通信情報保護學會學會誌
第 9 券 第 4 號, 1999. 12

VPN(Virtual Private Network)기술의 개요

강 문희*, 정 태명*

요 약

현재의 산업 상황은 제한적인 내부 네트워크의 사용만으로는 충분히 뒷받침할 수 없는 새로운 업무 형태로 바뀌었다. 기업에서는 내부 네트워크의 구성뿐만 아니라 증가하는 지사나 이동 근무자나 재택근무자들을 지원하기 위한 네트워크 확장이 필요하게 되었다. 그러나, 기존 네트워크 구성에서 사용하던 전용선이나 PSTN을 이용하는 방법은 많은 비용 때문에 기업에 과중한 부담을 가져오게 되었으며 이에 대한 해결책으로 VPN이 제안되었다. VPN은 공중망을 매개로 한 가상적인 네트워크 구성으로서 네트워크 확장에 소요되는 비용을 크게 절감하고 네트워크 관리를 용이하게 하였다. 특히 근래에 인터넷 사용자가 급격하게 증가하면서 보안 솔루션으로서의 IP 기반 VPN에 대한 관심이 집중되고 있다. 본 고에서는 VPN 기술의 전반적인 내용에 대해 소개하고 VPN의 핵심 기술이라 할 수 있는 터널링 기술을 IPsec 중심으로 살펴보기로 한다.

I. 서 론

정보 교류를 원활히 하기 위한 수단은 인류 역사를 통해 끊임없이 발전해 왔으며, 그 매체 또한 다양하게 변화해 왔다. 인류 최초에는 직접 정보를 전달하던 형태로 시작했으나, 이제는 전신, 전화의 단계를 벗어나 대부분의 정보가 전자 매체를 통해 전달되게 되었다. 특히 1960년대에 인터넷이 시작되고, 90년대 들어 인터넷 사용자가 기하급수적으로 늘어남에 따라 네트워크를 통한 정보의 공유가 매우 보편화되고 활성화되었다[1]. 이렇게 인터넷을 통해 이루어진 정보의 공유는 생활의 전반에 걸쳐 커다란 영향을 미칠 뿐만 아니라 전세계가 공유할 수 있는 문화로서 필수적인 요소가 되었다.

이런 영향으로 이제는 자신의 네트워크를 구성하는 것뿐만 아니라 외부의 네트워크와 상호 연결이 더욱 필요하게 되었으며 확대된 공중망에서 얻을 수 있는 여러 가지 이점들과 함께 정보보안의 문제점들도 발생하게 되었다. 본 고에서는 이런 네트워크의 발전 상황에 적절한 대처 방법을 제공하는 기술인 동시에, 21세기의 네트워크 구성에 필수적이며 보편적으로 적용될 VPN(가상 사설망)에 대하여 소개한다.

1. VPN의 출현 배경

기업이나 단체는 사설 네트워크를 이용하여 내부 자원을 체계적으로 정리하고, 필요한 경우 접근제어를 통해 자원을 공유한다. 그러나 현재의 산업 상황은 그런 제한적인 네트워크 구성으로는 충분히 뒷받침할 수 없는 새로운 업무 형태로 발전되었다. 기업들은 자신의 본사와 증가하는 지사들을 연결하기 위해 전용선을 이용하거나, 이동 근무자들과 재택근무자들이 사내의 네트워크로 접속할 수 있도록 확장할 필요가 생겼다. 지금까지는 이런 네트워크 확장을 위해 대부분 전용선을 사용하거나 PSTN을 이용해 왔다. 그러나 기존의 이런 방법들을 이용하면 네트워크 확장과 모뎀 풀 등을 관리하기 위한 인력뿐만 아니라 장비에 소요되는 비용이 급격히 증가하게 되어 큰 부담이 된다. 이에 반해 VPN은 네트워크 관련 비용을 절감하고 관리를 편리하게 함으로써 기존의 네트워크 확장에 해결책을 제시하고 있다[2].

실제로 VPN은 전용선을 사용하지 않고도 전용선을 사용하는 것과 동일한 효과를 얻기 위해 공중망 기반의 네트워크에 보안기능과 QoS를 제공하는 기술이다. 특히, 인터넷과 같은 공중망은 기본적으로

* 성균관대학교 전기전자 및 컴퓨터공학부 실시간시스템 연구실({mhkang, tmchung}@rtlab.skku.ac.kr)

보안에 취약한 구조이기 때문에 적절한 보안 메커니즘이 제공되어야 하며, 자원의 독점이 사실상 불가능하기 때문에 전용선과 같이 원하는 시간에 원하는 만큼의 데이터를 전달할 수 있는 정도의 서비스 품질을 제공하기 위한 QoS의 제공되어야한다[2][3].

