情 報 保 護 學 會 誌
第 11 券 第 6 號, 2001. 12

IP 기반 VPN 프로토콜의 연구동향: 확장성과 보안성

윤 재 우*, 이 승 형**

요 약

본 고에서는 현재 가장 주목받는 IP 기반의 VPN 기술인 IPSec과 BGP/MPLS, 그리고 최근에 제안된 프로토콜인 SMPLS와 BGP/IPSec에 대하여 각각의 특징 및 장단점을 비교하고 IP VPN 프로토콜의 연구동향 및 발전방향에 대하여 분석한다. 보안성(Security)에 강점을 갖는 IPSec과 확장성(Scalability)의 장점을 지닌 BGP/MPLS는 VPN의 구축 시에 반대로 각각 확장성과 보안성의 단점을 갖는다. 이에 대하여, BGP/IPSec은 IPSec에 확장성을 추가하여 VPN 구성을 효율적으로 하도록 했으며, SMPLS는 MPLS 페이로드에 대하여 암호화 및 인증이 가능하도록 하였다. VPN 사업자들이 서비스를 준비중이거나 시작한 IPSec과 BGP/MPLS 기술은 각각의 장단점 때문에 다른 기술과 융합하거나 계속하여 발전될 것이 예상되며, 이는 VPN 기술의 확장성과 보안성을 강화하는 방향으로 진행될 것이다.

Ⅰ. 서 론

IP 기반의 VPN(Virtual Private Network)은 인터넷의 성장에 따라 사용자에게 경제적으로 새로운 서비스를 제공할 수 있는 기술로 각광을 받고 있다. 네트워크 사업자는 새로운 서비스 모델에 의해 수익원을 창출할 수 있으며, 초고속국가망의 경우에는 각 기관가입자들을 하나의 네트워크에 수용하여 기관별 네트워크를 구축하는 것이 가능해졌다. VPN은 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 관련 워킹그룹들은 IP VPN에 적용할 수 있는 두 가지의 기술인 IPSec[1]과 MPLS[2,3]를 표준화하였다.

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 사업자들은 이 두 가지, 혹은 그 중 한 기술을 이용하여 VPN 서비스를 제공하고 있거나 계획중에 있으며, 각 기술은 보안성 및 확장성 등에서 장단점이 있으므로 두 기술을 동시에 적용하는 경우는 각각의 특성을 이용하여 서비스를 구현하여야 한다.

한편, IPSec VPN이 가지는 확장성의 문제와 MPLS VPN이 가지는 보안성의 문제를 해결하기 위하여 최근에 IETF에서는 여러 가지의 새로운 대안들이 제시되어 논의되고 있는데, 이들 중 대표적인 것이 SMPLS(Secure MPLS)[4]와 BGP/IPSec[5]이다. SMPLS는 MPLS VPN을 보완하여 인증, 암호화, 및 무결성에 대한 지원이 가능하도록 설계된 프로토콜이며, BGP/IPSec은 BGP/MPLS를 응용하여 IPSec VPN 구축 시에 확장성을 지원하도록 고안된 메커니즘이다. 이 기술들은 아직 표준화가 이루어지지 않은 단계이나, VPN 기술의 개발동향 및 향후 기술의 발전방향을 가늠해 볼 수 있는 새로운 제안들이다. 본 고에서는 BGP/MPLS, SMPLS, 및 BGP/IPSec에 대한 개요 및 기술적 특징들을 기술하고 각각의 장단점 및 관계에 대해 기술한다. 이후의 내용은 다음과 같다. 2장에서는 IP VPN의 두 가지 모델인 Overlay와 Peer 모델에 대해 설명하고, Peer 모델의 대표적인 예인 BGP/MPLS에 대해 기술한다. 3장에서는 최근에 제안된 새로운 기술인 SMPLS와 BGP/IPSec의 기술적 특징을 설명하고, 4장에서는 각각의 기술의

* 한국전자통신연구소 부설 국가보안기술연구소 (jyoon@dingo.etri.re.kr)
** 광운대학교 전자공학부 네트워크시스템연구실 (rhee@ieee.org)

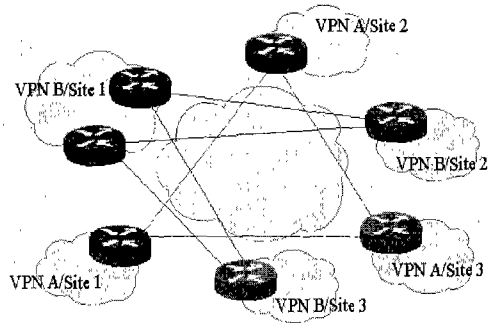
특징에 대한 비교 분석 및 관계에 대해 기술한다. 마지막으로 5장에서는 향후 VPN 기술의 발전전망에 대해 언급하고 결론을 맺는다.

II. IP VPN 구축 기술

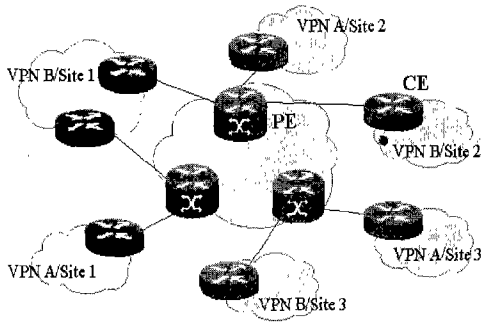
1. Overlay 모델 VPN

현재 가장 일반적인 VPN 구축기술은 Overlay 모델을 사용하는 것이다. 이는 VPN 사용자의 각 사이트의 라우터와 다른 사이트의 라우터 사이에 일대일의 가상링크를 설정하는 방식으로써, Frame Relay, ATM, IPSec 등의 여러 터널링 기술들이 채택된다. 이들 프로토콜 중에서, 2계층에 적용되는 PPTP, L2F 및 L2TP는 양단 간의 원격 접근을 위한 터널링 기술로써 현재 많이 쓰이는 Access VPN 기술이나[6], 확장성 및 효율성이 낮다는 문제점이 있다. 한편 3계층에서 적용되는 IPSec의 경우에는 아직은 널리 적용되고 있지 않으나, 뛰어난 보안성으로 인하여 향후 IP VPN의 구축을 위한 터널링 방식으로 가장 널리 쓰일 전망이다. 한편, Frame Relay 및 ATM 등의 2계층에서의 가상 채널을 이용하여 VPN 사용자에게 가상 링크를 제공하는 방법은 별도의 보안 메커니즘을 적용하지 않는다.

Overlay 모델을 적용한 VPN이 오늘날 가장 일반적인 것이긴 하지만, 몇 가지 단점을 가지고 있어서 큰 규모의 VPN을 효율적으로 구축하는데 걸림돌이 되고 있다[2]. 첫째, VPN 사용자가 자신들의 가상 백본(Virtual Backbone)을 설계하고 운용하는 것이 힘들다는 점이다. 가상 백본을 설계 및 운용하기 위해서는 IP 라우팅 및 QoS(Quality of Service)에 관한 전문가들을 필요로 하며, 이에 따라 VPN 사용자들은 자신들의 VPN을 구축하고 유



〔그림 1〕 Overlay 모델 VPN의 예[2]



〔그림 2〕 Peer 모델 VPN의 예[2]

지보수 하기 위하여 많은 비용을 필요로 한다. 이 문제를 해결하기 위하여 VPN 사업자들은 "Managed Router" 서비스를 제공하고 있다. 즉, 사업자가 각 VPN 사용자들을 대신하여 가상백본을 설계하고 운용하는 것인데, 이 경우에 VPN 사업자는 많은 수의 VPN을 제공하기 어려우며 경비의 절감을 기대하기도 어렵다.

두 번째 문제는 많은 수의 사이트를 갖는 VPN 사용자의 경우에 각 사이트 간에 완전한 메쉬(Mesh) 형태의 연결을 해야 한다는 점이다. 예를 들어, N 사이트를 갖는 VPN의 경우에 각각의 라우터들은 (N-1) 개의 일대일 연결을 다른 모든 라우터와 유지해야 한다. 따라서, 기존의 VPN에 새로운 사이트를 추가하거나 제거할 때, 각 사이트의 정보를 일일이 모두 수정을 해야 한다. Overlay 모델을 약간 수정한 것으로는 VPN 사업자가 가상 라우터(Virtual Router)를 사용하는 방법이 있다[8]. 이는 하나의 라우터가 마치 여러 대의 라우터인 것처럼 CPU와 메모리 등을 분할하여 동작하도록 한 것이나, 가상 라우터를 사용한다고 해서 Overlay 모델의 여러 단점이 없어지지는 않는다. 이러한 Overlay 모델의 여러 단점을 극복하기 위해 최근에 사용되기 시작한 기술이 그림 2와 같은 Peer 모델이다. VPN의 사용자 라우터는 사업자의 라우터와 일대일로 연결이 되며, 사업자의 라우터는 여러 VPN을 접속할 수 있고 메쉬 형태의 연결은 사업자 라우터 사이에만 필요하다.

2.2 BGP/MPLS - Peer 모델 VPN

BGP/MPLS[3, 7]는 Peer 모델의 VPN 구축기술로써, 이에 의해 VPN 사업자는 매우 큰 규모의 VPN 서비스를 제공할 수 있으며 VPN 사용자들은 IP 전문가나 전문적인 네트워크 지식을 필요로 하지

않게 된다. 동시에 사업자는 VPN 구축을 위한 비용을 절감할 수 있게 된다. 이 방식은 다음의 네 가지 주요 기술을 바탕으로 하여 고안되었다.

- 라우팅 정보의 제한적인 분배
- 다중 Forwarding Table
- 새로운 형태의 주소체계인 VPN-IP 주소 사용
- MPLS에 의한 패킷 전송

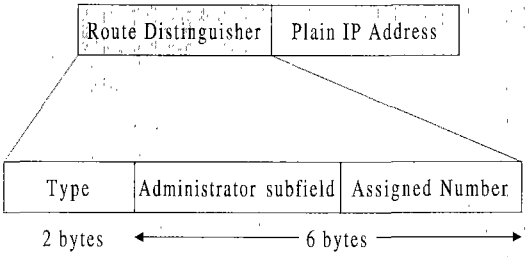
BGP/MPLS VPN에서 네트워크 장비들은 CE (Customer Edge) 라우터, PE(Provider Edge) 라우터, 그리고 P(Provider) 라우터의 세 가지로 구성된다. CE 라우터들은 사용자의 사이트에 설치되어 VPN 사업자의 네트워크에 접속이 되고, PE 라우터들은 VPN 사업자의 네트워크에 설치되어 CE 라우터와 연결이 된다. 마지막으로 P 라우터는 사업자의 네트워크에 있는 라우터들로, CE 라우터와 접속이 되지 않는 라우터를 말한다. 이 방식의 VPN 구축을 위해서는 PE 라우터에 위의 네 가지 기능이 구현되어 있어야 하며, CE 라우터와 P 라우터는 상대적으로 매우 제한적인 기능만을 필요로 한다.

(1) 라우팅 정보의 제한적인 분배

여러 개의 VPN을 사업자의 네트워크에 구축하기 위해서는 사이트들 간의 연결성을 제한해야 할 필요가 있으며, 이를 위해 라우팅 정보를 제한적으로 분배한다. 즉, 라우팅 정보의 분배를 제한함으로써 사이트들 간의 정보의 흐름을 제한하는 것이다. 이를 위해 BGP Community Attribute[9]를 이용한 경로 필터링(Route Filtering)을 적용하는데, 어떤 경로를 전파할 때 BGP Community를 사용하여 이 경로의 분배를 제한하는 방법이며, 이에 의해 얻을 수 있는 특징들은 다음과 같다. 첫째, 어떤 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. 둘째, 하나의 사이트를 추가하거나 제거하는 경우에 필요한 작업의 양이 항상 일정하며 VPN 내의 사이트의 수에 무관하다. 마지막으로, PE 라우터는 그 라우터가 연결되어 있는 VPN에 관련된 라우팅 정보들만 수집하여 유지하면 된다.

(2) 다중 Forwarding Table

PE 라우터는 여러 개의 VPN이 구성되어 있는 사이트와 연결되어 있을 수가 있기 때문에, 라우팅 정보를 제한적으로 분배하는 것만으로 사이트 간의 연결성을 제어하기는 불충분하다. PE 라우터가 하나의 Forwarding Table을 가지고 있는 경우에는 여러 VPN 들이 이 테이블을 모두 사용하므로, 한 VPN의 패킷이 다른 VPN으로 전송되는 경우가 발생하게 된다. 이를 위한 해결방법으로, 각 PE 라우터가 여러 개의 Forwarding Table을 유지 관리하도록 한다. PE 라우터의 다중 Forwarding Table은 다음의 두 가지 경우에 의하여 그 경로 정보가 구성된다. 첫째는 PE 라우터가 직접 연결된 CE 라우터에게 경로에 관한 정보를 받는 경우이다. 두 번째는 PE 라우터가 다른 PE 라우터로부터 경로 정보를 전달받는 경우이다.



〔그림 3〕 VPN-IPv4 주소

(3) VPN-IP 주소

앞의 두 가지 메커니즘은 BGP와 IP 주소체계를 사용하고 있다. 한편, 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 IP 주소 앞에 8 바이트의 경로 식별자(Route Distinguisher)를 부여함으로써 만들어지는데(그림 3)[7], 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 번호인데, 일반적으로 사업자는 하나의 VPN에 하나의 Assigned Number를 부여하므로, 모든 VPN 들은 서로 다른 경로 식별자를 가지게 된다.

(4) MPLS에 의한 패킷 전송

지금까지 VPN-IP 주소를 사용하여 경로 정보의 배분을 제어하는 내용을 설명하였다. 그러나, VPN 사업자의 네트워크 상에서 이러한 주소체계를 사용하여 패킷을 전송하기 위해서는 기존의 IP 헤더의 전송정보만으로는 패킷의 전송이 불가능하며, 따라서 새로운 교환전송의 방법이 필요하게 된다. 이를 해결하기 위해 MPLS[2] 메커니즘이 적용된다. MPLS가 사용이 가능한 이유는 MPLS가 IP 헤더의 전송정보와 라벨의 전송정보를 분리하기 때문이다. 따라서, 라벨 교환경로와 VPN-IP 경로를 서로 연관시켜서 패킷들을 이 라벨을 사용하여 전송되도록 한다. MPLS의 관점에서 보면, PE 라우터는 Edge LSR(Label Switching Router)[2]에 해당하며, 따라서 PE 라우터는 일반 패킷에 라벨을 붙이고 제거하는 일을 담당한다. CE 라우터가 패킷을 전송해오면, PE 라우터는 그 패킷에 어떤 Forwarding Table을 적용할 것인가를 판단하고, 이에 따라 라우팅 절차에 의해 다음 경로를 선정한 후에 라벨을 붙여서 전송한다. 확장성을 고려하여, 두 단계의 라우팅 정보 계층을 구성한다. 즉, 처음 레벨의 라벨은 PE 라우터에서 다른 PE 라우터까지의 전송에 사용되고, 두 번째 라벨은 다른 PE 라우터에서 최종 목적지까지 전달하는데 사용이 된다. 첫째 라벨의 전달은 LDP (Label Distribution Protocol)나 RSVP(Resource Reservation Protocol)[14]와 같은 프로토콜들이 사용되고, 두 번째 라벨은 BGP의 다중 프로토콜 확장[10] 기능을 이용하여 라우팅 정보 및 Community Attribute와 함께 전달된다.

Ⅲ. 최근에 제안된 프로토콜들

1. SMPLS (Secure MPLS)

SMPLS는 MPLS의 페이로드에 대한 암호화 및 인증을 위해 최근에 Nortel과 Alcatel에 의해 제안된 메커니즘이다[4]. 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)[11]의 적용방안으로 구성되어 있다.

1.1 SMPLS를 위한 IKE의 적용

IKE는 보안 메시지의 전달에 사용할 수 있는 일반적인 프로토콜로써[11], 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.

<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 4〕 SMPLS를 위한 새로운 RSVP 오브젝트: Secure_MPLS_Message[4]

예를 들어, IPSec은 IPSec DOI[12]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[13], IPSec DOI와 매우 유사하다. 예를 들어 SMPLS에서 사용될 프로토콜 식별자는 다음과 같이 정의되어 있다.

PROTO_SMPLS_AH	5
PROTO_SMPLS_ESP	6
PROTO_SMPLS_COMP	7

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[14]. 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 5), 이 오브젝트는 Transport 메시지를 이용하여 전송된다.

Next Payload	Reserved	Payload Length
ID Type	Reserved=0	Tunnel ID
Extended Tunnel ID		

〔그림 5〕 SMPLS에서 ISAKMP메시지의 ID페이로드[4]

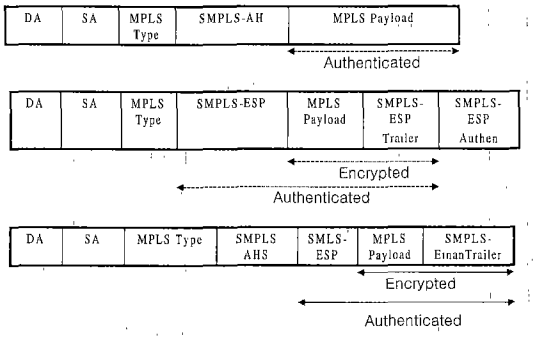
또한 상대방의 식별을 위해 IKE의 ISAKMP 메시지에서 사용하는 ID 페이로드 역시 MPLS에의 적용을 위하여 그림 5와 같이 수정되었다. ID 페이로드에서 Tunnel ID는 이 LSP의 고유번호이며, Extended Tunnel ID는 Ingress LSR의 IP 주소를 의미한다. ID 타입은 SMPLS DOI[8]에서 다음 값들이 정의된다.

ID_SMPLS_IPV4	12
ID_SMPLS_IPV6	13

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 LSR을 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 6은 SMPLS에서의 Encapsulation 포맷을 나타낸 것이다. (a)의 SMPLS-AH는 MPLS 페이로드에 대한 인증만을 수행한다. IPSec의 경우



〔그림 6〕 SMPLS Encapsulation 포맷[4]

에는 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. 그림 7은 MPLS의 AH 헤더 포맷을 나타낸다. SPI(Security Parameter Index)는 임의의 32 bit 값이며, Sequence 번호는 MPLS가 10G의 고속으로 구현되고 있는 점을 고려하여 IPSec에서 보다 많은 64 bit를 사용하도록 했다. SMPLS 패킷이 Egress LSR에서 Inbound processing이 되는 과정은 다음과 같다. 먼저 라벨에 의하여 자신이 Egress LSR이며 이 LSP가 SMPLS 데이터를 전송하고 있음을 확인하면 SMPLS 모듈을 가동한다. 라벨을 {Extended Tunnel ID :: Tunnel ID}에 매핑하고 이 ID와 SPI 값 및 헤더타입(AH 혹은 ESP)을 사용하여 해당하는 SA를 결정한다. 해당하는 SA가 없는 경우에는 폐기되며, 그렇지 않은 경우에는 Sequence 번호를 확인하고 ICV(Integrity Check Value)에 의해 무결성 검사를 수행한 후에 페이로드에 대한 복호화를 수행한다.

Type=SMPLS-AH	Length	Next Type
Security Parameter Index(SPI)		
Sequence Number(64bits)		
Authentication Data(variable...)		

〔그림 7〕 SMPLS-AH 헤더[4]

2 BGP/IPSec

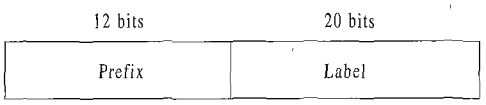
2.1 확장성 있는 IPSec VPN

BGP/IPSec VPN은 최근에 IETF에 제안된 프로토콜로써[5], IP 기간망을 사용하여 VPN 사업자가 확장성 있는 서비스를 제공하도록 하기 위한 또 다른 Peer 모델의 기술이다. 이 방안에서는 IPSec 터널이 기간망에 구축되고, 패킷의 전송은 일반적인 IP 전송방법에 따라 전달된다. 또한 BGP를 사용하여 경로정보를 기간망에 분배하도록 한다. 이 모델은 BGP/MPLS VPN과 유사한 모델인데, 여기에 IPSec을 적용한 이유는 다음과 같다. 첫째, IPSec을 기반으로 하는 VPN은 MPLS를 적용한 기간망의 존재를 필요로 하지 않으므로, 광범위한 사업자간의 VPN을 구축할 수 있다. 그러나, 흐름제어 및 전송품질보장 등의 목적으로 MPLS를 기간망의 일부 혹은 전부에 적용할 수 있다. 둘째, IPSec을 기반으로 하는 VPN은 MPLS 기반의 VPN 보안보다 훨씬 신뢰성 있는 보안 서비스를 제공할 수 있다. 2계층에서의 보안이 한 VPN 내부의 운용에서는 충분할 수도 있지만, 여러 기간망에 걸쳐서 VPN을 구축하는 경우에는 그 중의 일부 네트워크에서 VPN이 지원되지 않을 수도 있으므로 취약할 수 있다. 따라서 이 모델은 BGP에 의한 라우팅 정보의 차단 외에 추가적인 인증 및 보안을 제공한다.

이 모델은 기본적으로는 BGP/MPLS VPN 모델과 유사하다. 즉 각 PE 라우터는 자신과 연결된 각 사이트마다 VRF(VPN Routing and Forwarding Instance)를 유지관리하고, VRF의 경로정보들은 BGP의 Community Attribute 기능을 사용하여 제한적으로 분배된다. 그러나 MPLS와는 달리 Label Stacking[2]의 기능이 없어서, VRF간에 IPSec 터널을 적용하려는 경우에는 VRF들 사이에 완전한 메쉬를 구축해야 하므로 확장성에 문제가 발생하게 된다. 따라서 이 모델은 VRF가 아닌 PE 라우터들 사이에서만 메쉬 형태의 일대일 링크를 구성하는 방법을 제시하고 있다. PE로 들어오는 패킷은 SPI 값에 따라 적절한 VRF를 선택하여 전달하며, 다음절의 내용과 같이 하나의 SA와 여러 개의 SPI를 연결할 수 있는 방법을 제안하고 있다.

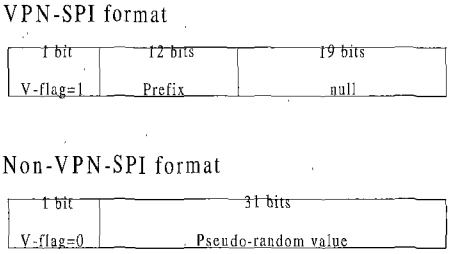
2.2 VPN-SPI

IPSec에서 SA는 SPI, 목적지 IP주소 및 프로토콜의 세 가지 요소로 구별되는데[1], 이 중 SPI는 32 bit의 Pseudo-random 값을 사용할 수 있으며, 아무런 포맷도 정의되어 있지 않다.



[그림 8] VPN-SPI의 포맷

BGP/IPSec에서 PE 라우터는 전송된 패킷에 대해서 적용할 SA를 선정하고 처리된 패킷을 전달할 VRF, 즉 VPN을 선정해야 한다. 이 두 가지 일을 수행하기 위하여 BGP/IPSec에서는 SPI를 두 부분으로 나누어 한 부분은 SA의 선정, 다른 부분은 VRF의 식별에 사용하도록 제안하고 있는데, 이를 VPN-SPI라 한다. IKE를 사용하는 경우와 IPSec 처리를 하는 경우의 두 가지로 나뉘는데, 그림 8은 IPSec 패킷에 포함된 VPN-SPI의 포맷을 나타내고 있다. 처음 12 비트는 SPI-prefix를 나타내는데, 이는 각 PE가 자신과 터널이 연결된 다른 PE들을 구별하기 위하여 할당한 값이다. 따라서 한 PE는 최대 212개의 PE와 IPSec 터널을 설정할 수 있다. BGP/IPSec에서는 이 값을 사용하여 패킷에 적용할 SA를 찾아내는데, 만약 SA의 식별에 소스 IP주소를 사용할 수 있으면, SPI-prefix는 다른 모든 PE에 대해 동일한 값을 사용하여도 된다. 32 비트의 SPI 값에서 나머지 20 비트가 패킷을 전달할 VRF를 식별하는데 사용되며, 이를 SPI 라벨이라 한다. 이 라벨값은 나중에 설명되는 바와 같이 BGP를 통하여 전파되며, 길이를 20 비트로 설정하여 BGP/MPLS에서 사용하는 라벨과 호환성을 유지하도록 했다. 따라서 하나의 PE는 최대 220개의 VRF를 연결할 수 있다.



[그림 9] IKE에서 사용하는 VPN-SPI

그림 9는 IKE에서 수신자가 전달하는 SPI를 나타낸 것인데, 처음 1 비트가 1인 경우에는 이 SPI가 VPN-SPI임을 의미하고, 0인 경우에는 보통의 SPI를 적용함을 의미한다. 따라서, VPN-SPI를 전달받은 PE는 상대방 PE에게 IPSec 패킷을 전송할 때, 상대방이 지정해 준 이 SPI-prefix를 사용해야 한다. 첫 비트가 0인 경우에는 VPN-SPI가 아닌 일반적인 SPI를 나타낸다. 이렇게 전달된 SPI-Prefix를 사용하여 패킷의 Inbound 및 Outbound 처리를 하는 과정은 다음과 같다. 먼저 패킷을 전송하는 경우에 VRF에서의 룩업에 의해 다음 홉(Hop)의 PE와 인터페이스, 그리고 패킷에 대한 라벨값을 사용하여 해당 SA를 식별하고 이에 의해 패킷에 대하여 보안 프로토콜을 적용한다. 이때 패킷의 SPI는 12 비트의 SPI-Prefix와 20 비트의 SPI 라벨로 이루어진다. 전송된 패킷을 처리하는 경우에는 목적지 IP주소, 프로토콜, 및 SPI-Prefix에 의해 패킷에 적용할 SA를 식별하고, 처리되어 사설 IP주소를 갖게된 IP 패킷은 SPI 라벨에 의하여 적절한 사용자 인터페이스, 즉 VRF로 포워딩된다.

CE 라우터로부터 전달된 라우팅 정보가 PE 라우터에 의해 전파되는 방법은 BGP/MPLS에서와 마찬가지로 BGP를 사용한다. PE는 라우팅 정보의 IP를 경로구분자를 사용하여 VPN-IP 주소로 변경한 후에 SPI 라벨, Extended Community, Site of Origin 등의 Attribute를 추가하여 이를 BGP의 Multi-Protocol[4] 기능을 이용하여 다른 PE로 전달한다. BGP/IPSec은 전술한 바와 같이 BGP의 Community Attribute를 사용하여 서로 다른 VPN 간의 연결성을 차단하여 보안성을 유지한다.

Ⅳ. IP VPN 프로토콜 비교

1. IPSec과 BGP/MPLS

VPN 기술의 비교와 평가를 위해서 확장성(Scalability), 보안성(Security), 전송품질보장(Quality of Service), 및 관리의 네 가지 항목을 일반적인 기준으로 할 수 있다[15]. 본 절에서는 [15]와 [16]을 바탕으로, 이와 같은 네 가지의 기준에 의해 현재 가장 주목을 받는 VPN 구축기술인 IPSec과 BGP/MPLS를 비교한다.

1.1 확장성

IPSec은 기본적으로 유니캐스트 SA를 가정하기 때문에 확장성이 낮다. 즉, 대규모의 IPSec 구축을 위해서는 키 분배 및 키 관리 등에 관련된 세밀한 계획을 수립할 필요가 있으며, 연결의 수가 많아질수록 관리 및 트래픽 처리의 부담이 커진다. 반면에 MPLS의 경우에는 사이트와 사이트간에 설정을 할 필요가 없으므로 확장성이 우수하며, 일반적으로 BGP/MPLS 기반의 VPN은 하나의 네트워크에서 수만 개 이상의 VPN을 지원할 수 있다.

1.2 보안성

IPSec은 IP 계층에서 비밀키를 사용한 암호 및 공개키를 사용한 인증 메커니즘에 의해 데이터를 보호한다. 따라서 IPSec에 의한 VPN은 충분한 길이의 키와 안전한 알고리즘을 적용하는 경우에 비밀성(Confidentiality), 무결성(Integrity), 및 인증(Authentication)의 측면에서 완전한 보안성을 제공한다. 한편, BGP/MPLS는 전통적인 2계층에서의 VPN 서비스와 마찬가지로 어드레스에 따라 트래픽을 분리하며, 또한 사용자는 기간망 및 다른 VPN의 어드레스 구조를 알 수 가 없으므로 BGP/MPLS 메커니즘 하에서 다른 VPN 네트워크로 침입하는 것은 사실상 불가능하다[16]. MPLS 구조는 기존의 ATM이나 Frame Relay를 사용한 서비스와 비슷한 정도의 보안을 제공할 수 있으며, 네트워크 사업자가 신뢰성이 있고 내부 기간망의 보안에 문제가 없는 이상 BGP/MPLS의 보안성에는 문제가 없다. 그러나, BGP/MPLS에서 제공되지 않는 암호화, 인증 및 데이터 무결성에 대한 필요성이 있다고 판단되는 경우에는 IPSec을 사용자 양단간에 혹은 에지 LSR 사이에 적용하여야 한다. 또한 사용자 네트워크 내에서의 보안은 BGP/MPLS에서 지원되지 않는다.

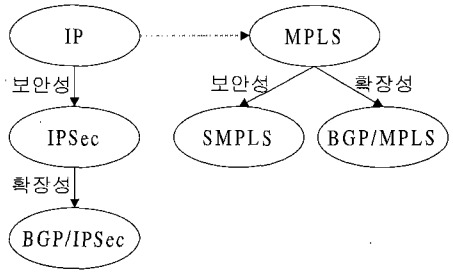
1.3 전송품질보장

일반적으로 IPSec 자체에는 QoS에 대한 고려가 없으며, 이를 지원하기 위해서는 라우터 같은 IPSec 응용제품에서 패킷에 대한 차별적인 처리를 수행하여야 한다. ATM 기반의 MPLS는 ATM의 큰 특징인 QoS 지원기능을 이용할 수 있으며, 전송경로가

미리 정해져 있으므로 Traffic Engineering을 수행하는 것도 가능하다.

1.4 관 리

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. 또한 네트워크 상의 위치로 볼 때, IPSec은 사용자 루프, 에지, 혹은 독립망의 경우에 주로 적용이 되어 데이터의 보안에 사용되며, MPLS는 서비스 제공자의 기간망에 적용되어 Traffic engineering과 대역폭 할당 등이 수행된다[2]. 네트워크에서 IPSec은 네트워크 계층에서 수행되고 MPLS는 IP+ATM 계층에서 동작하므로, 둘 다 사용자 응용계층에서는 투명성이 보장된다. 그러나, 사용자 측면에서 IPSec은 사전에 네트워크 레벨의 설정이 필요치 않으나, MPLS의 경우에는 처음에 서비스를 개시하기 전에 각 사이트의 CE 라우터와 PE라우터 사이에 미리 설정을 하여야 한다.



〔그림 10〕 IP VPN 기술의 발전 및 관계

〔표 1〕 IP VPN 프로토콜의 특성 비교

	IPSec	BGP/MPLS	SMPLS	BGP/IPSec
VPN 모델	Overlay	Peer	Overlay	Peer
보안성	우수	2계층 보안	우수	우수
QoS 메커니즘	3계층	2계층	2계층	3계층
관리 용이성	우수	중간	중간	중간
표준화	RFC 2401	RFC2547	Draft	Draft
MPLS 인프라	불필요	필요	필요	불필요
라우팅 프로토콜 사용	All	BGP	All	BGP
BGP의 확장	불필요	필요	불필요	필요
기존 프로토콜의 변경		VPN-IP	RSVP 오브젝트 SMPLS-AH SMPLS-ESP	VPN-SPI

2. SMPLS와 BGP/IPSec

그림 10은 본 고에서 논의된 네 가지 IP VPN기술의 발전단계 및 관계를 나타낸 것이다. 각각의 기술은 보안성 및 확장성의 증대를 위해 기존의 기술을 수정하거나 다른 기술을 적용하여 제안되었다. 최근에 제안된 SMPLS와 BGP/IPSec은 각각 BGP/MPLS와 IPSec의 단점을 보완하여 암호화/인증 및 확장성의 문제를 해결하도록 고안한 방식들이다. 따라서 이 두 가지 방식의 공통점은 첫째, 데이터 전송시의 암호화 및 인증이 제공되어 보안성 측면에서 매우 우수하다는 점이다. 두 번째로 두 방식 모두 추가적인 보안을 제공한다는 점이다. BGP/IPSec은 확장된 BGP 프로토콜에 의하여 라우팅 정보를 통제하므로 다른 VPN으로의 불법적인 침입이 사실상 불가능하며, SMPLS는 LSP에 의해 2계층에서의 터널링을 제공하므로 사용자의 불법적인 접근을 힘들게 한다. 또한, 제안된 방식들은 모두 기존의 프로토콜들을 수정 혹은 확장하여야 하므로, 이 방식들이 사용되기 위해서는 표준화가 필수적이다. SMPLS에서는 각 VPN에서의 주소공간을 구별하기 위한 VPN-IP을 사용하고 RSVP-TE를 이용하여 IKE 메시지를 전달하기 위하여 새로운 오브젝트 및 메시지 타입을 구현하여야 한다. BGP/IPSec에서는 하나의 PE라우터에서 서로 다른 VPN들을 구별하기 위하여 기존의 SPI를 변형한 VPN-SPI를 사용한다.

표 1은 본 고에서 논의된 네 가지 IP VPN 기술들에 대하여 각각의 특징을 비교한 것이다. BGP/MPLS와 BGP/IPSec은 Peer 모델을 채택하여 확장성을 높였으며, BGP/MPLS를 제외한 다른 기술들은 전송 데이터에 대하여 암호화와 인증을 적용하여 데이터의 보안성 및 무결성을 보장하도록 하였다. 한편, BGP/MPLS와 BGP/IPSec은 처음에 서비스를 개시하기 전에 각 사이트의 CE 라우터와 PE 라우터 사이에 미리 설정을 할 필요가 있다. SMPLS와 BGP/IPSec의 경우는 아직 표준화가 되지 않은 상태이므로 기술 발전의 추이 및 채택 여부를 주시해야 할 필요가 있다. 사용하는 프로토콜 관점에서는 IPSec VPN이 가장 적용범위가 넓다. 즉, 다른 기술들과 달리, AS 내에서 굳이 BGP를 적용하거나 MPLS 인프라를 구축할 필요가 없으며, 이미 표준화 된 IPSec 프로토콜들 외에 추가하거나 수정을 필요로 하지 않는다. 그러나, BGP/MPLS

와 BGP/IPSec은 각각 새로운 IP 주소체계와 SPI의 정의를 필요로 하며, SMPLS의 경우에는 새로운 RSVP 오브젝트 및 메시지, 또한 새로운 보안 프로토콜을 정의하고 있다는 단점이 있다.

V. 결 론

본 고에서는 IP VPN 기술로 주목을 받고있는 IPSec과 BGP/MPLS를 비롯하여, 최근에 새로이 제안된 SMPLS 및 BGP/MPLS에 대한 개요와 기술상의 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 제공한다. 그러나, 각 사이트를 연결하여 메쉬 형태의 가상 백본을 구성하여야 하므로 확장성의 결여라는 단점을 지니고 있으며, 이에 따라 BGP/IPSec이 제안되었다. BGP/IPSec은 기존의 BGP/MPLS의 기능을 모방하여 사용자의 라우터와 사업자의 라우터 사이에 Peer 관계를 맺도록 함으로써 확장성을 향상하도록 한 것이다. 한편, 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 있다. SMPLS의 경우에는 MPLS VPN이 갖는 보안성의 문제를 해결하기 위하여 MPLS 페이로드를 IPSec과 비슷한 방법으로 암호화하고 인증하기 위한 기술이다. BGP/MPLS는 각 VPN 사이의 라우팅 정보를 차단하여 보안성을 높이고 있으나, IPSec이나 SMPLS와 같은 데이터 자체에 대한 암호화 및 인증은 제공하지 못한다.

그림 10에서 나타내듯이, 최근의 여러 가지 VPN 프로토콜들은 확장성과 보안성을 강화하는 방향으로 계속하여 연구개발 되고 있다. VPN 사용자의 다양한 욕구를 만족시켜 줄 필요성과 네트워크 운용의 효율화를 통한 사업자의 수익증대 측면에서, 기존의 VPN 기술인 IPSec과 BGP/MPLS는 향후에 지속적인 개선과 발전이 예상되며, 이는 본 고에서 논의된 바와 같이 확장성과 보안성의 강화라는 두 방향으로 진행될 것이다. 따라서, VPN 서비스 사업자는 새로운 VPN 기술을 적용할 때 이러한 기술의 발전 방향 및 연구 동향을 참조하여야, 서비스를 운용하고 네트워크에 새로운 기술을 접목 혹은 융합할 때 이를 효율적으로 할 수 있다.

참 고 문 헌

[1] S. Kent and R. Atkinson, "Security architecture for the Internet protocol," RFC 2401, Nov. 1998.

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

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

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

[5] J. De Clercq *et al.,* "BGP/IPSec VPN," Work in progress, IETF, Feb. 2001.

[6] M. Kaeo, *Designing Network Security,* Cisco Press, 1999.

[7] E. Rosen *et al.,* "BGP/MPLS VPNs," Work in progress, IETF, July 2001.

[8] K. Muthukrishnan *et al.,* "A core MPLS IP VPN architecture," Work in progress, IETF, July 2001.

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

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

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

[12] D. Piper, "The Internet IP security domain of interpretation for ISAKMP," RFC 2407, Nov. 1998.

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

[14] D. Awduche et al., "RSVP-TE: Extensions to RSVP for LSP tunnels," Work in progress, IETF, Aug. 2001.

[15] "A comparison between IPSec and

MPLS virtual private networks," White paper, Cisco Systems, 2000.
[16] M. Behringer, "Analysis of the security of the MPLS Architecture," Work in progress, IETF, Feb. 2001.

〈者 著 紹 介〉

윤 재 우(Jae Woo Yoon)
1979년 ~ 1983년 : 전북대학교 전자공학과 (공학사)
1983년 ~ 1985년 : 전북대학교 전자공학과 (공학석사)
1985년 ~ 1988년 : LG 정보통신연구소 연구원
1989년 ~ 현재 : 한국전자통신연구원 책임연구원
관심분야 : ATM, 인터넷 보안, Key management

이 승 형(Seung Hyong Rhee) 종신회원
1984년 ~ 1988년 : 연세대학교 전자공학과 (공학사)
1988년 ~ 1990년 : 연세대학교 전자공학과 (공학석사)
1995년 ~ 1999년 : University of Texas at Austin, Dept. of ECE (Ph. D.)
1990년 ~ 1995년 : 국방과학연구소 연구원
1999년 ~ 2000년 : 삼성종합기술원 전문연구원
2000년 ~ 현재 : 광운대학교 전자공학부 전임강사
관심분야 : 인터넷 보안, QoS, 혼잡제어, 트래픽관리