IPv4와 IPv6가 혼재하는 상황에서의 IPSec

강지영° 정지웅 김종권 신성준 안정철
서울대학교 전기.컴퓨터공학부, 국가보안기술 연구소
{jmkang°, jwjeong, ckim}@popeye.snu.ac.kr, {jinsol, ukyang}@etri.re.kr

IPSec in co-existence of IPv4 and IPv6

Jimyung Kang, Jiwoong Jeong, Chong-kwon Kim, Seong-Jun Shin, Joung-Chul Ahn
School of Electronic Engineering and Computer Science, Seoul National University
National Security Research Institute

요 약

현재 사용되는 인터넷은 IPv4를 기반으로 하고 있다. 그러나 IPv4 주소의 부족을 예상하면서 128bit의 주소를 사용하는 IPv6가 제안되었다. IPv6로 네트워크가 이동해 가기 위해서는 IPv4와 IPv6가 공존하는 과도기적 상황을 필수적으로 겪어야 한다. 즉 IPv6와 IPv4와의 통신이 가능해져야지만, IPv6의 도래가 가능할 것이다. 이러한 상황을 고려한 통신 방안들이 IETF에서 제안되었다. 하지만 이러한 방안들은 네트워크의 보안이 거의 고려되지 못하였다. 본 논문에서는 IPv4와 IPv6가 공존하는 상황에서 차세대 보안 기술의 선두격인 IPSec을 사용할 때 발생할 수 있는 보안 문제들에 대해 분석하고, 이러한 네트워크 보안을 고려한 IPv4와 IPv6의 통신 프레임 워크를 제시한다.

1. 서 론

현재의 인터넷은 IPv4를 기반으로 하고 있다. IPv4에서 사용되는 주소는 32 비트로 이루어져 있어서 최대 약 40억 개 정도의 호스트가 인터넷에 접속할 수 있다. 그렇지만, 지금과 같이 인터넷에 접속하고자 하는 호스트의 수가 폭발적으로 증가하고 또한 이동통신 단말이나 텔레비전 및 냉장고와 같은 정보가전들이 인터넷에 접속하고자 하는 경우에는 이러한 IPv4 주소가 턱없이 부족해 질 것이다. 따라서 IP주소의 부족을 해소하기 위해서 128bit의 주소 체계를 가진 IPv6 기술이 제안되었다.

그렇지만, 앞에서 언급한 것과 같이 현재의 인터넷은 IPv4 기술을 이용하여 구축되고 운용되고 있기 때문에, 이러한 인터넷을 한 순간에 모두 IPv6로 바꾼다는 것은 불가능한 일이라 할 수 있다. 따라서 새로운 IPv6 네트워크로 가는 중간단계에서는 IPv6 망이 IPv4 망과 공존하게 되고, 점진적으로 IPv6 망을 확장시키고, IPv4 망은 축소시켜나가야 할 것으로 생각된다. 따라서 당분간은 IPv6 망과 IPv4 망이 혼재되어 존재하게 되므로, IPv6 망에 접속되어 있는 호스트와 IPv4 망에 접속되어 있는 호스트간 통신이 가능하도록 하기 위한 메커니즘이 필수적이다. 이를 위하여 IETF에서는 IPv4노드와 IPv6노드 사이의 통신을 위한 방안으로 NAT-PT (Network address translation - protocol translation)[1], DSTM (Dual Stack Transition Mechanism)[2] 등과 같은 여러 가지 전환 메커니즘을 제안하였다. 그러나 이러한 방안들은 보안의 관점이 전혀 고려되지 않았다. 현재 네트워크의 보안은 가장 큰 관심사가 되어 있으며 보안이 고려되지 않은 네트워크는 사용하기 어렵다고 생각된다. 본 논문에서는 이러한 과도기적 상황에서 보안 프레임워크의 대표격인 IPSec[3][4][5][6]을 사용할 경우 발생할 수 있는 문제점을 분석하고, IPSec을 사용 할 수 있는 프레임 워크를 제시하고자 한다.

