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

# IPsec 과 NAT 연동에 관한 연구

김건우*, 나재훈*, 손승원*
*한국전자통신연구원
e-mail : kimgw@etri.re.kr

# A Study on Interoperability between IPsec and NAT

Geon-Woo Kim*, Jae-Hoon Nah*, Sung-Won Sohn*
*Electronics and Telecommunications Research Institute

요 약

IPsec 기술은 양단간 보안은 물론, 모드, 암호 프로토콜, 다양한 암호화 알고리즘들의 조합을 통해서 다양하고 계층적인 보안 서비스를 제공한다. VPN 서비스가 제공되는 가장 일반적인 유형은 원격 접속자의 공동 인트라넷에 대한 접근을 허용하는 것이다. 하지만 NAT(Network Address Translation) 기술이 호텔과 같이 원격 접속자가 주로 사용하는 곳은 물론 홈 게이트웨이와 같은 네트워크 장치에 널리 사용되고 있어 IPsec 을 통한 양단간 통합 보안 서비스를 제공하는데 치명적인 장애가 발생한다. 따라서 본 논문에서는 IPsec 기술을 NAT 상의 네트워크에 적용할 때 발생하는 문제점과 기존의 해결 방안에 대해서 언급하고 이들의 장, 단점을 분석한다. 또한 효율적으로 IPsec 기술을 NAT 네트워크 상에 적용할 수 있는 새로운 연동 방안을 제시함으로써 네트워크 구조에 독립적인 보안 서비스를 제공하고자 한다.

## 1. 서론

IP Security(IPsec) Protocol Suite 는 Internet Protocol(IP)을 보호하기 위한 일련의 지침으로서[1] IPv4 와 IPv6 네트워크에 상호 호환되는 높은 레벨의 암호학적 보안 서비스를 제공하기 위해 설계되었다. IPsec 에서 제공되는 보안 서비스로는 접근 제어, 비연결형 무결성, 데이터 인증, 재연 공격에 대한 방지(부분적으로 무결성 제공), 기밀성(암호) 및 제한된 트래픽 흐름 기밀성 등이 있다. 이러한 서비스들은 IP 계층에서 제공되며, IP 계층 혹은 상위 계층을 보호한다[2].

VPN 서비스가 제공되는 가장 일반적인 유형은 원격 접속자의 공통 인트라넷에 대한 접근을 허용하는 것이다. 하지만 NAT 기술이 호텔과 같이 원격 접속자가 주로 사용하는 곳은 물론 홈 게이트웨이와 같은 네트워크 장치에 널리 사용되고 있어 IPsec 을 통한 양단간 통합 보안 서비스를 제공하는데 치명적인 장애물로 작용하고 있다[3]. NAT 와 같은 인증된 중간 노드에 의한 IP 헤더의 수정을 허용함으로써 호스트에서 집행한 보안 메커니즘에 위배되어 정상적인 IPsec 서비스를 제공할 수 없기 때문이다.

따라서 본 논문에서는 IPsec-NAT incompatibility 문제와 기존 해결 방안의 장, 단점을 분석하고, 새로운 IPsec-NAT 연동 방안을 통한 네트워크 구조에 독립적인 보안 서비스를 제안한다.

## 2. Incompatibilities between IPsec and NAT

NAT 는 IP 주소 부족 문제를 해결하기 위해 private 네트워크 내부의 로컬 IP 를 사용하는 호스트와 외부 글로벌 네트워크와의 투명한 통신을 제공한다[4].

NAT 는 로컬 네트워크와 글로벌 네트워크 경계에 존재하는 라우터에서 동작하며 네트워크 주소 변환을 수행한다. 이 방식은 현존하는 다양한 네트워크 주소 변환 방법들 중 가장 간단하며, 양방향 네트워크 주소 변환을 지원한다. 또한, 주소 변환이 네트워크 계층에서만 일어나므로 주소변환 속도도 빠르고 인터넷에서 사용되는 다양한 서비스를 지원할 수 있다.

하지만 실시간으로 전송되는 패킷의 IP 주소를 수정함으로 인하여 많은 문제점들이 발생한다.

IPsec 과 NAT 간에 발생하는 Incompatibilities 는 다음과 같이 세 개의 범주로 구분할 수 있다. (1) 근본적인 NAT 이슈. 이는 NAT 의 본연의 기능에서 파생되는 문제로서 모든 NAT 장비에서 발생한다. 본 논문에서는 이러한 문제점을 해결하는데 중점을 두고 있다. (2) NAT 의 구현상의 이슈. 이는 NAT 본연의 문제가 아

닌 구현상의 문제를 의미한다. 예를 들어, 인바운드/아웃바운드 패킷 처리 문제 등이 이에 해당한다. 많은 NAT 장비에서 발견되고 있지만 고려하지 않는다. (3) NAT 에서의 IPsec 적용을 돕기 위한 함수로 인한 새로운 문제점이 발생할 수 있다.

