[5B-38]

MPLS-VPN 에서의 보안기술 분석

이 정 균, 이 기 영
인천대학교 정보통신공학과
tnfeco@empal.com , kylee@incheon.ac.kr

The Analysis of Security in MPLS VPN

Jeong kyoon-Lee, Ki Young-Lee
Dept. Info.& Telecom. Eng. , University of Incheon

요 약

본 고에서는 IP based VPN에서의 L2TP/IPsec모델의 보안성과 차세대 VPN 기술로 주목받는 MPLS VPN에서의 보안성에 대하여 알아보았다. L2TP는 또한 터널 끝점을 상호 인증하는 데 사용될 수 있는 터널 인증 기능을 지원한다. 그러나 L2TP는 터널자체의 보호 메커니즘을 정의하고 있지는 않다. L2TP 제어 패킷과 L2TP 데이터 패킷의 보호를 위해 IPsec을 이용하여 구현해야 한다. L2TP/IPsec은 뛰어난 안전성을 제공하지만, 반면에 키 관리 및 분배와 같은 여러 기반 기술들이 필요하고, 사용자가 VPN 서비스를 직접 관리해 주어야 하며, QoS를 효과적으로 지원하지 못하는 등의 문제도 있다. MPLS VPN 모델은 기존의 IP VPN이 지니고 있는 많은 제약 사항을 해결할 수 있으며, 기존의 망에서 제공할 수 없었던 고속 서비스와 QoS 그리고 다양한 부가 서비스를 창출할 수 있기 때문에 망 사업자들로부터 차세대 인터넷으로 진화할 수 있는 새로운 핵심 기술로 평가 받고 있다.

Ⅰ. 서 론

지금까지 기업 가입자들은 망사업자로부터 점대점 기반의 전용선을 임대하여 자신만의 WAN을 구축한 후 사용하여 왔는데 이것을 사설망이라 한다. 사설망은 다양한 종류의 가상 회선들이 전용선을 대체함에 따라 "가상 사설망(Virtual Private Network: VPN)"이라 불리게 되었다[1]. 공중망을 기반으로 하는 사설망인 VPN은 기존의 사설망보다 매우 경제적으로 망을 운영할 수 있으며 사설망이 가지는 보안성 , 신뢰성, 관리 편의성, 사설주소 지원, 우선순위 설정 등의 기능을 수행할 수 있다. VPN 데이터가 패킷형태로 전달 되는 것을 IP VPN 이라고 한다. IP VPN은 일반적으로 기반이 되는 백본망이 인터넷이므로 광범위한 지역에 구축이 가능하고 접속 비용이 저렴할 뿐만 아니라 TCP/IP 데이터 에플리 케이션의 급속한 확산에 따라 수용 가능한 에플리케이션도 풍부하다.[2] IP VPN에 속하는 사이트 들간을 백본망을 통하여 안전하게 연결하기 위하여 터널링 메커니즘을 필요로 한다. 이러한 기술에는 IPsec, GRE(Generic Routing Encapsulation), IP/IP, L2TP (Layer 2 Tunneling Protocol), MPLS 등 다양하다. 이중에서 최근 관심을 끌고 있는 기술이 MPLS 기반 VPN 기술이다. MPLS는 QoS 기능이 우수하며 다양한 프로토콜과 폭넓은 보호 기능을 지원하기 때문에 기존의 터널링 프로토콜을 대치함으로써 망사업자가 제공하는 VPN 기술의 핵심 요소로 자리매김하고 있다. 본 논문은 IP VPN에서의 대표적인 2계층 터널링 기술인 L2TP의 보안성의 분석과 이를 보완해줄 IPsec 프로토콜의 보안성을 분석한다. 그리고 MPLS 기반의 VPN 기술의 보안적 요구 사항와 보안 기술을 소개한다.

Ⅱ. IP 터널링 VPN 기술의 보안성

1. L2TP 기술의 보안성

L2TP(Layer Two Tunneling Protocol)는 여러 형태의 네트워크(IP, SONET, ATM 등) 상에서 PPP(Point-to-Point Protocol) 트래픽을 터널해 주는 프로토콜이다. L2TP는 PPP 패킷을 인캡슐하기 위한 PPP 인증, PPP 암호 제어 프로토콜(Encryption Control Protocol: ECP), 그리고 압축 제어 프로토콜(Com-pression Control