主題

IP 기반의 PPVPN(Provider Provisioned Virtual Private Network) 기술

광운대학교 이승형 국가보안기술연구소 윤재우

차 례

요 약

본 고에서는 Peer모델 PPVPN 기술인 BGP/MPLS를 비롯하여, 현재 IETF의 PPVPN WG에서 논의되고 있는 IP 기반의 여러 가지 PPVPN 프로토콜들의 기술적 특징 및 장단점을 비교하고, 이들의 연구동향 및 발전방향에 대하여 분석한다. 3계층의 IPSec VPN은 확장성이 부족한 단점을 가지며, 2계층 MPLS VPN의 확장성을 개선한 BGP/MPLS는 보안성 및 범용성에 문제가 있다. 이러한 PPVPN 프로토콜의 기술적 특성을 강화하기 위하여 각 기술들을 융합하거나 기존 기술을 개량하는 등의 다양한 제안 및 논의가 이루어지고 있다. VPN 사용자의 다양한 욕구를 만족시켜 줄 필요성과 네트워크 운용의 효율화를 통한 사업자의 수익증대 측면에서 기존의 IP PPVPN 기술들은 향후에 지속적인 개선과 발전이 예상되며, 이는 본 고에서 논의하는 바와 같이 확장성, 보안성 등의 특성을 강화하는 방향으로 진행될 것이다.

Ⅰ. 서론

IP 기반의 PPVPN(Provider Provisioned Virtual Private Network)[1]은 인터넷의 성장에 따라 SP(Service Provider)가 사용자에게 경제적으로 새로운 서비스를 제공할 수 있는 기술로 각광을 받고 있다. 네트워크 사업자는 새로운 서비스 모델에 의해 수익원을 창출할 수 있으며, 예를 들어 초고속 국가망의 경우에는 각 기관가입자들을 하나의 네트워크에 수용하여 기관별 네트워크를 구축하는 것이 가능해졌다. VPN(Virtual Private Network)은 사용자가 전용선을 이용한 사설망을 사용하는 경우와 마찬가지의 연결성을 공중망에서 제공해야 하므로, IP VPN에 사용되는 기술은 인터넷에서 데이터의 전송 시에 생길 수 있는 문제점들을 보완하여, 데이터의 신뢰적인 전송, 전송품질의 보장 및 불법적인 접근에 대한 보안을 지원하여야 한다. 최근에 IETF의 PPVPN WG(Working Group)[1]은 이미 표준화된 BGP/MPLS VPN[2]의 개선을 비롯하여 여

러 가지의 새로운 PPVPN 구축기술을 논의하고 있는데, 이 기술들은 대부분 기존에 사용되던 IPSec[3]과 MPLS[4]를 적용 혹은 응용하고 있다. IPSec은 전송되는 패킷에 대한 인증, 암호화, 및 무결성에 대한 지원을 함으로써 데이터의 보안에 강점을 갖는 반면에, MPLS는 전송품질의 보장, 트래픽의 제어 및 효율적인 패킷 전달 등의 특징을 갖는다. 현재 SP들은 이 두 가지, 혹은 그 중 한 기술을 이용하여 VPN 서비스를 제공하고 있거나 계획 중에 있으며, 각 기술은 보안성 및 확장성 등에서 장단점이 있으므로 두 기술을 동시에 적용하는 경우는 각각의 특성을 이용하여 서비스를 구현하여야 한다. PPVPN에서 논의 중인 새로운 기술들은 대부분 이 두 가지 기술들을 적용 및 개량하여 확장성, 보안성 및 범용성 등의 특성을 개선하고자 하는 노력들이다. 이러한 기술들은 아직 표준화가 이루어지지 않은 단계이나, VPN 기술의 개발동향 및 향후 기술의 발전방향을 가늠해 볼 수 있는 새로운 제안들이다. 본 고에서는 PPVPN WG에서 논의 중인 여러 가지 VPN들의 개요 및 기술적 특징들을 기술하고 각각의 장단점 및 관계에 대해 기술한다.

이후의 내용은 다음과 같다. Ⅱ장에서는 PPVPN의 두 가지 참조 모델인 CE 기반 및 PE 기반 모델에 대해 설명하고 이에 따른 여러 가지 PPVPN 기술의 종류에 대해 언급한다. Ⅲ장에서는 Peer 모델의 대표적인 예인 BGP/MPLS에 대해 정리하고, 이를 개선하기 위해 제안된 최근의 기술들을 소개한다. Ⅳ장에서는 SMPLS와 CE 기반 IPSec 등의 Overlay 모델들의 기술적 특징을 정리하며, Ⅴ장에서는 각각의 PPVPN 기술의 특징에 대한 비교 분석 및 관계에 대해 기술한다. 마지막으로 Ⅵ장에서는 향후 IP 기반 VPN 기술의 발전전망에 대해 언급하고 결론을 맺는다.

Ⅱ. PPVPN 기술 및 모델

1. PPVPN의 종류

VPN은 매우 다양한 형태가 있으며 이를 위한 기술도 매우 여러 가지가 개발되어 적용되고 있는데, IP 기반의 3계층 PPVPN은 크게 PE(Provider Edge) 기반의 VPN과 CE(Customer Edge) 기반의 VPN으로 구분할 수 있다[5]. CE 기반의 VPN은 사용자들의 네트워크 관리 부담을 덜기 위하여 SP(Service Provider)가 사용자의 라우터(CE)들을 서로 연결하여 VPN을 구축하고 CE를 포함한 네트워크에 대한 관리를 하는 형태이다. 이때, CE 사이에 적용되는 터널을 위한 기술로는 MPLS[4], IPSec[3], GRE[6], IP-in-IP[7] 등의 다양한 기술이 쓰일 수 있다. PE 기반의 VPN은 SP 네트워크의 Edge 라우터에 해당하는 PE 라우터들을 터널로 연결하여 VPN 서비스를 제공하는 형태이다. 사용자들은 자신이 관리하는 CE 라우터를 PE 라우터에 연결하여 서비스를 받으며, SP가 PE들을 연결하기 위한 터널링 기술로는 CE 기반과 마찬가지로 MPLS, IPSec, GRE, IP-in-IP 등의 다양한 메커니즘이 적용될 수 있다.

