제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

SPS 상에서의 SPP 와 NAT-PT 을 이용한 정책 협상

송치평*, 김건우**, 나재훈**, 이상호*
*충북대학교 전자계산학과
**한국전자통신 연구원
e-mail : chicando@cnlab.chungbuk.ac.kr
shlee@cbucc.chungbuk.ac.kr

The Policy Association using SPP and NAT-PT on SPS

Chi-Pyoung Song*, Gun-Woo Kim**, Jae-Hoon Na**, Sang-Ho Lee*
*Dept. of Computer Science, Chung-buk National University
**Electronics and Telecommunications Research Institute

요 약

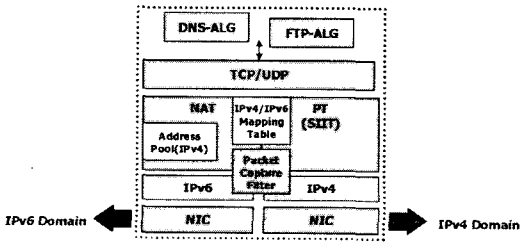
네트워크의 규모가 방대해지고 복잡해지면서 IP 주소 부족문제와 그에 따르는 보안문제가 중요시 되어지고 있다. 여기에서 IPv4/IPv6 변환 기술인 NAT-PT 는 구조적 특성상 보안에 대한 메커니즘을 제공하지 못한다. 즉, 종단간 IPSec 보안은 다른 주소 영역사이(IPv4-IPv6)를 교차하는 것이 불가능하기 때문이다. 따라서 이 논문에서는 이를 해결하기 위해 NAT-PT 와 SPP 가 결합된 SPS 환경에서의 정책협상을 위한 정책기반 보안 메커니즘을 제안 한다.

1. 서론

현재 사용되고 있는 IPv4(Internet Protocol version 4)주소는 32 비트의 주소체계를 사용하기 때문에 이론적으로는 약 43 억개의 인터넷 주소공간을 제공 할 수 있다. 매년 2 배 이상의 기하급수적으로 늘어나는 인터넷 사용자 수요를 감안할 때, 현재 사용되고 있는 IPv4 인터넷 주소체계로는 계속해서 요구되는 인터넷 주소 수요를 충족시킬 수 없다.[1]
이에 반해 IPv6 는 128bit 의 주소 체계를 사용해 거의 무한개의 (3.4×10^{38}) 인터넷 주소를 제공함으로써, 이러한 주소고갈 문제를 근본적으로 해결할 뿐만 아니라, IPv4 에서의 멀티캐스트나 보안 기술 등의 구조적 어려움을 해결한다.
본 논문에서는 기존의 IPv4 망에서 IPv6 망으로 변화되는 과도기적 단계에서 요구되는 변환 기술 중 하나인 NAT-PT(Network Address Translation - Protocol Translation)를 분석하고, NAT-PT 의 한계를 설명하며, NAT-PT 의 한계 중 가장 문제시 되는 보안문제를 해결할 수 있는 보안메커니즘을 제안한다.

2. NAT-PT

NAT-PT 은 IPv4 망과 IPv6 망과의 통신을 제공해주는 메커니즘으로 IETF RFC2766[2]에 의해 표준화된 기술이다. NAT-PT 는 크게 IPv4-IPv6 간 통신을 할 때 IPv6 주소에 IPv4 주소 pool 로부터 동적으로 선택된 IPv4 주소를 할당해 주는 NAT 기능과 SIIT(Stateless IP/ICMP Translator)[3] 프로토콜 변환 메커니즘을 제공하는 PT 기능을 수행한다.

