NAT-PT를 고려한 확장된 보안정책 프로토콜

현 정 식† · 황 윤 철† · 엄 남 경† · 이 상 호††

요 약

이 논문은 NAT-PT의 특성을 고려한 단-대-단 IPSec 보안 서비스를 제공하기 위한 보안정책 프로토콜에 대해 기술한다. NAT-PT는 IPv4 망에서 IPv6망으로 진화하기 위한 과도기적인 단계에 있어 IPv4/IPv6망간의 통신을 제공하기 위해 IETF에 제안된 기술 중 하나로, 이종 IP망간의 통신을 위한 IP 주소변환 및 프로토콜 변환에 대해 기술하고 있다. 그러나 NAT-PT는 인터넷의 필수 요구사항 중 하나인 보안에 대한 한계점을 가지고 있다. 그러므로 이 논문에서는 NAT-PT를 고려한 단-대-단 IPSec 보안 서비스를 제공하기 위해 가장 먼저 수행되어야 할 보안정책 협상을 제공하는 확장된 보안정책 프로토콜을 제시한다.

Extended Security Policy Protocol that considers NAT-PT

Jeung Sik Hyun† · Yoon Cheol Hwang† · Nam Kyoung Um† · Sang Ho Lee††

ABSTRACT

In this paper, we describe security policy protocol to provide end-to-end IPSec security service that considers characteristics of NAT-PT. NAT-PT is describing IP address translation and protocol translation for communication on heterogeneous IP network by one of the technology that is proposed by IETF to provide communication between IPv4 and IPv6 network in transitional step to evolve by IPv6 network to IPv4 network. But NAT-PT has the limitation on security one of the essential requirement of Internet. Therefore, we propose the extended security protocol that offers a security policy negotiation that should be achieved for the first time to provide end-to-end IPSec security service that considers NAT-PT in this paper.

키워드 : 주소변환(NAT : Network Address Translation), 프로토콜 변환(PT : Protocol Translation), IPSec, 보안정책(Security Policy), 보안정책 프로토콜(SPP : Security Policy Protocol)

1. 서 론

현재 사용되고 있는 IPv4(Internet Protocol version 4) 주소는 32비트의 주소체계를 사용하기 때문에 이론적으로는 약 43억개의 인터넷 주소공간을 제공할 수 있다. 그러나 클래스 단위의 할당 등으로 인해 실제 사용 가능한 주소의 개수는 약 5~10억개로 추정된다. 따라서 매년 2배 이상의 기하급수적으로 늘어나는 인터넷 사용자 수요를 감안할 때, 현재 사용되고 있는 IPv4 인터넷 주소체계로는 계속해서 요구되는 인터넷 주소수요를 충족시킬 수 없다. 다라서, 인터넷에 대한 모든 기술 및 표준화를 다루는 IETF(Internet Engineering Task Force)에서는 2013년경 IPv4 주소가 고갈될 것으로 예측하고 있다[1]. 그러나, 이와 같은 예측도 기존에 IPv4 주소를 많이 확보하고 있는 선진국에 해당되는 것으로 한국, 일본, 중국 등 아시아권 국가들은 지금부터도 새로운 신규 인터넷 사업에 요구되는 주소공간을 자유롭게 할당 받지 못하는 실정이다. 따라서 국내에서의 인터넷주소 고갈은 이보다는 더욱 더 앞당겨질 것으로 예상된다. 또한 세계적으로 무선인터넷 서비스가 활성화 됨에 따라 앞으로의 인터넷 단말은 PC보다는 휴대폰, PDA가 될 것임을 고려하면 2005년에 이미 10억의 인터넷 주소가 사용될 것으로 예측되고 있다.

이에 반해 IPv6는 128비트의 주소 체계를 사용해 거의 무한개의(3.4×10^{38}) 인터넷 주소를 제공함으로써, 이러한 주소고갈 문제를 근본적으로 해결할 뿐만 아니라, IPv4에서의 멀티캐스트나 QoS, 그리고 보안기술 등의 구조적 어려움을 해결한다. 따라서 세계 각국은 IPv6의 개발 및 확산을 위해 노력하고 있는데, 유럽은 무선인터넷 서비스 제공을, 일본은 무선인터넷과 정보가전 분야를, 그리고 미국은 중국 등을 포함한 세계시장을 겨냥해 IPv6의 기술을 발전시키고 있다. 현재 IPv6는 6Bone이라는 가상망을 이용하여 1996년부터 현재까지 운영되고 있다.

현재 IPv4에서 IPv6로의 진화는 2010년까지 단계적으로 변환될 것으로 예상되며, IEFT에서는 이 기간 동안 IPv4망

† 준 회 원 : 충북대학교 대학원 전자계산학과
†† 종신회원 : 충북대학교 전기전자및컴퓨터공학부 교수
논문접수 : 2002년 12월 26일, 심사완료 : 2003년 9월 2일