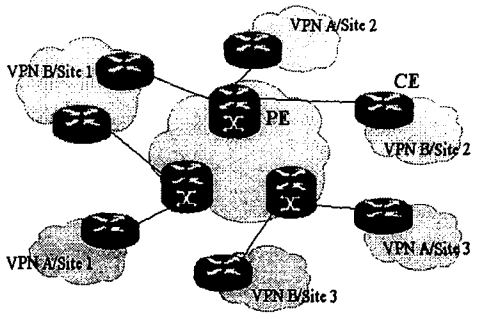


그림 1. Peer 모델 VPN의 예[4]

일반적으로 CE 기반의 VPN에서는 각 CE 라우터들을 터널로 연결하여 Mesh 혹은 Hub-and-spoke 형태의 토폴로지를 만드는 Overlay 모델을 적용한다. 이 모델은 많은 수 의 사이트를 갖는

VPN의 경우에 터널의 수가 크게 증가하며, 새로운 사이트를 추가하거나 제거하는 경우에 각 사이트의 정보를 수정하여야 하므로 확장성(Scalability)의 문제가 있다. 한편, PE 기반의 VPN에서는 하나의 PE에 여러 개의 CE 라우터가 연결되는데, 이는 하나의 PE라우터가 여러 개의 VPN을 동시에 지원한다는 의미이며, 이를 위해 Peer 모델을 사용한다. 이 모델은 그림1에서와 같이, CE 라우터는 PE 라우터와 일대일로 연결이 되며, PE 라우터는 여러 VPN을 접속할 수 있고 Mesh 형태의 연결은 PE 라우터 사이에만 필요하다. 따라서 Overlay 모델의 단점인 확장성 문제를 해결하여, 최근에 많은 연구가 이루어지고 있는 모델이다.

표 1. IETF의 PPVPN WG에서 논의되고있는 기술들

VPN 기술	종류	모델	문서
BGP/MPLS VPN[2,8]	PE 기반	Peer	RFC
PE-PE GRE/IP[9]			Draft
PE-PE IPSec[10]			
Virtual Router[11]		Overlay	
SMPLS[12]			
CE-CE IPSec[13]	CE 기반		

표 1은 현재 IETF의 PPVPN WG(Working Group)[1]에서 논의되고 있는 대표적인 기술들을 정리한 것이다. 앞서 언급한대로, 네트워크 장비 사이의 터널링 기술로는 MPLS와 IPSec이 가장 많이 적용되고 있으며, 각 기술들이 지니고 있는 보안성, 확장성, 범용성 등의 단점을 해결하기 위한 연구가 활발히 진행되고 있다. 이 중에서 BGP/MPLS[2,8]는 현재 IP 기반의 PPVPN 기술 중에서 가장 주목을 받고있는 기술이며, PE-PE GRE/IP[9] 및 PE-PE IPSec[10]은 각각 BGP/MPLS의 단점인 범용성 및 보안성의 개선을 위해 제안된 방법이다. BGP/MPLS는 현재 RFC 2547로 문서화되었으나[2], 현재도 계속하여 개선작업이 이루어지고 있다[8]. PE 기반의 기술인 Virtual Router[11]와 SMPLS[12]는 CE 기반의 CE-CE IPSec[13]과 마찬가지로 Overlay 모델을 적용하고 있다.

2. PPVPN의 참조모델

이 절에서는 앞서 언급한 PE 기반의 VPN과 CE 기반의 VPN에 대한 참조 모델을 [5]의 내용을 근거로 하여 소개한다. 두 모델 모두 사용자의 CE 라우터와 SP의 PE 라우터 및 P 라우터로 구성되어 있으나, 각 라우터가 VPN의 구성에서 담당하는 기능 및 역할이 두 모델에서 차이가 있다. PE 기반의 PPVPN 모델(그림 2)에서 CE는 VPN 관련 기능이 전혀 필요치 않은 라우터, 스위치, LSR, 혹은 호스트이며, 일반적으로 사용자 사이트의 Edge에 위치하여 SP의 PE에 직접 접속이 된다. PE는 SP 네트워크의 Edge에 위치하며, 접속된 CE에게 해당하는 VPN의 서비스를 제공하여 주고 VPN 정보를 관리하는 역할을 한다. 서로 다른 VPN의 트래픽을 분리하여 처리하기 위하여, PE는 자신이 관리하는 VPN의 수에 해당하는 VFI(Virtual Forwarding Instance)를 운용하여 다른 VPN의 트래픽 및 라우팅 정보가 섞이지 않도록 한다. P라우터는 SP 네트워크 내에서 PE 라우터들 사이를 연결하는데 사용되며, VPN의 구성 및 운용에 관한 정보를 갖고 있지 않는다.

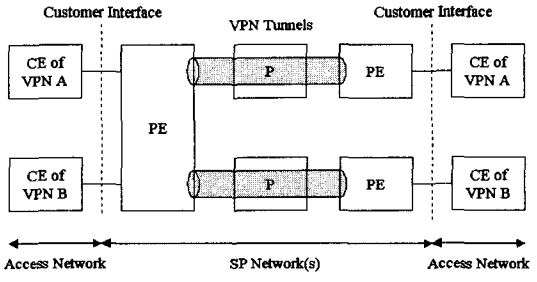


그림 2. PE 기반 3계층 PPVPN의 참조모델

이에 비해 그림 3의 CE 기반 모델에서는 CE 라우터가 하나 혹은 그 이상의 VPN 터널을 관리하며, PE 라우터는 VPN의 관리 및 운용에 관한 아무런 정보도 갖고 있지 않는다. VPN의 관점에서, PE 라우터와 P 라우터는 기능적으로 동일하며, VPN 트래픽의 처리 및 관리는 CE 라우터가 모두 담당한다. 이 참조모델은 앞 절에서 언급된 Overlay 모델의 구현에 적합하며, PE 기반의 PPVPN 참조모델은 Peer 모델의 구현에 알맞다.