2. 배경 지식

2.1 NAT-PT 시나리오 [1]

IPv6와 IPv4는 주소체계 뿐만 아니라 프로토콜 자체가 많은 차이를 가지고 있다. 이런 상황에서 서로 다른 두 노드가 통신을 진행하는 가장 일반적인 방법으로 NAT-PT를 들 수 있다.

NAT-PT는 서로 다른 IP 버전을 변환해 줌으로써 IPv4와 IPv6 노드들 간에 통신이 가능하게 해 주는 방법이다. NAT-PT를 담당 하는 노드는 IPv4와 IPv6 네트워크 사이에 위치해 있는 게이트웨이 노드이다. 그림 1은 NAT-PT가 동작하는 상황을 나타내고 있다.

기본적으로 NAT-PT의 동작은 NAT의 동작과 유사하다. 그러나 NAT-PT는 NAT와 더불어서 IP 프로토콜까지 바꿔줘야 하고, IPv4 주소를 임시로 할당해주는 메커니즘이 추가로 필요하다. NAT-PT는 IPv4 address pool을 유지하고 있다. IPv6 노드와 IPv4 노드가 통신을 진행해야 할 때마다 IPv6 노드를 위해서 이 IPv4 주소를 임시로 하나 할당해주고, mapping table에 이 정보를 저장하게 된다. 각자의 네트워크를 통해서 다른 네트워크와의 경계, 즉 NAT-PT에 도착한 패킷은 이 매핑 정보에 의해서 다른 프로토콜로 변환되면서 주소도 바뀌고, 다른 네트워크로 전달 된다. 즉 IPv4 노드 입장에서는 IPv6와의 통신이 아니라 임시로 할당된 주소를 가진 IPv4 노드와의 통신을

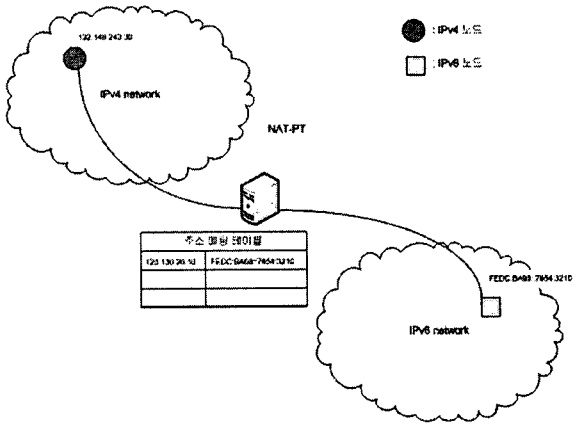

그림 1 NAT-PT의 동작

하는 것이다.

2.2 DSTM 시나리오 [2]

DSTM은 IPv6 망에 위치하는 노드들이 IPv4와 IPv6의 두 가지 프로토콜 스택을 구현하고 있을 경우에 이 듀얼 스택을 가진 노드와 IPv4노드가 통신을 할 때 사용할 수 있는 방안이다. 그림 2는 듀얼 스택 노드가 DSTM으로 동작하는 상황을 나타낸다.