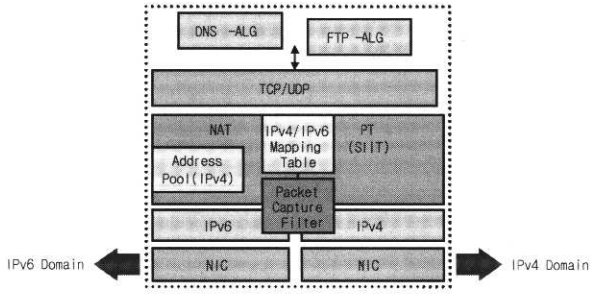
과 IPv6망간의 통신을 지원하기 위해 NAT-PT(Network Address Translation Protocol Translation)[2]라는 표준화된 변환기술을 제안하고 있다. NAT-PT는 기존의 IPv4망과 점점 그 범위가 확산되는 IPv6망 즉, 6Bone과의 통신이 가능하도록 제공되는 변환기술 중 하나로, 이종 IP망간의 통신을 위한 주소변환 및 프로토콜 변환에 대한 메커니즘을 제시하고 있다. 그러나 NAT-PT는 주소 및 프로토콜 변환과정에서 몇 가지 문제점을 가지고 있다. NAT-PT가 가진 문제 중 가장 큰 문제는 NAT-PT를 통해서는 어떠한 보안 서비스도 제공할 수 없다는 것이다. 이러한 NAT-PT의 보안 서비스 부재는 IPv4망과 IPv6망간의 통신에 있어 인터넷 상에 존재하는 수많은 부정적인 행위에 대해 어떠한 보호도 제공할 수 없게 한다.

따라서 이 논문은 기존의 IPv4망이 IPv6망으로 변환되는 과도기적 단계에서 요구되는 NAT-PT 변환기술을 분석하고, NAT-PT의 한계를 설명하며, NAT-PT의 한계 중 가장 큰 문제로 제시되는 보안문제를 해결하기 위한 방법 중 가장 먼저 수행되어야 하는 보안정책 협상을 제공하는 확장된 보안정책 프로토콜에 대해 제시한다. 이 논문에서 제시된 NAT-PT를 고려한 보안정책 프로토콜은 기존의 IETF의 draft로 제시된 SPP[3]를 확장함으로써 제공된다.

이 논문의 구성을 보면, 2장에서 NAT-PT를 분석하고 NAT-PT의 한계를 기술하며, 3장에서 기존의 보안정책 시스템과 보안정책 프로토콜에 대해 소개한다. 그리고 4장에서 NAT-PT를 통한 SPP가 가지는 문제점과 이러한 문제점을 고려한 확장된 SPP를 제시한다. 마지막으로 5장에서 결론 및 향후연구에 대해 기술한다.

2. NAT-PT

NAT-PT는 IPv4망과 IPv6망간의 통신을 제공해주는 메커니즘으로 IETF RFC2766[2]에 의해 표준화된 기술이다. NAT-PT는 크게 IPv4/IPv6간 통신시, IPv6 주소에 IPv4 주소풀(address pool)로부터 동적으로 선택된 IPv4 주소를 할당해 주는 NAT(Network Address Translation)[4] 기능과 SIIT(Stateless IP/ICMP Translator)[5] 프로토콜 변환 메커니즘을 제공하는 PT(Protocol Tranlsation) 기능, 그리고 응용에 따라 발생하는 추가적인 요구사항을 변환해주는 ALG (Application Level Gateway) 기능으로 이루어진다. (그림 2-1)은 이러한 NAT-PT의 구조를 나타낸다.



(그림 2-1) NAT-PT 구조

NAT-PT는 NIC(Network Interface Card)로부터 패킷을 캡쳐하여 IPv6 주소에 할당된 IPv4 주소가 현재 IPv4/IPv6 맵핑 테이블에 없으면 IPv4 주소풀로부터 동적으로 IPv4 주소를 선택하여 IPv6 주소에 할당하고, 그 결과를 IPv4/IPv6 맵핑 테이블에 기록한다. 이렇게 맵핑된 IP 주소를 이용하여 SIIT 프로토콜 변환 메커니즘은 IP 또는 ICMP를 변환한다. 그리고 상위 프로토콜을 검사하여 상위 프로토콜이 DNS이면 DNS-ALG를 통해 AAAA 레코드와 A 레코드의 변환 및 DNSv4와 DNSv6간의 주소 정보교환을 수행하고, FTP이면 FTP-ALG를 통해 확장된 FTP 명령어를 사용하는 FTPv6와 FTPv4간의 정보교환을 수행한다. 그리고 마지막으로 각 프로토콜 계층의 페이로드 길이 및 검사합(checksum) 값을 갱신하여 변환된 패킷을 목적지로 전송한다. 이때 한가지 주의할 점은 NAT-PT가 IPv4망과 IPv6망에 있는 호스트의 MAC 주소를 획득하기 위해 IPv4의 ARP와 IPv6의 ND(Neighbor Discovery)를 변환하거나 생성할 수 있어야 한다는 것이다.

NAT-PT는 하나의 IPv6 주소에 하나의 IPv4 주소가 맵핑 되어야 하므로, 많은 IPv4 주소가 필요하다. 실제로 IPv4 주소풀의 IP 주소가 모두 사용되고 나면, 그 이후의 새로운 IPv6 노드는 더 이상 IPv4망과 통신할 수 없게 된다. 이러한 NAT-PT의 IPv4 주소풀의 고갈문제를 해결하기 위한 것이 NAPT-PT(Network Address Port Translation Protocol Translation)이다. NAPT-PT는 포트를 이용해 각 통신을 구별하므로 더 이상 할당할 TCP 포트 또는 UDP 포트가 남아 있지 않게 될 때까지 하나의 IPv4 주소당 최대 63K TCP 통신 또는 UDP 통신을 지원할 수 있다.

이러한 NAT-PT는 그 특성상 다음과 같은 제약 및 단점을 가진다[2].