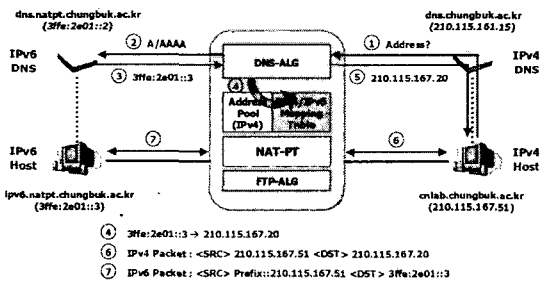


[그림 2-1] NAT-PT 변환기 구조

응용에 따라 발생하는 추가적인 요구사항을 변환해주는 ALG(Application Level Gateway) 기능들을 수행한다. [그림 2-1]은 이러한 NAT-PT 변환기의 기본구조를 나타낸다. 기본적인 NAT-PT 는 NIC(Network Interface Card)로부터 패킷을 캡쳐하여 IPv6 주소에 할당된 IPv4 주소가 IPv4/IPv6 맵핑 테이블에 없으면 IPv4 주소 pool 로부터 동적으로 IPv4 주소를 IPv6 주소에 할당하고 그 결과를 IPv4/IPv6 맵핑 테이블에 기록한다. 이렇게 맵핑된 주소를 이용하여 SIIT 프로토콜 변환 메커니즘은 IP 또는 ICMP 를 변환한다. 그리고 상위 프로토콜을 검사하여 상위 프로토콜이 DNS 이면 DNS-ALG 를 통해 AAAA 레코드와 A 레코드의 변환 및 DNSv4 와 DNSv6 간의 주소정보 교환을 수행하고, FTP 이면 FTP-ALG 를 통해 확장된 FTP 명령어를 사용하는 FTPv6 와 기존의 FTPv4 간의 정보 교환을 수행한다. 그리고 마지막으로 각 프로토콜 계층의 페이로드 길이 및 검사합 값을 갱신한 후 새롭게 변환된 패킷을 전송한다.

2.1 IPv4 망에서 IPv6 망으로의 Ingoing 연결

위에서 설명한 기능들을 예를 통해 자세히 설명하면, 두 가지 경우로 나누어 설명할 수 있다. 하나는 IPv4 망에서 IPv6 망으로 통신하는 Ingoing 연결이고, 다른 하나는 IPv6 망에서 IPv4 망으로 통신하는 Outgoing 연결이다. 먼저 IPv4 망에서 IPv6 망로 통신하는 Ingoing 연결의 경우를 살펴보면 [그림 2-2]와 같다.

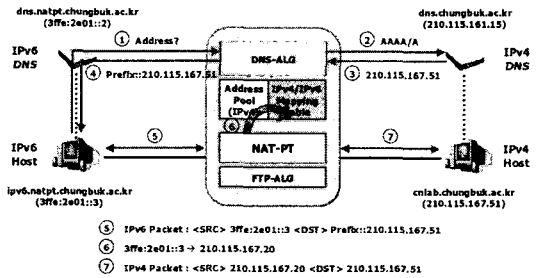


[그림 2-2] IPv4 망에서 IPv6 망으로의 Ingoing 연결과정

[그림 2-2]는 IPv4 호스트(210.115.167.51)이 IPv6 호스트(3ffe:2e01::3)과 통신을 할 경우의 동작순서를 나타낸 것이다. 우선 IPv4 호스트(cnlab.chungbuk.ac.kr)는 IPv6 호스트(ipv6.natpt.chungbuk.ac.kr)의 DNS 를 통해 통신을 시도한다. 그러면 IPv4 호스트는 DNS 를 IPv4 주소로 바꿔기 위해 IPv4 DNS 서버에게 DNS 요청을 한다. 그리고 IPv4 DNS 서버는 요청된 DNS 정보를 가지고 있는 IPv6 DNS 서버에게 DNS 요청을 한다. 이때 IPv4 DNS 서버의 DNS 요청은 NAT-PT 를 거치게 되는데, 이는 NAT-PT 가 IPv6 DNS 서버에 고정적으로 맵핑 된 IPv4 주소의 라우팅 정보를 가지고 있기 때문이다. NAT-PT 의 DNS-ALG 는 IPv4 DNS 서버로부터 전송된 DNS 요청 메시지를 A 레코드에서 AAAA 레코드로 변환하여 IPv6 DNS 서버에게 전송한다. IPv6 DNS 서버는 수신된 DNS 요청에 대한 응답을 IPv4 DNS 서버에게 전송한다. 그리고 NAT-PT 는 IPv6 DNS 서버가 전송한 DNS 응답을 수신하고, DNS-ALG 에 의해 DNS 응답 메시지를 AAAA 레코드에서 A 레코드로 변환한다. 이때 NAT-PT 의 DNS-ALG 는 AAAA 레코드로 된 IPv6 주소를 A 레코드의 IPv4 주소로 맵핑시키기 위해 IPv4 주소 pool 로부터 동적으로 IPv4 주소를 하나 할당 받는다. 이렇게 할당 받은 IPv4 주소는 IPv4/IPv6 맵핑 테이블에 저장되고 이후에 발생하는 통신에 사용한다.

