IPv6 전환 기술 중 NAT-PT에서의 IPsec 적용 방안

준회원 최 인 석*, 정회원 정 수 환*, 김 영 한*, 박 용 석**

IPsec Support for NAT-PT in IPv6 Transition Mechanisms

Inseok Choi* *Asoociate Member*, Souhwan Jung*, Younghan Kim*,
Yongseok Park** *Regular Members*

요 약

IPv6 전환 기술 중 NAT-PT에서 양단간의 보안을 위해 IPsec을 적용하는 경우 NAT-PT 서버에서의 IP 헤더 변환으로 인해 수신 측에서 TCP/UDP checksum과 인증 데이터에 대한 검증이 실패하는 문제가 발생한다. 본 연구에서는, NAT-PT 서버에서 IP Header Translation Information (HTI)를 IKE 수행 중에 NAT-PT 노드에게 제공하고, NAT-PT 노드가 이를 사용하여 TCP/UDP checksum과 인증 데이터를 생성함으로써 수신 측의 검증과정을 성공적으로 통과하는 방법을 제안하였다. 또한, 기존의 NAT 환경에서 IPsec 적용을 위해 제안 되었던 방법들과의 비교를 통해 본 논문에서 제안하는 방법이 효과적인 것을 알 수 있다.

Key Words : NAT-PT, SIIT, IPsec, NAT, RSIP.

ABSTRACT

NAT-PT is one of the IPv6 transition mechanisms, as defined in RFC2766, allowing IPv6-only devices to communicate with IPv4-only devices and vice versa. In NAT-PT, sender fail to verify TCP/UDP checksum and authentication data due to IP translation in the NAT-PT server. The NAT-PT, therefore, has a limit to applying the IPsec that provides the end-to-end security such as confidentiality, authentication, and integrity. This paper proposes a scheme to apply the IPsec using IP HTI in NAT-PT environment.

Ⅰ. 서 론

IPv6는 IPv4 프로토콜을 대체하기 위해 IETF에서 설계한 차세대 IP 프로토콜이다. 오늘날 가장 많이 사용되는 IPv4 프로토콜은 인터넷을 사용하는 새로운 디바이스에 대한 급속한 증가로 인해 IPv4 주소 부족 문제를 드러내고 있다. 이러한 문제를 해결하기 위해 IETF에서는 IPv4 프로토콜을 대체할 수 있는 IPv6 프로토콜을 새롭게 설계하였다. IPv6 도입 초창기에는 기존 IPv4와의 공존하는 형태로 존재할 것이 분명하기 때문에 IPv6와 IPv4와의 공존단계를 위한 메커니즘 즉, IPv6 전환 메커니즘이 필요하다. NAT-PT[1]는 이러한 IPv6 전환 메커니즘의 하나로서 IPv6 전용 노드와 IPv4 전용 노드 사이의 통신을 지원하기 위한 방법이다. NAT-PT 방법에서는 IPv4망과 IPv6 망간의 통신을 위한 주소 변환 및 프로토콜 변환에 관한 메커니즘을 제시하고 있으며, 이 과정에서 NAT-PT는 몇 가지 문제점을 가지고 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 IPv4 망과 IPv6 망간의 통신에 있어 인터넷상에 존재하는 수많은 불법적인 행위에 대한 어떠한 보호도 제공할 수 없게 한다. 현재 이

* 숭실대학교 정보통신전자공학부,
교신저자 : 정수환 souhwanj@ssu.ac.kr
논문번호 : KICS2004-12-334, 접수일자 : 2004년 12월 23일
** (주) 삼성전자 정보통신 연구개발센터

러한 NAT-PT의 보안 문제를 해결하기 위해 제안된 보안 메커니즘은 없으며, 단지 NAT-PT에서 IPsec 트랜스포트 모드[8]를 적용 시 발생하는 문제점[2]만이 인터넷 드래프트로 제시되어 있을 뿐이다. NAT-PT의 모태가 된 NAT[3]방법에서는 IPsec 트랜스포트 모드를 위해 UDP Encapsulation[4][5] 방법과 RSIP[6] 방법이 제안되어 있다. 하지만 NAT-PT 변환 메커니즘에서는 NAT-PT 서버를 기준으로 들어오는 패킷과 나가는 패킷의 IP 프로토콜이 서로 다르기 때문에 NAT에서의 UDP Encapsulation방법과 RSIP방법을 NAT-PT에 적용이 불가능해진다.

본 논문에서는 NAT-PT 변환 메커니즘을 분석하고, NAT-PT에서의 한계를 설명하고, 가장 큰 문제로 대두되는 양단간의 보안 적용 문제를 해결하기 위한 IPsec 트랜스포트 모드 적용 방안을 제시한다. 2장에서는 NAT-PT 메커니즘과 NAT-PT에서의 IPsec 적용 문제를 분석하고, 3장에서는 NAT-PT에서의 IPsec 트랜스포트 모드 적용 방법을 제시하고, 4장에서는 이 논문에서 제안하는 방법과 기존 NAT에서의 IPsec 적용 방법에 관한 비교 분석을 하고, 5장에서 결론을 맺기로 하겠다.