- **토폴로지 제약**

NAT-PT를 거쳐 IPv4망과 IPv6망간에 통신을 할 경우에는 한 세션에 대한 모든 응답과 요청이 동일한 NAT-PT를 거쳐 라우팅 되어야 한다. 그 이유는 NAT-PT의 IPv4/IPv6 맵핑 테이블에 등록되어 있지 않는 IP간의 통신은 모두 무효화 되기 때문이다. 이러한 라우팅 경로를 보장하기 위해서는 NAT-PT를 한 스텁 도메인에 유일한 경계 라우터로써 설치하는 것이다. 그러면 해당 도메인에서 나오거나 들어가는 모든 IP 패킷은 여기를 통과할 것이다. 이는 NAT의 일반적인 문제로써, RFC2663[6]에 자세히 설명되어 있다.

- **프로토콜변환 제약**

상당수의 IPv4 필드가 IPv6에서 의미가 변화되었으므로 직접적으로 변환될 수 없다. 예를 들어, IP 헤더의 옵션필

드의 의미 및 구문이 IPv6에서는 상당히 많이 변화되었다. IPv4와 IPv6 프로토콜 변환에 대한 상세한 내용은 SIIT에 따른다.

● 주소변환의 영향

NAT-PT는 IP 계층의 주소변환을 수행하므로, 상위계층에서 IP 주소를 사용하는 어플리케이션에 대해서는 정상적인 동작을 수행할 수 없다. 이 경우에는 해당 어플리케이션을 지원하는 ALG가 필요하다. 이는 NAT의 일반적인 문제로써, RFC2663에 자세히 설명되어 있다.

● 종단간 보안결여

NAT-PT가 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. 예를 들어, NAT-PT와 독립적인 종단간 IPSec 보안의 경우, IPSec의 특성상 다른 주소 영역사이(IPv4망과 IPv6망 사이)를 교차하는 것이 거의 불가능하다. IPSec 네트워크 레벨 보안을 추구하는 두 종단 노드들은 IPv4 또는 IPv6 중 하나를 둘 다 제공해야 한다.

● DNS 변환 및 DNSSEC

DNS-ALG는 일반 DNS 변환에는 사용될 수 있으나, 보안 DNS에는 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 종단노드는 NAT-PT에 의해 변형된 응답을 거부할 것이다. 그러나 좋은 점은 IPv4 영역으로부터 접근하는 IPv6 도메인내의 서버만이 이러한 제약을 겪게 된다는 것이다.

3. 보안정책 시스템

보안정책 시스템(Security Policy System)은 종단간의 안전한 통신 설정을 위해 같은 보안영역 내에서 뿐 아니라 다른 보안 영역의 호스트, 서브넷 혹은 망들의 정책정보에 접근하여 알아내고, 그 정책정보를 처리하기 위해 필요한 메커니즘을 제공하는 분산 시스템이다. 보안정책 시스템에 의해 다루어지는 정책정보는 여러 보안영역을 통과할 수 있다. 이러한 보안정책 시스템은 종단간의 통신과 관련된 주 보안 게이트웨이와 부 보안 게이트웨이를 발견하는 자동화된 메커니즘을 제공할 뿐만 아니라, 종단간 통신경로 상에 있는 보안 게이트웨이의 신원을 검증할 수 있다. 그리고 특정 보안 게이트웨이가 특정 호스트에 대한 권한을 갖는지를 검증할 수 있다.

3.1 보안정책 시스템 구성

보안정책 시스템은 각 보안영역에 대한 정책정보를 요청하는 정책 클라이언트 및 정책요청에 대해 응답하는 정책서버, 그리고 보안영역의 고유정보를 저장하는 마스터 파일과 여러 정책관련 정보를 저장하는 SPS DB(Security Policy System Database)로 구성된다.

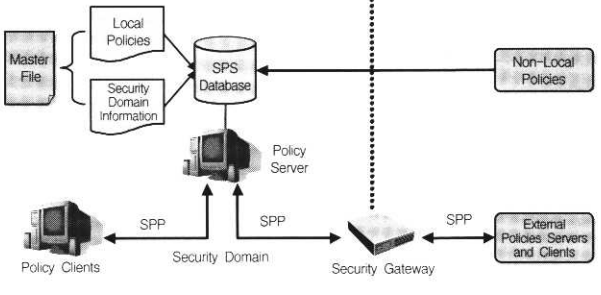
정책 클라이언트는 SPP(Security Policy Protocol)를 사용하여 정책서버에 정책정보를 요청하고, 정책서버로부터 응답이 수신되면 적절한 포맷으로 어플리케이션에게 전달한다. 그리고 정책서버는 정책 클라이언트와 다른 정책서버로부터 SPP를 사용한 정책요청을 수신하면 그것을 처리하고 적절한 응답을 요청자에게 제공한다. 또한 정책서버는 지역정책 및 비 지역정책에 대한 SPS DB를 유지한다.

마스터 파일은 특정 보안영역의 지역정책들과 그 보안영역에 관한 특정정보들을 포함하고 있으며, 그 구성은 <표 3-1>과 같다.

