PPP 캡슐화(encapsulation) 프로토콜이다. L2TP는 Microsoft, Cisco를 포함한 대부분의 major vendor들의 지원을 받아

인터넷 표준이 되었다. 이 두 프로토콜은 모두 layer 2의 PPP 트래픽에 대한 캡슐화를 통해 두 지점 사이의 터널을 생성/관리/소멸시켜주는 것이 기본 기능이며, 보안은 대부분 PPP에서 제공하는 보안기능에 의존하므로 L2TP 인터넷 표준에서는 보다 강한 보안을 위해 IPsec을 사용하도록 권고하고 있다.

- IPsec(IP Security protocol: Layer 3 터널링)

; IPsec은 최근 일련의 표준화 작업이 완성된 IP 계층의 인터넷 표준으로, 크게 AH/ESP 헤더를 이용한 IP 캡슐화 및 여기에 필요한 키관리 부분으로 구성된다. IPsec을 구현상의 관점에서 보면, 크게 IP 주소를 바탕으로 보안 정책 수행을 담당하는 정책 엔진(Policy engine), SA(Security Association)/키 관리를 담당하는 IKE(Internet Key Exchange)엔진, AH(Authentication Header)및 ESP(Encapsulating Security Payload)캡슐화를 담당하는 IPsec 엔진, 그리고 IPsec 및 IKE 엔진에 필요한 각종 암호연산 라이브러리 및 API로 구성되는 암호알고리즘 엔진(Cryptolib engine)으로 나눌 수 있다. 여기서 보안상 가장 중요한 역할을 하는 부분은 정책 엔진 및 IKE 엔진으로 실제로 IPsec 기반의 VPN은 이들에 의해 구현되고 관리된다.



- SOCKS V5(Layer 5 tunneling)

; SOCKS V5는 인증된 방화벽 통과(authenticated firewall traversal)를 위한 IETF 표준으로, 순수한 서킷 수준 프락시였던 SOCKS V4에 클라이언트 인증(client authentication), 암호화 패러미터 협상(encryption negotiation), UDP 프락시 등 다양한 보안기능을 보강하였기 때문에 같은 세션 계층 보안 프로토콜인 SSL/TLS와 결합되어 사용될 수 있다. SOCKS는 물론 어떤 하위 계층의 터널링 프로토콜 상에서도 사용될 수 있으며, 세션 수준의

프락시로서 동작하므로 IPsec보다 훨씬 정교한 접근제어 및 로깅 기능을 제공할 수 있다. IPsec 만큼 널리 알려지지는 않았으나, 최근에는 복잡해지는 네트워크에 대한 관리 용도로 사용이 점증하고 있다.

SOCKS V5를 이용한 VPN은 당연히 하위 계층의 터널링 프로토콜에 비해 뛰어난 접근 제어 기능을 제공할 수 있으므로 보다 복잡하고 정교한 정책 관리가 요구되는 엑스트라넷 VPN과 같은 경우에는 위력을 발휘할 수 있을 것이다.

각 프로토콜을 요약하면 다음의 표와 같이 나타낼 수 있다.

특징 \ 프로토콜	PPTP	L2TP	IPsec	SOCKS V5
표준화	Vendor-specific	RFC 2661	RFC 2401-2410	RFC 1928, 1929, 1961
OSI 계층	Layer 2	Layer 2	Layer 3	Layer 5
작동 모드	클라이언트/서버	클라이언트/서버	Peer-to-Peer	클라이언트/서버
지원하는 상위 프로토콜들	IP,IPX,NetBEUI, AppleTalk, etc.	IP,IPX,NetBEUI, AppleTalk, etc.	IP	TCP, UDP/IP
터널 서비스	접속당 단일 PPP 터널	접속당 다중 PPP 터널	SA(Security Association)에 기반한 다중 터널	각 세션에 대해서 별도의 터널
사용자 인증	PAP/CHAP	PAP/CHAP	없음	제공됨
데이터 암호/인증	없음(PPP에 의한 암호화)	없음(PPP에 의한 암호화) (IPsec으로 보호할 것을 권고함)	각 패킷에 대해서 AH/ESP에 의해서 암호화/인증 제공	GSS-API를 이용해서 메시지마다 암호화/인증
키 관리	없음	없음	ISAKMP/IKE	GSS-API/SSL
접근 제어	없음	없음	패킷 필터링	패킷/콘텐트 필터링, 프락시
가장 잘 적용되는 분야	원격 접속	원격 접속	랜-대-랜(Lan-to-Loan)인트라넷	익스트라넷

이러한 VPN 구현기술 중에서 가장 표준화가 잘 되어있고, 많은 벤더들의 지원을 받는 프로토콜이 IPsec이다. 이제부터는 IPsec 프로토콜에 대해서 심도 있게 살펴보도록 한다.

4. IPsec 프로토콜

IPsec 프로토콜의 특징을 요약하면 다음의 표와 같다. 이후의 각 소절에서는 IPsec의 특징에 대해서 자세하게 살펴보도록 하겠다.