Ⅱ. NAT-PT와 IPsec 적용 문제 분석

2.1 NAT-PT

NAT-PT (Network Address Translation-Protocol Translation, RFC-2766)는 IETF ngtrans 워킹그룹에서 표준화한 변환기술로서, IPv6 전용 노드와 IPv4 전용 노드사이의 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 차이점을 살펴보면 NAT는 단순히 동일한 IP 패킷에서 특정한 필드 (주소, 포트 등)를 변환하는 데 반해, NAT-PT는 IP 헤더 자체를 다른 버전의 IP 헤더로 변환하는 데 있다. 이 때 소스 IPv6 주소는 NAT-PT가 유지하는 IPv4 주소 풀에서 선택된 IPv4 주소로 대체되며, 목적지 IPv6 주소는 96 비트 프리픽스를 제외한 나머지 32 비트로 표현되는 IPv4 주소로 대체된다. 이외에 ICMP의 변환 적용 방법은 SIIT (Stateless IP/ICMP Translation Algorithm)[7]에서 명시하고 있는 변환 방법을 그대로 따른다. SIIT는 IPv4/IPv6 변환 시에 별도의 상태정보를 저장하지 않고도 변환을 수행할 수 있도록 해주는 메커니즘을 기술하고 있다. 따라서 SIIT는 IPv6 출발지 주소에 대한 IPv4 주소 풀을 유지하지도 않으며 IPv4 주소에 대한 동적인 매핑도 시도하지 않는다. 단지 출발지 주소와 목적지 주소에 IPv4 주소를 내장시켜서 변환 시 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 별도의 ALG (Application Level Gateway)가 필요하다. ALG는 NAT-PT에서의 헤더변환과는 별도로 응용계층 헤더를 변환하는 역할을 한다. 이와 같은 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.

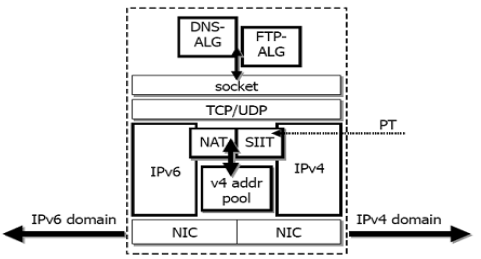


그림 1. NAT-PT 구조

그림 1은 이러한 NAT-PT의 구조를 나타낸다. NAT-PT는 NIC (Network Interface Card)로부터 패킷을 캡쳐하여 IPv6 주소에 할당된 IPv4 주소를 IPv4/IPv6 주소 매핑 테이블에 기록한다. 이렇게 매핑된 IP 주소를 이용하여 SIIT 프로토콜 변환 매커니즘은 IP 또는 ICMP 패킷을 변환한다. 하지만 NAT-PT는 그 특성상 양단간 보안을 제공하는 IPsec 트랜스포트 모드를 사용할 수 없다는 단점을 가지고 있다.

2.2 NAT-PT에서의 IPsec 적용 문제

NAT-PT에서 IPsec 트랜스포트 모드 적용 시 문

제점은 크게 두 부분으로 나눌 수 있다. 첫 번째로 TCP/UDP 체크섬 문제와 두 번째로 IP 헤더 변환으로 인한 AH[10]헤더의 ICV 계산 값에 관한 문제점으로 나눌 수 있다. TCP/UDP 체크섬은 일반적으로 응용 데이터, TCP 헤더 그리고 TCP/UDP pseudo 헤더를 사용하여 계산한다. 하지만 NAT-PT 서버에서의 IP 헤더 변환은 해당 IP 헤더의 IP 주소 정보가 포함된 TCP/UDP pseudo 헤더 계산에 영향을 미치게 되고, TCP/UDP 체크섬이 반영된 IPsec AH헤더의 ICV 값과 ESP[9]로 암호화된 TCP/UDP 체크섬을 올바르게 검증할 수 없는 문제가 발생한다. 또, IPsec AH헤더의 ICV 값을 계산할 때, IP헤더의 필드 값을 계산 값에 포함시키는데 이때, IP 헤더의 주소필드가 변하게 되면 AH 패킷을 생성한 노드가 계산한 ICV 값과 AH 패킷을 검증하는 노드가 계산한 ICV 값이 서로 달라지므로 IPsec AH 트랜스포트 모드를 사용한 통신은 불가능해진다.

Ⅲ. NAT-PT 환경에서의 IPsec 트랜스포트 모드 적용 방안

본 장에서는 NAT-PT 환경에서의 IPsec 트랜스포트 모드를 적용하기 위한 방안을 제시한다. 본 논문에서는 IPsec 트랜스포트 모드 적용을 위해 먼저 IP HTI (Header Translation Information) 메시지를 정의하고, IKE[11] 수행 중에 IP HTI 메시지를 전달하는 방법을 설명하고, IP HTI 메시지를 사용하여 IPsec ESP 또는 AH 트랜스포트 모드를 수행하는 방법을 제시하기로 하겠다.