2. VPN의 정의와 장단점

VPN은 그 자체가 하나의 네트워크를 구성하고 있으며 여러 가지 장단점을 가지고 있다. 그러나, VPN을 이용하는 이유인 장점을 살펴보면 다음과 같은 것들이 있다.

① VPN을 사용하는 경우 통신비용을 20-60% 정도를 절감할 수 있다. 이것은 전용선 구비에 소요되던 비용과 이동 근무자, 재택 근무자를 위한 원격지 dial-up 요금을 절감함으로써 오는 것이다. 또한, 집중화된 관리가 가능하게 되어 복잡한 구성의 네트워크를 관리하기 위한 인력에 소요되던 비용까지 감소시킨 것이다.

② 비용 절감 효과 외에 또한 큰 장점은 확장성이다. 전용선을 설치하는 경우 물리적인 설비를 갖추어 네트워크를 확장하는 것은 시간적, 공간적 제약이 따르지만, VPN을 사용하는 경우 손쉽게 다양한 형태의 네트워크를 구성할 수 있다.

③ 이동 근무자들은 본사의 네트워크에 안전하게 접속하여 자원을 공유, 사용함으로써 생산성이 증가될 수 있다. 또한 넓은 지역에 이미 수용된 인터넷을 이용하여 확장이 광범위해 질 수 있다.

그러나 VPN의 사용이 네트워크 구성의 최고 해결점이 될 수는 없다. VPN에서 제공되는 보안은 상당 부분 암호화나 인증 등의 보안 알고리즘에 의존하기 때문에 취약성을 가진 알고리즘을 사용하는 경우 보안상의 위협이 될 수 있다. 그렇기 때문에 적절한 보안 등급을 유지할 수 있는 관리가 필요하게 된다. 또 인터넷을 사용할 수 없는 지역에 있는 경우 (ISP가 존재하지 않는 경우) 이동 근무자가 VPN을 사용할 수 없게 되는 한계가 있다. 그러므로 VPN을 도입하려고 하는 경우 자신의 네트워크 상황과 필요를 정확하게 파악하여 가장 적절한 구성을 이루어야 VPN 사용의 장점을 충분히 얻을 수 있을 것이다.

3. VPN의 구현 형태와 구성

현재 제시된 VPN 제품들은 크게 파이어월 기반, 라우터 기반, 전용 제품의 세 가지로 분류할 수 있다. 파이어월 기반인 경우 기존의 파이어월 제품에 VPN 기능을 결합한 것으로 현재 큰 비중을 차지하고 있긴 하지만 파이어월에 집중되는 트래픽에 VPN 기능까지 제공하기 위해서는 심한 병목 현상이 생길 수 있는 단점이 있다. CheckPoint 제품이 대표적이다[4].

라우터 기반의 VPN은 전송 경로 상에 있는 라우터와 액세스 서버가 가상 사설망의 기능을 수행하도록 하는 방식으로 주로 Cisco 제품이 주를 이룬다. 이 방식에서 터널은 논리상의 점대점 방식으로 형성되며 라우터에 부가된 가상 사설망은 터널의 종단에 위치한 라우터의 성능에 의존하므로 어느 기기가 사용되는가 하는 것에 따라 네트워크의 성능이 결정된다

전용 시스템은 VPN 기능을 전담하는 장비로, 가상 사설망을 쉽게 확장할 수 있다는 장점이 있지만 장비구입을 위해 고가의 비용을 지불해야 한다. 대표적인 것으로는 Aventail, VPNet, Radguard의 제품군들이 있다.

라우터 기반의 VPN 제품이 99년 1분기에 4억4천3백만 달러에서 4분기에 6억9천7백만 달러의 시장 규모로 성장하였고 VPN 전용 하드웨어는 3천7백만 달러에서 1억6천만 달러로 거의 4배가 넘는 급성장 추이를 보이고 있다.

II. VPN의 요소 기술

트래픽에 터널링 프로토콜을 적용하는 것은 VPN 서비스를 위해 핵심적이고 중요한 과정이다. 터널링 기술과 함께 VPN을 구성하기 위해서 필요한 요소 기술들은 다음과 같은 것들이 있다.