헤더	AH(Authentication Header)	- 비연결형 무결성 / 인증 서비스
	ESP (Encapsulating Security Payload)	- 비연결형 기밀성 / 무결성 / 인증 서비스
키 교환	IKE(ISAKMP/Oakley)	- 두 개체간의 인증 - 키 및 보안에 관련된 패러미터들을 협상 - 공유 비밀키(Pre-shared Secret)또는 공인 인증서(Public Key Certificate)기반
	Diffie-Hellman	- PFS(Perfect Forward Secrecy)제공
모드	트랜스포트 모드	- 종단간(End-to-End)보안 서비스 - IP 헤더 제외한 부분에 대해서 보호 서비스 - 트래픽 분석에 취약할 수 있음 - 보안 외에 출발지와 도착지 주소를 기반으로 QoS(Quality of Service)를 제공할 수 있음
	터널 모드	- IP 헤더 포함한 전체에 대해서 보호 서비스 - 여러 호스트에 대해서 같은 터널을 쓸 수 있음 - 트래픽 분석에 대해서 보호 기능 - 비공인(사설)IP 주소를 사용할 수 있음
암호/인증 알고리즘	암호 알고리즘	DES, 3DES, RC5, IDEA, CAST, BLOWFISH, 3IDEA, RC4
	인증 알고리즘	MD5, SHA-1, DES

4.1. IPsec 프로토콜 구현방법

IPsec 프로토콜은 차세대 인터넷 프로토콜인 IPv6에서 필수 구현 프로토콜로 지정되어 있다. 그러나 현존하는 인터넷 프로토콜인 IPv4에서는 선택적으로 구현하도록 되어 있는 프로토콜이다. 그렇다면 어떻게 IPsec을 구현할 것인가? 표준에서는 다음과 같은 세가지 방법을 제안하고 있다.

- BITS (Bump-in-the-Stack)

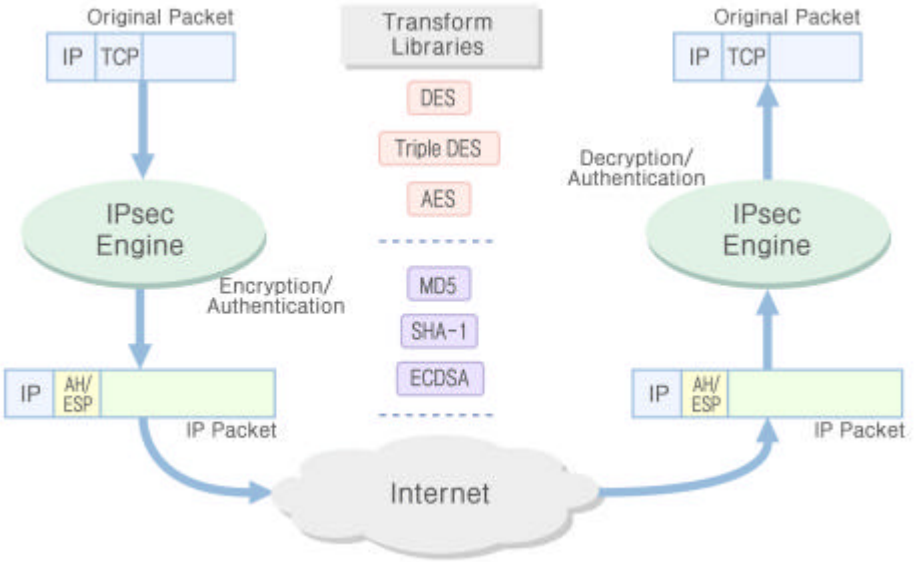
  ; 기존 TCP/IP 스택 및 NIC(Network Interface Card)사이에 IPsec 프로토콜 모듈을 끼워 넣어서 구현하는 방법을 말한다. MS-Windows 등과 같이 TCP/IP 스택의 소스 코드가 공개되어 있지 않는 환경에서 고려할 수 있는 방법이다.

- BITW(Bump-in-the-Wire)

  ; 네트워크 선로 상에 IPsec 장비를 끼워 넣는 방식이다. 별도의 VPN 서버로 구현된 장비들이 이 방법을 구현한다.

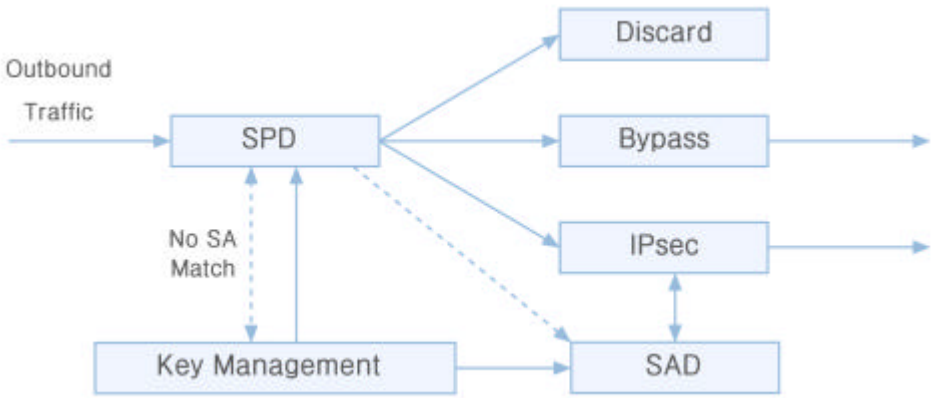
- Integrated

  ; TCP/IP 소스 코드가 공개되어 있는 경우 구현할 수 있는 방법이다.



위의 세가지 중 어떠한 방식으로 구현되었든 IPsec 프로토콜은 개개의 IP 패킷에 대해 정책으로 지정된 대로 암복호화를 수행하는 프로토콜이다. 여기서 주의할 것은 IPsec의 정책 및 처리 절차는 방향성(들어오는 패킷인가? 나가는 패킷인가?)에 따라서 다르다는 것이다. 이때 방향성이라는 것은 서비스의 방향성(누가 서버를 제공하는가?)이 아니라, 단지 현재 처리할 패킷이 나갈 방향을 말한다.