3.1 IP HTI

NAT-PT에서 IPsec 트랜스포트 모드를 적용할 수 없는 가장 큰 이유는 NAT-PT 서버에서의 IP 헤더 변환 시에 변화되는 IP 주소 정보들을 NAT-PT 노드가 알 수 없기 때문이다. 따라서 NAT-PT 노드는IP 헤더 변환으로 인한 TCP/UDP 체크섬과 AH헤더 필드의 ICV 값을 예측하지 못하므로 IPsec 트랜스포트 모드를 수행할 수 없는 것이다. 이러한 문제를 해결하기 위해서 본 논문에서는 IP HTI 메시지를 새롭게 정의한다. IP HTI는 NAT-PT 노드가 IPsec ESP 또는 AH 트랜스포트 모드 적용을 가능하도록 하기 위해서 NAT-PT 서버가 NAT-PT 노드에게 할당하는 IPv4 주소 정보와 해당 NAT-PT 서버가 가진 96비트 프리픽스 주소 정보를 담

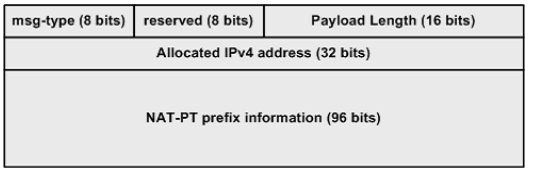


그림 2. IP HTI 메시지 포맷

고 있다. NAT-PT 노드는 IP HTI를 사용하여 IPsec 트랜스포트 모드를 수행할 수 있다.

3.2 NAT-PT 환경에서의 IPsec 트랜스포트 모드 적용을 위한 IKE negotiation 방법

위의 절에서 언급한 바와 같이 IP HTI 정보는 NAT-PT 환경에서 IPsec 트랜스포트 모드를 적용시에 사용된다. IP HTI는 IPsec ESP 또는 AH 트랜스포트 모드 적용을 위해 IKE 협상 수행이 완료되기 전에 제공되어야 할 것이다. 그림 3은 서명을 사용하는 인증 방식의 IKE 단계 1 과정 수행 중에 NAT-PT 서버가 NAT-PT 노드에게 IP HTI를 제공하는 방법을 나타내었다. NAT-PT 서버는 IPv4 노드로부터 전달받은 IPv4 패킷이 UDP 500 포트 (IKE 협상은 UDP 500번을 사용한다.)로 전달되는 패킷이면 IP HTI를 해당 NAT-PT 노드에게 제공하고, 해당 NAT-PT 노드에 대한 IP 주소 매핑 테이블에 IP HTI 제공 여부를 체크한다.

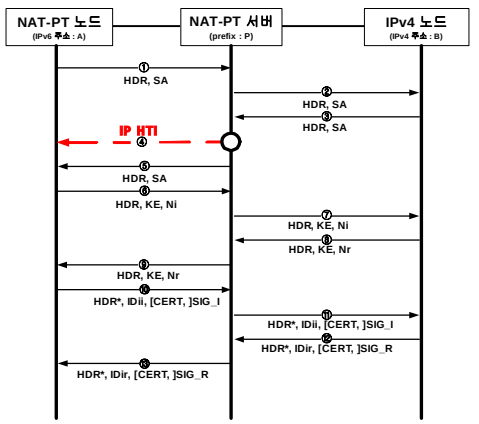


그림 3. IP HTI 전달을 위한 IKE 협상

3.3 IPsec ESP 트랜스포트 모드 적용 시나리오

NAT-PT 환경에서 IPsec ESP 트랜스포트 모드를 적용할 수 없는 근본적인 이유는 TCP/UDP 체크섬 문제에 있다. TCP/UDP에서의 체크섬은 해당 TCP/ UDP 헤더의 필드 값과 IP 주소 정보가 포함

된 pseudo 헤더의 필드 값을 사용하여 계산한다. 한편, NAT-PT 환경에서 TCP/UDP 체크섬과 관련된 문제를 살펴보면 일반적인 IP 패킷에 대해 NAT-PT 서버는 IP 헤더 변환 시에 변화하는 TCP/UDP 체크섬을 다시 계산하여 TCP 헤더를 재구성할 수 있지만 ESP로 암호화된 TCP/UDP 헤더의 체크섬 필드 값에 대해서는 NAT-PT가 수정할 수 없는 문제가 발생한다. 본 논문에서는 이러한 문제를 해결하기 위해서 NAT-PT 노드가 NAT-PT 서버에서의 IP 헤더 변환으로 인한 TCP/UDP 체크섬에 관한 변화를 예측하여 계산하는 방법을 제안한다. NAT-PT 노드는 TCP/UDP 체크섬에 관한 두 가지 사항들을 고려해야 한다. 첫 번째는 NAT-PT 노드가 ESP 패킷의 TCP/UDP 체크섬을 계산하는 문제와 두 번째는 IPv4 노드로부터 들어오는 ESP 패킷의 TCP/ UDP 체크섬을 검증하는 문제를 고려해야 한다. 해당 사항에 대한 방법은 다음과 같다.