2.2 IPv6 망에서 IPv4 망으로의 Outgoing 연결

IPv6 망에서 IPv4 망으로의 Outgoing 연결과정은 IPv4 망에서 IPv6 망으로의 Ingoing 연결과정과 거의 유사하나 약간의 차이점을 가지고 있다. [그림 2-3]은 IPv6 망에서 IPv4 망으로 통신하는 Outgoing 연결의 경우를 나타내주고 있다.



[그림 2-3] IPv6 망에서 IPv4 망으로의 Outgoing 연결과정

[그림 2-3]에서 알 수 있듯이 차이점은 IPv4 주소 pool 에서 IPv4/IPv6 맵핑 테이블을 만드는 시기가 다르다는 것이다. Ingoing 의 경우에는 DNS 응답을 DNS-ALG 가 처리하는 과정에서 해당 IPv6 주소에 대한 IPv4 주소를 IPv4 주소 pool 로부터 동적으로 할당 받아 IPv4/IPv6 맵핑 테이블에 저장하지만, Outgoing 의 경우에는 IPv6 호스트가 IPv4 호스트에 TCP 세션을 처음 시작하거나 UDP 통신을 하고자 할 때 해당 IPv6 에 대한 IPv4 주소를 IPv4 주소 pool 로부터 동적으로 할당 받아 IPv4/IPv6 맵핑 테이블에 저장한다는 것이다. 이런 이유로 Outgoing 의 경우에는 DNS 를 거치지 않고도 IPv4 호스트와 직접 통신이 가능하다. 물론 IPv4 호스트의 주소는 [NAT-PT 의 Prefix::IPv4 호스트 IP 주소] 형식으로 해주어야 한다.

2.3 NAT-PT 의 제약 및 단점

• **토폴로지 제약**

NAT-PT 를 거쳐 IPv4 망과 IPv6 망을 통신하는 경우에는 한 세션에 대한 모든 응답과 요청이 동일한 NAT-PT 를 거쳐 라우팅 되어야 한다. 그 이유는 NAT-PT 의 IPv4/IPv6 맵핑 테이블에 등록되어 있지 않는 IP 간의 통신은 모두 무효화 되기 때문이다. 이는 NAT[4]의 일반적인 문제로써, RFC2663[5]에 자세히 설명되어 있다.

• **프로토콜 변환 제약**

상당수의 IPv4 필드가 IPv6 에서 의미가 변화되었으므로 직접적으로 변환할 수 없다. 예를 들어, IP 헤더의 옵션필드의 의미 및 구문이 IPv6 에서는 상당히 많이 변화되었다. IPv4 와 IPv6 프로토콜 변환에 대한 상세한 내용은 SIIT[3]에 따른다.

• **주소 변환의 영향**

NAT-PT 는 IP 계층의 주소변환을 수행하므로, 상위계층

에서 IP 주소를 사용하는 응용은 정상적인 동작을 할 수 없다. 이 경우에는 해당 응용을 지원할 수 있는 ALG 가 필요하다. 이는 NAT[4]의 일반적인 문제로써, RFC2663[5]에 자세히 설명되어 있다.