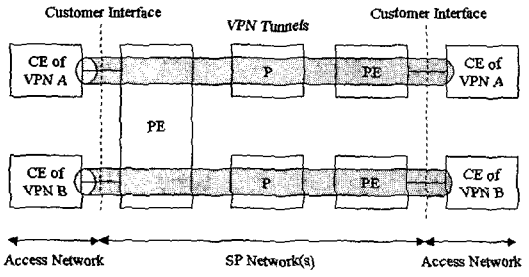


그림 3. CE 기반 3계층 PPVPN의 참조모델

Ⅲ. Peer 모델 PPVPN

1. BGP/MPLS VPN

BGP/MPLS VPN[2,8]은 Peer 모델을 적용하여 최근에 가장 주목받는 기술로써, 이에 의해 SP는 매우 큰 규모의 VPN 서비스를 제공할 수 있으며 VPN 사용자들은 IP 전문가나 전문적인 네트워크 지식을 필요로 하지 않게 된다. 동시에 SP는 VPN 구축을 위한 비용을 절감할 수 있게 된다. 이 기술은 ① 라우팅 정보의 제한적인 분배 ② 다중 Forwarding Table ③ 새로운 형태의 주소체계인 VPN-IP 주소 사용 ④ MPLS에 의한 패킷 전송 등의 네 가지 메커니즘을 바탕으로 하여 고안되었다. 이 방식의 VPN 구축을 위해서는 PE 라우터에 이 네 가지 기능이 구현되어 있어야 하며, CE 라우터와 P 라우터는 상대적으로 매우 제한적인 기능만을 필요로 한다.

1.1 라우팅 정보의 제한적인 분배

여러 개의 VPN을 SP의 네트워크에 구축하기 위해서는 사이트들 간의 연결성을 제한해야 할 필요가 있으며, 이를 위해 라우팅 정보를 제한적으로 분배한다. 이를 위해 어떤 경로를 전파할 때 BGP Community Attribute[14]를 이용한 경로 필터링(Route Filtering)을 적용하여 라우팅 정보가 해당 VPN의 사이트에만 분배되도록 제한한다. 라우팅 정보가 제한되므로 다른 VPN에 속한 사이트들 간의 정보의 흐름이 제한된다. 또한, 한 VPN 내에서 각각의 CE 라우터들은 직접 연결되어 있는 PE 라우터와 라우팅 관계를 유지할 뿐, VPN 내의 다른 CE 라우터와는 관계를 유지하지 않는다. 결과적으로 하나의 CE 라우터가 라우팅 관계를 유지해야 하는 라우터의 수가 항상 일정하므로, 매우 뛰어난 확장성을 가질 수 있다. 또한, 사이트를 추가하거나 제거하는 경우에 필요한 작업의 양이 항상 일정하며 VPN 내의 사이트의 수에 무관하다.

1.2 다중 포워딩 테이블(Forwarding Table)

PE 라우터는 여러 개의 CE 라우터, 즉 여러 개의 VPN에 연결되어 있을 수가 있기 때문에, 라우팅 정보를 제한적으로 분배하는 것만으로 사이트 사이의 연결성을 제어하기는 불충분하다. 여러 VPN에 연결된 PE 라우터가 하나의 포워딩 테이블을 가지고 있는 경우에는, 한 VPN의 패킷이 다른 VPN으로 전송되는 경우가 발생할 수도 있다. 이를 해결하기 위해, PE는 연결된 VPN 마다 별도의 포워딩 테이블을 유지 관리하도록 한다. PE의 다중 포워딩 테이블은 다음의 두 가지 방법에 의하여 그 경로 정보가 구성된다. 첫째는 PE 라우터가 직접 연결된 CE 라우터에게 경로에 관한 정보를 받는 경우이고 두 번째는 PE 라우터가 다른 PE 라우터로부터 경로 정보를 전달받는 경우이다.

1.3 VPN-IP 주소

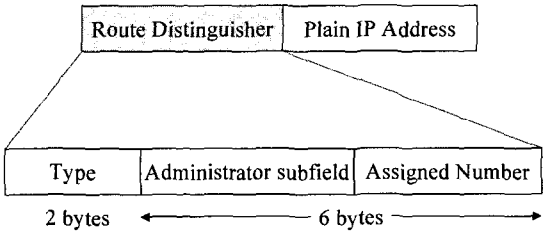


그림 4. VPN-IPv4 주소[8]

BGP는 IP 주소들이 유일하게 정의되는 것을 전제로 하고 있으나, VPN 서비스가 제공되는 환경에서는 같은 IP 주소들이 사용될 수가 있으므로 문제가 발생하게 된다. BGP/MPLS VPN에서는 VPN-IP이라는 새로운 주소체계를 도입하여 유일하지 않은 주소공간을 유일한 주소공간으로 변환하여 사용한다. VPN-IP 주소는 일반 IP주소 앞에 8 바이트의 경로 식별자(Route Distinguisher)를 부여함으로써 만들어지는데(그림 4), Type이 0인 경우에 Administrator Subfield는 AS의 번호를 나타내는 2 바이트가 되고, Type이 1인 경우에는 IP 주소를 나타내는 4 바이트가 된다. 나머지 4 혹은 2 바이트의 Assigned Number는 VPN 사업자가 임의대로 부여할 수 있는 번호이며, 따라서 모든 VPN 들은 서로 다른 경로 식별자를 가진다.

1.4 MPLS에 의한 패킷 전송

VPN 사업자의 네트워크 상에서 VPN-IP 주소체계를 사용하여 패킷을 전송하기 위해서는 기존의 IP 헤더의 전송정보만으로는 패킷의 전송이 불가능하며, 새로운 교환전송의 방법이 필요하게 된다. 이를 해결하기 위해 MPLS[4] 메커니즘이 적용되는데, MPLS가 사용이 가능한 이유는 MPLS가 IP 헤더의 전송정보와 라벨의 전송정보를 분리하기 때문이다. 즉, 라벨 교환경로와 VPN-IP 경로를 서로 연관시켜서 패킷들을 이 라벨을 사용하여 전송되도록 한다. MPLS의 관점에서 보면, PE 라우터는 Edge LSR(Label Switching Router)[4]에 해당하여, 일반 패킷에 라벨을 붙이고 제거하는 일을 담당한다. CE 라우터가 패킷을 전송해오면, PE 라우터는 그 패킷에 어떤 포워딩 테이블을 적용할 것인가를 판단하고, 이에 따라 다음 경로를 선정한 후에 라벨을 붙여서 전송한다. 확장성을 고려하여 두 단계의 라우팅 계층을 구성한다. 처음 라벨은 PE 라우터에서 다른 PE 라우터까지의 전송에 사용되고, 두 번째 라벨은 다른 PE 라우터에서 최종 목적지까지 전달하는데 사용된다. 첫째 라벨의 전달은 LDP(Label Distribution Protocol)나 RSVP(Resource Reservation Protocol)[15]와 같은 프로토콜들이 사용되고, 두 번째 라벨은 BGP의 다중 프로토콜 확장[16] 기능을 이용하여 라우팅 정보 및 Community Attribute[14]와 함께 전달된다.

