NAT-PT를 고려한 단대단 IPSec 보안 메커니즘

(An End-to-end IPSec Security Mechanism considering NAT-PT)

현 정 식 † 황 윤 철 † 정 윤 수 †† 이 상 호 †††
(Jeung-Sik Hyun) (Yoon-Cheol Hwang) (Yoon-Su Jung) (Sang-Ho Lee)

요 약 RFC2766에 정의된 NAT-PT(Network Address Translation-Protocol Translation)는 IPv6 디바이스들이 IPv4 디바이스들과 서로 통신할 수 있도록 제공된 IPv4/IPv6 변환 메커니즘이다. 그러나 NAT-PT는 IPSec의 주요 목적인 종단간 보안을 제공하기 못하는 제약을 가지고 있으므로 기밀성, 인증, 무결성과 같은 보안 서비스를 제공하지 못한다. 이 논문에서는 IPSec 보안 서비스를 제공하기 위한 SNAT-PT(Secure NAT-PT)와 이를 기반으로 동작하는 보안 호스트 구조를 제안한다. 그리고 제안된 구조에서 종단간 IPSec 프로토콜이 동작함을 보이기 위하여 더미(dummy) IP헤더를 이용한 터널링 기법을 제시한다.

키워드 : 주소변환, 프로토콜변환, IPSec 보안

Abstract Network Address Translation-Protocol Translation(NAT-PT) is an IPv4/IPv6 translation mechanism, as defined in RFC2766, allowing IPv6-only devices to communicate with IPv4-only devices and vice versa. But NAT-PT has the restriction that applies to IPv4 NAT where NAT-PT does not provide end-to-end security, which is a major goal of IPSec. Therefore it cannot support security services such as confidentiality, authentication, and integrity. In this paper, we propose secure NAT-PT(SNAT-PT) and the corresponding secure host architecture to support IPSec security service. And also tunneling scheme using dummy IP header is presented to show the valid operation of end-to-end IPSec protocol on the proposed architectures.

Key words : NAT(Network Address Translation), PT(Protocol Translation), IPSec Security

1. 서 론

현재 사용되고 있는 IPv4주소는 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 주소 수요를 충족시킬 수 없다.

따라서, IETF IPv6워킹그룹은 1995년 RFC1883[1]을 시작으로 지금까지 128비트 주소체계의 IPv6를 연구해 왔다. IPv6는 거의 무한개의 (3.4×10^{38}) 인터넷 주소를 제공함으로써, 이러한 주소고갈 문제를 근본적으로 해결할 뿐 아니라, 기존 IPv4에서의 멀티캐스트나 QoS, 그리고 보안 등의 구조적 어려움을 해결한다. 현재 세계 각국은 IPv6의 개발 및 확산을 위해 노력하고 있는데, 유럽은 무선인터넷 서비스 제공을, 일본은 무선인터넷과 정보가전 분야를, 그리고 미국은 중국 등을 포함한 세계 시장을 겨냥해 IPv6 기술을 발전시키고 있다. 현재 IPv6는 6Bone이라는 가상망을 이용하여 1996년부터 현재까지 운영되고 있다.

현재 IPv4에서 IPv6로의 진화는 2010년까지 단계적으로 변환될 것으로 예상되며, IETF에서는 이 기간동안 IPv4망과 IPv6망간의 통신을 지원하기 위해 NAT-PT[2]라는 변환기술을 제안하고 있다. NAT-PT는 기존의 IPv4망과 점점 그 범위가 확산되는 IPv6망 즉, 6Bone과의 통신이 가능하도록 제공되는 변환기술 중 하나이다. NAT-PT는 IPv4망과 IPv6망간의 통신을 위한 주소변환 및 프로토콜 변환에 대한 메커니즘을 제시하고 있으며, 이 과정에서 NAT-PT는 몇 가지 문제점을 가

† 학생회원 : 충북대학교 전자계산학과
ackbar@netsec.chungbuk.ac.kr
ychwang66@kebi.com
†† 비 회 원 : 충북대학교 전자계산학과
bukmunro@hanmail.net
††† 종신회원 : 충북대학교 전기전자컴퓨터공학부 교수
shlee@cbucc.chungbuk.ac.kr
논문접수 : 2002년 4월 2일
심사완료 : 2003년 6월 18일

지고 있다. NAT-PT가 가진 문제점 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 불법적인 행위에 대해 어떠한 보호도 제공할 수 없게 한다. 현재 이러한 NAT-PT의 보안 문제를 해결하기 위해 제안된 보안 메커니즘은 없으며, 단지 NAT-PT통해 IPSec을 제공할 경우 발생하는 문제점만이 인터넷 Draft로 제시되어 있을 뿐이다. 하지만 NAT-PT가 아닌 기존 NAT만을 위한 보안 서비스는 RSIP(Real Specific IP)[3]라는 새로운 변환기술에 의해 제공되고 있다.

RSIP는 기존 NAT의 문제점인 종단간 통신 연결성과 무결성을 제공하기 위해 터널링 기법을 사용한 주소 변환 방식으로 기존의 NAT를 대체할 수 있는 메커니즘이다. 하지만 RSIP는 RSIP 게이트웨이를 기준으로 Inbound되는 패킷과 Outbound되는 패킷이 서로 다르므로 IPv6로의 진화 과정에서 필요한 동일 IPv4/IPv6호스트 구조를 가질 수 없다. 그리고 IPSec이 터널링을 사용할 경우, IPSec 보안 게이트웨이가 RSIP 게이트웨이의 역할도 같이 수행해야 하는 문제점을 가지고 있다.

이 논문에서는 기존의 IPv4망이 IPv6망으로 진화하는 과정에서 요구되는 NAT-PT 변환기술을 분석하고, NAT-PT의 한계를 설명하며, 가장 큰 문제로 대두되는 보안 문제를 해결하기 위한 메커니즘을 제시한다. 이 논문은IKE(Internet Key Exchange)[4]에 의해 협상된 AH(Authentication Header)[5] 및 ESP(Encapsulating Security Payload)[6]를 통해 보안 서비스를 제공한다.