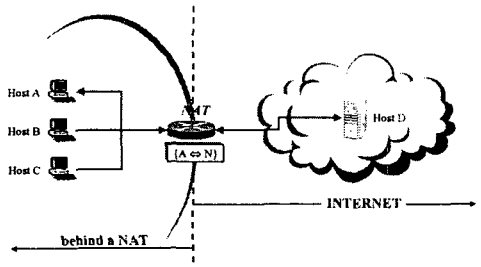


그림 1 일반적인 NAT 네트워크 구조

(a) AH 와 NAT 간의 incompatibility

AH 메커니즘은 IP 헤더에 대한 무결성을 보장하므로, NAT 에 의한 IP 헤더의 변화로 인하여 수신한 호스트에서의 무결성 검사는 실패하게 된다.

(b) Checksum 과 NAT 간의 incompatibility

TCP/UDP/SCTP Checksum 계산 시, pseudo-header 의 주소를 포함하므로 주소가 변경될 경우 Checksum Invalidation 이 발생한다.

(c) IKE 주소의 Identifier 와 NAT 간의 incompatibility

IKE 패킷의 Identifier 필드에 IP 주소를 사용할 경우, 패킷 내부의 Identifier 와 외부 IP 헤더의 주소가 일치하지 않아 패킷이 폐기된다.

(d) 중복되는 SPD 엔트리와 NAT 간의 incompatibility

NAT 내부의 다중 호스트들이 외부의 한 호스트와 보안 정책을 협상하는 경우, 패킷을 전송하는 호스트 측면에서는 모든 IPsec SA 들이 같은 양단을 가지므로 하나의 SA 처럼 보여서 잘못된 IPsec SA 를 적용한 패킷이 전송될 수 있다.

(e) IPsec SPI 와 NAT 같의 incompatibility

IPsec ESP 트래픽은 암호화되어 전송되기 때문에, de-multiplexing 하기 위해서는 IP/IPsec 헤더 정보를 사용해야 한다. 일반적으로 Destination Address, Security Protocol(AH/ESP), SPI 의 조합을 사용한다. 하지만 SPI 값만으로는 Destination Address 를 정할 수 없으므로 잘못된 호스트로 IPsec 패킷이 전송될 수 있다.

(f) Embedded IP Address 와 NAT 간의 incompatibility

내부 IP 주소와 외부 IP 주소의 불일치로 인하여 발생하는 문제이다[3].

## 3. 기존의 해결 방안

### 3.1 IPsec 터널 모드

IPsec 터널 모드는 다음과 같은 한정된 환경에서 IPsec/NAT 문제를 해결할 수 있다.

- IPsec ESP
  IPsec ESP 프로토콜은 외부 IP 헤더는 보호하지 않는다.
- No Address Validation
  Source Address 에 대한 별도의 검사를 하지 않음(IKE Identifier vs. Source Address)
- "Any to Any" SPD Entries
  "any to any" 정책을 협상하게 되면 주소가 변환되더라고 별 문제가 발생하지 않는다.
- Single client operation
  NAT 내부에서는 한 호스트만 동작
- No fragmentation
  인증서를 사용할 경우 IKE Fragmentation 발생
- Active Sessions
  Lifetime 동안 세션을 계속

### 3.2. RSIP (Realm Specific IP)

RSIP 는 기존의 IP 주소 변환 방식의 양단간 연결성 제공과 보안 지원, 다양한 사용자 응용 프로그램을 지원하기 위해 많은 ALG(Application Level Gateway)가 필요하다는 단점을 극복하기 위해 나타난 터널을 이용한 새로운 IP 주소 변환 방식이다. RSIP 는 기존의 NAT/NAPT 의 대안으로 출현하였으며 클라이언트/서버 구조를 갖는다. 또한, 로컬 네트워크 내에서 라우팅을 위해 터널을 사용하며 다양한 터널 방식(IP-IP, L2TP, GRE, ..)을 지원한다. 호스트와 게이트웨이와의 통신을 통해서 IPsec SPI 의 de-multiplexing 문제와 SPD 중복 문제에 접근하며 홈 네트워크는 물론 대규모 적합하다. NAT 내부의 모든 호스트는 게이트웨이의 외부 IP 주소를 공유하고 Embedded IP 와도 호환된다. 모든 프로토콜(AH/ESP)과 모드(Tunnel/ Transport)를 지원하지만 기존의 IPsec 시스템과의 연동에 대한 보장은 없다. 이 방법은 RSIP 가 가능한 게이트웨이를 요구하므로 IPsec-NAT 호환에 관계된 요구사항을 만족시키지 못하는 단점이 있으며 IPv6 에서 반드시 구현되어야 하므로 거의 사용되지 않는다[5].

