NAT-PT 변환 메커니즘의 적용성 분석

Analysis of NAT-PT Transition Mechanism Applicability

이주철(J.C. Lee) 차세대인터넷표준연구팀 연구원
신명기(M.K. Shin) 차세대인터넷표준연구팀 선임연구원
김형준(H.J. Kim) 차세대인터넷표준연구팀 책임연구원, 팀장

NAT-PT는 IETF의 NGTrans WG에서 표준화한 IPv4/IPv6 변환기술 중 하나로서 IPv4/IPv6 헤더 변환기술(IPv4/IPv6 header translation)을 적용한 변환 메커니즘의 대표적인 사례로 꼽힌다. NAT-PT 변환기술은 그 이름에서 유추할 수 있듯이 NAT 기술에 기반을 두고 있는데, 이러한 연유로 NAT가 가지고 있는 여러 장·단점을 그대로 계승하고 있다. 따라서 이러한 NAT-PT 변환기술의 태생적인 제약점은 NAT-PT가 standard track RFC임에도 불구하고 이 기술의 사용에 대한 갖가지 논란을 불러 일으키는 근본적인 이유가 되어 왔다. NGTrans WG의 종료 후 새로 결성된 v6ops WG에서는 추가적인 변환기술에 대한 작업보다 IPv6 도입을 위한 시나리오 작업에 중점을 두고 있는데, 이 시나리오에 사용될 변환기술에 대한 논의가 진행되면서 자연스럽게 NAT-PT의 사용에 대한 문제점이 제기되었다. NAT-PT 기술의 향후 진로에 대한 의견은 결국 이 기술의 적용성에 대한 문서를 정리하여 권고안을 만들자는 쪽으로 모아졌고, NAT-PT applicability 저자그룹이 결성되어 지난 57차 IETF 미팅때 첫번째 버전의 문서가 제출되었다. 본 고에서는 이 NAT-PT applicability 00 버전의 문서를 중심으로 NAT-PT 기술의 적용성과 문제점 등을 분석할 것이다.

I. 서 론

NAT-PT(Network Address Translation-Protocol Translation, RFC-2766)[1]는 IETF(Internet Engineering Task Force) NGTrans WG에서 표준화한 변환기술로서, IPv6 전용 노드와 IPv4 전용노드 사이의 통신을 가능케 해주는 메커니즘에 대하여 기술하고 있다. NAT-PT 기술은 NAT 기술에 바탕을 두고 있으며, NAT와 같이 헤더 변환을 위한 IPv4 주소 풀을 유지하고 있다. NAT-PT와 NAT의 차이점은 NAT는 단순히 동일한 IP 패킷에서 특정한 필드—주소, 포트 혹은 ID 값 등—을 변환하는 데 반해, NAT-PT는 IP 헤더 자체를 다른 버전의 헤더로 변환하는 데 있다. 이 때에 소스 IPv6 주소는 NAT-PT가 유지하는 IPv4 풀에서 선택된 IPv4 주소로 대체되며, 목적지 IPv6 주소는 96비트 더미 프리픽스를 제외한 나머지 4바이트로 표현되는 IPv4 주소로 대체된다. 이외에 ICMP의 변환 룰은 SIIT(Stateless IP/ICMP Translation Algorithm)[2]에서 명시하고 있는 변환 방법을 그대로 따른다.

SIIT는 IPv4↔IPv6 변환기 상에 별도의 상태정보를 저장하지 않고도 변환을 수행할 수 있도록 해주는 메커니즘을 기술하고 있다. 따라서 SIIT는 IPv6 소스 주소에 대한 IPv4 주소 풀을 유지하지도 않으며 IPv4 주소에 대한 동적인 매핑도 시도하지 않는다. 단지 소스 주소와 목적지 주소에 IPv4 주소를 내장시켜서 변환시 별도의 정보가 없어도 변환이 가능하게 하였다. 이외에 SIIT에서 눈여겨 볼 부분은 ICMP에 대한 변환 룰을 제시한 부분인데, 이 부분은 NAT-PT에서 그대로 사용하고 있다.

NAT-PT는 NAT와 마찬가지로 IP 주소를 내재하고 있는 응용레벨 프로토콜을 올바르게 변환하기 위해서 ALG(Application Level Gateway)가 필요하다. ALG는 NAT-PT에서의 헤더변환과는 별도로 응용계층 헤더를 변환하는 역할을 한다. 이와 같

은 사례로서 대표적인 것은 DNS나 FTP이다.