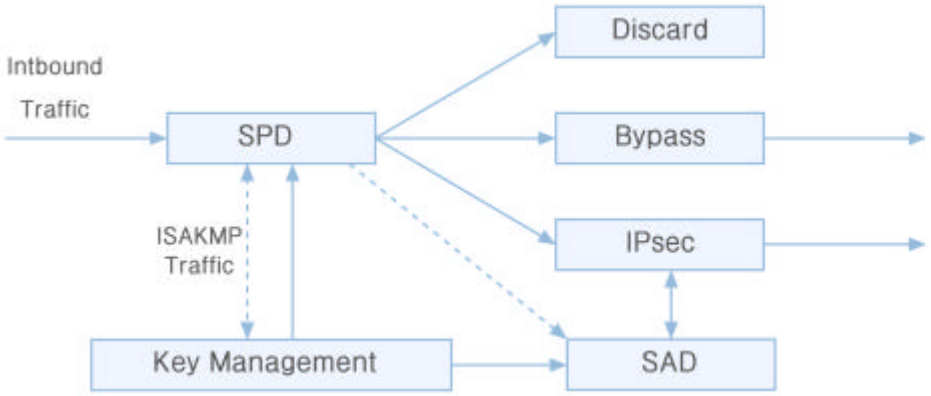
먼저 나가는(outbound)패킷의 처리 과정을 보면 다음과 같다.



패킷의 헤더 정보(출발지 및 도착지의 IP 주소, Port 번호)를 기준으로 적용할 보안정책을 찾아보고, 이 패킷을 버릴 것인지, 그냥 암호화하지 않을 것인지, 아니면 IPsec에 의해 암호화할 것인지를 결정하고 해당 결정에 따라 처리하게 된다. 이때 IPsec에 의해 암호화를 하는 경우에 현재 적용할 수 있는 IPsec SA(Security Association)가 있는지 찾아보고(SA에 대해서는 뒷 부분에서 설명한다.), 적용할 수 있는 SA가 있으면 SA에 정의된 패러미터에 따라 암호화를 한다. 하지만

적용할 수 있는 SA가 없는 경우에는 키 관리 데몬(IKE 프로토콜로 인증할 수 있는 데몬)에게 상대 개체와 SA를 설정해달라고 요청한다. 그때까지 IPsec 엔진은 패킷을 보류하는 상태로 놓아두고, 키관리 데몬이 SA 설정을 끝낸 후 알려주면, 해당 SA를 이용해서 암호화하게 된다.

들어오는(inbound) 패킷의 처리과정도 다음의 그림과 같이 유사하다.

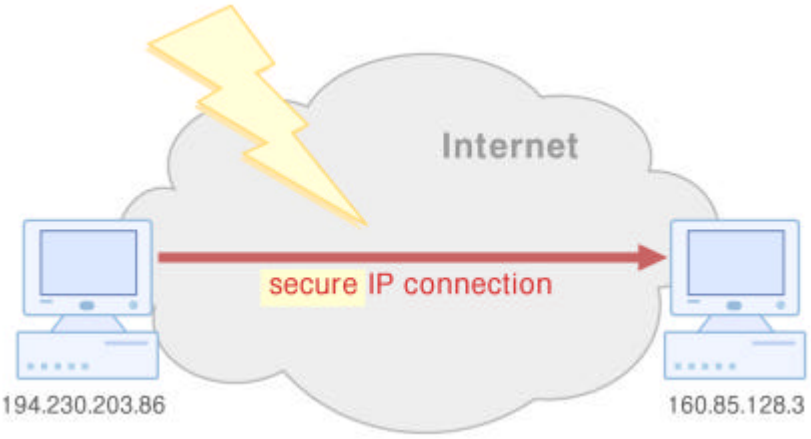


하지만 들어오는 패킷 처리 시에, IPsec 처리를 해야 하는 경우에 SA가 없다면 나가는 경우와는 달리 바로 패킷을 버려야만 한다.

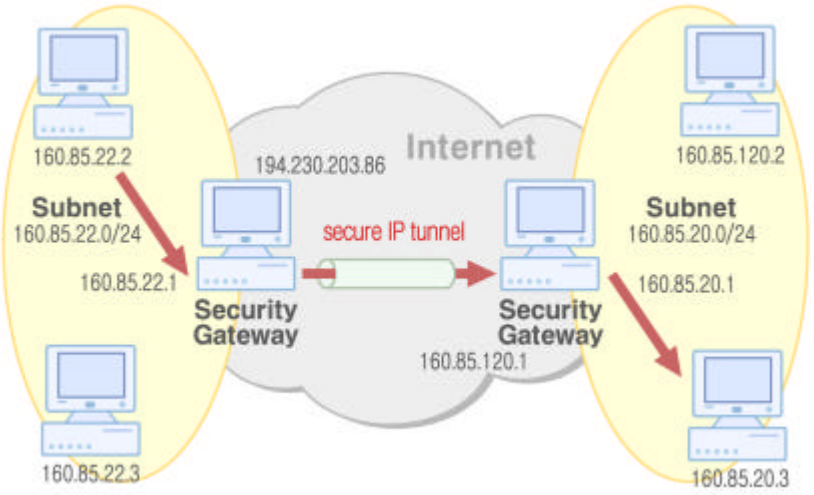
IPsec 프로토콜은 AH 프로토콜과 ESP 프로토콜로 구성된다. AH 프로토콜은 비연결형 무결성 서비스(connectionless integrity service)를 제공하는데, 이때 비연결형이라고 하는 이유는 각 패킷에 대해서 무결성을 보장하는 서비스이기 때문이다. ESP 프로토콜은 기밀성 서비스를 기반으로 선택적으로 무결성 서비스를 제공하는 프로토콜이다. 또한 각 프로토콜은 터널 모드 또는 트랜스포트 모드로 작동하게 된다. 표준에서는 통신하는 두 개체(Peer) 중에 하나라도 보안 게이트웨이(Security Gateway라고도 하며, 흔히 말하는 VPN 장비를 생각하면 된다.)인 경우에는 터널 모드로 통신하도록 정의하고 있다.