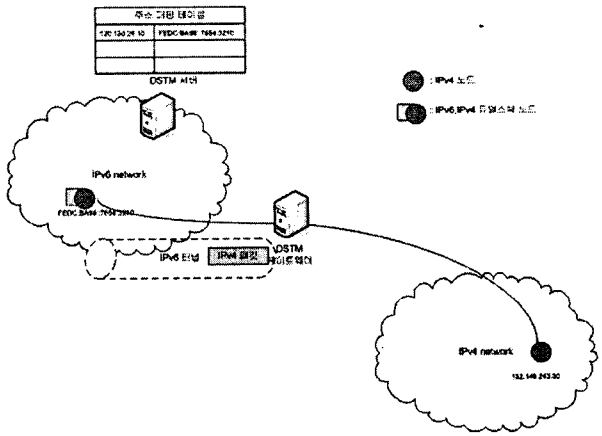

그림 2 DSTM의 동작

여기에서 IPv6노드는 듀얼 스택을 가지고 있기 때문에 IPv4 노드와 통신을 할 때는 자신을 IPv4 노드로 사용한다. 먼저 DSTM 서버에서 IPv4주소를 임시로 할당 받아와서, IPv4 패킷을 발생시킨다. 그러나 이 패킷은 IPv6 네트워크 안에 있기 때문에 이 네트워크를 빠져나가기 위해서 노드는 이 패킷을 IPv6로 encapsulation하게 된다. encapsulation된 패킷은 이제 IPv6 네트워크에서 진행할 수 있게 되고, 이 패킷은 DSTM 게이트웨이로 라우팅된다. DSTM 게이트웨이에서는 바깥 쪽 헤더가 제거 되어, IPv4 네트워크로 나가서 목적 IPv4노드로 전송된다. 반대 방향으로는 DSTM 게이트웨이로 라우팅된 IPv4 패킷을 DSTM 게이트웨이가 IPv6 로 encapsulation해서 통신을 진행하게 된다. DSTM 서버는 IPv4 address pool을 관리하고, 할당한 IPv4 주소와 IPv6 주소와의 매핑 정보를 관리해야 한다.

3. IPv4와 IPv6가 공존하는 상황에서의 IPSec

IPv4와 IPv6가 공존하는 상황에서 IPSec의 적용은 현재까지 거의 연구 되지 않았다. 이번 장에서는 위에서 설명된 시나리오에 IPSec을 적용시킬 경우에 대해서 살펴보도록 하겠다. IPSec을 적용시킬 때 두가지 문제로 나눠서 고려해 볼 수 있다. 먼저 1) IPv4노드와 IPv6노드 사이에서 IPSec 프로토콜 자체가 잘 동작할 것인가에 대해 고려한 뒤, 2) IPv6노드를 위해 임시로 받아온 IPv4주소를 어떻게 신뢰할 수 있을지에 대해서 고려해보기로 한다.

3.1 IPv4와 IPv6의 공존상황에서 IPSec의 동작

그림 1에서 NAT-PT를 중간에 두고 IPSec SA를 맺을 경우를 생각해보자. 현재에도 IP주소의 부족을 해결하기 위해서 NAT는 사용되고 있고, NAT를 사용할 경우에 IPSec에서 발생할 수 있는 몇가지 문제점들이 [7]에서 나타나 있는데 NAT-PT에서도 기본적으로 이러한 문제점들을 포함한 여러 문제점이 발생하게 된다.

가장 기본적으로 NAT-PT는 프로토콜 자체를 바꾸어 버리기 때문에 NAT-PT를 지나면서 헤더의 형태는 완전히 달라지게 된다. IPSec은 AH와 ESP두가지 프로토콜로 이루어 지는데 이 중에서 AH는 authentication만을 지원하고 ESP는 privacy와 authentication을 모두 지원하는 프로토콜이다. 그런데 IPSec에서 AH는 패킷 헤더까지 인증 데이터에 포함시키고 있다. 즉 source와destination을 포함해서 IP 헤더까지도 integrity 를 체크하게 되는데 NAT-PT를 통과하면서 IP 주소가 바뀔 뿐만 아니라 프로토콜 자체가 바뀌기 때문에 AH는 NAT-PT가 있는 환경에서 기본적으로 사용이 불가능하다. 또한 IPSec을 사용하기 위해서는 그 전단계에서 IKE를 이용해 Key 공유를 하고 SA를 맺는 것이 필수적인 과정이라고 생각되는데 이 IKE는 노드의 identifier로 IP주소를 기본적으로 사용하도록 되어 있다. IKE 프로토콜을 통해 전달된 identifier로서의 IP주소가 실제 IP 헤더에 있는 IP주소와 다를 때는 패킷을 거부하도록 IKE프로토콜이 설계되어 있기 때문에 IKE 프로토콜 자체가 동작하지 않는 문제가 발생할 수 있다. 여기에 더불어 IKE에서는 Traffic stream Selector라는 페이로드에 IPSec SA를 적용시키는 대상이 되는 IP주소들을 기입해야 하는데, IPv4와 IPv6는 서로 다른 주소 체계를 사용하기 때문에 이것 또한 불가능하다. 즉 IPv4 노드와 IPv6노드가 IKE를 맺기 위해서는 IKE가 IPv4와 IPv6의 IKE Setup에 관해서 미리 알고 이러한 것을 지원해 주어야 하는데, 현재 IKE에서는 이러한 기능이 존재하지 않는다.