### 3.3 6to4

6to4 방식은 IPv6 사이트들끼리 별도의 터널 설정 없이 IPv4 네트워크를 통해 통신하거나 relay router 를 사용해서 native IPv6 도메인과 통신하기 위해서 개발된 임시 메커니즘이다. 이 방법은 최소한 하나 이상의 글로벌 IPv4 주소를 가지는 사이트에 IPv6 Prefix 를 할당하고 이를 이용해서 IPv6 패킷을 Encapsulation 하는 메커니즘을 정의한다[6].

| 3 | 13 | 32 | 16 | 64 bits |
|---|---|---|---|---|
| FP 001 | TLA 0x0002 | V4ADDR | SLA ID | Interface ID |

그림 2. IPv6 Prefix Format

그림 2 와 같이 48 비트의 IPv6 Prefix 가 생성되면 이는 2002:V4ADDR::/48 로 표현될 수 있다. 이러한 형식으로 파생된 IPv6 Prefix 를 이용해서 6to4 pseudo-interface 에서 IPv4 헤더로 Encapsulation 하여 IPv4 네트워크를 통과하면 목적지 6to4 pseudo-interface 에서 Decapsulation 한다.

IPv6 네트워크나 6to4 호스트와의 자유로운 IPsec 통신을 가능하게 하고, 호스트에는 별도의 수정을 요구하지 않지만 NAT 에는 6to4 를 지원하기 위한 별도의 기능이 추가되어야 한다. 기존에 존재하는 방법 중

에서는 가장 효율적이지만 단시간에 구현되어 적용되기에는 어려움이 있으며 IPv6/IPv4 연동에 국한되는 경향이 있다.

그림 3 은 6to4 가 적용되는 예를 보여주고 있다.

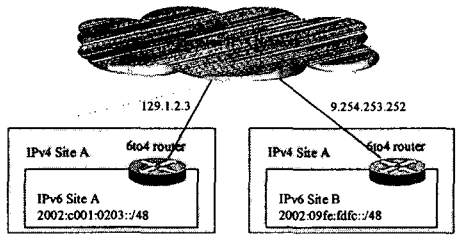


**그림 3 6to4 Example**

## 4. Interoperability between IPsec and NAT

통신하고자 하는 양단 호스트는 각각의 SPD 에 정의되어 있는 보안 정책을 기반으로 새로운 SA 를 협상한다. IPsec 패킷을 전송하는 호스트는 협상된 SA 에 의해서 보안 알고리즘을 적용하여, 전송 도중 불법 접근으로부터 패킷의 무결성, 기밀성 등을 보장한다. 또한 모드와 프로토콜의 중복 적용으로 다양한 security granularity 를 보장한다. IPsec 의 기본 개념은 보안 레벨에 따라 중간 노드에 의한 불법 접근을 허용하지 않는 것이다. 하지만 NAT 는 기본적으로 IP 헤더의 주소 영역에 직접 접근하기 때문에 IPsec 의 개념과 정면으로 대치되는 상황이다. 앞 장에서 보는 바와 같이, IPsec 와 NAT 간의 incompatibilities 을 해결하기 위해서 많은 연구가 이루어지고 있지만 기존 서비스에 많은 변화나 오버헤드를 요구한다. 따라서 기존 시스템에는 변화를 요구하지 않는 범위 내에서 NAT 의 영향을 최소화 시키는 방안을 모색해야 한다.

### 4.1 IP Address Substitution

패킷을 전송하는 호스트의 입장에서는 IPsec 본연의 서비스에 충실하되 NAT 에 대한 투명성을 가져야 한다. 만일 호스트가 NAT 가 설치되어 있는 라우터에서 변환될 IP Address 를 미리 알 수 있다면 문제는 의외로 간단해진다. 알고리즘을 적용할 때 변환될 IP Address 로 대체하면 된다.

그림 4 는 IP Address 의 대체 과정을 보여주고 있다.