이 논문의 구성은, 2장에서 NAT-PT를 분석하고 NAT-PT의 한계를 기술하며, 3장에서 IPSec의 IKE 및 AH/ESP에 대해 소개한다. 그리고 4장에서 NAT-PT를 통한 IPSec이 가지는 문제점을 분석하고, 5장에서 NAT-PT를 고려한 SNAT-PT와 보안 호스트 구조를 제시한다. 6장에서는 제시된 보안구조를 통한 단-대-단 IPSec 보안 서비스를 예시하고, 마지막으로 7장에서 결론에 대해 기술한다.

2. NAT-PT

NAT-PT는 IPv4와 IPv6간의 통신을 제공해 주는 메커니즘으로 IETF RFC2766[2]에 제시된 기술이다. NAT-PT는 크게 IPv4/IPv6간 통신시, IPv6 주소에 IPv4 주소풀(address pool)로부터 동적으로 선택된 IPv4 주소를 할당해 주는 NAT(Network Address Translation)[7] 기능과 SIIT(Stateless IP/ICMP Translator)[8] 프로토콜 변환 메커니즘을 제공하는 PT(Protocol Tranlsation) 기능, 그리고 응용에 따라

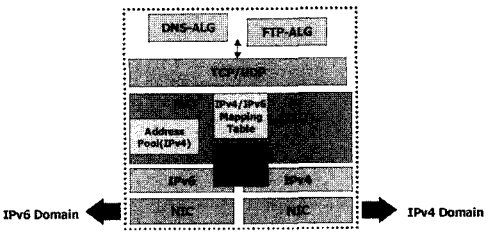


그림 1 NAT-PT 구조

발생하는 추가적인 요구사항을 변환해주는 ALG (Application Level Gateway) 기능으로 이루어진다. 그림 1은 이러한 NAT-PT의 구조를 나타낸다.

NAT-PT는 NIC(Network Interface Card)로부터 패킷을 캡쳐하여 해당 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 맵핑되어야 하므로, 많은 IPv4 주소가 필요하다. 실제로 IPv4 주소풀의 IP 주소가 모두 사용되고 나면, 그 이후의 새로운 IPv6 노드는 IPv4 망과 통신할 수 없게 된다. 이러한 NAT-PT의 IPv4 주소풀의 고갈문제를 해결하기 위한 방법이 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 IPv4 망과 IPv6 망이 통신할 경우, 한 세션에 대한 모든 응답과 요청은 동일한 NAT-PT

를 거쳐 라우팅되어야 한다. 그 이유는 NAT-PT의 IPv4/IPv6 맵핑 테이블에 등록되어 있지 않는 IP통신은 모두 무효화 되기 때문이다. 이러한 라우팅 경로를 보장하기 위해서는 NAT-PT를 한 스텝 도메인에 유일한 경계 라우터로써 설치하는 것이다[9].

• 프로토콜변환 제약

상당수의 IPv4 필드가 IPv6에서 상당히 많이 변화되었으므로 직접적인 의미 변환을 수행할 수 없다. IPv4와 IPv6 프로토콜 변환에 대한 상세한 내용은 SIIT에 따른다.

• 주소변환의 영향

NAT-PT는 IP계층의 주소변환을 수행하므로, 상위계층에서 IP주소를 사용하는 어플리케이션은 정상적인 동작을 수행할 수 없다. 이 경우에는 해당 어플리케이션을 지원하는 ALG가 필요하다.

• 종단간 보안결여

NAT-PT가 제안하고 있는 가장 중요한 제약 중 하나가 바로 종단간 네트워크 계층 보안이 불가능하다는 것이다. 또한 전송 및 응용 계층 보안에서 IP주소를 사용할 경우에도 불가능하다. 이는 NAT 기능의 자체적인 한계이다. 예를 들어, NAT-PT와 독립적인 종단간 IPSec의 경우, IPSec의 특성상 서로 다른 주소 영역사이(IPv4 망과 IPv6 망 사이)를 교차하는 것이 불가능하다. 따라서 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 이러한 단점은 IPv4 영역으로부터 접근하는 IPv6 도메인내의 서버만이 이러한 제약을 겪게 된다.

3. IPSec

3.1 IKE

이 절에서는 IPSec를 수행하기 위한 키 교환과 관련된 IKE에 대해 기술한다. IKE는 RFC2407[10]에 기술된 IPSec DOI(Domain of Interpretation)를 수용하고 있는 ISAKMP(Internet Security Association and Key Management Protocol)[11]에 의해 수행되는 키 교환에 대해 정의하고 있다.

ISAKMP는 SA(Security Association) 관리를 위한 구조 및 인터넷을 위한 암호학적 키 설정에 대해 정의하고 있으며, 다양한 DOI에서 정의한 교환 및 페이로드, 그리고 처리지침 등을 수용할 수 있다. 하지만 ISAKMP는 인증 및 키 교환을 위한 프레임워크 만을 제공할 뿐, 키 교환에 대해서는 정의하고 있지 않다. 즉, ISAKMP는 여러 가지 상이한 키 교환들을 지원하기 위해 키 교환과는 독립적으로 설계된 것으로, 키 교환에 대해서는 IKE에 의해 정의된다.

3.1.1 ISAKMP 개요

ISAKMP는 SA 설정, 협상, 변경, 삭제를 행하기 위한 절차 및 패킷 형식을 정의하고 있으며, 키 생성 데이타와 인증 데이타를 교환하기 위한 페이로드를 정의하고 있다. 그리고 ISAKMP는 SA 관리 및 키 관리를 키 교환의 세부사항과 완전히 분리하기 위해 키 교환 프로토콜과는 구별된다. 즉, 각각의 다른 보안 특성을 갖는 많은 키 교환 프로토콜이 존재할 수 있으며, ISAKMP는 이러한 키 교환 프로토콜들을 위한 SA 협상, 변경, 삭제에 대한 공통된 프레임워크를 제공한다.

ISAKMP의 목적은 네트워크 스택의 모든 계층에 존재하는(IPSec, TLS, TLSP, OSPF 등) 보안 프로토콜을 위한 SA 협상을 지원하는 것이다. 이렇게 ISAKMP로 SA 관리를 한 곳에 집중시킴으로써 각 보안 프로토콜들의 기능이 중복되는 것을 줄일 수 있을 뿐만 아니라, 서비스 스택 전체에 대한 SA 협상을 한번에 수행할 수도 있다.