〈표 3-1〉 마스터 파일의 구성 항목

Certificate	유지자 정보에 의해 참조되는 하나 이상의 인증서를 가르킴(이 인증서에서 발견되는 공개키에 대응되는 개인키는 마스터 파일에 포함된 정보에 서명하기 위해 사용되고, 공개키는 무결성과 출처의 확실성(Authenticity)을 증명하기 위해 사용됨)
Maintainer	특정 마스터 파일 내의 정책 정보를 관리할 수 있는 권한를 가진 엔터티를 가르킴
Policy-Server	특정 보안영역에 대한 주와 부 정책서버의 신원을 기술함
Nodes	첨부된 정책들을 갖는 인터페이스 집합을 지정함(보안영역 내에는 최소한 하나 이상의 노드가 있어야 함)
Gateway	특정 보안영역의 정책을 실행하는 호스트와 연관된 인터페이스 집합을 지정함
Domain	보안영역에 속한 노드, 게이트웨이 및 정책서버들에 의한 보안영역 정의
Policy	정책들의 순서화된 집합

마지막으로 SPS DB는 마스터 파일로부터 오는 정보와 보안영역내의 모든 정책을 포함하는 지역정책 DB, 다른 보안영역들로부터 수신된 지역 및 비 지역정책을 포함하는 캐쉬 DB, 그리고 보안영역내의 모든 보안 호스트, 보안 게이트웨이, 그리고 보안정책 서버들의 리스트를 포함하는 보안영역 DB로 구성된다. (그림 3-1)은 지금까지 설명한 보안정책 시스템의 구성을 나타낸다.

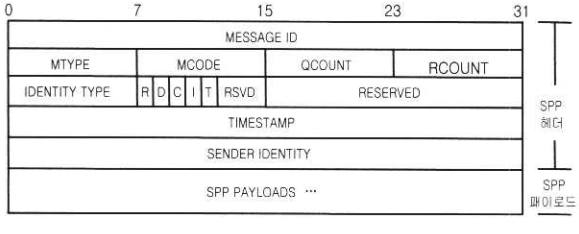


(그림 3-1) 보안 정책 시스템의 구성

3.2 보안정책 프로토콜

보안정책 시스템의 정책서버와 클라이언트는 SPP을 사용하여 정보를 교환하며, 이 프로토콜은 정책정보가 클라이언트와 서버에 의해 어떻게 교환되고, 처리되고, 보호되는지를 정의한다. SPP는 수송계층 프로토콜로 UDP 혹은 TCP를 사용하며, 포트는 501번을 사용한다. 만약 SPP가 UDP를 사용할 경우, 메시지의 길이는 IP 및 UDP 헤더를 제외한 512bytes로 제한되고, 만약 512bytes 보다 큰 메시지를 전송할 경우에는 단편화(fragmentation)가 허용된다. 그리고 SPP의 SPP-XFR 메시지는 반드시 TCP를 사용해야 한다. SPP가 제공하는 메시지의 종류는 다음과 같다.

- Query(SPP-QUERY) 메시지 : 호스트, 보안 게이트웨이 혹은 정책서버가 정책서버에게 특별한 정책정보를 요청할 때 사용하는 메시지로, 그 구성은 1개 이상의 Query 페이로드와 0개 이상의 Record 페이로드, 그리고 선택적인 서명(Signature) 페이로드로 이루어진다.
- Reply(SPP-REPLY) 메시지 : 정책서버가 특정 Query에 대해 응답하는 정책을 표현하는 메시지로, 그 구성은 1개 이상의 Query 페이로드와 0개 이상의 Record 페이로드, 그리고 선택적인 서명 페이로드로 이루어진다.
- Policy(SPP-POL) 메시지 : 정책서버로 업로드 되거나 서버로부터 다운로드 되는 정책정보를 표현하는 메시지로, 그 구성은 1개 이상의 Record 페이로드와 선택적인 서명 페이로드로 이루어진다.
- Policy Acknowledgment(SPP-POL_ACK) 메시지 : 정책(SPP-POL) 메시지에 대한 수신통지를 위한 메시지로, 그 구성은 선택적인 서명 페이로드로만 이루어진다.
- Transfer(SPP-XFR) 메시지 : 정책서버들간에 벌크(bulk) 정책정보의 교환에 이용되는 메시지로, 그 구성은 1개 이상의 Record 페이로드와 선택적인 서명 페이로드로 이루어진다.
- Keep alive(SPP-KEEP_ALIVE) 메시지 : 정책서버가 보안 게이트웨이나 다른 감시장치들에게 서버의 상태를 알리기 위해 사용되는 메시지로, 그 구성은 선택적인 서명 페이로드로만 이루어진다.



(그림 3-2) SPP 메시지 포맷

SPP 메시지의 포맷은 (그림 3-2)와 같으며, 모든 SPP 메시지는 메시지 헤더 부분과 페이로드 부분으로 구성된다. 메시지 헤더 부분은 모든 SPP 메시지에 대해 동일한 필드들로 구성되고, 페이로드 부분은 메시지 타입에 따라 다르며 3가지 페이로드 타입들의 조합으로 구성된다.

SPP 메시지 헤더의 각 필드들은 다음과 같이 정의된다.

- **MESSAGE ID**
  - 메시지와 그들의 Reply를 대응시키기 위해 사용 (예 : Query 메시지에 대해 Reply 메시지를, 정책 메시지에 대해 정책 수신통지 메시지를 대응)
  - 이 값은 0에서 시작, 모든 새 메시지에 대해 1씩 증가
- **MTYPE**
  - SPP 메시지 타입을 표시.

〈표 3-2〉 MTYPE 필드 값

값	메시지 타입
0	Value Not Assigned
1	SPP-QUERY
2	SPP-REPLY
3	SPP-POL
4	SPP-POL_ACK
5	SPP-XFR
6	SPP-KEEP_ALIVE
7~250	Reserved to IANA
251~255	Private use

- **MCODE**
  - 이 메시지에 대한 정보를 제공, 모든 메시지 타입이 이 MCODE 값을 공통으로 정의하여 사용한다.