DSTM을 사용하는 시나리오에서는 End-to-end IPSec이 사용가능하다. 듀얼 스택을 사용하는 IPv6네트워크의 노드가 IPv4노드로 동작하고 IPv6네트워크에서는 encapsulaton을 통해서 라우팅되기 때문에 기본적으로 IPv4 주소 체계를 사용한

IPSec SA를 맺을 수 있다. 그러나 제약점은 존재한다. IKE에서는 Traffic Stream payload를 통해서 IPSec을 적용시킬 대상이 되는 주소들을 지정하게 된다. 그런데 이 때 사용할 주소가 IPv4 address pool에서 임시로 할당 받아 온 것이기 때문에, End 노드가 아닌 Firewall과 같은 여러 주소를 상대로 하는 IPSec SA는 맺기가 어렵게 된다. 그리고 이 DSTM 시나리오에서는 IPv4를 지원하지 않는 IPv6노드는 IPv4와 통신을 진행 할 수 없다.

3.2 임시 IPv4 주소의 신뢰

IPv6노드와 IPv4노드가 통신을 진행하기 위해서는 임시 IPv4 주소를 받아오는 과정이 필수적이다. 이 과정상에서 DSTM인 경우 DSTM 서버로부터 이 주소를 안전하게 받아와야 하고, IPv4노드 입장에서는 이 주소를 상대방 노드로 인식해야 한다. 이를 위해서 IPv6노드는 DSTM 서버와 미리 IPv6로 IPSec SA가 맺어져 있어야 한다. DSTM 프레임 워크에서는 이 가정이 무리한 가정이라고 생각 되지는 않는다. 할당 받은 IPv4주소를 상대방에게 확인 시키기 위해서는 네트워크의 경계에 있는 DSTM 게이트웨이와 IPSec을 맺는 방안을 생각해 볼 수 있다. 네트워크의 경계에 있는 게이트 웨이는 IPv4와 IPv6모두 지원 가능한 듀얼 스택이므로, IPv4노드와 IPSec을 맺을수 있다. IPv4노드는 IPv6노드의 IPv4주소를 확인하기 위해서 DSTM 게이트웨이에 주소를 요청하고 DSTM 게이트웨이는 이 메시지를 다시 DSTM 서버로 포워딩 해주게 된다. DSTM 게이트웨이와 DSTM 서버는 IPv6로 IPSec SA가 맺어져 있다고 가정할 수 있으므로 DSTM 서버로 부터의 메시지가 다시 DSTM 게이트웨이를 통해서 IPv4 노드로 돌아오게 되면 IPv4노드는 이 IPv6 주소를 신뢰하게 된다.

IPv6노드를 위해 사용하는 IPv4주소는 임시로 사용하는 주소이다. 즉 이것은 언제든지 회수 될 수 있고, 다른 노드에게 재분배 될 수 있는 상황이 되는 것이다. 여기에서 IPv4주소의 신뢰성이 다소 떨어질 수 있는데 이러한 문제점은 IPv4주소의 주기적인 확인을 통해서 방지할 수 있다. 즉 한번 발급된 후에 회수된 IPv4주소는 특정한 시간동안에는 재분배 될 수 없게 하고, IPSec을 수행하는 노드는 이 특정한 시간마다 한번씩 임시 IPv4 주소의 신뢰성을 DSTM 서버로부터 확인 하는 것이다.