ISAKMP는 두 단계의 협상을 제공하고 있다. 첫번째 단계는 두 ISAKMP 서버들간 ISAKMP SA를 설정하는 것으로, 실제 데이타 전송시 사용할 보안 프로토콜의 SA에 대한 협상을 보호하기 위해 사용된다. 두 번째 단계는 실질적으로 트래픽을 보호하는 보안 프로토콜에 대한 SA를 설정하는 것이다.

3.1.2 IKE 개요

IKE는 키 교환에 대해 정의하고 있으며, 두 단계에 걸쳐 처리된다. 첫번째 단계인 Phase 1은 두 ISAKMP 종단간 안전한 통신을 지원하기 위한 인증된 채널을 생성한다. 이 과정을 ISAKMP SA라 부르며, Main Mode와 Aggressive Mode에 의해 수행된다.

두 번째 단계인 Phase 2는 IPSec이나 키 재료 그리고/또는 파라메터 협상을 필요로 하는 다른 서비스를 대신한 SA협상 과정이다. 이 과정은 Quick Mode에 의해 수행된다. New Group Mode는 실제적으로 Phase 1도 Phase 2도 아니지만 Phase 1 이후에만 수행되며, 앞으로의 협상에서 사용될 수 있는 새로운 그룹을 생성하기 위한 서비스를 제공한다.

ISAKMP SA는 양방향으로 한 번 설정되면 어느 방향으로든 Quick Mode, Informational 또는New Group Mode를 시작할 수 있다. 기본 ISAKMP 문서에 의하

면, ISAKMP SA는 Initiator's Cookie와 그 다음에 오는 Responder's Cookie에 의해 식별된다. Phase 1 교환에 있어서 각 종단의 역할은 Cookie의 생성자에 의해 결정된다. Phase 1 교환에 의해 생성된 Cookie는 ISAKMP SA와 관계없이 Quick Mode, Informational 또는New Group Mode를 확인하는데 사용될 수 있다. 그러므로 Cookie는 ISAKMP SA가 변경되었을 때, 스왑(swap) 되어서는 안된다.

ISAKMP 과정은 필요시 매우 빠른 키 교환을 수행하도록 구현될 수 있다. 즉, 하나의 Phase 1 협상이 하나 이상의 Phase 2 협상에 사용될 수도 있고, 하나의 Phase 2 협상이 여러 개의 SA를 요청할 수도 있는 것이다. 이러한 최적화는 1회미만의 SA 왕복뿐만 아니라 1번 미만의 DH(Diffie-Hellman) 지수 계산을 사용하도록 구현될 수 있다. Phase 1의 Main Mode는 신원 보호(Identity Protection)를 제공한다. 만약 신원 보호가 필요하지 않으면, Aggressive Mode가 메시지 왕복을 줄이기 위해 사용될 수 있다. 또한 Aggressive Mode 교환을 인증하기 위해 공개키 암호를 사용하면 신원보호가 제공된다는 점을 유념해야 한다.

3.2 AH 및 ESP

이 절에서는 NAT-PT을 통한 IPSec 보안 서비스를 제공하기 위해 이 논문에서 선택한 IPSec 보안기술에 대해 기술한다.

IPv4와 IPv6에 정보보호 서비스를 제공하기 위해 1993년 6월부터 개발하기 시작한 IPSec은 표 1과 같은 정보보호 서비스를 제공하기 위해 AH와 ESP 확장헤더를 정의하고 있다.

이러한 IPSec은 IPv6에서는 필수옵션으로, IPv4에서는 옵션으로 제공된다.

AH 헤더 구조는 그림 3과 같다.

여기서 인증 데이타(Authentication Data)는 패킷 전체에 대해 단방향 해쉬함수(MD5 혹은 SHA-1)를 이용하여 계산한 MAC(message Authentication Code)값으로써, 키를 알고 있는 사용자만이 해쉬값을 알아낼 수 있고 수신된 패킷이 중간 경로상에서 위변조 되었는지를 검사할 수 있다. 그리고 SN(Sequence Number)은

표 1 IPSec 서비스

보안 서비스 \ 프로토콜 타입	AH	ESP (암호화)	ESP (암호화+인증)
Access Control	○	○	○
Connectionless integrity	○	×	○
Data Origin Authentication	○	×	○
Protection Against Replay	○	○	○
Confidentiality	×	○	○
Limited Traffic Flow Confidentiality	×	○	○

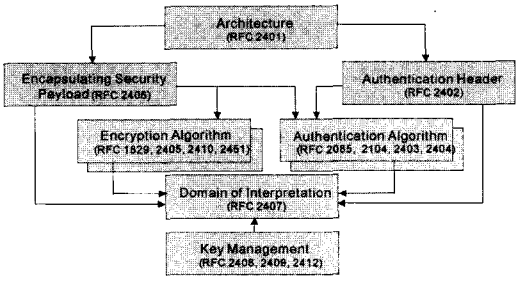


그림 2 IPSec Document Map

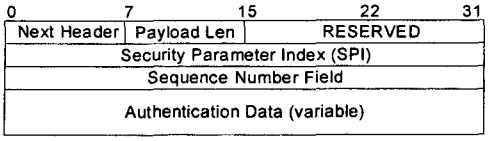


그림 3 AH 헤더 구조

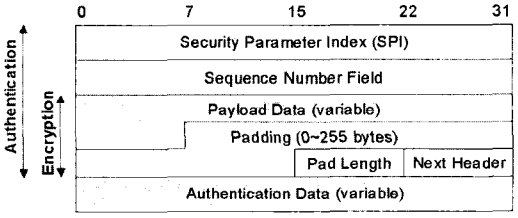


그림 4 ESP 헤더 구조

재현 공격을 방지하기 위하여 동일한 패킷이 중복되어 수신되었는지에 대한 여부와 일정한 타임 윈도우내에 도착하였는지에 대한 검사를 하는데 사용된다. 마지막으로 SPI는 목적지 주소와 더불어 SN과 인증 데이타에 대한 특정 IPSec 처리 방식을 지시한다. 이러한 AH는 확장헤더로서 사용되는 전송모드(Transport mode)와 외부헤더로서 IPSec을 적용하기 이전의 전체 패킷을 보호하는 터널모드(Tunnel mode)에 적용될 수 있다.