3.3.1 NAT-PT 노드에서의 ESP 패킷 생성하는 절차

NAT-PT 노드가 전송하는 패킷에 대해 TCP/UDP checksum 계산 문제를 해결하기 위해 NAT-PT 노드는 아래와 같이 TCP/UDP 체크섬을 계산한다.

—TCP/UDP 체크섬 계산 방법

① Pseudo 헤더의 출발지 IPv6 주소 대신 IP HTI 헤더의 Allocated IPv4 address 값을 사용한다.

② Pseudo 헤더의 목적지 IPv6 주소 값 대신 IP HTI 헤더의 NAT-PT prefix information값을 제외한 나머지 32bit 값을 사용한다.

그림 4는 NAT-PT 노드가 ESP 패킷을 생성하여 IPv4 노드로 전달하는 과정을 나타내었다. 그림에서 ①과정에서는 source IP address는 IP HTI헤더 필드의 Allocated IPv4 address (A2)로 설정하고, destination IP address는 NAT-PT 서버의 prefix (P)를 제외한 IPv4 노드의 IPv4 주소 (B)로 설정하여 TCP/UDP checksum 계산을 수행한 후 ESP 패킷을 구성하여 NAT-PT 서버로 패킷을 전달한다. ②과정에서는 NAT-PT 서버는 해당 IP 패킷에 대한 IP 헤더 변환을 수행한 후 IPv4 노드로 ESP 패킷을 전달한다.

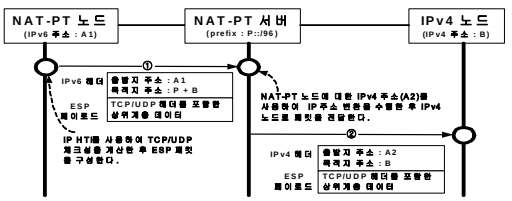


그림 4. NAT-PT 노드로부터 IPv4 노드까지의 ESP 패킷 전달 과정

3.3.2 NAT-PT 노드가 IPv4 노드로부터의 ESP 패킷을 검증하는 절차

NAT-PT 서버의 IP 변환으로 인해 IPv4 노드의 ESP 패킷을 전달받은 NAT-PT 노드는 TCP/UDP 체크섬 계산 시 문제가 발생한다. 따라서 NAT-PT 노드는 아래와 같이 TCP/UDP 체크섬을 계산하여 TCP/UDP 체크섬을 검증한다.

—TCP/UDP 체크섬 검증 방법

① TCP/UDP 체크섬으로부터 출발지 IPv6 주소와 목적지 IPv6 주소 값을 감산한다.

② TCP/UDP 체크섬으로부터 IP HTI 헤더의 Allocated IPv4 address 값과 해당 목적지 IPv6 주소에서 NAT-PT prefix information 값을 제외한 나머지 32비트 값을 TCP/UDP 체크섬 계산값으로 한다.

그림 5는 NAT-PT 노드가 IPv4 노드의 ESP 패킷을 검증하는 과정을 나타내었다. 그림에서 ①과정에서는 IPv4 노드가 ESP 패킷을 생성하여 NAT-PT 서버에게 패킷을 전달하고, ②과정에서는 NAT-PT 노드에서는 NAT-PT 서버로부터 전달받은 ESP 패킷에 대한 복호화를 수행한 후 상기와 같은 방법을 통해서 TCP/UDP 체크섬에 대한 검증을 수행한다.

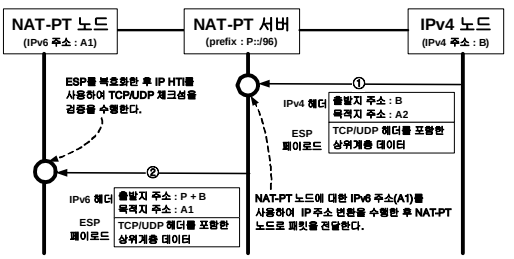


그림 5. IPv4 노드로부터 NAT-PT 노드까지의 패킷 전달 과정

3.4 IPsec AH 트랜스포트 모드 적용 시나리오

NAT-PT 노드가 AH 헤더의 ICV 값을 계산할 때 두 가지 사항을 고려해야 한다. 첫 번째는 NAT-

PT 서버로 인한 TCP/UDP 체크섬의 변화를 고려해야 하고, 두 번째는 IP 헤더의 변화를 고려해야 한다.

본 논문에서는 IP AH 트랜스포트 모드를 적용을 위해서 NAT-PT 노드가 TCP/UDP 체크섬과 IP 헤더의 변화를 고려하여 ICV 값을 계산하는 방법과 ICV 값을 검증하는 방법을 제안한다.