4.2. 트랜스포트 / 터널 모드

트랜스포트 모드는 IPsec 프로토콜을 구현한 클라이언트간에 통신하는 경우에 사용하는 모드이다. 다음의 그림과 같이 종단간 보안 프로토콜에 의해서 보호된다.



터널 모드는 앞에서 얘기한대로 두 개체 중에 하나 이상이 보안 게이트웨이인 경우에 작동하는 모드이며, 전형적으로 VPN 장비를 도입하는 경우에 게이트웨이 간에 작동하는 모드이다. 다음의 그림과 같이 주로 네트워크간에 트래픽을 보호하는데 사용된다.



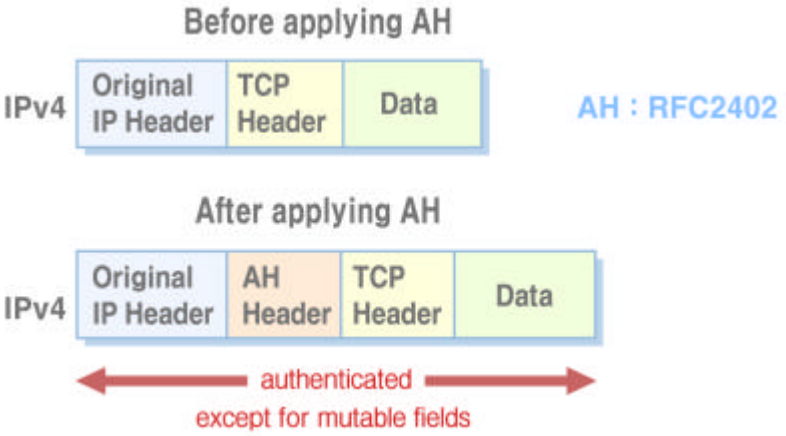
IPsec은 각 모드에 대해서 AH 또는 ESP 프로토콜을, 또는 두 프로토콜을 같이 적용하여 패킷을 보호한다. 다음 소절에서는 AH 및 ESP 프로토콜에 대해서 살펴보도록 한다.

4.3. AH(Authentication Header)프로토콜

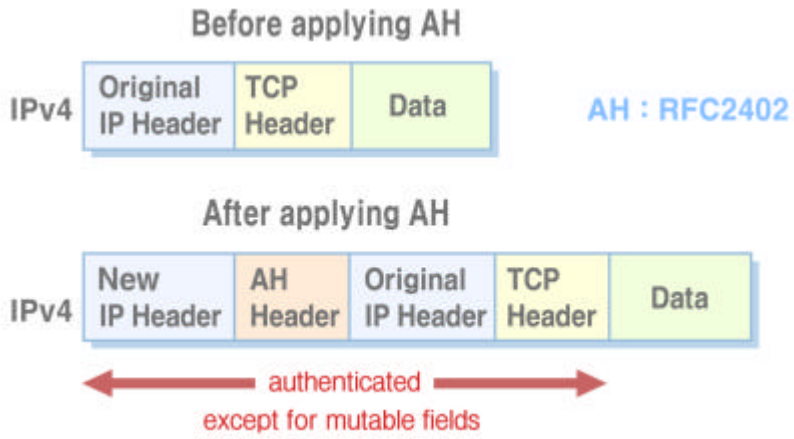
AH 프로토콜은 패킷에 대해서 무결성 및 근원지 인증 서비스를 제공하는 프로토콜로서 패킷을 암호화하지는 않는다. AH 헤더의 구조는 다음 그림과 같다.

Next Header(8)	Pay Loadlength(8)	Reserved(16)
SPI(Security Parameters Index)(32)		
Sequence Number (32)		
Authentication Data (32*n)		

IPsec 처리에 의해서 위와 같은 AH의 헤더가 들어가는 위치와 보호의 범위는 모드에 따라 달라진다. 먼저 트랜스포트 모드에서 AH 프로토콜로 인증하는 경우에는 다음과 같이 패킷이 변하게 된다. 이때 인증 데이터에 의해서 보호되는 범위는 원래의 IP 헤더의 일부 필드(TTL 등 전송 중에서 달라질 수 있는 필드)를 제외한 전체 범위가 된다.



터널 모드에서 AH 프로토콜을 적용할 때의 헤더 구조는 다음과 같다.