1. 터널링 기술

터널링 기술이란 전용망 환경에서 점대점으로 회선을 연결한 것과 같은 효과를 위해 두 종단 사이에 가상적인 터널을 형성하는 것을 의미한다. 현재 표준안으로 진행되고 있는 프로토콜은 네트워크 계층의 IPsec과 데이터링크 계층의 L2TP, 응용 계층의 SOCKS가 있다. 여기서는 가장 표준안에 근접한 3 계층의 IPsec을 중심으로 살펴보기로 한다.

1) L2TP

1998년 Cisco의 L2F와 Microsoft, Ascend,

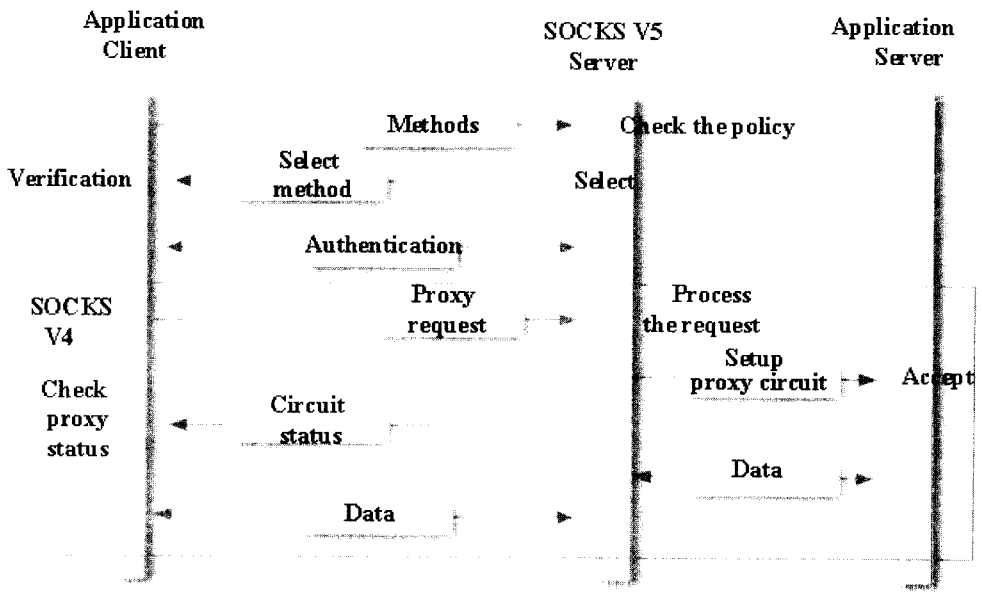


그림 1. SOCKSv5의 flow

3Com의 PPTP가 통합되어 IETF의 RFC로 발전된 터널링 프로토콜이다. 앞으로 설명될 IPsec은 IP 네트워크 상에서만 적용이 가능한 것에 반해, L2TP는 X.25, 프레임 릴레이, ATM 네트워크 등 다양한 프로토콜 상에서 PPP 프레임을 캡슐화한다[16]. 또한, L2TP는 데이터 링크 계층의 프로토콜이므로 점대점의 보안을 제공할 수는 없으며, 이를 위해 IPsec과 함께 사용되기도 한다. L2TP는 또한 사용자 패킷의 크기를 줄이기 위해 소프트웨어 기반의 압축을 사용한다.

L2TP의 핵심적인 기능은 LAC와 LNS를 통해 이루어진다. 원격지의 사용자가 모뎀을 통해 ISP로 PPP 접속을 하면, LAC(L2TP Access Server)는 터널을 초기화하고 PPP 페이로드에 여러 가지 헤더를 캡슐화하여 Home 네트워크의 LNS(L2TP Network Server)를 통해 터널을 형성한다. 터널 종료 지점의 디바이스는 라우터, 서버 또는 다른 액세스 장치가 될 수 있다.

2) SOCKSv5

IETF의 RFC 1928가 근간인 SOCKSv5는 기존의 SOCKSv4에서 지원하지 않던 UDP까지 지원하며 강력한 인증을 위한 방법을 제공하고 있다.

SOCKSv5는 TCP와 UDP 기반의 트래픽을 네트워크 프락시를 통해 안전하게 통과시킬 수 있도록 클라이언트-서버 애플리케이션을 위한 프레임워크를 제공하는 프로토콜이다[10].

그림1은 SOCKSv5의 흐름을 나타낸 것이다.

3) IPsec

IPsec은 IETF에서 제안한 네트워크 계층의 터널링 프로토콜로서 점대점 보안의 제공이 가능하다[14][15]. IPv6에서는 IPsec의 지원이 필수적으로 제공되어야 하므로 IP 계층에서의 VPN은 곧 부가적인 서비스가 아니라 IP 네트워크에서 제공되는 기본 기능으로 인식될 것이다.