• 종단간 보안 결여

NAT-PT 가 제안하고 있는 가장 중요한 제약 중 하나가 바로 종단간 네트워크 계층 보안이 불가능하다는 것이다. 또한 전송 및 응용 계층 보안에서 IP 주소를 사용하는 경우에도 불가능하다. 이는 NAT 기능의 자체적인 한계이다. NAT-PT 와 독립적으로, 종단간 IPSec 보안은 다른 주소 영역사이(IPv4-IPv6)를 교차하는 것이 불가능하다. IPSec 네트워크 레벨 보안을 추구하는 두 종단 노드들은 IPv4 또는 IPv6 중 하나를 둘 다 제공하여야 한다.

• DNS 변환 및 DNSSEC

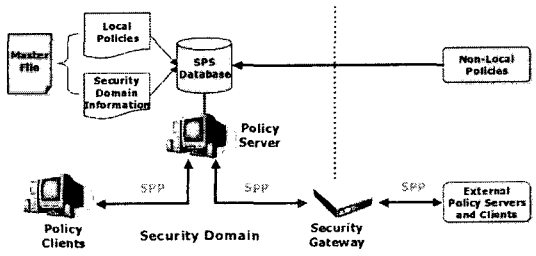
DNS-ALG 는 일반 DNS 변환에는 사용될 수 있으나, 보안 DNS 에는 적용될 수 없다. IPv6 도메인내에 있는 신뢰 DNS 서버는 IPv4 영역으로부터 수신한 DNS 요청에 대한 응답에 서명할 수 없으며, 결과적으로 서명된 DNS 응답을 기다리는 IPv4 종단 노드는 NAT-PT 에 의해 변형된 응답을 거부할 것이다. 그러나 좋은 점은 IPv4 영역으로부터 접근하는 IPv6 도메인내의 서버만이 이러한 제약을 겪게 된다는 것이다.

3. 보안 정책 시스템 (Security Policy System)

보안 정책 시스템(Security Policy System)은 종단간의 안전한 통신 설정을 위해 같은 보안 영역 내에서 뿐 아니라 다른 보안 영역의 호스트, 서브넷 혹은 망들의 정책 정보에 접근하여 알아내고, 그 정책 정보를 처리하기 위해 필요한 메커니즘을 제공하는 분산 시스템이다. 즉, 보안 정책 시스템에 의해 다루어지는 정책 정보는 여러 보안 영역을 통과할 수 있다. 보안 정책 시스템은 종단간의 통신에 관련된 주 보안 게이트웨이와 부 보안 게이트웨이를 발견할 수 있는 자동화된 메커니즘을 제공한다. 또한, 종단간 통신의 경로 상에 있는 보안 게이트웨이의 신원을 검증할 수 있고, 특정 보안 게이트웨이가 특정 호스트에 대한 권한을 갖는지를 검증할 수 있다.

3.1 보안 정책 시스템 구성

보안 정책 시스템은 각 보안 영역에 대한 정책 정보 요청하는 정책 클라이언트, 정책 요청에 대해 응답하는 정책 서버, 그리고 보안 영역의 고유 정보를 저장하는 마스터 파일과 여러 정책관련 정보를 저장하는 SPS DB(Security Policy System Database)로 구성된다. [그림 3-1]은 보안 정책 시스템의 구성을 나타낸다.



[그림 3-1] 보안 정책 시스템의 구성

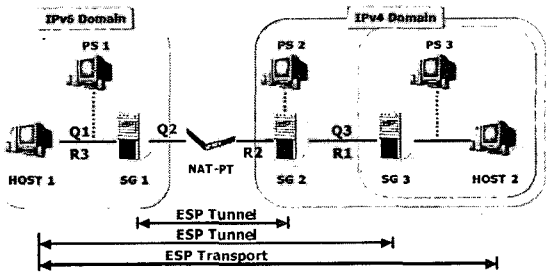
3.2 보안 정책 프로토콜 (Security Policy Protocol)

보안 정책 시스템의 정책 서버와 클라이언트는 SPP 을 사용하여 정보를 교환하며, 이 프로토콜은 정책 정보가 클라이언트와 서버에 의해 어떻게 교환되고, 처리되고, 보호되는지를 정의한다. SPP 는 수송 계층 프로토콜로 UDP 혹은 TCP 를 사용하며, 포트는 501 번을 사용한다. 그리고 SPP 의 SPP-XFR 메시지는 반드시 TCP 를 사용해야 한다. SPP 가 제공하는 메시지의 종류는 다음과 같다.