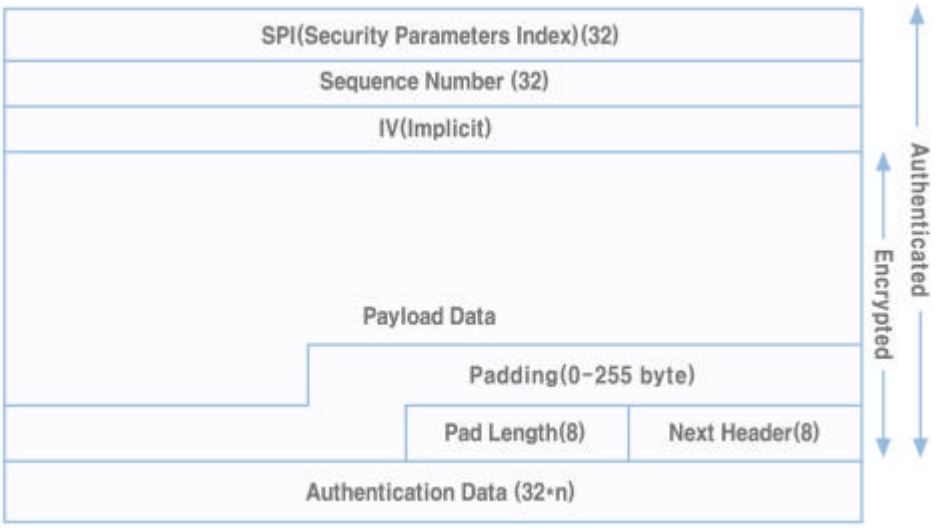


이때 바깥쪽 부분의 IP 헤더는 보안 게이트웨이의 IP 주소이다. 터널모드로 처리한 패킷들은 위의

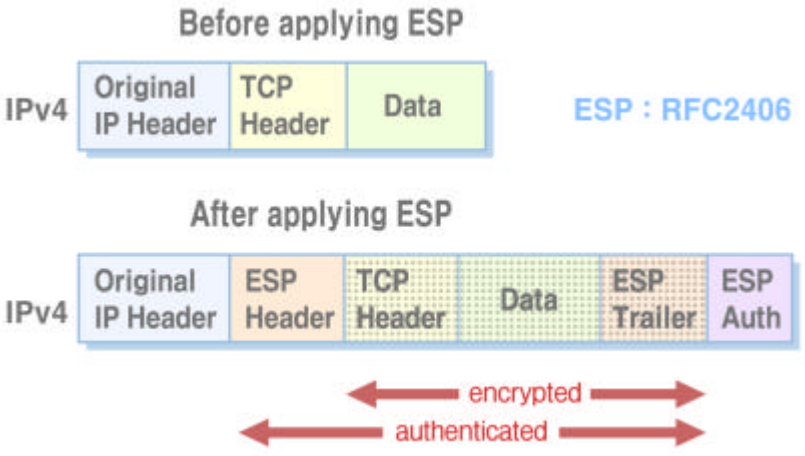
그림에서처럼 외부에서 볼 때 보안 게이트웨이의 IP 주소만이 보인다. 그러나 AH 프로토콜에서는 실제 패킷을 암호화하지는 않으므로 패킷 내부를 분석하면 원래 패킷의 IP 주소를 확인할 수는 있지만, 인증 데이터를 조작할 수 없으므로 패킷을 변조하거나 위조할 수는 없다.

4.4. ESP(Encapsulating Security Payload)프로토콜

ESP 프로토콜은 패킷을 암호화함으로써 기밀성 서비스를 제공하며 근원지 인증 및 선택적으로 무결성 서비스를 제공한다. 다음 그림은 ESP 프로토콜의 헤더 부분을 나타낸 것이다. 이때 Payload 데이터 부분은 상위 데이터 부분으로서 암호화된다.



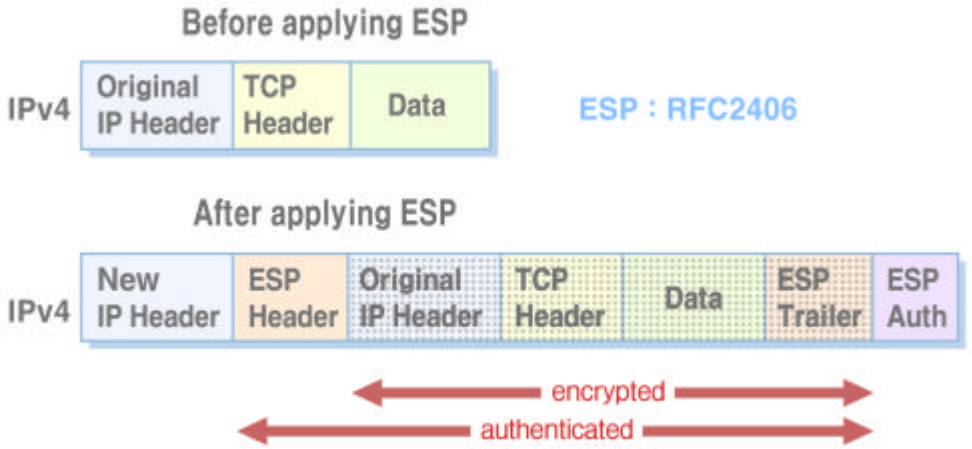
먼저 트랜스포트 모드에서 패킷을 암호화하는 경우의 구조를 보면 다음의 그림과 같다.



위의 그림에서 점으로 음영 표시가 된 부분은 원래의 데이터가 암호화되는 부분이다. ESP에서도 선택적으로 인증 서비스를 제공하는데, 이때 인증은 원래의 데이터가 아니라 암호화한 후의

데이터에 대해서 인증한다. 트랜스포트 모드는 IP 상위의 프로토콜을 보호하는 모드이므로 원래의 IP 헤더가 암호화되지 않은 상태로 남아있다.

다음은 터널 모드에서 ESP 프로토콜을 적용하는 경우 패킷의 구조이다.