2. PE-PE GRE/IP

BGP/MPLS VPN은 Peer 모델을 도입하여 우수한 확장성을 지니지만, SP 네트워크 양단의 PE 라우터 사이에 MPLS LSP(Label Switched Path)가 반드시 있어야 한다. 즉, PE 라우터 사이의 네트워크 일부분이 MPLS를 지원하지 않으면 BGP/MPLS는 적용할 수 없다. PE-PE GRE/IP[9]는 RFC 2547 VPN의 이러한 단점을 해결하기 위하여, Ingress PE에서 Egress PE로 전달될 때는 GRE[6] 혹은 IP Encapsulation[7]을 사용하도록 하고 있다.

PE 라우터가 CE에게 패킷을 받으면 그에 해당하는 VFI(Virtual Forwarding Instance)에 의해 VPN-IP 경로를 식별하고, 이를 다음 Hop의 PE 라우터로 전달하기 위하여 정해진 MPLS Label을 부착한다. 이를 SP 네트워크를 통하여 Egress LSR로 전달하기 위해, BGP/MPLS와는 달리 GRE[6] 혹은 IP에 의한 Encapsulation[7]을 수행하여 MPLS-in-IP 혹은 MPLS-in-GRE 패킷을 만든다. 이 패킷들은 PE 라우터 사이에 MPLS가

지원되지 않는 모든 IP 기반의 네트워크를 통하여 전송이 가능하다. 그림 5는 이러한 적용의 예를 나타낸 것으로, PE 라우터 사이의 경로 정보는 RFC 2547과 마찬가지로 Extended BGP에 의해 VPN-IP 정보를 전달하며, 이에 따른 Label은 VPN 패킷의 가장 처음(Bottom)에만 적용되고, 그 다음 단계에는 GRE 혹은 IP에 의한 Encapsulation이 이루어진다.

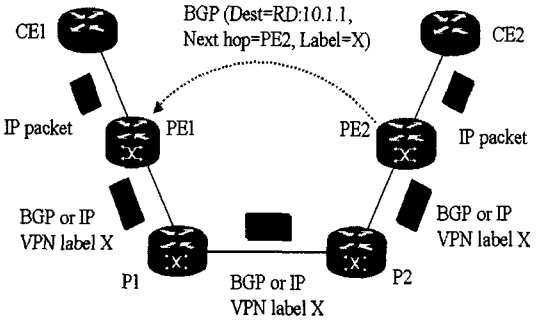


그림 5. PE 사이에 GRE 혹은 IP의 적용례

3. PE-PE IPSec

RFC 2547 BGP/MPLS VPN은 Peer 모델에 의한 우수한 확장성으로, SP들이 많은 수의 대규모 VPN들을 효율적이고 경제적으로 설계, 운용 및 관리 할 수 있다는 장점이 있지만 한편으로 다음과 같은 점들이 단점으로 논의되고 있다. 첫째, SP의 네트워크 전체가 MPLS를 지원하여야 한다는 점이다. SP 네트워크 양단의 PE 라우터 사이에 MPLS LSP(Label Switched Path)가 반드시 있어야 하며, PE 라우터 사이의 네트워크 일부분이 MPLS를 지원하지 않으면 BGP/MPLS는 적용할 수 없다. 둘째, PE 사이에 Label 혹은 IP에 의해 Encapsulation을 하는 경우에, VPN 패킷들에 대한 잘못된 라우팅에 의하여 다른 VPN으로 전달되는 문제가 생길 수 있다. 이런 경우에 Ingress PE에서 PE-PE 간에 인증을 지원하면, 잘못된 라우팅 혹은 고의적인 변조에 의한 문제를 막을 수 있다. 셋째, 하나의 VPN이 여러 SP의 네트워크를 이용하여 구축된 경우에 한 SP의 오류가 다른 SP로 전파되어 문제가 야기될 수 있다. 예를 들어, VPN1은 SP1과 SP2의 네트워크를 모두 사용하여 설정이 되어 있고, VPN2는 SP2의 네트워크만을 이용하고 있는 경우에, VPN2는 SP1 네트워크를 사용하지 않으므로, SP1에 오류가 있는 경우에 영향을 받지 않아야 한다. 즉, SP1이 네트워크 설정을 잘못하여 VPN1이 우연하게 VPN2에 접속하게 되는 일이 생기지 않아야 한다. 마지막으로, SP 네트워크를 통하여 전달되는 VPN 패킷들에 대한 보안이 유지되지 않는다는 점이다. SP 혹은 전송매체가 신뢰성이 부족한 경우에 암호화에 의해 적절한 보안성을 유지할 필요가 있다.

PE-PE IPSec[10]은 이러한 BGP/MPLS의 단점을 개선하기 위하여 제안된 방법으로, PE-PE 간에 추가적인 MPLS Label 대신에 IPSec[3]을 적용하여 보안성을 높임과 동시에, 패킷에 인증을 적용하여 잘못된 라우팅이나 다른 SP의 잘못된 설정에 의한 문제를 사전에 예방할 수 있다. Ingress PE가 CE로부터 VPN 패킷을 받았을 때 이를 BGP에 따른 다음 Hop, 즉 다른 PE 라우터까지 전송하기 위한 방법은 다음과 같다. VPN 패킷의 VPN-IP 경로를 식별하여 이에 따라 MPLS Label을 붙이는 것은 이전의 RFC 2547과 동일하다. 그러나 이 MPLS 패킷을 다시 IP 패킷으로 만들기 위하여 MPLS-in-IP Encapsulation을 하고, 이에 의해 만들어진 패킷에 Transport 모드의 IPSec을 적용하여 전송한다. VPN에서 다이내믹 라우팅을 하는 경우에 PE 라우터에서 Tunnel 모드의 IPSec을 적용하면 운용 및 구현상에 문제가 생길 수 있으므로[17], MPLS 패킷을 일단 IP Encapsulation한 후에 IPSec을 적용한다.