IPsec은 AH와 ESP의 두 가지의 보안 메커니즘으로 구성되어 있다. IPsec에 대한 자세한 내용은 Ⅲ장에서 자세히 설명하기로 한다.

2. 키 관리 기술

터널링 프로토콜에서 필요한 보안을 충족시키기 위해서는 여러 알고리즘들과 키가 필요하다. 키 관리 기술은 이런 알고리즘과 키 값을 협상하는 역할을 한다. 아무리 강력한 암호화와 인증 알고리즘을 선택한다고 하더라도 키 관련 정보가 노출되는 경우 이후의 보안 알고리즘은 무용지물이 되기 때문에 무

엇보다도 키 관리 과정은 중요하다.

키 관리 과정은 수동으로 처리될 수도 있지만, 네트워크의 범위가 큰 경우에는 자동 키 관리 알고리즘이 필요하게 된다.

특히 IPsec의 경우 키 관리를 위해 IETF의 ISAKMP(Internet Security Association and Key Management Protocol)가 표준안으로 진행되고 있다. ISAKMP는 키 관리를 위한 프레임워크를 제공하는 프로토콜로서, SA를 설정하고 협상하고 수정하고 삭제하는 등의 작업을 위한 수행 과정과 패킷 포맷을 정의한다. IPsec은 키 관리 알고리즘과는 서로 독립적이다. 이렇게 IPsec은 어떤 키 관리 알고리즘을 쓰는지에 상관없도록 구현됨으로써 발전된 형태의 키 관리 알고리즘으로 대체하는 경우에도 IPsec 자체의 구현에는 영향을 미치지 않도록 요구하고 있다. ISAKMP는 키 관리 과정에 보안을 위한 요소를 제공하기 위하여 DoS(Denial of Service)와 Man-in-the-middle 공격을 막고, PFS(Perfect Forward Secrecy)를 제공하기 위해 키 관리 과정 중에 보안을 위한 요소들을 제공한다[8][9][11].

3. VPN 관리 기술

VPN은 물리적인 네트워크 요소들을 이용하여 제공되는 서비스라는 관점에서 봤을 때, VPN이 제공하는 개념적인 장점들을 충분히 살리기 위해서는 그에 적절한 관리가 필수적이다[12][13].

사용자와 VPN 서비스를 제공하는 업자 사이에 협상한 SLA(Service Level Agreement)의 내용이나, 자신의 네트워크에서 VPN 서비스에 대한 요구 사항을 마련함으로써 VPN을 사용하는 목적을 명확히 하고 협상한 것들을 준수했는지를 검증하는 기준으로 사용될 수 있다. VPN 관리 시스템은 그 요구 사항에 명시된 대로 서비스가 수행되는지를 사용자에게 보여줄 수 있어야 한다.

VPN 관리 대상에는 VPN 서비스를 위해 이용되는 여러 가지 장비들을 포함하여 사용하는 터널링 프로토콜과 키 관리 과정, 사용자에 대한 관리 등을 포함한다. VPN 관리는 이런 대상들에 대하여 정책을 설정하고, 정책과 보안 연계를 위한 데이터베이스를 관리하며, 터널링 프로토콜 진행 과정을 모니터링한다. 이런 과정을 통해 VPN 서비스에 제공되는 보안이나 QoS가 적절한 수준인지를 관리자가 검증할 수 있도록 한다. 따라서, 관리자는 관리 시스템이 제공하는 정보를 통해 서비스 상황을 살펴보고 정책을 바꾸거나 새롭게 장비를 구입할 계획을 세우는 등 효과적인 VPN 서비스를 위해 노력할 수 있다.

터널링 프로토콜에 대한 표준화와 함께 VPN 서비스를 위한 관리에 대한 표준화도 시급하다. 현재는 IETF에서 IPsec monitoring MIB이 draft로 나온 상태이지만 VPN 서비스 과정을 전체적으로 관리할 수 있는 MIB과 관리 구조는 아직 마련되지 않은 상태이다.

Ⅲ. IPsec

1. AH(Authentication Header)

AH는 사용자의 IP 데이터그램에 대한 인증과 무결성을 보장하고 리플레이 방지를 위한 기능을 포함한다[6]. 데이터의 무결성은 MAC(Message Authentication Code)에 의해 생성된 검사값(Chesksum)을 이용해 보장된다. 그림 2는 인증 데이터를 계산하는 과정을 나타낸 것이다.