4. IPv4와 IPv6가 공존하는 상황에서의 IPSec 프레임워크

3장에서 고려된 여러문제점과 해결책들을 고려해 볼 때 IPv4노드와 IPv6노드가 공존하는 상황에서 IPSec을 사용할 수 있는 프레임 워크를 그림 3과 같이 구성 할 수 있다.

NAT-PT는 위에서 제시된 여러 가지 문제점들로 인해서 IPSec을 적용하기는 어렵다. 그러므로 DSTM을 사용해야 하는데, 새롭게 deploy되는 IPv6 노드에 IPv4 스택을 같이 구현하는 것은 어려운 일이 아니기 때문에 무리 없이 DSTM 시나리오를 적용할 수 있을 것이다. 임시의 IPv4 주소를 안전하게 확인하기 위해서는, IPv6노드와 DSTM 서버 사이, DSTM 서버와 DSTM 게이트웨이 사이, DSTM 게이트웨이와 IPv4 노드사이에 미리 설치된 IPSec SA가 필요하다. 게이트 웨이는 IPv4와

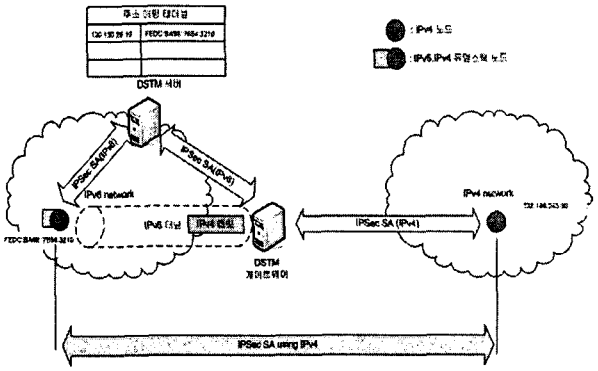

그림 3 IPSec이 사용가능한 프레임워크

IPv6프로토콜을 이용해서 양쪽으로 IPSec SA를 맺게 된다.

5. 결론 및 향후계획

IPv6 네트워크로 이동해 나가기 위해서는 그 과도기적인 단계로 IPv4와 IPv6가 공존하는 상황이 존재할 수 밖에 없다. 본 논문에서는 이러한 상황에서 IPSec을 적용할 때 발생할 수 있는 문제점을 고찰하고, 이러한 문제점들을 고려해서 DSTM에 기반을 둔 보안 프레임워크를 구성하였다. 이 프레임 워크를 사용해서, 임시 IPv4 주소의 신뢰성을 확인할 수 있고, 프로토콜의 수정 없이 IPSec을 동작 시킬 수 있다.

향후에는 실제 IPSec을 이러한 환경에서 동작시켜서, IPSec의 동작을 확인하고, 더 효과적으로 IPSec을 적용시킬 수 있는 프레임 워크에 대한 연구를 진행해 나갈 계획이다.

참고 문헌

[1]G.Tsirlsis, P. Sdsuresh, "Network Address Translaltion - Protocol Translation (NAT-PT)", RFC 2166, 2000.2.

[2]Jim Bound et al, "Dual Stack Transition Mechanism (DSTM)", draft-ietf-ngtrans-dstm-07, 2002.2

[3]S. Kent, R. Atkinson "IP Encapsulating Security Payload (ESP)" RFC 2406 1998.11

[4]S. Kent, R. Atkinson "IP Authentication Header" RFC 2402, 1998.11

[5]P. Hoffman "Algorithms for Internet Key Exchange version 1 (IKEv1)" RFC 4109, 2005.5

[6]S. Kent, R. Atkinson "Security Architecture for the Internet Protocol" RFC 2401, 1998.11

[7]B. Aboba, W. Dixon "IPsec-Network Address Translation (NAT) Compatibility Requirements" RFC 3715, 2004.3