그림 6은 MPLS 패킷에 Tunnel 모드의 IPSec을 적용하는 경우와 IP Encapsulation을 한 후에

Transport 모드 IPSec을 적용하는 경우를 비교한 것이다. Tunnel 모드의 경우에는 원래 패킷(MPLS 패킷)의 헤더에 의해 적용할 SA(Security Association)를 결정하고, 그 후에 외부 IP 헤더를 결정하여 붙이게 된다. 이 네트워크에서 다이내믹 라우팅을 하는 경우에는 목적지 PE로의 경로가 자주 바뀔 수 있으며, 이에 따라 외부 IP 헤더의 목적지 주소도 변하게 된다. 이 때의 문제는, PE-PE 간에 여러 개의 경로가 있는 경우에 각 경로에 대한 IPSec 터널마다 다른 암호 키를 사용하도록 하고 있으므로, MPLS패킷에 IPSec을 적용하는 경우에 경로 선정을 하기 전에는 어떤 암호 키를 적용하여야 할지 모른다는 것이다. 따라서 PE-PE IPSec에서 제안하는 방법[10,17]은 MPLS 패킷에 대해 먼저 경로 선정에 의해 IP Encapsulation을 하고, 이 헤더정보에 의해 SA를 정하여 Transport 모드의 IPSec을 적용한다.

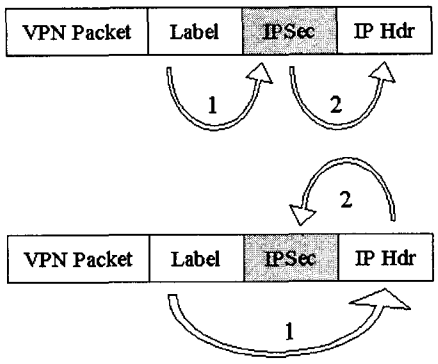


그림 6. Tunnel 모드를 적용하는 경우(위)와 IP|P Tu + Transport 모드를 적용하는 경우(아래)

Ⅳ. Overlay 모델 PPVPN

1. SMPLS (Secure MPLS)

SMPLS는 MPLS의 페이로드에 대한 암호화 및 인증을 위해 최근에 Nortel과 Alcatel에 의해 제안된 메커니즘이다[12]. 이 문서는 크게 두 가지의 내용을 담고 있는데, MPLS 패킷을 캡슐화하여 인증 및 암호화를 하기 위한 방안, 그리고 이를 위해 양단 간에 SA를 설정하기 위한 IKE(Internet key Exchange)[18]의 적용방안으로 구성되어 있다.

1.1 SMPLS를 위한 IKE의 적용

IKE는 보안 메시지의 전달에 사용할 수 있는 일반적인 프로토콜로써[18], IPSec, OSPF, SNMP 등 여러 가지 프로토콜들은 보안을 위한 SA의 설정이 필요한 경우에 IKE를 사용하여 필요한 메시지를 교환할 수 있다. 이때, IKE를 적용하려는 프로토콜에 대하여 DOI(Domain Of Interpretation)를 정의하여야 하는데, 이는 그 프로토콜에서 사용할 식별자(Identifier) 값들을 정의하여 IKE 메시지의 교환 시에 사용하기 위한 것이다. 예를 들어, IPSec은 IPSec DOI[19]에서 AH(Authentication Header), ESP(Encapsulating Security Payload), ISAKMP(Internet SA Key Management Protocol) 등의 프로토콜과 Tunnel, Transport 등의 모드, 그리고 MD5, SHA-1 등의 알고리즘을 식별하기 위한 값들을 정의하고 있다. SMPLS의 경우에도 SMPLS DOI가 제안되어 있는데[20], IPSec DOI와 매우 유사하다. 예를 들어 SMPLS에서 사용될 프로토콜 식별자는 PROTO_SMPLS_AH이 5, PROTO_SMPLS_ESP이 6 등으로 정의되어 있다.

<table>
<tr><td colspan="3">Receiver Node Address</td></tr>
<tr><td colspan="3">Sender Node Address</td></tr>
<tr><td colspan="3">Extended Tunnel ID</td></tr>
<tr><td colspan="2">Tunnel ID</td><td>Reserved</td></tr>
<tr><td>Message Type</td><td>Length</td><td>Reserved</td></tr>
<tr><td colspan="3">ISAKMP message(variable length...)</td></tr>
</table>

그림 7. SMPLS를 위한 새로운 RSVP 오브젝트: Secure_MPLS_Message[12]

한편, SMPLS에서 IKE 메시지를 전달하기 위하여 RSVP-TE가 제안되었는데, RSVP-TE는 MPLS에서의 터널 설정을 위해 기존의 RSVP에 라벨의 전달 및 경로의 지정을 할 수 있도록 확장한 프로토콜이다[15]. 그러나 IKE는 SA의 설정을 위해 여러 번의 메시지 교환이 수행되어야 하는데, 이는 RSVP-TE에서 지원되지 않으므로, SMPLS에서는 새로운 RSVP 메시지와 새로운 오브젝트를 제안하였다. RSVP Transport 메시지는 기존의 RSVP 메시지들이 Hop-by-Hop으로 처리되는 것과는 달리 End-to-End로 전달된다. 즉, Ingress 및 Egress LSR 만이 Transport 메시지를 처리할 수 있도록 하여 RSVP가 양단 간의 메시지 전달 서비스를 제공하도록 한다. 또한 IKE 메시지의 전달을 위해 Secure_MPLS_Message가 새로운 RSVP 오브젝트로 정의되었으며(그림 7), 이 오브젝트는 Transport 메시지를 이용하여 전송된다.