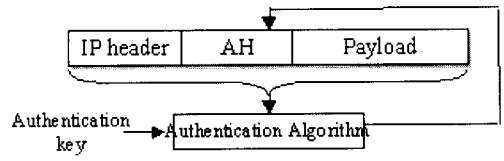


그림 2 인증 데이터의 계산

송신자가 MD5나 SHA-1의 알고리즘에 IP 패킷의 데이터를 키와 함께 입력하고 알고리즘이 계산한 인증 데이터의 값을 인증 헤더(AH)라는 필드에 기록한다. 그러면, 수신자는 동일한 키를 가지고 역으로 인증 데이터의 값을 검증하게 되는 것이다. AH는 전송중에 변화하는 필드를 제외하면 모든 데이터그램의 내용을 보호한다. 그러므로 인증 데이터 값을 검증할 때도 변화하는 값들을 모두 0으로 간주하고 계산하게 된다. AH는 또한 리플레이 방지를 위해 AH 내에 sequence number 필드를 제공한다.

AH는 트랜스포트 모드와 터널 모드의 두 가지 모드로 사용될 수 있다. 트랜스포트 모드는 원래의 IP 헤더를 그대로 이용하여 호스트간에 터널을 형성하는 데 주로 사용한다. 이에 반해, 터널 모드는 데이

터그램 전체를 AH로 캡슐화하고 새로운 IP 헤더를 추가하는 방식으로 송수신자를 새로이 지정할 수 있으며 주로 보안 게이트웨이사이의 터널 형성에 사용된다. 이 경우 내부의 IP 헤더는 데이터그램의 원래 목적지와 전송지의 IP 주소를 포함하며 바깥쪽에 새로이 생성된 IP 헤더는 터널을 형성하는 게이트웨이의 주소를 포함한다.

2. ESP(Encapsulation Security Payload)

ESP는 IP 데이터그램에 기밀성을 제공하며 선택적으로 인증 기능까지도 제공할 수 있는 프로토콜이다[7]. AH와 마찬가지로 리플레이 방지를 위해 Sequence number를 사용한다. ESP를 사용하면 IP 패킷 자체가 DES 혹은 Triple DES 암호방식으로 암호화되어 기밀성이 보장된다. 이때의 암호화 알고리즘이나 키등은 터널의 종단간에 협상을 통해 조정된다. ESP도 트랜스포트와 터널모드의 두 가지로 캡슐화가 가능하다. 트랜스포트 모드는 데이터그램의 원래 IP 주소를 그대로 사용하여 IP 헤더를 제외한 부분을 암호화하게 되므로 호스트간의 터널을 형성하는 데 사용하며, 터널모드는 IP 패킷 전체를 암호화하고 새로운 IP 헤더를 추가하므로 보안 게이트웨이간의 터널을 형성하거나, 송수신자의 IP 주소까지 숨기기를 원하는 경우 사용될 수 있다.

ESP 역시 트랜스포트 모드는 대부분 통신의 종단점인 호스트와 호스트 사이의 연결에서 사용되며 터널 모드는 호스트와 게이트웨이, 또는 게이트웨이와 게이트웨이 사이에서 주로 사용된다.

그림 3은 AH와 ESP가 각각 트랜스포트 모드와 터널 모드로 사용되었을 때를 나타내는 그림이다. AH와 ESP 모두 인증 기능을 제공하지만 그림에서 볼 수 있듯이 ESP에서의 인증은 그 제공 범위가 다르다. AH는 AH헤더 앞의 IP 헤더까지 인증하지만 ESP 헤더의 경우 제일 나중에 캡슐화한 IP 헤더는 인증 범위에 포함되지 않는다.
AH와 ESP 헤더가 한 데이터그램에 대하여 함께 제공될 수도 있으며, IPsec 헤더는 사용자가 원하는 보안 서비스에 따라 적절히 구성되어야 한다.