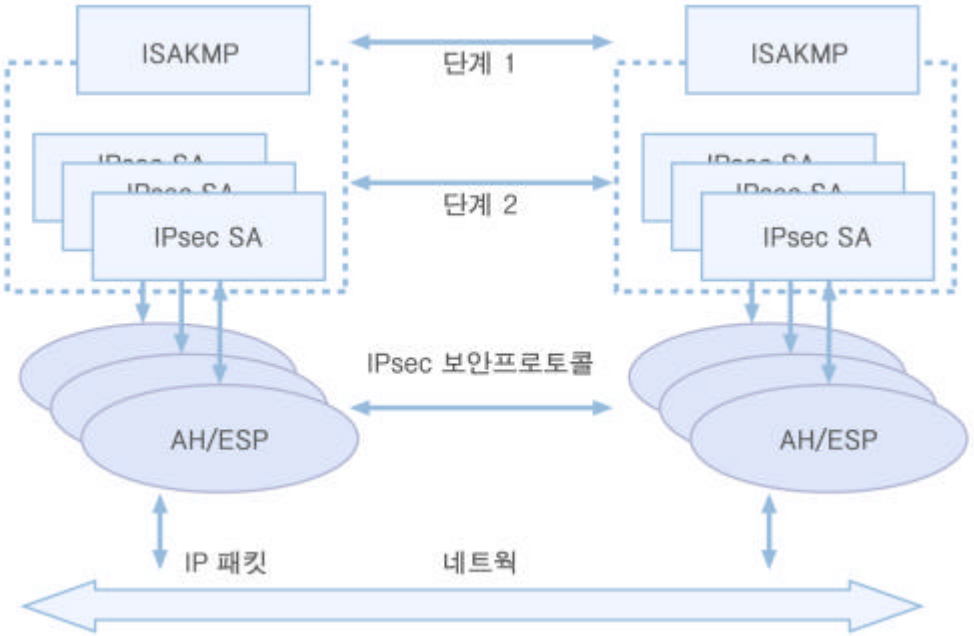
위의 구조에서 보면 원래의 패킷은 IP 헤더 부분을 포함하여 상위부분 전체가 암호화되는 것을 확인할 수 있다. 즉 앞에서도 얘기한 바와 같이 터널 모드에서 ESP 프로토콜로 암호화하는 경우에는 원래 패킷의 출발지와 도착지를 노출시키지 않음으로써 트래픽 엔지니어링에 대해서도 보호할 수 있다.

4.5. SA(Security Association)

특정한 키로 암호화된 데이터는 해당 키를 써야만 복호화를 할 수 있다.(대칭키 암호화 시스템의 경우 암호화키와 복호화키가 같다. 또한 실제 인증 과정 중에서는 공개키 인증서를 사용할 수도 있지만, IPsec 프로토콜을 이용하여 패킷을 암복호화는 경우는 성능상의 이유로 대칭키 암호화 시스템을 사용한다. 위의 암호화 알고리즘 리스트에서 알 수 있는 바와 같이 RC5, DES, IDEA 등의 알고리즘을 이용하여 암호화하는데 이 알고리즘들은 모두 대칭키 암호화 시스템들이다.)

네트워크에서 하나의 개체가 암호화한 데이터를 다른 개체에서 복호화하려면 어떻게 해야 할까? 두 개체는 암호화할 알고리즘을 하나로 통일해서 정해야 하며, 암호화 및 복호화에 쓰일 키에 대해서 공유하고 있어야만 한다. 이런 논리적인 결합을 SA(Security Association, 아직 적절히 한글화된 용어는 없다.)라고 하며, IPsec으로 암복호화기 전에 두 개체간에 미리 설정되어 있어야 한다.

IPsec에서의 SA는 계층적인 구조를 가지고 있는데, 1단계 SA와 2단계 SA로 나누어진다.



1단계 SA는 두 IPsec 개체간에 인증 및 2단계 SA를 맺는 메시지를 보호하기 위한 세션 키를 협상한 SA이다. 1단계 SA는 2단계 SA를 설정하기 위한 메시지를 보호하는 데에만 쓰이고, IPsec으로 트래픽을 보호하기 위해서 쓰이지는 않는다. 또한 1단계 SA는 방향성을 가지지 않는다.

2단계 SA는 실제 IPsec 프로토콜에서 사용할 SA를 말한다. 이때 SA에 포함되는 정보는 다음과 같다.

- 인증 메커니즘(비밀키 또는 공개키 인증서)
- 암호화 알고리즘(모드, 키길이, Initialization Vector, 등)
- 해시 알고리즘
- 암호화 및 인증 키값
- SA 갱신기간(현재의 SA를 폐기하고 새로 갱신해야 하는 시점)

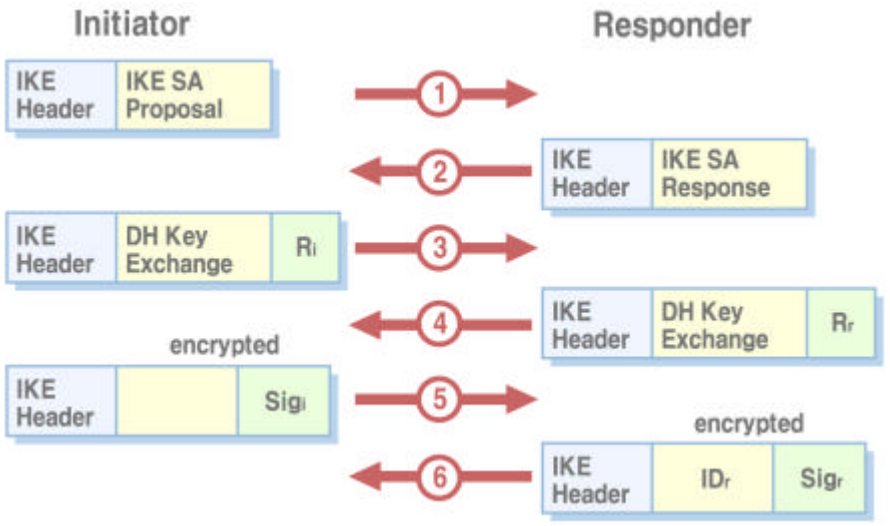
또한 2단계 SA는 방향성을 가진다. 즉 IPsec으로 나가는 패킷과 들어오는 패킷에 대해서 사용되는 SA가 다르다.