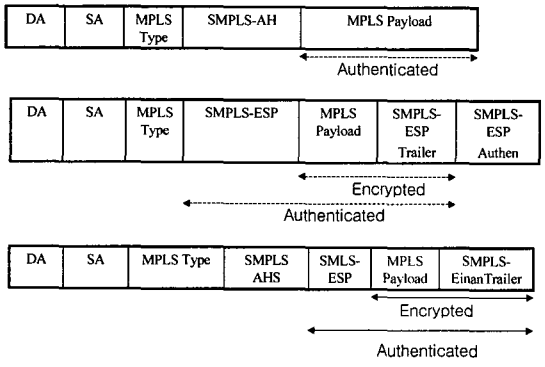


그림 8. SMPLS Encapsulation 포맷[12]

1.2 SMPLS 프로토콜

IPSec에서 패킷의 인증과 암호화를 위해 AH와 ESP의 두 가지 프로토콜을 표준화한 것과 마찬가지로, SMPLS에서는 SMPLS-AH와 SMPLS-ESP의 두 가지 프로토콜을 제안하고 있다. SMPLS-AH는 라벨과 페이로드에 대한 인증을 제공하며, SMPLS-ESP는 페이로드에 대한 암호화 및 인증을 제공한다. MPLS의 경우에는 페이로드가 LSR 사이에 전송되고 라벨스택(Label Stack)도 LSR 을 지날 때마다 변경되므로, SMPLS에서 SA의 설정은 Ingress LSR과 Egress LSR 사이에 이루어지도록 했다. 따라서 IPSec의 경우에는 보안 연결의 범위에 따라 터널 모드와 트랜스포트 모드의 두 가지 SA 설정이 가능하나, SMPLS의 경우에는 Transport 모드만 의미가 있다.

그림 8은 SMPLS에서의 Encapsulation 포맷을 나타낸 것이다. (a)의 SMPLS-AH는 MPLS 페이로드에 대한 인증만을 수행한다. IPSec의 경우에는 AH 프로토콜이 IP 패킷 헤더의 고정 필드, AH 헤더 및 페이로드에 대한 인증을 하지만, MPLS 라벨의 경우에는 IP 패킷 헤더와는 달리 고정값을 갖는 필드가 없으므로, 인증의 범위가 AH 헤더와 페이로드로 제한된다. SMPLS-ESP의 경우에는 IPSec과 마찬가지로 페이로드와 Trailer에 대한 암호화 및 ESP 헤더를 포함하는 인증을 한다. (c)와 같이 AH와 ESP를 동시에 적용하는 것도 가능하다.

2. Virtual Router

Virtual Router[11]은 네트워크 기반, 즉 PE 기반의 VPN 구축기술로써, 하나의 PE 라우터가 여러 개의 VPN에 대하여 별도의 라우팅 및 관리를 하도록 하는 방법이다. VR(Virtual Router)란 소프트웨어 혹은 하드웨어 단계에서 실제의 라우터를 에뮬레이션 하는 것이다. 즉, 각각의 VR은 별도의 라우팅 테이블과 포워딩 테이블을 관리하고 있기 때문에 서로 독립적으로 운용 및 관리가 된다. 따라서 다른 VR들로 연결된 다른 VPN은 서로 중복된 IP 어드레스 공간을 사용하여도 문제가 없다. 각각의 VR은 하나의 VPN에 소속이 되어 그 VPN내에서 OSPF, RIP 등의 라우팅 프로토콜을 사용하여 라우팅 테이블을 만들며, 이를 이용하여 같은 VPN에 속한 VR로부터 전달되는 패킷을 포워딩한다.

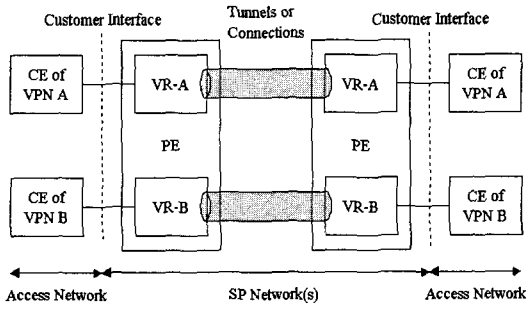


그림 9. PE-PE 간에 Virtual Router의 연결

그림 9에서와 같이 같은 VPN에 속한 VR들을 서로 연결하기 위해서는 다음과 같은 여러 가지 방법이 사용될 수 있다. 첫째, VR들을 2계층에서 연결하는 방법이다. 예를 들어 ATM이나 Frame Relay의 가상회선을 이용하여 두 VR을 연결할 수 있다. 이 방법을 사용하면, VPN 마다 직접적으로 QoS (Quality of Service)를 보장할 수 있다는 장점이 있다. 두 번째로는 두 VR을 IP 혹은 MPLS에 의한 터널링(Tunneling)으로 연결할 수도 있다. 즉, 두 VR 사이의 VPN 패킷을 IP Encapsulation 혹은 MPLS Labeling에 의해 전송하는 방법인데, 첫째 방법에 비해 하부 네트워크에 의존적이지 않게 된다. 세 번째 방법으로 제시된 것은 사용자의 VPN 사이트를 연결하는 VR들 외에 별도의 Backbone VR을 PE 안에 설치하여 두 PE 사이에 여러 VR을 연결할 경우에 Backbone으로 사용하는 방법이다. Backbone VR을 이용하는 경우에 한 VPN의 VR들은 직접 연결된 것과 같은 효과를 주며, VR과 Backbone VR 사이의 관계는 BGP/MPLS의 CE와 PE 사이가 Peer 관계인 것과는 달리 Overlay 관계이다[11].

3. IPSec을 이용한 CE-based PPVPN

[13]은 IPSec을 이용하여 CE 기반의 PPVPN을 구축하는 방법을 기술하고 있다. II장의 참조모델에서 보듯이, CE 기반의 VPN은 사용자의 CE 라우터 사이를 일대일의 터널로 연결하는 Overlay 모델이 적용이 되는데, 이 터널링에 IPSec을 사용하고 PE라우터들은 아무런 VPN 관련 기능을 갖지 않는 방법이다. CE 라우터는 사용자 네트워크에 두거나 경우에 따라 SP 네트워크에 PE 라우터와 같이 설치하여 운용할 수 있다. 어느 경우든지 SP는 CE라우터의 설정과 관리를 위하여 모든 CE 라우터에 대하여 보안이 유지되는 관리용 채널을 가지고있을 필요가 있다. SP는 이 채널을 이용하여 해당 CE가 속한 VPN에 관련된 정보를 그 VPN의 데이터베이스와 CE 사이에 주고받게 된다.