그림 4는 IPsec 프로토콜의 전체 흐름을 나타내는 것으로 RFC 2402의 AH와 RFC 2406의 ESP의 내용을 하나로 정리한 것이다. 트래픽이 네트워크에 유입되면 제일 먼저 SPD를 이용해 트래픽에 적용될 정책을 결정한다. 정책의 설정과 수정, 삭제에 관련된 사항은 IPsec에서는 정의하지 않으므로 관리 인터페이스가 별도로 제공되어야 한

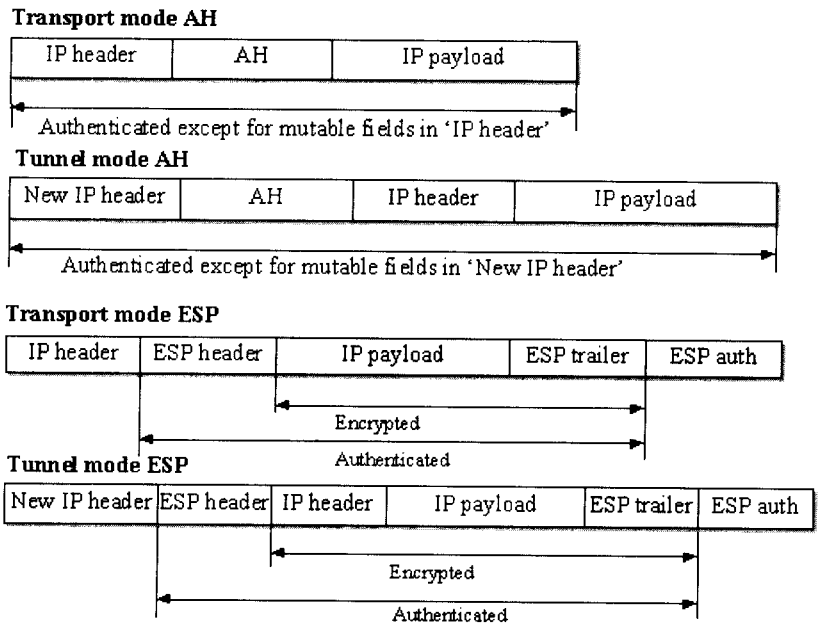


그림 3. 트랜스포트 모드와 터널 모드의 AH와 ESP

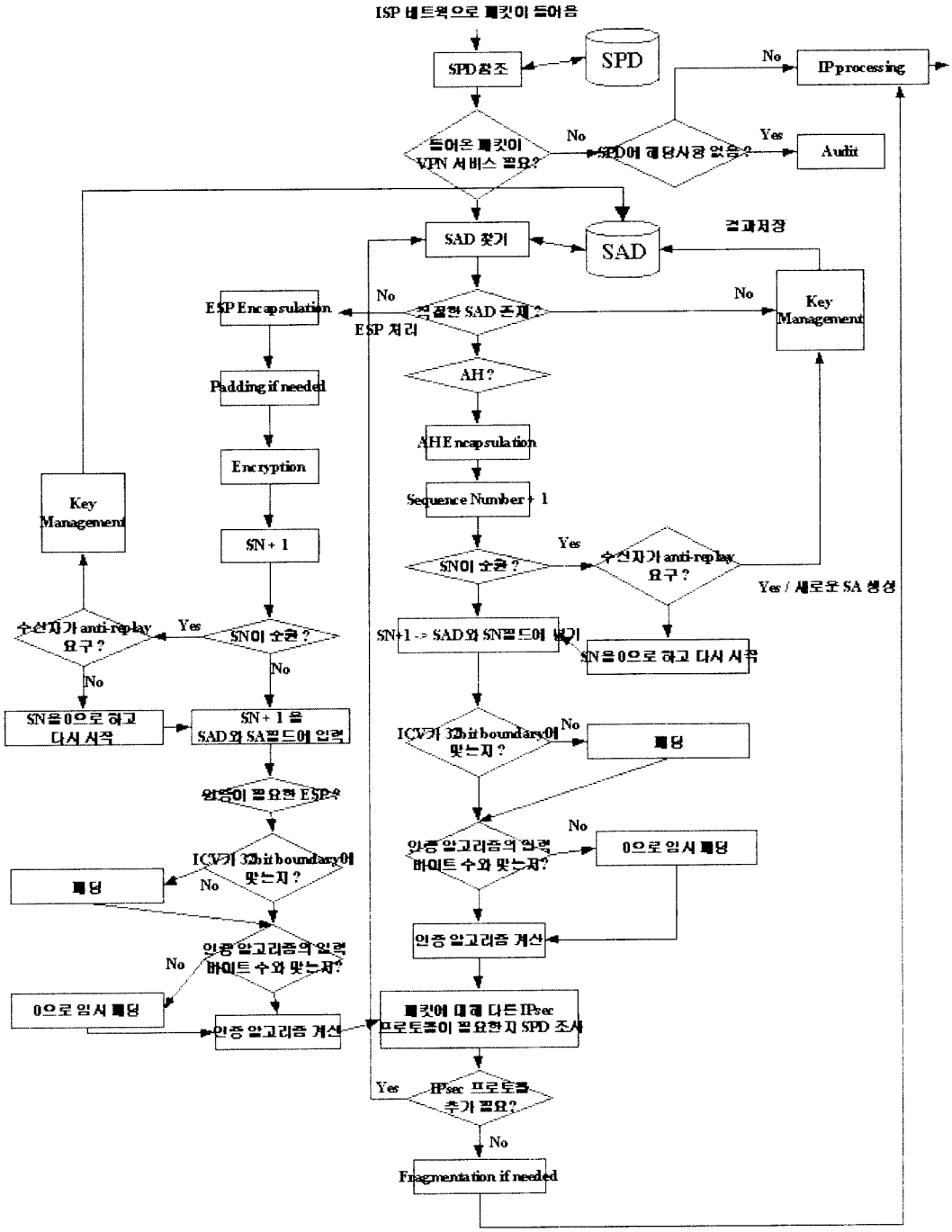


그림 4. IPsec의 전체 흐름도

다. 트래픽에 대한 정책은 '폐기', '일반 IP 처리', 또는 'IPsec 적용' 등이 있을 수 있다. IPsec이 적용되는 패킷은 IPsec 처리 모듈로 전송된다.

IPsec 처리를 요구하는 트래픽에 대해서는 미리 키 관리 과정을 통해 SAD의 엔트리가 구성되어 있어야 한다. SAD가 구성되어 있지 않은 경우 키 관리 모듈을 통해 SAD를 구성해야 한다.

SAD의 구성이 완료되면 트래픽에 협상된 보안 서비스를 적용하여 터널링 한다. 단일 SA는 하나의 IPsec 프로토콜의 적용에 대해 협상된 내용이므로 IPsec 프로토콜을 추가적으로 적용하기 위해서는 다른 SA가 필요하다.

3. 데이터베이스 관련 기술

RFC 2401에서 IPsec을 지원하기 위한 두 가지 데이터베이스에 대해 언급되어 있으며, 대표적으로 SAD(Security Association Database)와 SPD(Security Policy Database)가 있다[5].