〈표 3-3〉 MCODE 필드 값

코드 필드	Action 타입
0	Value Not Assigned
1	Message accepted
2	Denied, administratively prohibited
3	Denied, timestamp failed
4	Denied, failed signature
5	Denied, insufficient resources
6	Denied, malformed message
7	Denied, unspecified
8	Partially available
9	Unavailable
10	Communication prohibited
11	Partially available, server unreachable
12~250	Reserved to IANA
251~255	Private use

- **QCOUNT**
  - 메시지에 포함된 Query 페이로드의 수.

- **RCOUNT**
  - 메시지에 포함된 레코드 페이로드의 수.

- **IDENTITY TYPE**
  - Sender Identity 필드에서 발견된 identity의 유형.

〈표 3-4〉 IDENTITY TYPE 필드 값

값	메시지 타입
0	Value Not Assigned
1	IPV4_ADDR
2	IPV6_ADDR
3	Host DNS Name
4~250	Reserved to IANA
251~255	Private use

- **R**
  - Raw policy flag(즉, 이 flag가 set되어 있으면, 정책서버는 그가 반환하는 정책에 대해 정책결정(resolution)을 해서는 안 된다).

- **D**
  - Domain flag(즉, 이 flag가 set되어 있으면, 정책결정을 요구한 호스트에 대한 transitively 권한을 갖는 마지막 정책서버만이 그 정책을 resolve 할 수 있다).

- **C**
  - Don't cache flag(즉, 이 flag가 set되어 있으면, 정책을 캐쉬해서는 안된다).

- **I**
  - Ignore cache flag(즉, 이 flag가 set 되어 있으면, query를 처리할 때 캐쉬를 참조해서는 안된다).

- **T**
  - No chain-of-trust flag(즉, 이 flag가 set되어 있으면, 클라이언트가 그의 서버에게 chain-of-trust 정보가 필요하지 않음을 알리는 것이다. 이 flag는 정책서버가 set할 수 없다).

- **TIMESTAMP**
  - Replay attacks에 대해 제한된 protection을 위해 사용되는 timestamp(이는 Network Time Protocol에 의해 기술된 대로 포맷).

- **SENDER IDENTITY**
  - SPP 메시지의 송신자(호스트, 보안 게이트웨이 혹은 정책 서버)의 identity.
  - IDENTITY_TYPE 필드는 이 필드의 content의 포맷을 나타냄.
  - 이 필드는 IP 주소 범위나 wildcards를 허용하지 않음.

〈표 3-5〉 SENDER INDENTITY 필드 값

Identity 타입	Sender Identity
IPV4_ADDR	IPV4 주소
IPV6_ADDR	IPV6 주소
Host DNS Name	Host DNS Name

- **SPP PAYLOADS**
  - SPP 페이로드는 정책정보에 대한 요청을 표현하기 위한 Query 페이로드, 정책정보의 표현을 위한 Record 페이로드, 그리고 전체 SPP 메시지에 대해 전자서명 함수를 적용한 결과 데이터를 포함하는 서명 페이로드를 정의함.

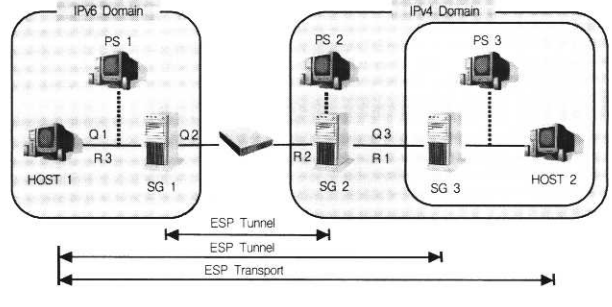
4. NAT-PT를 고려한 보안정책 시스템

현재 사용중이 인터넷이 IPv4에서 IPv6로 진화하기 위해서는 과도기적인 단계로 IPv4망과 IPv6망간의 변환이 자유로운 NAT-PT 변환기술이 필요하다. 하지만 NAT-PT는 그 구조적 특성상 앞으로의 인터넷 필수사항 중 하나인 보안에 대한 한계를 가지고 있다.

이 장에서는 이러한 NAT-PT의 한계를 극복하기 위한 IPSec 보안 서비스를 지원하는 보안정책 시스템에 대해 제안한다.

4.1 NAT-PT상의 SPP 고려사항

이 절에서는 (그림 4-1)와 같은 네트워크 구조에서 보안정책 협상을 위한 SPP(Security Policy Protocol)가 NAT-PT를 통해 수행될 때 고려해야 할 사항을 검토한다. 참고로 (그림 4-1)에서 PS는 보안 정책서버를, SG는 보안 게이트웨이를 의미한다.

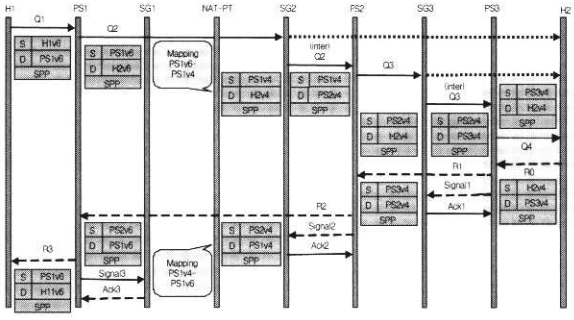


(그림 4-1) NAT-PT상의 SPP 수행 네트워크

SPP는 그 자체적으로 IPv4 및 IPv6 주소를 모두 적용할 수 있도록 설계되어 있으므로, 여기서는 단지 SPP가 NAT-PT를 통해 통신을 할 때 어떠한 문제들이 발생하는지에 대해 알아본다.