- Query(SPP-QUERY) 메시지 : 호스트, 보안 게이트웨이 혹은 정책 서버가 정책 서버에게 특별한 정책 정보를 요청할 때 사용하는.
- Reply(SPP-REPLY) 메시지 : 정책 서버가 특정 Query 에 대해 응답하는 정책을 표현하는 메시지.
- Policy(SPP-POL) 메시지 : 정책 서버로 업로드되거나 서버로부터 다운로드되는 정책 정보를 표현하는 메시지.
- Policy Acknowledgment(SPP-POL_ACK) 메시지 : Policy 메시지에 대한 수신 통지를 위한 메시지.
- Transfer(SPP-XFR) 메시지 : 정책 서버들 간에 Bulk 정책 정보의 교환에 이용되는 메시지.
- Keep alive(SPP-KEEP_ALIVE) 메시지 : 정책 서버가 보안 게이트웨이나 다른 감시 장치들에게 서버의 상태를 알리기 위해 사용되는 메시지.

4. NAT-PT 와 SPP 을 이용한 SPS 간의 정책 협상

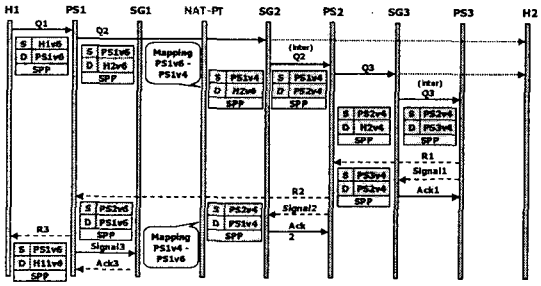
본 절에서는 [그림 4-1]와 같은 네트워크 구조에서 SPP 가 NAT-PT 를 통해 수행되는 과정에서의 문제점, 해결방법, 고려사항 등을 살펴보겠다. [그림 4-2]는 HOST 1 과 HOST 2 사이의 통신을 위해 SPP 동작과정을 나타내주고 있다. SPP 는 IPv4 와 IPv6 에 유연하게 적용할 수 있도록 설계 되었다. 단지 여기서 고려해야 할 사항은 SPP 가 NAT-PT 를 통해 통신을 하더라도 아무런 문제가 없는지를 알아보는 것이다.



[그림 4-1] NAT-PT 상의 SPP 수행 네트워크

우선 SPP 의 동작에 앞서 IPv6 도메인 내의 정책 클라이언트, 즉 [그림 4-1]에서 HOST1 의 정책 클라이언트는 IPv4 도메인 내의 목적지 IPv4 주소를 [Prefix::IPv4]형식의 IPv6 주소에서 추출할 수 있다고 가정한다. 만약 그렇지 않으면 SPP 에 원래의 IPv4 주소 대신 [Prefix::IPv4] 주소가 들어가므로 NAT-PT 는 SPP 내의 이 주소를 IPv4

주소로 일일이 변환해 주어야 한다. 다시 말해서, SPP 내의 주소 필드에는 원래의 IPv4 주소와 IPv6 주소가 그대로 들어가야 한다는 것이다. 그리고 정책서버 역시 IPv4/IPv6 주소를 모두 수용할 수 있어야 한다. 이러한 가정이 성립되고, [그림 3-18]과 같이 IPv4/IPv6 정책 서버 간 SPP 를 통한 정책 협상을 하면, 주소 변환은 IP 헤더에서만 발생하므로 SPP 내의 정책에는 아무런 변화도 일어나지 않는다. 결론적으로 SPP 를 통한 정책 협상 과정에서는 NAT-PT 가 SPP 에 어떠한 영향도 미치지 않는다.