DNS는 도메인 이름에 대한 질의의 결과로서 IP 주소를 돌려주기 때문에 NAT-PT 노드를 통과하여 IP 버전이 서로 다른 서브넷으로 전달될 경우, DNS 메시지가 포함하고 있는 IP 주소의 변환이 필요하다. DNS-ALG는 특히 NAT-PT에서 중요한 의미를 가지는데, IPv6 노드가 NAT-PT 노드를 통해서 다른 IPv6 노드, 혹은 IPv4 노드와 자연스럽게 통신하기 위해서는 DNS-ALG가 중간에 적절하게 동작하여 IPv6 노드와 IPv4 노드 모두에 대해서 IPv6 주소를 돌려주어야 하기 때문이다.

본 고에서는 NAT-PT를 이루는 이러한 각 요소들을 바탕으로 각각의 제약점을 분석하고, 이러한 분석자료를 바탕으로 IPv6 망 도입 시나리오에서 NAT-PT 변환기술 적용에 대한 가이드를 제시할 것이다.

II. SIIT 제약사항

1. 변칙적인 IPv4 mapped 주소의 이용

본래 IPv4 mapped 주소의 용도[3]는 듀얼 스택 노드에서 AF_INET6 소켓으로 통신할 경우에 IPv4 노드를 IPv6 주소로 표현하기 위한 것이었다. 즉 AF_INET6 소켓을 열어놓고 IPv4 노드와 IPv6 노드, 양쪽으로부터의 통신을 기다리고 있는 응용이 있다면 IPv4 스택은 수신한 IPv4 패킷의 소스 주소를 다음과 같이 IPv4 mapped 주소의 형식으로 만들어 AF_INET6 소켓에 넘겨준다.

a.b.c.d → ::ffff:a.b.c.d

이러한 IPv4 mapped 주소가 SIIT에서는 약간 다른 의미로 해석된다. SIIT의 가정으로부터 IPv4 mapped 주소를 사용하는 노드는 IPv6 전용 노드이다. 따라서 IPv4 mapped 주소는 IPv4 노드의 IPv6 주소표현이라는 원래의 의미로 해석되지 않고 IPv6 전용 노드로 해석된다. 이러한 IPv4 mapped 주소 용도의 전용은 IPv4 mapped 주소로 표현된 상대를 IPv4 노드로 취급해야 할지, 아니면 IPv6 노드로 취급해야 할지에 대한 혼돈을 낳게 된다[4].

2. 변환 룰 적용 시의 정보 상실

SIIT에서는 기본적인 IP 패킷의 변환과 ICMP 패킷의 변환에 대해 명시하고 있는데, 이 문서에서 기술하고 있는 ICMPv4↔ICMPv6 변환 룰을 그대로 적용했을 경우 완전한 변환이 불가능하다. 예를 들면, ICMPv4와 ICMPv6 메시지 사이에 서로 의미적으로 같은 역할을 하는 메시지들도 많지만, 서로 변환 불가능한 메시지들도 많다. ICMPv6의 Router Advertisement 메시지 같은 것들이 그 대표적인 예이다.

3. 멀티캐스트 주소의 매핑 불가

IPv4 멀티캐스트 주소의 IPv6 주소 매핑이 불가능하다. 즉, 224.1.2.3이라는 IPv4 멀티캐스트 주소는 ::ffff:224.1.2.3으로 변환되는데 이것은 IPv6 멀티캐스트 주소가 아니다.

4. SCTP와 멀티호밍

SCTP(Screaming Control Transmission Protocol)[5]은 종래의 TCP가 가지는 단점을 보완하고자 디자인된 프로토콜로서 한 SCTP 어소시에이션이 여러 개의 주소를 사용할 수 있게끔 하여 멀티호밍(multihoming)을 지원한다. SCTP가 연결을 맺기 위해서는 이 주소들을 INIT와 INIT-ACK chunk들에 넣어서 보내는데 SIIT는 이들 SCTP 세그먼트 내의 주소를 변환할 수 없다.