(그림 4-2)는 HOST1과 HOST2 사이의 통신을 위한 보안협상의 SPP 전달과정으로, SPP을 전송하는 IP 헤더의 변

환과정을 보여주고 있다. 단, Q4와 R0 메시지는 PS3에 HOST2의 정책이 캐쉬되어 있지 않을 경우 발생하는 메시지들이다. (그림 4-2)에서도 알 수 있듯이, NAT-PT는 그 특성상 IPv6망의 고유한 IPv6 주소에 대해서만 IPv4 주소 맵핑 테이블(mapping table)을 유지한다. 왜냐하면, IPv4망의 IPv4 주소는 NAT-PT의 Prefix에 자신의 IPv4 주소를 합한 [Prifix::IPv4] 주소 형태를 가지므로 쉽게 IPv4 주소에서 IPv6 주소로 변환할 수 있고, 또한 역으로도 변환할 수 있기 때문이다. 그러므로 SPP를 운반하는 IP 헤더에 대해서는 아무런 문제도 발생하지 않는다. 문제는 SPP내의 IP 주소와 서명 페이로드이다.



(그림 4-2) 동작 시퀀스 차트

우선 SPP내의 IP 주소와 서명 페이로드에 대해 NAT-PT가 아무런 작업도 수행하지 않는다고 가정해 보자. 이러한 가정에서 IPv4망과 IPv6망에 존재하는 모든 정책서버는 IPv4 및 IPv6 주소를 모두 수용하는 정책을 설정할 수 있어야 한다.

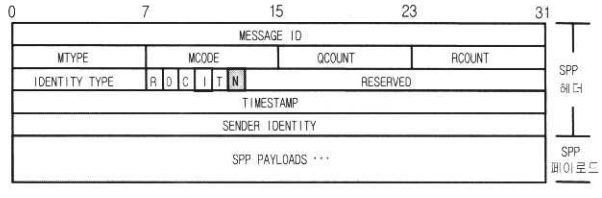
먼저 IPv6망에서 IPv4망으로 정책을 요청할 경우를 살펴보면, PS1는 HOST1으로부터 수신한 Q1 메시지를 처리하는데 아무런 문제도 없다. 그리고 PS1이 송신한 Q2 메시지의 IP 헤더 주소가 NAT-PT에 의해 바뀌게 되더라도 SPP내에 원래의 소스 IP 주소가 존재하므로 SG2에 의해 전달받은 Q2 메시지에 대해 PS2는 서명을 검증할 수 있다. 결국 PS2가 송신한 Q3 메시지에 대해서도 PS3는 문제없이 수행 될 수 있다. 정책응답(R1~R3, Signal1~Signal3, Ack1~Ack3)의 경유에도 마찬가지로 문제없이 수행될 수 있다. 하지만 협상된 정책을 수행하기 위해서는 정책서버가 보안 게이트웨이에게 보내는 정책 메시지(SPP-POL : Siganl1~Signal3)는 약간 다르게 처리되어야 한다. 보안 게이트웨이가 정책서버에 의해 협상된 정책을 수행하기 위해서는 해당 네트워크의 IP 주소가 필요하다. 다시 말해, IPv4망에서 정책을 수행하기 위해서는 IPv4 주소가, IPv6 망에서 정책을 수행하기 위해서는 IPv6 주소가 필요하다. 즉, 위의 예와 같이 NAT-PT가 SPP내의 IP 주소에 대해 아무런 관여도 하지 않으면 HOST1은 IPv6 주소를 가지고 HOST2는 IPv4 주소를 가지게 된다. 결국 PS3가 협상된 정책을 반영하기 위해 SG3에게 Signal1를 전송하더라도 SG3는 실제 HOST1과 HOST2의 통신에서 Signal1에 포함된 정책을 수행할 수 없다. 왜냐하면 실제 HOST1과 HOST2의 통신에서는 HOST1의 IPv6 주소가 NAT-PT에 의해 IPv4 주소로 맵핑되기 때문에 정책협상에 의해 전송된 HOST1의 IPv6 주소를 무의미하기 때문이다. 이러한 문제를 해결하기 위해서는 정책협상 과정에서 NAT-PT가 SPP를 수신하면 NAT-PT에 의해 맵핑된 HOST1의 IPv4 주소를 SPP에 추가해 주어야 한다. 이렇게 하면 보안 게이트웨이는 수신된 Signal에서 해당 네트워크의 IP 주소만을 참조하면 되므로, 앞에서 설명한 문제를 해결할 수 있다. 물론 NAT-PT에는 SPP를 처리할 수 있는 SPP-ALG라는 기능이 추가되어야 한다.

앞에서 설명한 문제를 해결하기 위한 또 다른 방법으로, SPP-ALG로 SPP내의 IP주소를 아예 해당 네트워크의 주소 형식으로 변환해 줄 수도 있다. 하지만 NAT-PT의 특성상 맵핑된 IPv4 주소는 동적으로 할당되므로 신뢰할 수 없을 뿐만 아니라, 서명을 검증하는데 사용할 수도 없다.

반대로 IPv4망에서 IPv6망으로 정책을 요청할 경우, SPP내의 IP 주소만 틀릴 뿐 위의 예와 비슷하다. 결론적으로 NAT-PT를 통한 보안정책을 협상하기 위해서는 보안정책 프로토콜인 SPP에 새로운 기능이 추가되어야 한다.

4.2 확장된 보안정책 프로토콜

(그림 4-3)의 SPP 메시지 헤더 포맷은 기존의 SPP 메시지 헤더 포맷에 NAT-PT 발견기능 및 NAT-PT 맵핑 페이로드와 NAT-PT 서명 페이로드를 추가하기 위해 수정된 헤더 포맷이다.