ESP 헤더 구조는 그림 4와 같고, 암호화하기 위한 데이타를 페이로드(Payload) 필드에 둔다. SPI와 SN은 AH헤더와 동일하다. 페이로드 부분은 전송모드에서는 상위계층 데이타가 되고, 터널모드에서는 IPSec을 적용하기 이전의 패킷 전체가 해당된다.

ESP에서 사용되는 암호 알고리즘으로는 대칭 키 블록 알고리즘이 사용되며, 패딩(Padding)부분은 알고리즘이 요구하는 평문 길이를 조정하기 위해 사용된다. 인증 데이타는 ESP 헤더, 페이로드, ESP Trailer에 대한 MAC값을 의미한다. ESP는 암호화와 인증 중 하나는 반드시 제공되어야 하며 둘 다 동시에 NULL이 되어서는 안된다. ESP도 AH와 마찬가지로 전송모드와 터널모드에 적용될 수 있으며, 패킷 데이타가 제3자에게 노

출되지 않도록 한다.

4. NAT-PT에서의 IPSec 분석

현재 사용 중 또는 개발 중인 IPSec은 IPv4망에서 IPv6망으로 진화하기 위한 과도기적 단계의 변환기술인 NAT-PT를 통해서는 통신할 수 없다. NAT-PT가 이러한 보안 서비스를 제공하지 못하는 가장 큰 이유는 IP주소변환에 있다. 대부분의 보안 서비스들은 각 통신 개체에 대한 식별자로 IP주소를 사용하고, 보안 서비스 내에 이들 IP주소를 포함하고 있기 때문에 중간 노드에 의한 주소변환은 보안 서비스의 인증 및 무결성 등에 위배되는 행위이다. 이러한 IP주소변환과 보안 서비스간의 상충된 특징은 결과적으로 IPv4망과 IPv6망간의 통신에 보안에 대한 부제를 초래하게 된다. NAT-PT를 통해 통신을 할 경우 IPSec에서 발생할 수 있는 문제들은 다음과 같다[12].

• IPSec과 NAPT-PT간의 비호환성 :

NAPT-PT에 의해 가려진 여러 호스트들이 동일한 응답자와 IPSec 통신을 할 경우, 응답자는 동일한 소스 IP주소를 가지는 여러 호스트들을 포트번호로 식별할 수 있어야 한다. IPSec에서 사용되는 SA식별자는 Initiator 및Responder Cookie, Message ID, 그리고 SPI 이다. 그러므로 만약 응답자가 동일한 IP주소를 가진 중복된 식별자를 가지는 여러 호스트들과 통신을 할 경우에는 예측할 수 없는 결과를 초래할 수 있다. 이와 같이 동일한 IP주소를가진 중복된 식별자를 수신할 경우에는 새로운 SA협상을 수행하거나, 또는 정책적으로 각 포트에 대해 항상 새로운 SA협상을 수행하도록 함으로써 이 문제를 해결할 수 있다.

• IKE 주소 식별자와 NAT-PT간의 비호환성 :

IKE에서 IP주소는 기본적인 IKE 식별자로 사용되며, IKE 협상 중 Identification 페이로드에 의해 확인된다. 그러므로 NAT-PT에 의한 IP주소의 변환은 결국 수신측으로 하여금 IKE 메시지를 식별하지 못하도록 한다. 이와 같이 식별되지 않는 IKE 메시지는 RFC2409[4]에 기술된 바와 같이 수신자에 의해 폐기된다.

이러한 IP주소에 대한 IKE 식별을 피하기 위해서는 Identification 페이로드의 ID타입에 IP주소 대신 ID_FQDN 또는 ID_USER_FQDN를 사용하는 것이다. RFC2407[10]에 기술된 바와 같이 ID_FQDN은 도메인 인증을 수행할 경우에 사용하는 타입이고, ID_USER_FQDN은 사용자 인증을 수행할 경우에 사용하는 타입이다. 이러한 타입들의 사용은 인증서에 있는 신원과 확인하는 과정을 필요로 한다. 그러나 ID_FQDN 또는 ID_USER_FQDN 타입은 IKE내에서나 가능한 방법으로 IKE 이외의 통신에서는 사용할 수 없다.

• AH와 NAT-PT간의 비호환성 :

AH는 IP 페이로드 전체(IP헤더 포함)에 대한 데이타 무결성을 제공하므로, NAT-PT에 의해 IP주소가 중간에 수정된 패킷은 데이타 무결성 검사에 의해 버려지게 된다. 반면, ESP는 ESP 페이로드에 대한 인증 및 데이타 무결성만을 제공하므로, 이와 같은 문제는 발생하지 않는다.

• 검사합(Checksum)과NAT-PT간의 비호환성 :

TCP/UDP의 검사합은 IP주소가 포함된 "pseudo-header"를 같이 계산한 결과이므로, NAT-PT는 IP주소를 변환할 경우 TCP/UDP의 검사합도 다시 계산해 주어야 한다. 하지만 AH의 경우 TCP/UDP의 검사합을 다시 계산할 경우 데이타 무결성이 깨어지므로 해당 패킷은 수신측에 의해 폐기된다. 그리고 ESP의 경우에는 TCP/UDP 헤더가 ESP의 내부에 암호화된 상태로 존재하므로 TCP/UDP의 검사합을 수정해 줄 수 없다. 따라서 결국 ESP 역시 수신측에 의해 폐기된다. 이와 같은 문제는 ESP 터널모드에 의해 피할 수 있다.

• 터널링 된 내부 IP주소와 NAT-PT간의 비호환성 :

IPSec 터널모드에 의해 IPSec 내부에 존재하는 IP주소에 대해서는 NAT-PT에 의한 주소변환이 불가능하다. 왜냐하면 IPSec 터널모드는 내부 IP헤더에 대한 무결성 및 기밀성을 제공하므로 NAT-PT의 접근을 허락하지 않기 때문이다. NAT-PT는 ALG라는 기능을 사용하여 어플리케이션 프로토콜에 대한 변환을 수행하지만 IPSec과 같은 보안 서비스들에 의해 보호되는 프로토콜들에 대해서는 접근 및 변환을 수행할 수 없다.