SP가 CE 라우터에 설정하여야 하는 최소한의 정보는 다음과 같다. 먼저, SP의 VPN 데이터베이스를 억세스하고 정보를 교환하기 위한 관리용 채널에 대한 정보가 있어야 하며, 동일한 VPN에 속한 이웃의 CE 라우터의 주소를 알고 있어야 한다. VPN의 토폴로지가 Hub-and-Spoke인 경우에는 하나의 CE에 대한 정보만 설정하며, Mesh 형태인 경우에는 VPN에 속한 전체 CE의 모든 정보가 있어야 한다. 또한, 다른 CE와 IPSec SA(Security Association)을 유지, 관리하기 위한 정보를 설정하여야 한다. 마지막으로, 해당 CE 라우터가 속한 VPN의 유일한 식별번호(ID)를 설정한다.

CE 라우터들 사이에 IPSec 터널을 설정하여 사용하는 경우에, VPN에서 정적인 라우팅을 하는 경우에는 IPSec SA의 설정을 Traffic-driven, 즉 트래픽이 있는 경우에 동적으로 설정하여 운용할 수도 있다. 그러나, CE들 사이에 라우팅 정보를 동적으로 주고받는 경우에는 트래픽에 무관하게 IPSec 터널을 고정적으로 설정하여 사용할 필요가 있다. 또한, VPN 내의 CE 라우터들 사이에 라우팅 정보를 교환하는 방법은, CE들 사이의 IPSec 터널을 통하여 정보를 주고받는 방법과, SP와 연결된 채널을 이용하여 SP의 관리 하에 정보를 교환하도록 할 수도 있다.

V. IP기반의 PPVPN 프로토콜 비교

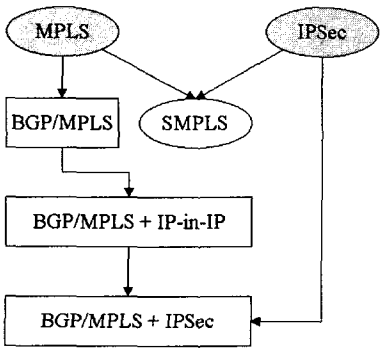


그림 10. L3 PPVPN 기술의 관계

그림 10은 본 고에서 논의 된 여러 가지 PPVPN 기술들의 관계를 나타낸 것으로, 원으로 표시된 프로토콜은 Overlay 모델을, 사각형은 Peer 모델을 나타낸다. 최근에 IETF에서 논의되는 여러 기술들은 기본적으로 MPLS, IPSec 혹은 두 기술의 결합에 의한 새로운 방식을 적용하여 기존의 단점을 보완한 것이다. 기존에 MPLS 및 IPSec은 각각 2계층 및 3계층에서 Overlay 모델의 VPN을 구현하기 위한 기술로 널리 적용되어 왔다. VPN 기술의 비교와 평가를 위해서 일반적으로 적용되는 네 가지 항목인[21] 확장성(Scalability), 보안성(Security), 전송품질보장(Quality of Service), 및 관리(Management)에 따라 MPLS[4] 및 IPSec[3]의 두 기술을 다음과 같이 비교할 수 있다.

먼저, IPSec은 기본적으로 유니캐스트 SA를 가정하고, MPLS의 경우에도 양단 간에 LSP(Label Switched Path)를 설정하여야 하므로 확장성의 면에서 문제가 있다. 다음으로 보안성의 측면에서, IPSec에 의한 VPN은 충분한 길이의 키와 안전한 알고리즘을 적용하는 경우에 비밀성(Confidentiality), 무결성(Integrity), 및 인증(Authentication)의 측면에서 완전한 보안성을 제공한다. 그러나, MPLS VPN은 ATM이나 Frame Relay를 사용한 서비스와 비슷한 정도의 보안을 제공할 수 있으며, 네트워크 사업자의 신뢰성 및 내부 기간망의 보안이 요구된다. 세 번째로, IPSec 자체에는 QoS에 대한 고려가 없으며, 이를 지원하기 위해서는 라우터 같은 IPSec 응용제품에서 패킷에 대한 차별적인 처리를 수행하여야 한다. MPLS는 기반 네트워크의 QoS 지원기능을 이용할 수 있으며, 전송경로가 미리 정해져 있으므로 Traffic Engineering을 수행하는 것도 가능하다. 마지막으로 관리 측면을 고려할 때, IPSec은 기존의 모든 IP 네트워크에 즉시 적용할 수 있으므로 서비스 제공자가 시장에 진입하는 것이 매우 빠를 수 있지만, MPLS의 경우에는 서비스를 제공하려는 경우에 네트워크의 인프라를 점진적으로 혹은 완전히 교체하여야 하므로 초기 투자 및 시간이 많이 든다.

이러한 장단점을 가지는 MPLS와 IPSec을 결합하거나 다른 기술들을 추가하여, 본 고에서 논의된 바와 같은 다양한 방식의 기술들이 제안되었다. BGP/MPLS[2,8]는 BGP의 특수한 확장 라우팅 기능을 이용하여 MPLS VPN의 단점인 확장성 문제를 해결한 것이다. 이 경우, 사이트와 사이트간에 설정을 할 필요가 없으므로 확장성이 우수하며, 일반적으로 BGP/MPLS 기반의 VPN은 하나의 네트워크에서 수만 개 이상의 VPN을 지원할 수 있다. 또한 SMPLS[12]는 MPLS VPN의 MPLS 패킷을 IPSec 패킷과 유사하게 인증 및 암호화를 하도록 해서 MPLS의 단점인 보안성을 강화하도록 했다. 그러나 MPLS LSP 마다 IPSec SA를 적용하여야 하므로 MPLS의 확장성 문제는 여전히 가지고있게 된다. BGP/MPLS는 새로운 IP 주소체계의 정의를 필요로 하며, SMPLS의 경우에는 새로운 RSVP 오브젝트 및 메시지, 또한 새로운 보안 프로토콜을 정의하고 있다는 단점이 있다.

다음으로 PE-PE GRE/IP[9]는 BGP/MPLS가 MPLS 기반구조를 필요로 한다는 단점을 극복하기 위해서 SP 네트워크의 에지 라우터 사이에서는

GRE 혹은 IP Encapsulation을 이용하여 터널링을 함으로써 모든 다른 IP 기반의 네트워크를 활용할 수 있도록 하였다. 그러나, 여전히 SP의 신뢰성 및 네트워크의 보안성을 필요로 하므로, 이를 위하여 PE라우터 사이의 터널링에 IPSec을 적용한 것이 PE-PE IPSec[12]이다. 따라서 PE-PE IPSec은 현재까지 제안된 IP 기반의 PPVPN 기술 중에서 확장성 및 보안성의 관점에서 가장 진보된 기술이라고 할 수 있다.