(그림 4-3) 확장된 SPP 메시지 헤더 포맷

기존의 SPP 메시지 헤더 포맷에서 추가된 필드는 다음과 같이 정의된다.

- **N**
  - NAT-PT flag(즉, 이 flag가 set되어 있으면, 정책협상 과정 중 NAT-PT에 의한 주소 변환이 일어났음을 나타냄).

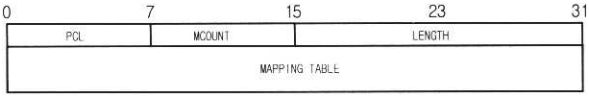
추가된 N 플래그(NAT-PT flag)는 SPP가 NAT-PT를 거칠 경우 NAT-PT의 SPP-ALG에 의해 설정되는 플래그이다. 이때 SPP-ALG는 SPP의 I 플래그(Ignore cache flag)를 설정하여 정책협상시 캐쉬를 참조하지 못하도록 설정한다.

왜냐하면, NAT-PT에 의해 맵핑된 IPv4주소는 통신 세션을 열할 때 마다 랜덤하게 설정되므로 항상 새로운 정책을 협상하도록 해야 한다.

그리고 기존의 SPP에서 선택적으로 이루어졌던 서명 페이로드는 SPP의 무결성과 원격지 인증을 위해 반드시 모든 SPP에 추가되어야 하며, 서명 범위는 NAT-PT에 의해 중간에 변화될 수 있는 플래그를 제외하고는 기존의 SPP와 동일하다.

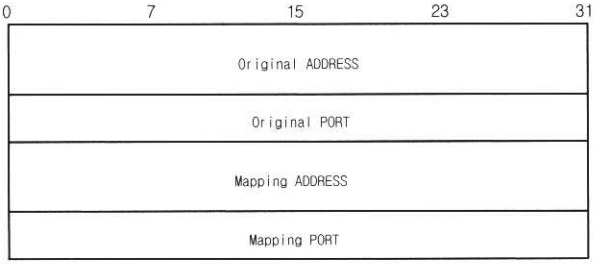
4.2.1 NAT-PT 맵핑 페이로드

NAT-PT 맵핑 페이로드는 NAT-PT에 의해 변환되는 주소 테이블을 표현할 수 있다. NAT-PT 맵핑 페이로드는 NAT-PT의 SPP-ALG에 의해 추가되며, 기존의 SPP내의 페이로드를 보고, 주소 맵핑이 필요한 모든 주소에 대해 맵핑 페이로드를 생성한다. 맵핑 페이로드를 가진 SPP를 수신한 정책서버나 호스트는 맵핑 페이로드의 맵핑 테이블을 SPP의 Query와 Record 페이로드에 적용하여 정책 결정을 수행한다.



(그림 4-4) NAT-PT 맵핑 페이로드 포맷

- **PCL**
  - 페이로드 클래스. NAT-PT 맵핑 페이로드의 값은 4.
- **MCOUNT**
  - 페이로드에 포함된 주소 맵핑 테이블의 수.
- **LENGTH**
  - Mapping table 필드의 길이.
- **MAPPING TABLE**
  - MCOUNT 만큼의 주소 맵핑 정보를 가지는 가변길이 필드이다.
  - MAPPING TABLE의 모든 필드는 기존 SPP의 정책 속성 인코딩 포맷에 의해 기술되며, (그림 4-5)와 같은 포맷으로 이루어진다.

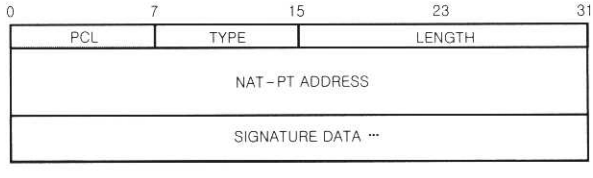


(그림 4-5) 주소 맵핑 테이블

  - Original ADDRESS : NAT-PT에 의해 주소변환이 수행되기 이전의 주소. 허용되는 인코딩 포맷의 DATA_TYPE 값은 1과 2이다.
  - Original PORT : NAT-PT에 의해 포트변환이 수행되기 이전의 포트. 허용되는 인코딩 포맷의 DATA_TYPE 값은 19이며, RESERVED 영역에서 새로운 포트 데이터 타입을 정의하여 사용할 수도 있다.
  - Mapping ADDRESS : NAT-PT에 의해 주소변환이 수행된 주소. 허용되는 인코딩 포맷의 DATA_TYPE 값은 1과 2이다.
  - Mapping PORT : NAT-PT에 의해 포트변환이 수행된 포트. 허용되는 인코딩 포맷의 DATA_TYPE 값은 21이며, RESERVED 영역에서 새로운 포트 데이터 타입을 정의하여 사용할 수도 있다.

4.2.2 NAT-PT 서명 페이로드

NAT-PT 서명 페이로드는 수정된 SPP 메시지 헤더 포맷의 N 플래그가 설정되면 반드시 추가되어야 할 페이로드로, NAT-PT에 의해 추가되는 페이로드에 대한 무결성과 원격지 인증을 수행한다. NAT-PT 서명 페이로드는 전체 SPP 메시지에 대한(NAT-PT 서명 페이로드의 서명 data 필드 제외) 전자서명 함수에 의해 생성된 데이터를 포함한다. 전자서명 함수는 NAT-PT에 의해 선택된다.