SPD는 트래픽에 적용할 정책을 결정하기 위해 선택자(Selelctor)로 사용될 값들이 선택자 필드를 구성하며 네트워크 내부로 들어오거나 나가는 모든 트래픽에 대해 적절한 정책을 적용할 수 있도록 한다. SPD에 의해 트래픽은 폐기되거나 일반 IP 트래픽으로 처리되거나 IPsec이 적용되는 세 가지의 정책이 적용될 수 있다. IPsec이 적용되어야 하는 트래픽인 경우 터널 종단이 되는 두 시스템간에 보안 연계(Security Association)가 구성되어야 하며 구성된 보안연계는 SAD의 엔트리가 된다.

Ⅳ.VPN의 응용 분야

앞에서 소개한 VPN의 장점을 이용하여 여러 가지 응용이 가능하며, 특히 요즘 전자 상거래에 대한 관심이 높아지면서 VPN의 중요성이 높아지고 있다. 전자 상거래는 물품의 구입 과정에서 현금과 관련된 중요 정보들이 인터넷을 통해 전송되므로 보안의 제공이 필수적이기 때문이다.

전자 상거래와 함께 인터넷을 통한 증권 거래, 경매와 같은 작업에 VPN이 사용된다. 즉, 증권 거래와 경매는 절대적으로 안전하게 전달되어야 하며 또한 정확하고 신속하게 전달되어야 하는 필요성이 있으므로 VPN 이용에 적합한 좋은 예가 될 수 있다.

기업의 네트워크 구성에 VPN을 응용하는 경우 여러 가지 이득을 볼 수 있다. 원격지에 있는 많은 지사들과의 교류가 필요한 경우, 지사들과의 연결에 전용선 대신 인트라넷 VPN을 구성할 수 있으며, 자동차 회사와 같이 많은 부품 업체와 협력하는 기업은 협력업체와의 연결에 익스트라넷 VPN이 이용될 수 있다. 또한 보험회사와 같이 이동 근무자가 많은 기업은 근무자에게 원격접속 VPN을 제공함으로써 작업 효율을 높일 수 있어서 생산성 향상에 도움을 줄 수 있다.