5. NAT-PT를 고려한 보안구조

5.1 SNAT-PT 구조

위의 4장에서 분석된 NAT-PT에서의 IPSec 동작과정에서 발생되는 문제점들은 NAT-PT가 종단 노드간에 설정된 보안 서비스에 의해 보호되는 프로토콜들을 중간에서 강제적으로 변경함으로써 발생되는 것이다. 특히 IPSec에 의해 종단 노드간에 제공되는 기밀성, 인증, 무결성 등과 같은 보안 서비스들은 중간노드에 의해 위변조된 패킷을 모두 불법적인 행위로 간주하여 폐기한다. 따라서 이러한 문제를 해결하기 위해서는 종단노드에 의해 생성된 IPSec 프로토콜을 NAT-PT가 중간에 변환하지 않도록 해야 할 것이다. 그림 5는 이러한 기능을 제공하기 위한 SNAT-PT(Secure NAT-PT)의 구조를 나타낸다.

SNAT-PT는 기존 NAT-PT에서 수행하던 DNS-ALG 기능을 그대로 수행하여 IPv4/IPv6 간의 DNS 서비스를 제공하고, 보안정책 협상에서 사용되는 SPP (Security Policy Protocol)를 통해 SNAT-PT 탐지 및

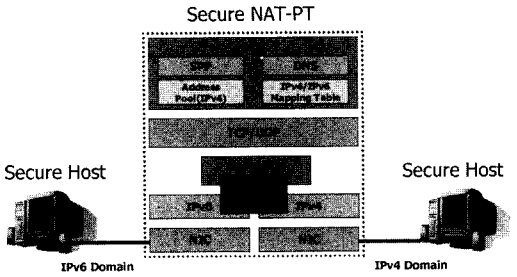


그림 5 SNAT-PT의 구조

IP주소 맵핑을 수행하여 종단호스트에 IP 맵핑주소를 전송하는 SPP-ALG 기능을 수행한다. 또한 SNAT-PT는 더미 IP로 전송되는 IPSec 패킷의 더미 IP 헤더를 제거하고 포워딩하는 기능을 수행한다. 따라서 SNAT-PT는 종단 호스트들의 주소 맵핑을 관리하고 통보하는 기능과 더미IP헤더를 제거하고 포워딩하는 기능만을 수행함으로써 종단노드에 의해 생성된 IPSec 패킷에 대한 변환을 수행하지 않는다.

5.2 보안 호스트 구조

SNAT-PT를 통해 종단 호스트간 IPSec 통신을 수행하기 위해서는 송신측이 수신측 망에 적합한 주소체계를 따르는 IPSec 프로토콜을 생성할 수 있어야 한다. 즉, IPv6망에서 IPv4망으로 통신할 경우, IPv6 호스트는 IPv4망의 주소체계를 따르는 IPv4 패킷을 생성할 수 있어야 하고, IPv4망에서 IPv6망으로 통신할 경우, IPv4 호스트는 IPv6망의 주소체계를 따르는 IPv6 패킷을 생성할 수 있어야 한다. 그리고 이렇게 생성된 수신측 망의 주소체계를 따르는 IP 패킷은 송신측 망의 주소체계를 따르는 더미 IP 헤더로 캡슐화되어 SNAT-PT로 전송된다. 그림 6은 이러한 기능을 수행하는 보안 호스트 구조를 나타낸다. 이렇게 보안 호스트에 의해 생성된 더미 IP 패킷은 SNAT-PT에 의해 더미 IP 헤더만이 제거되어 수신측 망에 포워딩됨으로써 최종 수신측 호스트까지 패킷이 안전하게 전송될 수 있다.

보안 호스트가 SNAT-PT를 통해 IPSec 통신을 수행하기 위해서는 먼저 SPS(Security Policy System)를

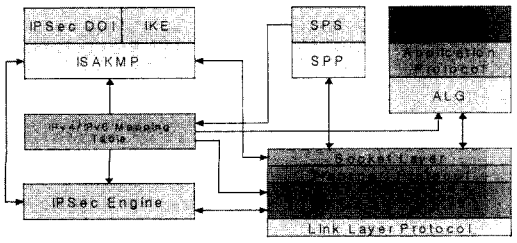


그림 6 NAT-PT를 고려한 보안 호스트 구조

이용하여 SNAT-PT로부터 맵핑될 IP주소들을 획득해야 한다. 여기서 SPS는 기존의 정책협상을 수행하는 SPP를 이용하여 통신 트래픽상에 SNAT-PT가 존재하는지 먼저 확인하고, 만약 통신 트래픽상에 SNAT-PT가 존재하면 각 종단 호스트들의 IP맵핑 주소를 SNAT- PT로부터 획득하여 보안 호스트에게 알려준다. 이렇게 SPS에 의해 정책협상 과정에서 획득된 SNAT-PT의 IP 맵핑 주소는 보안 호스트의 주소 맵핑 테이블에 저장되어 실제 통신 트래픽 발생시 사용된다. 참고로 각 보안 호스트의 주소 맵핑 테이블에서 관리되는 IP맵핑 주소들은 SNAT-PT의 주소 맵핑 테이블에서 관리되는 IP 맵핑 주소들과 일관성 있는 동기화가 이루어져야 한다. 즉, SNAT-PT의 주소 맵핑 테이블의 IP 맵핑 주소가 만료되면 해당 보안 호스트의 주소 맵핑 테이블의 IP 맵핑 주소도 만료되어야 한다.

SPS에 의한 정책협상이 종료되면, 송신 호스트는 수신측 망의 주소체계에 적합한 IP 패킷을 생성한다. 이때 생성된 IP 패킷의 IP 주소는 SPS에 의해 SNAT-PT로부터 획득한 맵핑 주소를 참조한다. 따라서 각 보안 호스트는 IPv4/IPv6 듀얼 스택을 가져야 한다.

이렇게 보안 호스트에 의해 생성된 IP 패킷은 송신 호스트로부터 SNAT-PT 경계 라우터까지 직접 전송될 수 없으므로, 송신측 주소체계에 적합한 더미 IP 헤더로 다시 캡슐화한다. 더미 IP 헤더의 IP 주소 또한 SPS에 의해 SNAT-PT로부터 획득한 맵핑 주소를 참조한다. 이러한 더미 IP 캡슐화 방법은 기존의 IP 터널링과 유사하지만 터널링을 제공하는 외부 IP 헤더와 내부 IP 헤더가 각각 서로 다른 주소체계를 따른다는 점에서 기존 IP 터널링과 다르다. 이 또한 각 보안호스트가 IPv4/IPv6 듀얼 스택을 가져야 하는 이유 중 하나이다.

SNAT-PT는 더미 IP 헤더로 캡슐화된 패킷을 수신하면 더미 IP 헤더만을 제거하여 바로 송신측에 전송한다. 이러한 기능은 기존 NAT-PT에 의해 수행되던 주소변환 및 프로토콜 변환이 각 호스트에 의해 수행됨으로써 가능하다. 그리고 각 보안 호스트는 기존 NAT-PT의 ALG 기능에 의해 수행되던 어플리케이션 프로토콜의 변환도 함께 수행할 수 있어야 한다. 왜냐하면 IPSec에 의해 암호화된 어플리케이션 프로토콜에 대해서는 어떠한 중간노드도 직접 접근할 수 없기 때문이다. 따라서 각 보안 호스트는 어플리케이션 프로토콜이 IPSec에 의해 보호되기 전에 보안 호스트의 ALG에 의해 먼저 변환해야 한다.

지금까지 기술한 보안 호스트는 SNAT-PT의 맵핑 주소를 획득하여 기존 NAT-PT가 수행하던 주소변환 및 프로토콜 변환을 직접 수행함으로써 기존 NAT-PT가 제공하지 못했던 IPv4/IPv6망간의 보안 서비스를 제

공할 수 있게 되었다. 뿐만 아니라 기존 NAT-PT에 집중되었던 주소변환 및 프로토콜 변환을 각 보안 호스트에 분산시킬 수 있으므로 IPv4/IPv6망간의 통신 속도도 개선할 수 있을 것으로 기대된다.

6. SNAT-PT를 통한 보안 서비스

이 절에서는 각 보안 호스트가 그림 7과 같은 네트워크 구조를 가질 경우 어떻게 SNAT-PT를 통한 IPSec 보안 서비스가 제공되는지에 대해 기술한다. 그림 7에서는 불필요한 중복된 보안 서비스가 실제 통신에 제공되지 않도록 각 종단 보안 호스트간에는 IPSec 전송모드를, 각 도메인의 게이트웨이간에는 터널모드를 제공하도록 보안정책을 설정하였다고 가정한다. 그리고 SPS에 의한 보안정책 협상이 이미 완료되어 각 보안 호스트(SHOST1, SHOST2)와 게이트웨이(SG1, SG2)는 SNAT-PT를 발견하고 각각의 IPv4/IPv6 맵핑 주소를 획득한 상태라고 가정한다. 즉, SHOST1의 주소 맵핑 테이블에는 SHOST1 자신과 SHOST2의 IPv4/IPv6 맵핑 주소가 획득되어 있고, SG1의 주소 맵핑 테이블에는 SG1 자신과 SG2의 IPV4/IPv6 맵핑 주소가 획득되어 있는 상태이다. SHOST2와 SG2 역시 이와 동일하다.

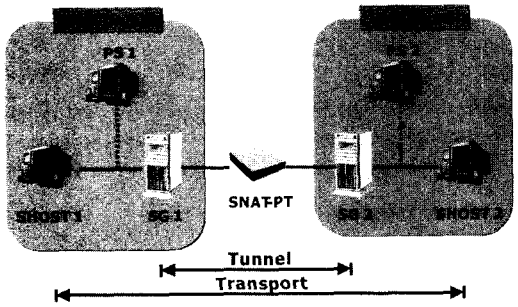


그림 7 SNAT-PT상의 보안 서비스 수행 네트워크

6.1 SNAT-PT를 통한 IKE

SNAT-PT를 통한 IKE 협상이 그림 7과 같은 네트워크 구조에서 SHOST1과 SHOST2사이에서 AH/ESP 통신을 수행하기 위해 이루어진다고 가정하면, SHOST1은 이미 SPS에 의해 획득된 맵핑 주소에 의해 SHOST2가 SNAT-PT를 통한 IPv4망에 존재하는 대상이라는 것을 알 수 있다. 따라서, SHOST1은 IPv4망의 주소체계를 따르는 IKE 패킷을 자신의 주소 맵핑 테이블을 참조하여 생성한다. 그리고 이렇게 생성된 IKE 패킷에 UDP 헤더와 IP 헤더를 붙여 하나의 완전한 IPv4 패킷을 생성한다. SHOST1이 IKE 패킷을 생성하는 과정은 다음과 같다.

- 주소 맵핑 테이블을 참조하여 수신측 망을 확인한다. SHOST1은 SHOST2가 IPv4망에 속해 있음을 자신의 주소 맵핑 테이블을 보고 알 수 있다.
- 수신측 주소체계에 적합한 ISAKMP 패킷을 생성한다. 이때 ISAKMP 내의 IP 주소는 해당 수신측 망의 IP 주소로 설정한다. SHOST1은 IPv4망에 적합한 ISAKMP를 생성하고, ISAKMP 내의 IPv4 주소는 SHOST1의 주소 맵핑 테이블을 참조하여 설정한다.
- UDP 헤더를 ISAKMP에 붙인다. 만약 주소 맵핑 테이블에 PT(Port Translation)를 수행하는 포트번호가 존재할 경우, UDP 헤더의 포트번호는 주소 맵핑 테이블을 참조하여 설정한다.
- 수신측 망의 IP 헤더를 생성한다. 이때 IP 헤더의 각 IP 주소는 주소 맵핑 테이블을 참조하여 설정한다. SHOST1은 자신의 주소 맵핑 테이블을 참조하여 SHOST1 자신의 IPv4 주소와 SHOST2의 IPv4 주소를 IPv4 헤더에 설정한다.

이와 같이 SHOST1에 의해 생성된 IPv4 패킷은 그림 8(a)와 같다. 그리고 SHOST1은 자신이 생성한 IPv4 패킷을 SNAT-PT까지 전송하기 위해 더미 IPv6 헤더를 생성하여 IPv4 패킷을 캡슐화한다. 이때 더미 IPv6 헤더의 IPv6 주소는 SHOST1의 주소 맵핑 테이블을 참조하여 설정한다. 그림 8(b)는 이러한 더미 IPv6 헤더로 캡슐화된 IKE 패킷을 나타낸다.

SHOST1에 의해 더미 IP헤더로 전송된 IKE 패킷을 수신한 SNAT-PT는 IKE 패킷의 더미 IP 헤더를 제거한 후 SHOST2에게 전송한다. 이때 SHOST2가 수신할 IKE 패킷은 그림 8(a)와 동일하다.

SHOST2 역시 SHOST1과 같은 절차로 IKE 패킷을 생성하여 SHOST1으로 전송한다. 단, 이 경우 더미 IP 헤더는 IPv4 포맷을 따르고, 내부 IP 헤더는 IPv6 포맷을 따른다. 이와 같은 과정은 SG1과 SG2간의 AH/ESP 터널링을 위한 IKE 협상에서도 동일하다.

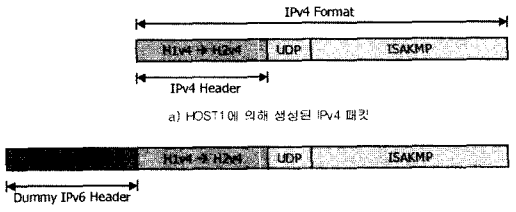


그림 8 SHOST1에 의해 생성된 IKE 패킷

6.2 SNAT-PT를 통한 AH/ESP

그림 7과 같은 네트워크 구조에서 각 보안 호스트가 6.1절과 같은 과정을 통해 IKE 협상을 수행한 후에는

실제 IPSec 통신이 각 보안 호스트간에 이루어지게 된다. 각 보안 호스트간의 IPSec 통신도 6.1절과 거의 유사하다. 우선 SHOST1이 AH를 이용하여 SHOST2와 통신한다고 가정하자. SHOST1은 다음과 같은 과정에 의해 IPSec 패킷을 생성한다.

- 주소 맵핑 테이블을 참조하여 수신측 망을 확인한다. SHOST1은 SHOST2가 IPv4망에 속해 있음을 자신의 주소 맵핑 테이블을 보고 알 수 있다.
- 수신측 주소체계에 적합한 어플리케이션 프로토콜을 생성한다. 이때 어플리케이션 프로토콜내의 IP 주소는 해당 수신측 망의 IP 주소로 설정한다. SHOST1은 어플리케이션 프로토콜을 ALG을 사용하여 IPv4망에 적합한 어플리케이션 프로토콜로 변환하여 생성하고, 이때 어플리케이션 프로토콜내에 사용되는 IPv4 주소는 SHOST1의 주소 맵핑 테이블을 참조하여 설정한다.
- TCP/UDP 헤더를 각 어플리케이션 프로토콜에 붙인다. 만약 주소 맵핑 테이블에 PT를 수행하는 포트번호가 존재할 경우, TCP/UDP 헤더의 포트번호는 주소 맵핑 테이블을 참조하여 설정한다.
- 수신측 주소체계에 적합한 IP 헤더를 생성한다. 이때 생성된 IP 헤더의 IP 주소는 해당 수신측 망의 IP 주소로 설정한다. SHOST1은 자신의 주소 맵핑 테이블을 참조하여 IPv4 패킷을 생성한다.
- AH/ESP 패킷을 생성한다. AH/ESP 패킷은 IP 버전에 상관없이 동일하게 수행된다.

이와 같이 SHOST1에 의해 생성된 IPv4용 AH 패킷은 그림 9(a)와 같다. 그리고 SHOST1은 자신이 생성한 IPv4용 AH 패킷을 SNAT-PT까지 전송하기 위해 더미 IPv6 헤더를 생성하여 IPv4용 AH 패킷을 캡슐화한다. 이때 더미 IPv6 헤더의 IPv6 주소는 SHOST1의 주소 맵핑 테이블을 참조하여 설정한다. 그림 9(b)는 이러한 더미 IPv6 헤더로 캡슐화된 AH 패킷을 나타낸다.

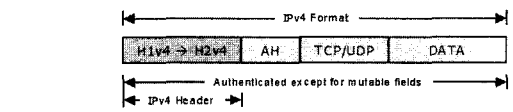
여기서 SHOST1에 의해 생성된 AH 패킷이 다시 그림 7과 같이 SG1에 의해 AH 터널모드가 수행된다고 가정하자. SHOST1에 의해 생성된 AH 패킷을 수신한 SG1은 다음과 같은 과정에 의해 IPSec 패킷을 터널링한다.

- 수신한 IPSec 패킷에 더미 IP 헤더가 있을 경우, 더미 IP 헤더를 제거한다. SHOST1으로부터 수신한 AH 패킷의 더미 IPv6 헤더를 제거한다.
- 주소 맵핑 테이블을 참조하여 터널링 되는 수신측 망을 확인한다. SG1은 SG2가 IPv4망에 속해 있음을 자신의 주소 맵핑 테이블을 보고 알 수 있다.
- 수신측 주소체계에 적합한 IP 헤더를 생성하여 더미 IP가 제거된 IPSec 패킷을 캡슐화한다. 이때 생성된 IP 헤더의 IP 주소는 해당 수신측 망의 IP 주소로 설정한다. SG1은 자신의 주소 맵핑 테이블을 참조하여 IPv4 패킷을 생성한다.
- AH/ESP 패킷을 생성한다. AH/ESP 패킷은 IP 버전에 상관없이 동일하게 적용된다.

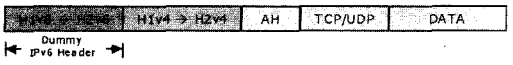
이와 같이 SG1에 의해 생성된 IPv4용 AH 터널링 패킷은 그림 10(a)와 같다. SG1은 자신이 생성한 IPv4용 AH 터널링 패킷을 다시 SNAT-PT 경계 라우터까지 전송하기 위해 더미 IPv6 헤더를 생성하여 IPv4용 AH 터널링 패킷을 캡슐화한다. 이때 더미 IPv6 헤더의 IPv6 주소는 SG1의 주소 맵핑 테이블을 참조하여 설정한다. 그림 10(b)는 이러한 더미 IPv6 헤더로 캡슐화된 AH 터널링 패킷을 나타낸다.

SG1에 의해 생성된 AH 터널링 패킷을 수신한 SNAT-PT는 AH 터널링 패킷의 더미 IPv6 헤더를 제거한 후 SG2에게 전송한다. SG2가 수신한 AH 터널링 패킷은 일반적인 IPv4용 AH 터널링 패킷과 동일하므로 일반적인 IPv4용 IPSec 처리를 수행하면 된다.