(그림 4-6) NAT-PT 서명 페이로드 포맷

- **PCL**
  - 페이로드 클래스. NAT-PT 서명 페이로드의 값은 5.
- **TYPE**
  - 사용된 서명 알고리즘을 기술.
  - 현재 정의된 타입은 기존 SPP의 서명 타입과 동일하다.
- **LENGTH**
  - 서명 data 필드의 길이.
- **NAT-PT ADDRESS**
  - NAT-PT의 주소로써 NAT-PT 서명을 식별하기 위해 사용된다. 이 필드는 기존 SPP의 정책 속성 인코딩 포맷에 의해 기술되는 가변길이 필드이다.
  - 허용되는 인코딩 포맷의 DATA_TYPE 값은 1과 2이다.

- **서명 DATA**
  - 전체 SPP 메시지에 대해(NAT-PT 서명 페이로드의 서명 data 필드 제외) 전자서명 함수를 적용시킨 결과로 구성되는 가변 길이 필드.

5. 결론 및 향후연구

IPv4망과 IPv6망간의 통신을 위해 주소변환과 프로토콜 변환을 수행하는 NAT-PT는 그 특성상 응용 프로토콜내에 존재하는 IP 주소에 대해서는 ALG를 통해 개별적으로 변환해 주어야 한다. 하지만 보안정책 협상에 사용되는 SPP내의 IP 주소를 NAT-PT의 ALG에 의해 변환하게 되면 실제 보안정책 수행에 사용되는 개체의 신원을 보장할 수 없을 뿐만 아니라 SPP에서 제공되는 서명을 확인할 수도 없게 된다. 반면 SPP내의 IP 주소에 대해 NAT-PT가 어떠한 변환도 수행하지 않고 정책협상을 수행하면, 정책협상 과정에는 아무런 문제도 발생시키지 않으나 협상된 정책을 수행할 경우에는 NAT-PT에 의해 변환된 IP 주소로 인해 통신 개체에 대한 신원을 확인할 수 없게 된다.

이러한 문제를 해결하기 위해 이 논문에서는 기존의 SPP에 정책협상 과정에 NAT-PT를 발견하는 기능과 보안정책 시스템에 의해 협상된 정책이 수행될 때 필요한 각 대상의 실제 IP 주소와 NAT-PT에 의해 맵핑된 IP 주소를 각 정책 수행 노드에 전달하는 기능을 추가한 확장된 SPP를 제시하였다. 이러한 확장된 SPP에 의해 각 보안개체에 전달된 IPv4/IPv6 주소 맵핑 테이블은 보안정책 수행시 보안 게이트웨이에 의해 각 통신 개체의 맵핑된 IP 주소로부터 신원을 확인할 수 있을 뿐 아니라, SPP의 서명 또한 확인할 수도 있다. 그리고 NAT-PT를 통한 IPSec 보안 서비스를 제공하기 위해 IPv4/IPv6 주소 맵핑 테이블을 참조할 수도 있다.

하지만 이 논문에서는 확장된 SPP에 의해 제공된 IPv4/IPv6 맵핑 테이블을 사용하여 실제 NAT-PT를 통한 IPSec 보안 서비스에 대해 기술하고 있지 않으므로, 향후에는 이 논문에서 제시한 확장된 SPP를 사용하여 어떻게 NAT-PT를 통한 IPSec 보안 서비스를 제공할 것인가에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture," RFC2373, 1998.

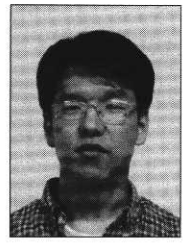
[2] G. Tsirtsis, P. Srisuresh, "Network Address Translation Protocol Translation (NAT-PT)," RFC2766, 2000.

[3] L. Sanchez, M. Condell, "The Security Policy Protocol," draft-ietf-ipsp-spp-01.txt, January, 2002.

[4] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)," RFC1631, 1994.

[5] Nordmark, E., "Stateless IP/ICMP Translator (SIIT)," RFC 2765, 2000.

[6] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC2663, 1999.

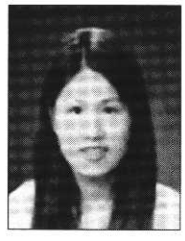


현 정 식

e-mail : ackbar@cnlab.chungbuk.ac.kr
1999년 청주대학교 컴퓨터정보공학과
2001년 청주대학교 전자계산학과(MS)
2001년~현재 충북대학교 전자계산학과 박사과정
관심분야 : 네트워크 보안, P2P, 그리드

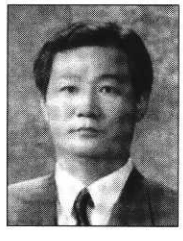
황 윤 철

e-mail : ychwang@kebi.com
1994년 한남대학교 전자계산공학과
1996년 한남대학교 전자계산공학과(MS)
1999년~현재 충북대학교 대학원 전자계산학과 박사과정수료
관심분야 : 인터넷, 정보보호, 네트워크 보안



엄 남 경

e-mail : family@cnlab.chungbuk.ac.kr
1999년 충북대학교 컴퓨터과학과
2002년 충북대학교 전자계산학과(MS)
2000년~2001년 한국전자통신연구원 위촉연구원
2002년~현재 충북대학교 전자계산학과 박사과정 재학
관심분야 : 프로토콜 테스팅, 네트워크 장애 관리



이 상 호

e-mail : shlee@cbucc.chungbuk.ac.kr
1976년 숭실대학교 전자계산학과
1981년 숭실대학교 전자계산학과(MS)
1989년 숭실대학교 전자계산학과(PHD)
1976년~1979년 한국전력 전자계산소
1981년~현재 충북대학교 전기전자및 컴퓨터공학부 교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture