Secure IPv6 Tunnel Broker 설계

장인동* · 이승윤* · 박기식*
*한국전자통신연구원 표준연구센터

Design on Secure IPv6 Tunnel Broker

In-dong Jang* · Seung-yun Lee* · Kishik Park*
*ETRI PEC
E-mail : indoi@etri.re.kr

요 약

차세대인터넷망에서 사용될 IPv6 프로토콜은 이미 실용화 단계에 와 있다. 하지만 기존 프로토콜인 IPv4망을 버리지 못하고 있는 것이 현재 실정이고, 이에 기존의 IPv4망과 차세대 프로토콜인 IPv6망간의 변환기술은 현 시점에서 가장 중요하다고 할 수 있다. 여러가지 변환기술 중 IPv6 터널 브로커 방법은 사용자에게 웹 방식의 친숙한 인터페이스를 제공하며, 본 논문은 IPv6 터널 브로커 시스템에 보안기능을 추가하여 보다 안전한 서비스를 제공하기 위한 방법을 제시한다.

키워드
IPv6, Tunnel Broker

I. 서 론

최근 차세대인터넷 프로토콜인 IPv6[1]에 대한 관심이 높아지고 있다. 현재 사용하고 있는 IPv4 인터넷의 단점을 보완한 IPv6는 IETF의 IPv6 WG을 중심으로 대부분 표준화는 거의 완료된 상태이며, 이제는 활성화를 도모할 때이다. 하지만, 네트워크의 특성상 IPv4에서 IPv6로의 변환은 그림 1과 같이 순식간에 이루어지지 않고, 상당히 오랜 기간동안 IPv4와 IPv6는 공존할 것으로 예상된다. 완전한 IPv6 인터넷 환경으로 가기 전의 이러한 공존기간동안 IPv4와 IPv6간의 통신은 이루어져야 하며, 그러한 노력들은 많이 이루어졌고, 현재도 계속적으로 노력중이다. 본 논문에서 다룰 IPv6 터널 브로커 또한 이러한 노력중에 하나이며, 이 기술은 현재 여러 기관에서 서비스 중이다. IPv6 터널 브로커는 RFC3053[2]을 기본으로 하고 있으며, 본 논문에서는 기본적인 IPv6 터널 브로커에 보안기능을 추가한 보다 안전한 IPv6 터널브로커에 대해 기술하고자 한다.

본 논문의 구성은 IPv6의 변환 기술에 대한 내용과 그중 현재 서비스되고 있는 IPv6 터널 브로커에 대한 내용을 살펴보고, 동향과 문제점을 분석한 후 보다 안전한 IPv6 터널브로커 방법에 대해 기술한 후 향후 활용 및 발전방향에 대해 알아본다.

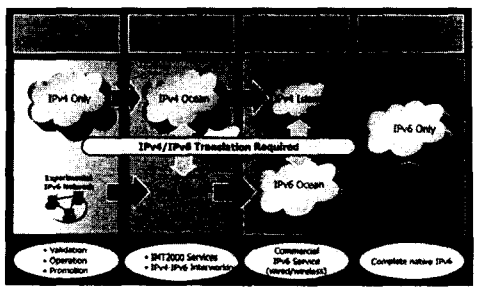

그림 1. IPv4에서 IPv6로의 변화 예상 모습

II. 본 론

2.1 차세대인터넷 기술 및 변환 기술

현재 인터넷에서 사용하고 있는 IPv4 프로토콜은 주소의 수가 조만간에 고갈될 것으로 예상하고 있다. 부족한 주소를 위해서도 IPv6의 빠른 도입이 필요하지만 IPv6 프로토콜은 단순히 주소확장이라는 부분에서 뿐만 아니라, QoS, Mobility, Security 등 여러 가지 부분에서 이로운 점이 많다. 하지만, IPv4에서 IPv6로의 전환은 상당기간동안 이루어질 것으로 예상되고, 이러한 IPv4와 IPv6의 공존기간

동안은 변환기술은 반드시 필요한 기술이라고 할 수 있다. 이러한 IPv4/IPv6 변환기술은 변환되는 계층에 따란 아래와 같이 분류될 수 있다.