5. IPSec

가. IPSec ESP 헤더

ESP[6]는 기밀성(confidentiality)과 무결성(integrity)을 지원하는 IPSec 서비스이다. IPSec은 터널모드와 트랜스포트 모드 두 가지를 지원하는데 ESP가 트랜스포트 모드로 동작할 경우 IP의 상위 레이어 프로토콜이 IP 주소를 포함하고 있지 않을

경우 SIIT를 통해서 변환이 가능하다. 하지만 ICMP 메시지 같이 페이로드에 변화가 생기는 패킷은 변환이 불가능하다. 또한 터널모드로 동작할 경우는 트랜스포트 모드에서 암호화한 영역에 IP 헤더부분까지 포함되므로 변환이 불가능하다.

결론적으로 트랜스포트 모드에서 동작하는 ESP는 부분적으로 SIIT 변환이 가능하며 터널모드에서는 TCP/IP, UDP/IP, SCTP/IP, 그리고 ICMP/IP 모두 불가능하다.

나. IPSec AH 헤더

AH[7]는 무결성을 지원하는 IPSec 서비스이다. IPSec은 IP 상위 레이어의 프로토콜뿐만 아니라 IP 헤더 자체도 무결성 체크의 범위에 포함되므로, 트랜스포트 모드와 터널모드 양쪽 다 SIIT를 통한 변환이 불가능하다.

다. 키 관리

일단 키 관리에 대해서는 IPv6 노드와 IPv4 노드 사이에서 키 관리 프로토콜이 제대로 동작할 수 있는지에 대한 확인이 먼저 필요하다. 예를 들면, IKE에서 이용하는 ISAKMP[8]의 identification 페이로드를 보면 SA를 맺는 호스트들을 식별하기 위해서 자신의 IP를 페이로드에 포함시킨다. 따라서 이러한 주소를 포함한 패킷들은 SIIT에서 변환이 불가능하므로 키 관리 프로토콜이 제대로 동작할 수 없다.

III. NAT-PT 제약사항

앞에서 언급했듯이 NAT-PT는 NAT를 기반으로 하여 설계되었으며, NAT가 가지는 특성을 기본적으로 대부분 물려받았다. 따라서 그 동안 논의되어온 NAT의 문제점[9] 또한 대부분 가지고 있으며 SIIT가 제공하는 변환 룰을 사용하되 IPv4 노드를 표현하는 주소가 반드시 IPv4 mapped 주소가 될 필요가 없다는 점을 제외하면 동일한 제약점을 갖는다. 단, IP 상위 레이어 프로토콜의 페이로드가 IP 주소를 가짐으로써 야기되는 문제는 적절한 ALG를 적용함으로써 해결될 수 있다.

1. 응용의 제약

응용이 사용하는 프로토콜 내부에 IP 주소나 TCP/UDP 포트 정보를 포함하고 있는 응용은 적절한 ALG가 지원되지 않는 경우 대부분 동작에 실패한다. 이러한 응용들은 매번 새롭게 등장할 때마다 각 응용에 알맞은 ALG를 필요로 하므로 신속한 대처가 쉽지 않다.

2. 확장성 및 단일한 취약지점 문제

모든 IPv6 노드들이 하나의 NAT-PT 노드로 집중되므로 병목현상이 생길 수 있으며, 이로 인해 성능저하가 문제시된다. 또한 이 NAT-PT 노드가 다운될 경우 NAT-PT 노드에 물려있는 모든 IPv6 노드가 외부와 통신할 수 없으므로 확장성 및 단일한 취약지점 문제(single-point-of-failure)가 생긴다.

3. IPSec

가. IPSec ESP/AH

ESP/AH와 관련된 모든 SIIT의 문제점이 NAT-PT에도 동일하게 적용된다. 더욱이 NAT-PT는 SIIT와는 다르게 IPv4 translated 주소와 IPv4 mapped 주소의 조합을 쓰지 않을 수도 있으므로 (IPv4 mapped 주소대신 NAT-PT의 고유/96길이의 프리픽스와 IPv4 주소를 사용할 수도 있다.) 이 경우 TCP/UDP의 pseudo checksum 계산을 다시 수행해야만 한다. 따라서 몇몇 경우를 제외하고는 터널모드, 트랜스포트 모드에서 NAT-PT를 통해 변환이 불가능하다.