Ⅴ. 결론

인터넷의 사용자가 이렇게 급격히 증가하게 될 것이라고는 아무도 예상하지 못했다. 그런 만큼 인터넷 사용에 있어서 여러 가지 보안상의 문제점과 네트워크 자원을 공유하기 때문에 생기는 QoS의 불만족이 심각해지게 되었다. 또한 네트워크를 통한 자료의 공유 또한 보편화되고 활성화됨에 따라 네트워크 확장의 문제와 그 비용의 문제도 크게 대두되었다. 이런 공중망의 필요성들을 VPN이 많은 부분 채워줄 수 있다고 기대된다.

그러나, VPN이 네트워크 구성의 최선책이 되기 위해서는 VPN을 도입하기 전에 먼저 내부 네트워크의 상황과 필요성에 대해 정확한 분석이 필요하며, 그 필요에 알맞은 네트워크 구성이 필요하다. 그와 함께 구성된 VPN을 효과적으로 운영하고 유지할 수 있는 관리 시스템이 필수적이다.

현재 VPN의 유용함에 대해 많은 기업과 사용자들이 관심을 가지고 있다. VPN은 보안 관련 기술이 기본이 되는 만큼 국내에서도 자체적인 기술을 개발할 필요성이 있으며 그러기 위해서는 먼저 VPN의 기반 기술을 익혀 경쟁력을 갖추는 것이 중요할 것이다.

참 고 문 헌

[1] Daniel Lynch and Marchall Rose, *"Internet System Hand book"*, *Addison Wesley*, 1993

[2] Steven Brown, *"Implementing Virtual Private Networks"*, *McGrow-Hill*, 1999

[3] Charlie Scott, Paul Wolfe, and Mike Erwin. *"Virtual Private Network"*,

O'Reilly, 1998.

[4] Chris Brenton, "*Network Security*", pp319-349, *SYBEX*, 1999

[5] Stephen Kent, Randall Atkinson, "*Security Architecture for the Internet Protocol*", RFC 2401, *IETF*, Nov., 1998.

[6] Stephen Kent, Randall Atkinson, "*IP Authentication Header*", RFC 2402, *IETF*, Nov., 1998,

[7] Stephen Kent, Randall Atkinson, "*IP Encapsulating Security Payload (ESP)*", RFC 2406, *IETF*, Nov., 1998.

[8] Derrell Piper, "*The Internet IP Security Domain of Interpretation for ISAKMP*", RFC 2407, *IETF*, Nov,. 1998.

[9] Douglas Maughan, Mark Schneider, et. al. "*Internet Security Association and Key Management Protocol (ISAKMP)*", RFC 2408, *IETF*, Nov., 1998.

[10] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas and L. Jones, "*SOCKS Protocol Version 5*", RFC 1928, *IETF*, Mar., 1996.

[11] D. Harkins, D. Carrel, "*The Internet Key Exchange(IKE)*", RFC 2409, *IETF*, Nov., 1998.

[12] Cisco, "*Network Management Solutions for IP-VPN Services*", white paper, *Cisco Systems*, 1998.

[13] Cisco, "*Managing Virtual Private Networks - An Introduction to VPNs*", white paper, *Cisco Systems*, 1999

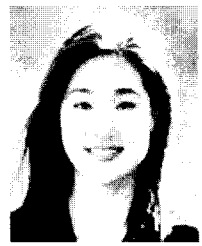
[14] IBM, "*Using IPsec to Construct Secure Virtual Private Networks*", white paper, *International Business Machines Corporation*, 1998.

[15] Timestep, "*Understanding the IPsecc protocol suite*", white paper, *Timestep*, 1997.

[16] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, "*Layer Two Tunneling Protocol(L2TP)*, RFC 2661, *IETF*, Aug., 1999.

著者紹介

강 문 희(Moon H. Kang) 준회원

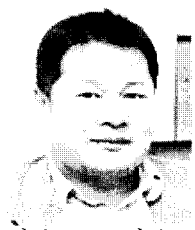


1998년 8월 : 성균관대학교 정보공학과 졸업

1998년 8월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 석사과정

<관심분야> VPN, 보안관리, 이동 에이전트 보안

정 태 명(Tai M. Chung) 정회원



연세대학교 전기공학과 공학사

미국 일리노이 주립대학 전자계산학과 이학사 및 컴퓨터공학 석사

미국 Purdue University 컴퓨터공학 박사

미국 Waldner & Co. 엔지니어

미국 BBN 연구소 연구원

IEEE Senior Member,

정보과학회, 정보처리학회 회원

(현)성균관대학교 전기전자 및 컴퓨터 공학부 교수

<관심분야> 전자상거래보안, 보안관리, 네트워크 관리, 실시간 시스템, Active Network