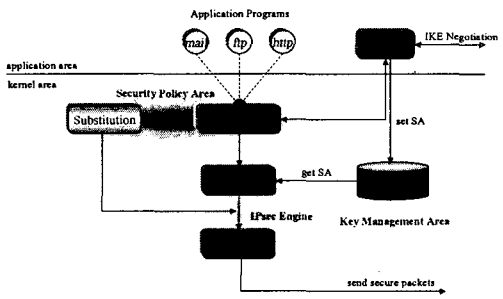


**그림 4 Address Substitution**

AH 프로토콜이나 터널 모드를 지원할 때, 해당 IP Address 를 변환될 IP Address 로 대체해서 알고리즘을 적용한다. 이 때, IP Address 가 설정되어 있는 헤더 정보를 수정하는 것이 아니라 알고리즘 함수의 입력 인자인 주소 영역만을 대체한다. 즉, NAT 에 의해서 변환될 IP Address 를 포함하여 인증과 기밀성을 제공한다. 엄격히 말하자면, 호스트에서는 잘못된 해쉬와 암호 값을 생성하고 NAT 에서 이를 교정하는 방식이다. IP 주소를 대체하는 함수를 추가하는 것은 별로 어려운 과정이 아니다. 이러한 변환될 정보들을 저장하고 관리하는 것은 구현에 독립적이며, 보안 정책 시스템의 데이터베이스에 필드를 추가하는 것도 하나의 방법이 될 수 있다.

### 4.2 Recognition of NAT-related information

통신하고자 하는 양단 호스트는 변환될 주소를 미리 인지하여 이를 암호화 메커니즘에 적용한다. IPsec 패킷을 전송할 때 실시간으로 변환 정보를 인지해야 하므로, 별도의 Request/Reply 메시지를 사용하면 호스트와 라우터에 불필요한 오버헤드를 가중시킨다. 따라서 시스템에서 사용하는 패킷을 이용하여 Request 메시지의 기능을 대신하게 하고, 더불어 발생하는 Address Pool 의 변화를 감지하여 양단 호스트에 주소 변환 정보를 포함하는 메시지를 전송한다.

그림 5 는 이러한 과정을 도식화한 그림이다.

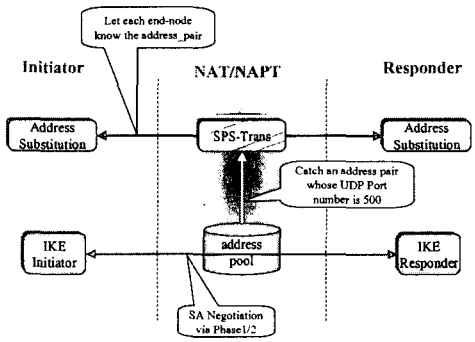


**그림 5 Recognition of NAT-related information**

Initiator 가 Responder 와 IPsec 세션을 설정하고자 하는 경우, IPsec 이 정하는 표준 플로우에 따라 먼저 IKE 가 새로운 SA 를 협상한다. IKE 패킷은 보통 평문 형태로 전송되며 NAT 가 설치되어 있는 라우터를 통과할 것이다. 다른 패킷과 마찬가지로 NAT 에 의해서 새로운 주소로 변환되며 이러한 내용을 캐쉬에 저장한다. 바로 이 순간 SPS-Trans 가 UDP Port 500 을 사용한 패킷이 변환된 주소 쌍을 검색하여 이를 양단 호스트에 전송한다. 따라서 시스템과 네트워크에 최소한의 오버헤드로 IKE 협상이 끝나기도 전에 이미 양단 호스트는 NAT 관련 정보를 인지하고 있는 것이다.

### 4.3 Example

그림 6 은 NAT 내부 네트워크에 위치한 129.254.10.1 의 가상 주소를 가지는 호스트 A 와 외부 네트워크에 위치한 129.10.1.1 의 글로벌 주소를 가지는 호스트 B 가 통신하는 과정을 기술하고 있다.