나. 키 관리

SIIT의 제약사항이 모두 적용되며 NAT-PT는 각 커넥션에 대한 state 관리를 하므로 ISAKMP 페이로드에 IP 주소가 포함되지 않는 경우라 하더라도

문제가 생길 수 있다.

4. DNS-ALG

DNS-ALG는 IPv6 노드와 IPv4 노드가 통신을 하기 위해, 상대방 IPv4 노드에 대한 IPv6 주소 또는 IPv6 노드에 대한 IPv4 주소를 찾아내는 역할을 한다(address discovery).

이러한 DNS-ALG는 듀얼스택노드가 IPv6 전용노드 혹은 IPv4 전용노드와 통신을 시도하는 경우 원하지 않은 결과를 낳을 수도 있다. 즉 듀얼스택 노드가 IPv4 노드와 IPv4 통신을 원하는 경우에도 IPv6 주소를 돌려줄 수 있으며, IPv6 주소를 가진 IPv6 노드와 IPv6 통신을 원하는 경우에도 translated IPv6 주소를 돌려주어 통신을 못하게 될 수도 있다. 또한 IPv4 주소를 원하는 IPv4 노드에게 IPv6 주소를 돌려줄 수도 있다. 하지만 이러한 문제들은 DNS-ALG를 지능적으로 구현함으로써 어느 정도 해결될 수 있다[10].

이 외에도 DNS-ALG는 A 타입 주소(IPv4 주소)를 AAAA 타입 주소(IPv6 주소)로 바꾸는 동작을 하므로 DNSSEC의 동작을 불가능하게 한다.

5. 서비스 거부

가. 주소 풀 소모 공격(Address Pool Depletion Attacks)

NAT-PT의 IPv6 도메인에 존재하는 임의의 악의적인 IPv6 노드가 소스주소를 달리하며 패킷을 보낼 경우 NAT-PT 노드가 관리하는 주소풀이 금방 바닥날 수 있다. 이것은 기타 다른 실제의 서비스를 원하는 IPv6 노드들로 하여금 서비스 거부(denial of service) 공격을 당하게 하는 효과를 낳는다.

나. 역 공격(Reflection Attacks)

임의의 악의적인 IPv6 노드가 IPv6 소스주소를 멀티캐스트나 브로드캐스트 주소로 만든 후 패킷을 전송한다면, 이 패킷에 대한 IPv4 노드로부터의 응답이 NAT-PT 노드의 내부 IPv6 망에 존재하는 노드들에 대한 공격으로 바뀔 수 있다.

IV. NAT-PT Applicability 분석

1. SIIT

SIIT가 IPv6 노드를 위해서 실제 망에서 제대로 쓰이려면 반드시 적절한 ALG가 동반되어야 한다. 또한 SIIT를 구현한 박스에 state를 유지해야 하는데, 이것은 NAT-PT의 작동 시나리오와 별반 다름이 없고, SIIT라는 명칭이 의미하는 state를 유지하지 않아도 되는 장점을 버린 것이다. 따라서 현재 SIIT가 유용하게 쓰일 수 있는 곳은 일반적인 IPv6 환경 하에서 변환기 단일노드로 쓰이기 보다는, SIIT의 단점을 감수하면서 특수한 목적에 임시로 쓰이는 정도일 것이라 예상된다.

2. NAT-PT

일반적으로 NAT-PT 노드가 쓰여질 것이라고 예상되는 곳은 IPv6 스텁 도메인(stub domain)의 경계라우터(border router)이며, IPv6 망의 출입구 쪽에 위치하여 변환 및 패킷의 포워딩을 담당한다. 이 외에 다음과 같은 적용 시나리오가 있을 수 있다.

가. IPv6 망 안에 소수의 IPv4 노드가 존재하는 경우

IPv6 망이 광범위하게 퍼져있는 상태에서 IPv6로 업그레이드가 불가능한 IPv4 노드가 있는 경우, 이 IPv4 노드와 기존의 IPv6 노드와의 통신을 지원하기 위해 NAT-PT가 사용될 수 있다. 이런 상황에서 소수의 IPv4 노드들을 지원하기 위해서 듀얼스택 노드들을 다시 설치하는 것은 비현실적인 일이며, 가능하면 프록시 솔루션을 사용하되 그렇지 못한 상황에서는 NAT-PT를 적용한다.