위와 같은 SA의 속성을 설정하는 방법에는 두 가지가 있다. 첫번째는 수동키(Manual Keying) 방식으로 두 IPsec 개체에 대해서 관리자가 수동으로 입력해 주는 방식이 있고, 두 번째 방법으로는 자동키 교환 방식을 쓰는 것이다. 자동으로 키 교환하는 방법은 두 IPsec 개체에서 수행되는 IKE 프로토콜을 지원하는 데몬에 의해서 협상에 의해서 자동으로 설정하게 된다. 그럼 이제 IKE 프로토콜에 대해서 살펴보도록 하자.

5. IKE 프로토콜

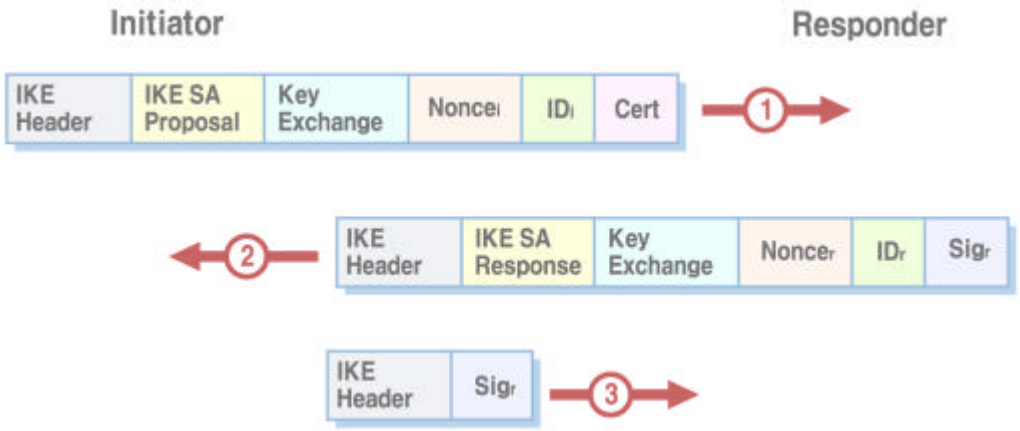
앞에서도 말했듯이 SA는 1단계 SA와 2단계 SA 두 계층으로 이루어진다. 1단계 SA는 IPsec 개체간에 단 한 개만 맺어져서 쓰이고, 2단계 SA는 1단계 SA를 기반으로 IPsec 정책에 설정된 대로 설정해서 각각의 트래픽에 대해서 고유하게 보안 서비스를 제공하게 된다.

IKE 메시지는 UDP 프로토콜을 사용해서 전달되면 출발지 및 도착지 주소는 500번 포트를 사용하게 되어 있다. 1단계에는 Main 모드 또는 Aggressive 모드 중에 하나가 쓰일 수 있다. 가장 기본적인 모드는 Main 모드로서 6개의 메시지 교환으로 구성되며 전달되는 내용은 다음의 그림과 같다.



IKE 프로토콜은 초기에는 ISAKMP/Oakley라는 이름으로 불렸다. 이는 ISAKMP에서 정의한 Payload의 구성 및 메시지 해석 방법과 Oakley라는 키 결정 프로토콜에서 정의한 방식으로 세션키를 유도했기 때문인데, IKE 표준은 각각을 적절히 조화시켜서 표준화한 것이다. 구체적인 과정은 참고문헌에서 언급한 RFC 또는 책을 참고하기 바란다.

1단계에서 Aggressive 모드로 인증할 수도 있는데 이때의 메시지 교환은 다음의 그림과 같다.



Aggressive 모드의 경우 처음 두개의 메시지에 모든 데이터를 교환함으로써 SA를 설정하는 과정을 단순하게 마친다. 위와 같이 Aggressvie 모드 또는 Main 모드를 통해서 1단계 SA를 맺게 되고, 실제 IPsec에서 사용할 SA를 설정하기 위해서 2단계의 SA를 설정해야 한다. 2단계의 SA를 설정하는 메시지는 1단계 SA에 의해서 보호되기 때문에 간단한 메시지로 구성되면, Quick 모드만이 사용된다.

6. 결론

이번에는 VPN에 대한 개념을 살펴 보았으며, 현재 가장 많이 받아들여지고 있는 VPN 프로토콜인 IPsec 프로토콜을 살펴보았다. IPsec 프로토콜은 AH와 ESP 두개의 프로토콜로 구성되며, 터널 모드 또는 트랜스포트 모드로 작동하게 되어 있다. IPsec 개체들은 SA 설정을 통해서 암호화 및 복호화 시에 필요한 패러미터들을 설정하게 되어 있으며, 이 SA는 수동으로 설정하거나 또는 IKE 프로토콜을 통해서 자동으로 설정될 수 있다. 다음에는 IPsec 프로토콜 중에 인증 기능을 제공하는 AH 프로토콜에 대해서 살펴보도록 한다.