Ⅵ. 결론

본 고에서는 IP 기반의 PPVPN 기술로 주목을 받고있는 BGP/MPLS를 비롯하여, 최근에 새로이 제안된 여러 가지 기술들에 대하여 특징을 기술하고 비교하였다. IPSec은 표준화가 완료되어 많은 사업자들이 서비스를 시작하거나 준비중에 있는데, 이 기술은 기존의 다른 VPN 기술에 비하여 보안, 인증 및 무결성의 측면에서 가장 뛰어난 기능을 제공하지만, 각 사이트를 연결하여 메쉬 형태의 가상 백본을 구성하여야 하므로 확장성의 결여라는 단점을 지니고 있다. MPLS망은 ATM이나 Frame Relay망과 마찬가지로 두 사이트 사이에 2계층의 연결을 함으로써 가상망의 기능을 제공할 수 있는데, 이 역시 확장성에 문제가 있으므로 BGP/MPLS가 제안되어 표준화된 바 있으나, 데이터 자체에 대한 암호화 및 인증은 제공하지 못하며 MPLS 네트워크가 설치되지 않은 곳에서는 구현이 곤란하다. 이에 따라 본 고에서 논의된 SMPLS, PE-PE GRE/IP, PE-PE IPSec 등의 기술들은 이전의 IPSec을 이용하여 보안성을 강화하거나, BGP를 이용한 확장성을 강화하거나, 혹은 GRE 및 IP Encapsulation에 의해 Non-MPLS 네트워크를 통한 전송이 가능하게 하도록 하는 등의 기술적 진보를 이룬 제안들이다.

이와 같이 최근의 여러 가지 VPN 프로토콜들은 확장성, 보안성 및 범용성을 강화하는 방향으로 계속하여 연구개발 되고 있다. VPN 사용자의 다양한 욕구를 만족시켜 줄 필요성과 네트워크 운용의 효율화를 통한 사업자의 수익증대 측면에서 기존의 IP PPVPN 기술들은 향후에 지속적인 개선과 발전이 예상되며, 이는 본 고에서 논의된 바와 같이 확장성, 보안성 등의 특성을 강화하는 방향으로 진행될 것이다. 따라서, SP는 새로운 VPN 서비스를 제공하거나 네트워크를 구축 혹은 확장할 때 이러한 기술의 발전 방향 및 연구 동향을 참조하여, VPN 서비스의 운용방향을 설정하고 향후 네트워크에 새로운 기술을 접목하거나 도입하는 것을 효율적으로 할 수 있다.

참 고 문 헌

[1] PPVPN Working Group, http://www.ietf.org/html.charters/ppvpn-charter.html

[2] E. Rosen and Y. Rekhter, "BGP/MPLS VPN," RFC 2547, Mar. 1999

[3] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998

[4] B. Davie and Y. Rekhter, *MPLS: Technology and Applications*, Morgan-Kaufmann, 2000

[5] R. Callon *et al.*, "A Framework for Layer 3 Provider Provisioned Virtual Private Networks," Work in progress, Internet Draft, Apr. 2002.

[6] S. Hanks *et al.*, "Generic Routing Encapsulation (GRE)," RFC 1701, Oct. 1994

[7] C. Perkins, "IP Encapsulation within IP," RFC 2003, Oct. 1996

[8] E. Rosen *et al.*, "BGP/MPLS VPN," Work in progress, Internet Draft, Jan.

2002

[9] Y. Rekhter and E. Rosen, "Use of PE-PE GRE or IP in RFC 2547 VPNs," Work in progress, Internet Draft, Feb. 2002

[10] E. Rosen *et al.*, "Use of PE-PE IPSec in RFC 2547 VPNs," Work in progress, Internet Draft, Feb. 2002

[11] P. Knight *et al.*, "Network based IP VPN architecture using Virtual Routers," Work in progress, Internet Draft, July 2002

[12] T. Senevirathne and O. Paridaens, "Secure MPLS - Encryption and authentication of MPLS payloads," Work in progress, Internet Draft, Feb. 2001.

[13] J. De Clercq *et al.*, "An architecture for Provider Provisioned CE-based virtual private networks using IPSec," Work in progress, Internet Draft, June 2002

[14] J. Stewart, *BGP4: Inter-domain Routing in the Internet*, Addison-Wiley, 1999

[15] D. Awduche *et al.*, "RSVP-TE: Extensions to RSVP for LSP tunnels," Work in progress, Internet Draft, Aug. 2001.

[16] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol Extensions for BGP4", RFC 2283, Feb. 1998

[17] J. Touch and L. Eggert, "Use of IPSec Transport mode for Virtual Networks," Work in progress, Internet Draft, Mar. 2000

[18] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998.

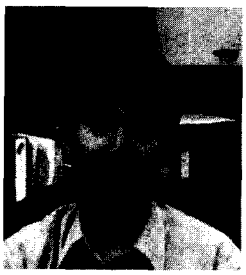
[19] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407, Nov. 1998.

[20] T. Senevirathne and O. Paridaens, "Secure MPLS Domain of Interpretation for ISAKMP," Work in progress, Internet Draft, Feb. 2001

[21] "A comparison between IPSec and MPLS virtual private networks," White paper, Cisco Systems, 2000.

이 승 형

1988년 연세대학교 전자공학과 졸업(공학사), 1990년 연세대학교 전자공학과 졸업(공학석사), 1999년 University of Texas at Austin 졸업(Ph. D.), 1990~1995년 국방과학연구소 연구원, 1999~2000년 삼성종합기술원 디지털통신랩 전문연구원, 2000년~현재 광운대학교 전자공학부 조교수, 관심분야 : 인터넷 보안, 인터넷 QoS 및 Flow Control, 무선 네트워크



윤 재 우

1983년 전북대학교 전자공학과 졸업(공학사), 1985년 전북대학교 전자공학과 졸업(공학석사), 1985~1988년 : LG 정보통신연구소 연구원, 1989년~현재 : 한국전자통신연구원 책임연구원, 관심분야 : ATM, 인터넷 보안, Key Management