3.4.1 NAT-PT 노드가 IPv4 노드로부터의 AH 패킷을 생성하는 절차

NAT-PT 노드는 IPv4 노드의 ICV 검증을 통과하기 위해서 ICV 값을 아래와 같은 절차를 사용하여 계산한다.

－AH 헤더의 ICV 값 계산 방법

① Pseudo 헤더의 출발지 IPv6 주소 대신 IP HTI 헤더의 Allocated IPv4 address 값을 사용한다.

② Pseudo 헤더의 목적지 IPv6 주소를 사용하지 않고, IP HTI 헤더의 NAT-PT prefix information값을 제외한 나머지 32비트 값을 사용한다.

③ 1과 2에서 계산된 TCP/UDP 체크섬 및 TCP/UDP 헤더와 ICV 계산에 포함되는 IP헤더 필드를 표 1과 같이 설정하여 ICV 값을 계산한다.

표 1은 IP 헤더 변환을 고려하여 ICV 값을 계산할 때 적용해야 할 IP 헤더 필드와 변환 값을 나타내었다. 한편, NAT-PT 노드는 ICV 값을 계산할 때 IPv6 패킷이 IPv4 패킷으로 변환될 때의 Identification 값을 예측할 수 없으므로 IPv6 fragmentation 헤더가 존재하지 않는다면 Identification 값을 0으로 하여 ICV 값을 계산하고, IPv6 fragmentation 헤더가 존재할 때는 fragmentation 헤더 필드의 Identification을 ICV 계산 시 사용한다.

그림 6은 NAT-PT 노드가 AH 패킷을 생성하여 IPv4 노드로 전달하는 과정을 나타내었다.

표 1. ICV 계산을 위한 IPv4 헤더 변환 규칙

Version	4 (IPv4)
Header Length	20
Total Length	Payload Length + 20
Protocol	51 (AH protocol)
Identification	① IPv6 fragmentation 헤더가 존재하지 않는다면 0으로 설정 ② IPv6 fragmentation 헤더가 존재한다면 Fragmentation 헤더의 Identification값을 설정
Source Address	IP HTI 메시지의 Allocated IPv4 address
Destination Address	IP HTI 메시지의 NAT-PT prefix Information을 제외한 나머지 32비트 주소

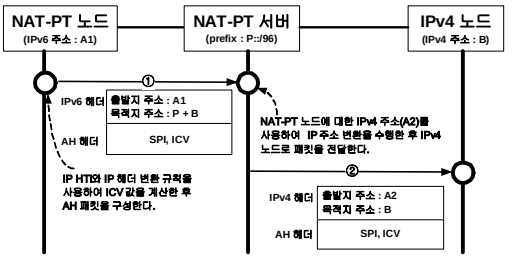


그림 6. NAT-PT 노드가 IPv4 노드까지의 AH 패킷 전달 과정

그림에서 ①과정에서는 TCP/UDP 체크섬을 그림 4에서의 ①과정과 같은 방법으로 계산을 수행하고, NAT-PT 서버에서의 IP 헤더 변환을 고려하여 IP 헤더 필드를 표 1과 같이 설정하여 ICV 값을 계산한다. 그림 6에서는 Source Address는 A2가 되고, Destination Address는 B가 될 것이다. 한편 NAT-PT 서버는 NAT-PT 노드에서의 Identification 값에 대한 예측이 가능하도록 NAT-PT 노드가 전달한 IPv6 패킷이 IPv6 fragmentation 헤더를 포함하고 있다면 해당 헤더의 Identification 값을 IPv4 헤더 구성 시 사용하고, IPv6 fragmentation 헤더가 존재하지 않는다면 0으로 설정한다. ②과정에서는 NAT-PT 서버는 해당 IP 패킷에 대한 IP 헤더 변환을 수행한 후 IPv4 노드로 AH 패킷을 전달한다.

3.4.2 NAT-PT 노드가 IPv4 노드로부터의 AH 패킷을 검증하는 절차

NAT-PT 노드가 올바르게 검증을 수행하기 위해서 ICV 값을 아래와 같은 절차를 사용하여 계산한다.

－AH 헤더의 ICV 값 검증 방법

① TCP/UDP 체크섬으로부터 출발지 IPv6 주소와 목적지 IPv6 주소 값을 감산한다.

② TCP/UDP 체크섬으로부터 IP HTI 헤더의 Allocated IPv4 address 값과 해당 목적지 IPv6 주소에서 NAT-PT prefix information 값을 제외한 나머지 32비트 값을 TCP/UDP 체크섬 계산값으로 한다.

③ 1과 2에서 계산된 TCP/UDP 체크섬 및 TCP/UDP 헤더와 ICV 계산에 포함되는 IP 헤더 필드를 표 2와 같이 설정하여 ICV 값을 검증한다.