7. 참고문헌

1) Carlton R. Davis, IPsec: Securing VPNs, Osborne/McGraw-Hill, 2001.
2) Elizabeth Kaufman, Andrew Newman, Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets, Wiley Computer Publishing, 1999.
3) Richard E. Smith, Internet Cryptography, Addison-Wesley Longman, 1997.
4) Ivan Pepelnjak, Jim Guichard, MPLS and VPN Architectures, Cisco Press, 2001.
5) 한국정보보호진흥원, IP 계층과 응용계층에서의 VPN 보안기술 표준(안), 1999. 3.

6) RFC 2411, IP Security Document Roadmap.(http://www.ietf.org/html.charters/ipsec-charter.html)
7) RFC 2401, Security Architecture for the Internet Protocol.
8) RFC 2402, IP Authentication Header.
9) RFC 2406, IP Encapsulating Security Payload(ESP).
10) RFC 2409, The Internet Key Exchange(IKE).[11] RFC 2412, The Oakley Key Determination Protocol.

8. 용어 설명

» MPLS(Multi Protocol Label Switching)

; IETF에서 정의한 3계층(네트워크 계층)스위칭을 위한 표준이다. Cisco의 태그 기반 스위칭과 마찬가지로, MPLS도 태그(또는 레이블이라고도 함)을 이용하는데, 여기에 패킷 전달에 관련된 정보를 포함시킨다. 전체 인터넷상에서 완전히 구현되면 MPLS는 정의된 SLA(Service Level Agreement)를 만족시키는 QoS(Quality of Service)를 제공할 수 있을 것으로 보여진다.

» ISAKMP(Internet Security Association and Key Management Protocol)

; IP(인터넷 프로토콜)뿐만이 아니라 여러 프로토콜 환경에서 범용적으로 사용할 수 있도록 IETF에서 정의한 SA 및 키 관리 프로토콜이다. ISAKMP 프로토콜을 인터넷 환경에 적용해서 IPsec에서 사용할 수 있도록 정의한 프로토콜이 IKE(Internet Key Exchange)프로토콜이며, 현재까지 적용된 프로토콜은 IKE만 있다.

» PPP(Point-to-Point Protocol)

; 직렬 케이블 상에서 인터넷 프로토콜을 구현한 통신 프로토콜이다. IETF에 의해서 1994년 개발되었고, 기존에 쓰이던 SLIP(Serial Line Internet Protocol)프로토콜을 대체하였다. PPP는 사용자의 컴퓨터와 ISP간에 링크 제어 프로토콜(Link Control Protocol)을 이용하여 세션을 설정하는데, 이 프로토콜에 의해서 사용자 인증, 압축 및 암호화 기능을 제공한다.

» GSS-API(Generic Security Service Application Program Interface)

; GSS-API는 클라이언트-서버 인증을 위한 범용 API이다. 표준화된 API를 사용함으로써 응용 프로그램의 개발자는 하위에서 제공되는 보안 시스템의 구체적인 스펙에 종속적이지 않게 일관된 보안 서비스를 제공받을 수 있다. IETF에서 GSSAPI ver. 2가 RFC 2743 표준으로 정의되어 있다.

» SSL(Secure Socket Layer)/ TLS(Transport Layer Security)

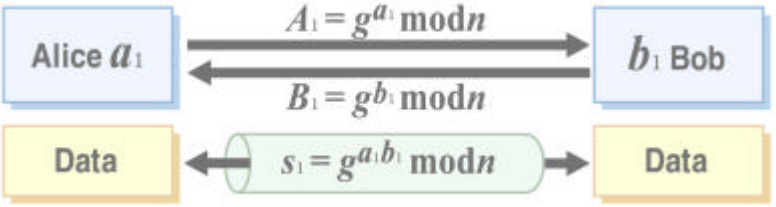
; Internet에서 널리 쓰이고 있는 보안 프로토콜이다. 소켓 인터페이스 수준의 보안 프로토콜로서, HTTP, FTP, TELNET 프로토콜 등을 보호하기 위해서 사용된다. SSL 세션이 시작되면 서버는 자신의 인증서를 클라이언트에게 보내고 클라이언트는 세션키를 생성하고 서버의 공개키로 암호화해서 서버에게 전달하여 세션키를 공유하고, 이 세션키를 기반으로 암호화 통신을 한다. 원래는 Netscape사에 의해서 Web 통신을 보호하기 위해서 개발되었으나, IETF에서 표준화되어 TLS 1.0 표준이 만들어지게 되었다. TLS 1.0 표준은 SSL version 3.1에 해당한다.

» PAP(Password Authentication Protocol)/ CHAP(Challenge Handshake Authentication Protocol)

; PAP은 네트워크에 로그인하는 가장 간단한 프로토콜로서, 서버는 사용자 ID와 패스워드를 저장하고 있다가 사용자가 로그인할 때 전송된 ID와 패스워드를 확인해서 검증하게 된다. PAP이 네트워크로 패스워드를 그대로 전달하는 반면 CHAP 프로토콜은 서버에서 던져주는 챌린지 값으로 암호화된 패스워드만이 네트워크로 전달된다.

» PFS(Perfect Forward Secrecy)

; 하나의 세션키가 공개되어진 경우에도 다른 세션키는 여전히 안전할 수 있는 성질을 말한다. 그림으로 설명하면 다음과 같다.



먼저 S_1세션키가 공격자에 의해서 풀렸다고 해도 S_2에 의한 세션키는 여전히 안전하다고 할 수 있다.(a_1, a_2, b_1, b_2 가 랜덤하게 생성된 경우에 이렇게 가정할 수 있다.)