SHOST2 역시 SHOST1과 같은 절차로 IPSec 패킷을 생성하여 SHOST1에 전송하고, SG2 역시 SG1과 같은 절차로 IPSec 패킷을 터널링하면 된다. 단 SHOST2 또는 SG2에 의해 생성된 IPSec 패킷의 내부 IP헤더는 SHOST1 또는 SG1의 IPv6 헤더이고, 더미 IP 헤더는 IPv4 헤더이다.

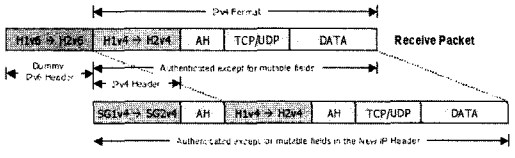


a) HOST1에 의해 생성된 IPv4 패킷



b) HOST1에 의해 생성된 더미 IPv6 패킷

그림 9 SHOST1에 의해 생성된 AH 패킷



a) SG1에 의해 생성된 IPv4 터널링 패킷

b) SG1에 의해 생성된 더미 IPv6 터널링 패킷

그림 10 SG1에 의해 생성된 AH 터널링 패킷

ESP를 사용한 IPSec 통신 역시 AH를 사용한 IPSec 통신과 같은 절차로 수행된다.

7. 결 론

IPv4/IPv6망 간의 통신을 제공하기 위해 주소변환과 프로토콜 변환을 수행하는 NAT-PT는 IPSec과 같은 보안 프로토콜에 대해서도 강제적인 변환을 수행함으로써 기밀성, 인증, 무결성과 같은 정보보호 서비스를 제공하지 못한다. 이러한 NAT-PT의 보안문제를 해결하기 위해 이 논문에서는 기존 NAT-PT를 확장한 SNAT-PT를 통해 IPSec 패킷에 대한 변환 없이 더미 IP 헤더를 이용한 터널링으로 종단간 IPSec 보안 서비스를 제공하는 보안 메커니즘을 제시하였다.

이 논문에서 제시된 SNAT-PT는 SNAT-PT 기반에서 동작하는 보안 호스트에 의해 생성된 IPSec 터널링 더미 IP 패킷으로부터 더미 IP 헤더를 제거함으로써 기존 IPSec 서비스가 IPv4/IPv6망 간에 지원되도록 하였다. 제안된 SNAT-PT와 보안 호스트의 구조가 가지는 장점은 기존의 IKE와 IPSec을 그대로 사용할 수 있고, 보안 호스트가 IPv4망에서 IPv6망으로 진화함에 따라 자연스럽게 시스템에 탑재되는 IPv4/IPv6 듀얼 스택과 이를 지원하는 IPSec 엔진에 의해 쉽게 구현될 수 있다는 것이다. 특히 IPSec 엔진은 IP버전에 관계없이 동일하게 수행되므로 모든 IPv4/IPv6 보안 호스트가 동일한 구조를 가질 수 있다.

기존 NAT-PT에 비해 SNAT-PT 구조의 보안 메커니즘이 가지는 오버헤드는 다음과 같다.

- SPP-ALG 기능에 따른 SNAT-PT의 부하가 증가함
- 각 보안 호스트도 주소 맵핑 테이블을 관리해야 함
- 각 보안 호스트가 IPv4/IPv6 듀얼 스택 구조를 가져야 함

하지만 기존 NAT-PT에서 집중적으로 처리되었던 주소변환 및 프로토콜 변환이 각 보안 호스트로 분산됨으로써 NAT-PT의 작업로드를 줄일 수 있어 통신속도를 개선할 수 있을 것으로 기대된다.

결론적으로 NAT-PT를 통해 보안 서비스를 제공하기 위해서는 NAT-PT에 의해 맵핑되는 IPv4/IPv6 맵핑 주소를 각 보안 호스트가 유지관리할 수 있어야 하고, NAT-PT는 보안 프로토콜에 대해 어떠한 변경도 하지 말아야 한다.

따라서 이 논문에서 제시된 SNAT-PT와 보안 호스트 구조를 확장하면 IPSec 이외의 다른 보안 서비스도 제공할 수 있을 것으로 기대된다.

참 고 문 헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC1883, 1995. 12.

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

[3] M. Borella, J. Lo, D. Grabelsky, G. Montenegro, "Realm Specific IP: Framework," RFC3102, October 2001.

[4] Harkins, D., and D. Carrel, D., "The Internet Key Exchange (IKE)," RFC2409, November 1998.

[5] Kent, S., and R. Atkinson, "IP Authentication Header," RFC2402, November 1998.

[6] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC2406, November 1998.

[7] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)," RFC1631, 1994. 5.

[8] Nordmark, E., "Stateless IP/ICMP Translator (SIIT)," RFC2765, 2000. 2.

[9] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC2663, 1999. 8.

[10] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407, November 1998.

[11] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol(ISAKMP)," RFC 2408, November 1998.

[12] Bernard Aboba, William Dixon, "IPSec-NAT Compatibility Requirments," draft-ietf-ipsec-nat-reqts-02.txt, August 2002.

현 정 식

1999년 청주대학교 컴퓨터정보공학과 졸업. 2001년 청주대학교 전자계산학과 졸업(MS). 2001년~현재 충북대학교 전자계산학과 박사과정. 관심분야는 네트워크 보안, P2P, 그리드

황 윤 철

1994년 한남대학교 전자계산공학과 졸업 1996년 한남대학교 전자계산공학과 졸업(MS). 1999년~현재 충북대학교 대학원 전자계산학과 박사과정수료. 관심분야는 인터넷, 정보보호, 네트워크 보안

정 윤 수

1998년 2월 청주대학교 졸업(이학사) 2000년 2월 충북대하교 대학원 전자계산학과 졸업(이학석사). 2003년 3월~현재 충북대 이공대학 전자계산학과 재학. 관심분야는 무선보안기술, 차세대이동통신 망기술

이 상 호

1976년 숭실대학교 전자계산학과 졸업 1981년 숭실대학교 전자계산학과 졸업(MS). 1989년 숭실대학교 전자계산학과 졸업(PHD). 1976년 1월~1979년 5월 한국전력 전자계산소. 1981년 6월~현재 충북대학교 전기전자컴퓨터공학부 교수 관심분야는 Protocol Engineering, Network Security, Network Management, Network Architecture