표 2. ICV 검증을 위한 IPv4 헤더 변환 규칙.

Version	4 (IPv4)
Header Length	20
Total Length	Payload Length + 20
Protocol	51 (AH protocol)
Identification	IPv6 fragmentation 헤더의 Identification
Source Address	NAT-PT prefix Information을 제외한 나머지 32비트 주소
Destination Address	IP HTI 메시지의 Allocated IPv4 address

표 2는 IP 헤더 변환을 고려하여 ICV 값을 계산할 때 적용해야 할 IP 헤더 필드와 변환 값을 나타내었다.

그림 7은 NAT-PT 노드가 IPv4 노드로부터 전달받은 AH 패킷을 검증하는 과정을 나타내었다. 그림에서 ①과정은 IPv4 노드는 AH 패킷을 생성하여 NAT-PT 서버로 전달하고, ②과정은 TCP/UDP 체크섬을 그림 5에서의 ①과정과 같은 방법으로 계산을 수행하고, NAT-PT 서버에서의 IP 헤더 변환을 고려하여 IP 헤더 필드를 Table 2와 같이 설정하여 ICV 값을 검증한다. 그림에서는 Source Address는 B가 되고, Destination Address는 A2가 될 것이다. 한편 NAT-PT 서버는 NAT-PT 노드에서의 Identification 값에 대한 예측이 가능하도록 IPv4 노드로부터 전달 받은 패킷에 대한 변환을 수행할 때 IPv4 헤더의 Identification 값을 사용하여 IPv6 fragmentation 헤더를 추가시킨다.

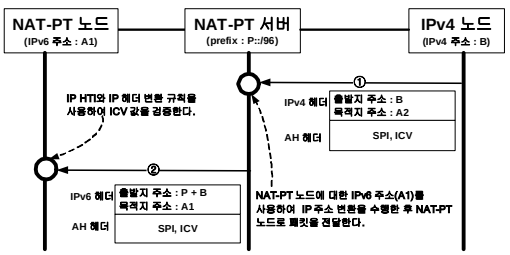


그림 7. IPv4 노드로부터 NAT-PT 노드까지의 AH 패킷 전달 과정

Ⅳ. 기존 NAT에서의 IPsec 적용 방법과 NAT-PT에서의 IPsec 적용 방법과의 비교

본 장에서는 본 논문에서 제안한 NAT-PT에서의 IPsec 적용 방법을 기존 NAT에서의 IPsec 적용 방법과 비교 분석하겠다.

NAT-PT는 NAT를 기반으로 설계된 메커니즘이다. 따라서 NAT에서 IPsec 트랜스포트 모드를 적용할 수 없는 이유는 NAT-PT에서의 IPsec 트랜스포트 모드를 적용했을 때의 문제점과 동일하다[12]. 그렇기 때문에 NAT에서의 IPsec 트랜스포트 적용을 위한 방법을 비교하는 것은 매우 중요한 일이다.

4.1 기존 NAT에서의 IPsec 적용 방법

4.1.1 UDP Encapsulation

NAT에서 IPsec 트랜스포트 모드를 적용하기 위한 방법의 하나로써 IP 패킷을 UDP로 encapsulation하는 방법이 IETF의 인터넷 드래프트로 올라와 있는 상태이고, 실제로 많은 벤더들이 이를 구현해서 사용하고 있다. UDP Encapsulation 방법을 살펴보면 우선 IKE 수행 과정에서 NAT 존재여부나 위치를 파악하고, 만약 통신과정 중 NAT가 존재할 때는 상대쪽 노드의 NAT-Traversal을 지원하는지에 대한 여부를 확인한다. ESP 패킷을 검증하는 노드가 TCP/UDP 체크섬의 올바른 검증을 수행할 수 있도록 상대방의 사설 IP 주소를 교환한다. 이후 실제 ESP 프로토콜에서는 IP 헤더와 ESP 헤더 사이에 UDP 헤더를 추가하여 UDP Encapsulation을 수행한 후 NAT를 통해 ESP 패킷을 전달한다. 또한 IKE/IPsec 세션 중에 한동안 트래픽이 없더라도 NAT에서 주소/포트 바인딩 정보를 유지시켜 주도록 하기 위한 'Keep-alive' 메커니즘도 정의되어 있다.

4.1.2 RSIP

RSIP는 기존의 NAT에서의 IPsec 과 같은 양단간의 보안 적용 문제를 해결하기 위한 방법으로써 명시적인 IP 주소 할당을 지원하는 서버/클라이언트 구조를 갖는다. 또한 로컬 네트워크 내에서 라우팅을 위해 터널링 방법을 사용하며 다양한 터널 방식(IP-in-IP, L2TP, GRE)을 지원한다. RSIP 서버는 클라이언트와 RSIP 통신 프로토콜을 통해 RSIP 클라이언트에서 사용할 IP 주소 변환에 관련된 파라미터 (IP 주소, 포트정보 등)와 터널링 방식을 협상하며 각 클라이언트에 관한 상태 정보를 관리한다. 이러한 방법에서의 RSIP 클라이언트는 IP 주소 변환에 관련된 파라미터를 사용하여 패킷을 직접 구성할 수 있기 때문에 일반적인 노드가 수행하는 IPsec 수행이 가능하다.

4.2. NAT에서의 IPsec 적용 방법과 제안된 NAT-PT IPsec 적용 방법과의 비교

4.2.1 UDP Encapsulation

본 논문에서 제안하는 방법의 장점은 기존의 IKE 프로토콜을 수정할 필요가 없다는 것이다. UDP

Encapsulation을 수행하는 노드는 ESP 수행을 위해 IKE 수행 시 NAT의 존재 여부를 알아내기 위한 NAT-D 메시지와 TCP/UDP 체크섬 검증을 위한 NAT 노드의 사설 IP 주소 정보가 포함된 NAT-OA 메시지를 IKE 페이로드에 부가적으로 넣어서 보내야 하는 문제가 발생한다. 따라서 이것은 곧 기존 IKE 메커니즘을 수정해야 하는 문제로 이어지게 된다. NAT-PT에서는 IKE 수행 시 NAT-PT 서버가 IP 헤더 변환에 사용된 정보 (IP HTI)만 제공하기 때문에 기존의 IKE 메커니즘을 수정하지 않아도 된다. 또, 상대 노드의 UDP Encapsulation과 같은 특정 메커니즘을 지원하느냐의 여부와 관계없이 IPsec 수행이 가능하다. UDP Encapsulation 방법에서는 TCP/UDP 체크섬 문제를 해결하기 위해서 검증을 위해 ESP 패킷을 전달받은 노드 측에서 TCP/UDP 재계산을 수행해야 하므로 상대 노드가 NAT-Traversal을 지원해야 한다. 마지막으로 UDP Encapsulation 방법에서는 AH 적용에 관한 방법이 제시되어 있지 못하다.

표 3. ICV 검증을 위한 IPv4 헤더 필드.

UDP Encapsulation 방법	NAT-PT에서의 IPsec 적용 방법
상대노드에서 TCP/UDP 체크섬에 대한 올바른 검증을 위해 기존 IKE 메커니즘의 수정이 필요하다.	NAT-PT 서버는 단순히 IP HTI 정보를 보내줌으로써 IPsec 적용이 가능하므로 IKE 메커니즘의 수정이 필요 없다.
상대측 노드가 NAT-Traversal을 지원해야만 적용이 가능하다.	NAT-PT 노드 측에서 ESP와 AH 패킷에 대한 책임을 가지고 있으므로 상대노드가 특정 메커니즘을 지원 할 필요가 없다.
AH 적용 방법이 부재하다.	IPsec ESP와 AH 적용이 가능하다.

4.2.2 RSIP

RSIP방법은 기존의 IPsec 메커니즘을 수정하지 않고도 IPsec 트랜스포트 모드를 제공할 수 있도록 설계되어 있다. 하지만 RSIP에서는 기존 NAT 메커니즘을 변경시켜야 하는 문제가 존재하고, RSIP client는 외부 노드와의 통신 시 IP-in-IP tunneling 방법을 사용하는데 이는 NAT-PT에서는 근본적으로 IPv4 패킷을 생성할 수 없으므로 RSIP와 같은 IP Tunneling 방법을 사용할 수 없다. 그렇지만 본 논문에서 제안한 방법은 NAT-PT 노드가 IP Tunneling 방식을 통해 IPsec 트랜스포트 모드를 수행하는 것은 아니지만 NAT-PT 서버에서 제공하는 IP HTI를 통해 RSIP방법처럼 IPsec 트랜스포트 모드를 제공할 수 있고, RSIP처럼 기본 메커니즘을 크게 손상시키지 않고도 IPsec 트랜스포트 모드를 제공할 수 있다.

표 4. ICV 검증을 위한 IPv4 헤더 필드.

RSIP 방법	NAT-PT에서의 IPsec 적용 방법
기존 NAT 메커니즘에 대한 전체적인 수정이 필요하다.	IPv4 노드에서 UDP 500번 포트로 패킷이 들어올 때 해당 NAT-PT 노드에게 IP HTI 메시지를 제공하는 메커니즘만 구현하면 된다.
IP-in-IP 캡슐화를 통해서 IPsec을 수행한다.	NAT-PT 노드는 IPv4 패킷을 생성할 수 없으므로 IP-in-IP 캡슐화를 통한 IPsec 수행 방법을 적용할 수 없다.

V. 결 론

본 논문에서는 NAT-PT 환경에서 IPsec을 적용하였을 때의 문제점을 분석하였고, NAT-PT에서 IPsec을 적용하기 위한 방법을 제안하였다. 지금까지 NAT-PT에서의 IPsec을 해결하기 위해 제안된 메커니즘은 없으며 단지 IPsec 트랜스포트 모드 적용 시 발생하는 문제점만이 인터넷 드래프트로 제시되어 있다.