- 헤더 변환(Header Conversion) 방식
- 수송계층 릴레이(Transport Relay) 방식
- 응용계층 게이트웨이
  (Alg-Application Level GAteway)방식

헤더변환 방식은 IP 계층에서의 변환으로, IPv4 패킷을 IPv6 패킷, 또는 그 반대로 변환하는 것으로 변환하는 규칙은 SIIT[3]에서 정의하고 있다. NAT-PT[4]는 헤더 변환 방식의 전형적인 예이다. 수송계층 릴레이 방식은 {TCP,UDP}/IPv4 세션과 {TCP,UDP}/IPv6 세션을 중간에서 릴레이하는 것을 가리킨다. 수송 릴레이에는 각 세션이 IPv4와 IPv6에 각각 밀폐되어 있기 때문에 프레그먼트나 ICMP 변환과 같은 문제는 없지만 응용 프로토콜에 내장된 IP주소의 변환과 같은 문제는 여전히 남아있다. 응용계층 게이트웨이 방식은 사이트 정보를 숨기고 캐시 메커니즘으로 서비스의 성능을 향상시키기 위해 사용된다. ALG가 IPv4 및 IPv6 두 프로토콜을 모두 지원하는 경우에는 두 프로토콜간에 변환 메커니즘이 사용될 수 있다. 이 방식은 헤더변환방식에서 나타나는 단점은 없지만, 각 서비스를 위한 ALG는 IPv4와 IPv6 모두에서 실행될 수 있어야 한다. 대표적인 방식은 SQUID 등을 들 수 있다.

그 외에 향상된 터널링 기법을 이용한 IPv4/IPv6 변환 메커니즘이 있다. 6to4[5]는 하나 이상의 유일한 IPv4 주소를 가지고 있는 IPv6 전용 사이트에 IPv6 6to4 주소를 할당하여 외부 IPv6 네트워크와 자동 터널링을 가능하도록 하는 메커니즘이다. 터널브로커[2]는 네트워크 관리자가 수동으로 설정하여 관리 작업이 많은 6bone 네트워크의 오버헤드를 줄이기 위해 개발되었다. DSTM (Dual Stack Transition Mechanism)은 IPv6 네트워크 내에서 IPv6와 IPv4의 호환을 지원하는 IPv4 주소를 사용하여 IPv4 노드와 통신할 수 있다. ISATAP(Intra-Site Automatic Tunnel Addressing Protocol)은 IPv4 기반의 인트라넷에서 IPv6 노드를 점증적으로 배치할 수 있는 간단하고 확장성있는 방법을 제공한다.

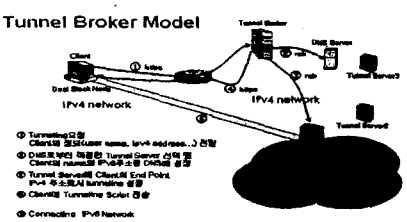

그림 2. 터널 브로커 모델

2.2 IPv6 터널 브로커

IPv6 프로토콜이 만들어지고, 1996년부터 세계적으로 IPv6의 연동 및 시험을 목적으로 IPv6-in-IPv4 터널방식인 6bone[6]이라는 가상망이 구축되어 운영되고 있다. 우리나라에서는 한국전자통신연구원에서 6bone-kr[7]을 운영하고 있다. 6bone 네트워크의 단점은 관리자의 관리작업이 지나치게 많다는 것이다. 이러한 관리 오버헤드를 줄이기 위한 방법 중의 하나가 바로 터널 브로커 메커니즘이다.

터널 브로커 개념은 터널 브로커라는 전용 서버를 구축하여 사용자의 터널 요청을 자동으로 관리하는 방법이다. 터널 브로커는 이미 IPv4 인터넷에 연결된 사용자에게 IPv6 연결을 제공하는 가상의 IPv6라고 보면 된다. 사용자는 터널브로커의 목록을 웹페이지(IPv4 HTTP)를 통해 쉽게 접근할수 있으며, 이 웹페이지를 통해 터널을 맺을 수 있고, IPv6 네트워크에 연결될 수 있다.

2.2.1 터널 브로커(TB)

TB는 사용자가 터널을 등록하고 활성화 하는 장소이다. TB는 사용자를 위해 터널을 생성, 수정 및 삭제를 관리한다. 이러한 명령을 터널 서버에 보내고, 사용자의 IPv6 주소와 이름을 DNS에 등록할 수도 있다. TB와 터널서버(TS)간의 통신은 IPv4 또는 IPv6를 통해 이루어 질수 있다.

2.2.2 터널 서버(TS)

TS는 글로벌 인터넷에 연결된 듀얼스택 라우터이다. TB로부터 설정 명령을 받으면 TS는 각 터널의 서버측을 수정 또는 삭제한다. 그리고 모든 활성 터널에 대해해 사용 통계 관리도 가능하다.

2.2.3 클라이언트

터널 브로커 서비스의 클라이언트는 IPv4 네트워크에 연결된 듀얼스택 IPv6 노드이다.

TS와 클라이언트 사이의 터널이 설정되고, 터널의 양측에 지정된 IPv6 주소는 TB가 관리하는 IPv6 어드레싱 공간에 속하는 글로벌 IPv6 주소이어야 한다.

각 엔티티간의 상호작용은 각기 다르다. TB와 사용자간의 상호작용은 http에 기초한 웹방식이다. 그리고, TB와 TS간의 상호작용은 IPsec을 통한 일련의 간단한 RSH 명령을 사용할 수 있고, SNMP를 사용하거나 그 밖의 임의의 네트워크 관리 솔루션을 채택할 수도 있다. TB에 의해 제어되는 자동 DNS 업데이트를 위해서는 동적 DNS 업데이트 프로토콜(Dynamic DNS Update Protocol)을 사용해야 한다.

2.3 IPv6 터널 브로커 동향

현재 RFC 3053을 기반으로 IPv6 터널 브로커 서비스를 하고 있는 곳은 표 1과 같다. 이와같이 실제 소스를 제공하면서 서비스를 하는곳은 대부분 해외 기관들이고, 국내에는 자체 개발하여 IPv6 터널브로커 서비스를 하고 있는 기관은 아

직 없는 실정이다.

표 1. IPv6 터널브로커 서비스

기관	링크	비고
MANIS	http://tbroker.manis.net.my	국제
Freenet6	http://www.freenet6.net	국제
CERNET	http://www.tb.6test.edu.cn	국제
Internet Initiative	http://www.iij.ad.jp	국제
Hurricane Electric	http://www.tunnelbroker.com	국제
BTexact	http://www.tb.ipv6.btexact.com	국제

2.4 안전 고려사항

IPv6 터널브로커 기본 구조에서 안전을 필요로 하는 상호작용들은 아래와 같다.

- 클라이언트와 TB간의 상호작용
- TB와 TS간의 상호작용
- TB와 DNS같의 상호작용

각 요구된 상호작용들에 적용된 안전 기술들은 구현사항들에 의존적이다. 클라이언트 TB 상호작용을 위해, http의 사용은 웹 서버로 보내어지고 다운받은 자료를 암호화하는 SSL(Secure Socket Layer)과 같은 널리 적용된 안전 특성들의 이용을 허락한다. 이것은 또한 간단한 "사용자 이름"과 "패스워드"의 인증 과정과 접근 제어를 실행하기 위한 기존 AAA 시설(예, RADIUS)에서 신뢰할 수 있도록 하는 것이 가능하게 만들었다.

TB-TS 상호작용을 위한 안전한 SNMP가 적용될 수 있다. 만약 동적인 DNS 업데이트 과정이 TB-DNS 상호 작용을 위해 사용되면, 안전성 문제는 [8]에서 논의 된 것과 같다. 반대로, 만약 RSH 명령들에 의거하는 단순한 방법이 사용되면, 표준 IPsec 메커니즘이 적용될 수 있다.

더욱이, 만약 클라이언트의 구축이 TB에 의해 준비된 실행 스크립트들이 얻어지면, 이런 스크립트들은 관리자나 루트의 역할이 같은 네트워크 인터페이스들을 관리 할 수 있는 권한과 함께 실행되어야 한다. 이것은 위험할 수 있고 터널 브로커 방법의 단지 초기 구현에서 고려되어야 한다. https의 MIME 타입에서 터널 구축 파라미터의 전송은 보다 안전한 방법이다.

게다가 TB를 통해 전에 만들어진 터널의 손실없이 인터넷으로부터 다이얼업 사용자가 접속 중단될 때 기밀의 손실은 일어날 수 있다. 실제, TS는 IPv4 주소가 다이얼업 ISP의 다른 가입자에 동적으로 할당할 수 있는 동시에 사실에 관계없이 오래된 IPv4의 사용자는 IPv6 트래픽 주소의 터널링을 유지한다. 따라서 TB가 연결 중지된 사용자들에 대한 IPv6 트래픽을 즉시 중지하는 것을 가능케 한다.

결국, TB들은 아주 확실한 많은 터널들의 요청에 대비하여 만들어진 터널 서버에서의 모든 자원들을 악의의 사용자가 다 써버리는 서비스 공격의 부정에 대해 보호해야 한다. 이 공격에 대한 가능한 보호는 싱글 유저가 같은 시간에 셋업시 허용되는 터널들 수의 관리자적인 제한에 의해 이루어진다.

이러한 터널을 셋업하기까지의 과정에서의 상호작용을 하나의 프로토콜로 정의한 것이 TSP(Tunnel Setup Protocol)[9][10]이고, 터널이 셋업되기까지 좀더 안전된 방법을 제시한다.

III. 결 론

차세대인터넷 프로토콜인 IPv6는 관련 핵심 기술들의 표준화가 거의 끝난 상태이며, 이제 빠른 활성화만 기다리고 있는 상태이다. 완전한 IPv6로 가기전의 IPv4와의 공존기간동안 변환기술은 필수이며, 여러 가지 변환기술중 사용자에게 친숙한 웹 인터페이스를 가진 IPv6 터널브로커 서비스는 IPv4에서 IPv6로의 빠른 전환을 도울 것이라고 기대한다. 본 논문은 이러한 IPv6 터널 브로커 서비스에서 취약한 보안기술을 살펴보고, 보다 안전한 방법의 IPv6 터널브로커에 대해 살펴 보았다. 이 시스템은 현재 구현중이며, 향후 실제로 서비스할 계획을 가지고 있다.

참고 문헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, 1998.12.

[2] A. Durand, P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker", RFC 3053, 2001. 1.

[3] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, 2000.2.

[4] G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, 2000.2.

[5] C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, 2001.5.

[6] 6bone, http://www.6bone.net

[7] 6bone-kr, http://www.6bone.ne.kr

[8] D. Eastlake, "Secure Domain Name System Dynamic Update", RFC 2137, 1997.4.

[9] M. Blanchet, "Tunnel Setup Protocol (TSP) : A Control Protocol to Setup IPv6 or IPv4 Tunnels", draft-vg-ngtrans-tsp-01, 2002.7.

[10] M. Blanchet, "IPv6 over IPv4 profile for Tunnel Setup Protocol (TSP)", draft-vg-ngtrans-tsp-v6v4profile-01, 2002.7.