나. NAT-PT를 사용해야 하는 특수한 경우

- 메모리나 탑재 가능한 코드 크기 등의 하드웨어

적인 제약으로 IPv6 스택만이 탑재 가능한 장비인 경우

- 특정하게 정해진 응용만 돌리도록 설계된 장비인 경우
- 듀얼스택을 지원하도록 만들 수 있는 장비이지만, 네트워크 리소스 소모를 최소화해야 하는 상황인 경우

다. 3GPP 망에서의 제한적인 사용

3GPP 망에서의 3GPP 호스트는 IPv6 상에서 SIP을 기반으로 구동되는 IMS 응용을 동작시킬 수 있어야 하며, 이것은 다른 IPv4 SIP 호스트와 통신이 가능해야 한다. 또한 모바일 망에서의 PDP 콘텍스트의 수를 줄이기 위해서도 3GPP 호스트는 IMS 응용과 non-IMS 응용을 하나의 IPv6 PDP 콘텍스트로 접근할 수 있어야 한다. 따라서 NAT-PT 노드는 IPv6 망 상에서 전송되는 IMS 미디어 트래픽을 변환하는 데 사용되어 질 수 있다.

V. 결 론

이번 57차 IETF 회의 때 제출된 NAT-PT applicability 드래프트[11]는 그 목적이 문서에서 언급한 몇몇 시나리오를 제외한 일반적인 변환 메커니즘으로서의 NAT-PT 사용의 제고를 권고하는 데에 있다. 즉, NAT-PT가 비록 standard track RFC이긴 하지만 그 기술이 NAT를 기반으로 하고 있다는 점, 그리고 그 때문에 발생하는 많은 활용상의 제약점, end-to-end connectivity가 깨지는 점 등의 이유로 가능하면 NAT-PT가 일반적인 IPv4/IPv6 전환 솔루션의 용도로 쓰여지는 것을 막아서 IPv4 NAT에서 범했던 오류를 반복하지 않으려는 IETF 멤버들의 의지로 보여진다.

그러나 본 문서에서 언급한 제한된 환경에서 short-term 기간 동안의 사용을 전제로 쓰여진다면 NAT-PT도 나름대로의 장점을 갖는 전환 솔루션이라고 생각된다. 특히 기타 다른 변환 메커니즘과는 다르게 IPv4 노드나 IPv6 노드의 수정 없이 NAT-PT 박스 하나만으로 바로 서비스 적용이 가능하다는 점은 나름대로의 장점이 될 수 있다.

본 문서는 이제 00 버전이 나온 만큼 차후로도 업데이트 될 소지가 많다고 보여지며, 특히 요즈음 이슈가 되고 있는 mobility 환경에서 NAT-PT가 적용되었을 경우 발생할 수 있는 문제점 등에 대해서도 차후 업데이트가 필요하다고 보여진다.

참 고 문 헌

[1] G. Tsirtsis, "Network Address Translation-Protocol Translation(NAT-PT)," RFC-2766, Feb. 2000.

[2] E. Nordmark, "Stateless IP-ICMP Translation Algorithm(SIIT)," RFC-2765, Feb. 2000.

[3] R. Gilligan, "Basic Socket Interface Extensions for IPv6," RFC-3493, Feb. 2003.

[4] Metz and Hagino, "IPv4-Mapped Addresses on the Wire Considered Harmful," draft-itojun-v6ops-v4mapped-harmful-01 Expired, Oct. 2002.

[5] R. Stewart, "Stream Control Transmission Protocol," RFC-2960, Oct. 2000.

[6] S. Kent, "IP Encapsulating Security Payload(ESP) ," RFC-2406, Nov. 1998.

[7] S. Kent, "IP Authentication Header," RFC-2402, Nov. 1998.

[8] D. Maughan, "Internet Security Association and Key Management Protocol(ISAKMP)," RFC-2408, Nov. 1998.

[9] Hain, "Architectural Implications of NAT," RFC 2993, Nov. 2000.

[10] P. Hallin, "NAT-PT DNS ALG Solutions," draft-hallin-natpt-dns-alg-solutions-01, July 2002.

[11] S. Satapati, "NAT-PT Applicability," draft-satapati-v6ops-natpt-applicability-00, Oct. 2003.