[그림 4-2] 동작 시퀀스 차트

하지만 협상된 정책을 수행하기 위해 정책서버가 보안 게이트웨이에게 보내는 정책 메시지(SPP-POL)는 약간 다르게 처리되어야 한다. 보안 게이트웨이가 정책 서버에 의해 협상된 정책을 수행하기 위해서는 해당 네트워크의 IP 주소가 필요하다. 다시 말해, IPv4 망에서 정책을 수행하기 위해서는 IPv4 주소가, IPv6 망에서 정책을 수행하기 위해서는 IPv6 주소가 필요하다. 예를 들어, [그림 4-2]에서와 같이 NAT-PT 가 SPP 내의 IP 주소에 대해 아무런 관여도 하지 않으면, HOST 1 은 IPv6 주소를 가지고 HOST 2 의 IPv4 주소를 가지게 된다. 그리고 PS3 가 협상된 정책을 반영하기 위해 SG3 에게 Signal 1(SPP-POL 메시지)를 전송한다. 결국 SG3 는 실제 HOST 1 과 HOST 2 의 통신에서 Signal 1 에 포함된 정책을 수행하려 하지만 수행할 수 가 없다. 왜냐하면 실제 HOST 1 과 HOST 2 의 통신에서는 HOST 1 의 IPv6 주소가 NAT-PT 에 의해 IPv4 주소로 맵핑되기 때문에 정책협상에 의해 전송된 HOST 1 의 IPv6 주소를 SG3 가 찾을 수 없기 때문이다. 이러한 문제를 해결하기 위해서는 정책협상 과정에서 NAT-PT 가 SPP 를 수신하면 NAT-PT 에 의해 맵핑된 IPv4-IPv6 주소를 SPP 에 추가해 주어야 한다. 이렇게 하면 보안 게이트웨이는 수신된 Signal 에서 해당 네트워크의 IP 주소를 참조하면 되므로, 앞에서 설명한 문제를 해결할 수 있다. 물론 NAT-PT 는 SPP-ALG 라는 기능을 하나 더 추가해야 한다.

앞에서 설명한 문제를 해결하기 위한 다른 방법으로, SPP-ALG 로 SPP 내의 IP 주소를 아예 변환해 줄 수도 있다. 그러나 NAT-PT 의 특성상 맵핑된 IPv4 주소는 동적으로 할당되므로 신뢰할 수 없을 뿐만 아니라, 서명을 검증하는데 사용할 수도 없다. 이러한 이유로 SPP 내의 IP 주소를 변환하지 않고, 맵핑된 IP 주소만을 추가해 주는 것이다.

5. 결론

본 논문에서는 IP 주소 부족문제를 해결하기위한 IPv4 주소를 IPv6 주소로 변환하기 위한 기술 중에 하나인 NAT-PT 환경에서의 보안결여 문제를 해결하기 위한 'SPS 상에서의 SPP 와 NAT-PT 을 이용한 정책 협상' 메커니즘을 제안하였다. 즉, IPv4 망과 IPv6 망사이에서의 보안을 위해 SPP 을 사용하여 정책협상을 하면 NAT-PT 을 통과하여도 주소변환은 IP 헤더에서만 발생하므로 SPP 내의 정책에는 아무런 변화도 일어나지 않는다. 그리고 변환된 주소에서 협상된 정책이 올바르게 적용되기 위해서는 SPP 내의 주소필드에는 원래의 IPv4 주소와 IPv6 주소가 그대로 들어가야 한다는 것이다.
앞으로 이 논문에서 제시된 NAT-PT 환경에서의 정책기반 보안 메커니즘 모델을 구현하기 위해서는 NAT-PT 에서의 IPSEC 과 IKE 등의 보안기술에 대한 연구가 필요하다.

참고문헌

[1] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", RFC2373, 1998. 7.
[2] G. Tsirtsis, P. Srisuresh, "Network Address Translation – Protocol Translation (NAT-PT)", RFC2766, 2000. 2.
[3] Nordmark, E., "Stateless IP/ICMP Translator (SIIT)", RFC2765, 2000. 2.
[4] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC1631, 1994. 5.
[5] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663, 1999. 8.Roger S. Pressman. "Software Engineering, A