본 논문에서 제안된 방법은 NAT-PT 노드가 IKE 수행 중에 NAT-PT 서버가 제공하는 IP HTI를 사용하여 IPsec 트랜스포트 모드를 적용하므로 RSIP와 같은 방법에서처럼 주소 할당에 관한 서버와 클라이언트 모델이 필요하지 않으며, RSIP와 같이 기존 NAT-PT 메커니즘을 수정하지 않고도 IPsec 트랜스포트 모드 적용이 가능하다. 또, UDP Encapsulation방법에서와 같이 기존 IKE 메커니즘을 수정이 필요치 않으며, IPsec적용을 위해 상대 노드가 IPsec 지원을 위한 특별한 메커니즘이 구현될 필요가 없다. 마지막으로 실제 구현에 있어서 NAT-PT 서버는 단순히 IP HTI 메시지를 제공하는 메커니즘만 구현하면 되고, NAT-PT 노드에서의 TCP/UDP checksum과 AH헤더의 ICV 값 계산에 관한 메커니즘을 구현하면 되기 때문에 실제 구현에 관한 큰 문제점은 없을 것이다. 본 논문에서 제안한 방법을 사용함으로써 기존 NAT-PT 메커니즘이 가지고 있는 end-to-end security 문제를 해결할 수 있을 것으로 기대한다.

참 고 문 헌

[1] G. Tsirtsis, P. Srisuresh, “Network Address Translation Protocol Translation (NAT-PT),” RFC 2766, February 2000.

[2] S. Satapati, “NAT-PT Applicability,” draftsa-tapati-v6ops-natpt-applicability-00, October 2003.

[3] Egevang, K. and P. Francis, “The IP Network Address Translator (NAT),” RFC 1631, May 1994.

[4] Kivinen, T., “Negotiation of NAT-Traversal in the IKE,” draft-ietf-IPsec-nat-t-ike-08, February 2004.

[5] Huttunen, A. et. al., “UDP Encapsulation of IPsec Packets,” Internet Draft, draft-ietf-IPsec-udp-encaps-6.txt, January 2003.

[6] G. Montenegro, M. Borella, “RSIP Support for End-to-end IPsec,” RFC 3104, October 2001.

[7] E. Nordmark., “Stateless IP/ICMP Translation Algorithm (SIIT),” RFC 2765, February 2000.

[8] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, November 1998.

[9] S. Kent, R. Atkinson., “IP Encapsulating Security Payload (ESP),” RFC 2406, November 1998.

[10] S. Kent, R. Atkinson., “IP Authentication Header,” RFC 2402, November 1998.

[11] D. Harkins, D. Carrel., “The Internet Key Exchange (IKE),” RFC 2409, November 1998.

[12] Aboba, B. et. Al., “IPsec-Network Address Translation (NAT) Compatibility Requirements,” RFC 3715, March 2004.

최 인 석 (Inseok Choi) 준회원

2003년 2월 숭실대학교 정보통신전자공학과 학사

2005년 2월 숭실대학교 정보통신공학과 석사

2005년 2월~현재 (주)주홍정보통신연구원

<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안 RFID/USN 보안

정 수 환 (Souhwan Jung) 정회원

1985년 2월 서울대학교 전자공학과 학사

1987년 2월 서울대학교 전자공학과 석사

1998년~1991년 한국통신 전임연구원

1996년 6월 미 워싱턴 주립대(시애틀) 박사

1996년~1997년 Stellar One SW Engineer

1997년~현재 숭실대학교 정보통신전자공학부 부교수

<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안 RFID/USN 보안

김 영 한 (Younghan Kim) 정회원

1984년 2월 서울대학교 전자공학과 학사

1986년 2월 한국과학기술원 전기 및 전자공학과 석사

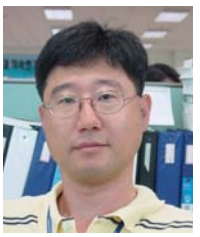
1990년 8월 한국과학기술원 전기 및 전자공학과 박사

1987년 1월~1994년 8월 디지콤 정보통신연구소 데이터통신연구부장

1994년 9월~현재 숭실대학교 정보통신전자공학부 부교수, 통신학회 인터넷 연구회 위원장, VoIP포럼 차세대기술분과위원장

<관심분야> 컴퓨터네트워크, 인터넷 네트워킹, 이동 데이터 통신망.

박 용 석 (Yongseok Park) 정회원



1986년 2월 서울대학교 전자공학과 학사

1988년 2월 서울대학교 전자공학과 석사

1996년 5월 미 퍼듀 대학교 박사

1996년~2000년 AT&T STSM

2000년~2001년 Coree Networks, Systems Engineer

2001년~2001년 Lucent Technologies, Systems Engineer

2002년~현재 삼성전자 통신연구소 수석연구원

<관심분야> IP Routing, Wireless Networking