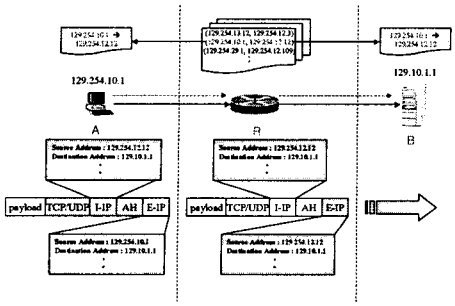


그림 6. Example

IPsec 패킷을 전송하기 위해서 먼저 해당하는 Security Association 을 조회한다. 만일 해당하는 SA 가 존재한다면 이는 IKE 협상의 완료와 변환될 주소 정보를 이미 저장하고 있다는 의미한다. 해당하는 SA 가 존재하지 않으면 새로운 IKE SA 협상을 시작하는데 협상 패킷은 UDP Port No. 500 을 가지며 암호화되지 않은 평문 형식으로 NAT 가 설치되어 있는 라우터 R 을 통과한다. NAT 를 통과하는 순간, 외부 헤더의 Source Address 인 129.254.10.1 이 129.254.12.12 로 변환되고 이 정보를 캐쉬 데이터베이스에 저장된다. 동시에 SPS-Trans 는 변환 정보를 양 호스트에 전송한다..

만일 IKE 에 의해서 협상된 SA 가 AH Tunnel 모드라고 가정하자. IPsec 패킷을 전송하는 호스트 A 는 다음과 같은 작업을 수행한다

■ TCP/UDP Checksum 계산

IPv4 에서는 TCP checksum, IPv6 에서는 TCP/UDP checksum 계산이 mandatory 로 설정되어 있다. 미리 인지된 변환 주소 정보를 이용한다. 즉, pseudo-header 의 Source Address 를 129.254.12.1 이 아닌 129.254.12.12 로 대체하여 계산한다.

■ 내부 IP 헤더

내부 헤더의 Source Address 를 129.254.12.1 이 아닌 129.254.12.12 로 대체한다. 왜냐하면 내부 헤더는 NAT 에 의해서 변환되지 않는 영역이며, 또한 사용하는 주소 또한 외부 글로벌 네트워크에서는 사용할 수 없는 가상 주소이다. 따라서 미리 변환될 주소로 대체하여 헤더를 구성하는 것이 바람직하다.

■ AH 헤더

AH 프로토콜은 외부 IP 헤더에 대해서도 인증을 제공한다. 따라서 해쉬 값을 계산할 때 외부 IP 헤더의 Source Address 를 129.254.12.12 로 대체하여 계산한다. 외부 IP 헤더의 Source Address 를 수정하는 것이 아니라 다만 AH 함수의 입력 주소의 값만을 대체하는 것이다. 이러한 과정을 통하여 전송된 패킷은 NAT 에서 외부 IP 헤더의 Source Address 가 예상된 주소로 변환될 것이고, 수신 호스트에서 정확하게 Validation 된다. 반대 방향의 경우, 즉 호스트 B 가 호스트 A 에 패킷을 전송하는 경우는 Source Address 가 아닌 Destination Address 를 대체하여 위와 같은 과정을 반복하면 된다.

## 5. 결론

IPsec 은 IPv4 와 IPv6 네트워크에 상호 호환되는 높은 수준의 암호학적 보안 서비스를 제공하기 위해 설계되었다. IPsec 에서 제공되는 보안 서비스로는 접근 제어, 비연결형 무결성, 데이터 인증, 재연 공격에 대한 방지, 기밀성 및 제한된 트래픽 흐름 기밀성 등이 있다. 이러한 서비스들은 IP 계층에서 제공되며, IP 계층을 포함하는 상위 계층을 보호한다. 또한 모드, 암호 프로토콜, 알고리즘 등의 조합을 통해서 사용자에게는 다양한 security granularity 를 제공한다.

AH 프로토콜은 외부 IP 헤더를 포함한 메시지 전체에 대한 인증 서비스를 제공하지만 NAT 에 의한 패킷 헤더의 수정으로 인하여 AH invalidation, IKE Identifier 와 IP 헤더 Address 와의 불일치 , Embedded IP 헤더, TCP/UDP checksum invalidation, SPD overlapping 및 SPI selection 등 다양한 심각한 문제가 발생한다.

IPsec ESP 터널 모드를 사용하는 것은 제한된 환경에서만 가능하며 다양한 IPsec 보안 서비스의 사용을 제한하므로 바람직하지 않다. RSIP 를 사용하는 방식은 클라이언트/서버 구조로 모든 IPsec 와 NAT 를 지원하는 모든 시스템들이 RSIP 프로토콜을 지원하도록 설계되어야 하므로 과중한 오버헤드가 부가되고 RSIP 과 IPsec 과의 상호호환성에 대해서도 아직 입증된 바가 없다. 6to4 방식을 사용하는 방식은 현재 가장 널리 연구되는 방식으로 IPv6 를 지원하는 호스트에는 추가적인 지원이 필요 없지만, 모든 NAT 에서 6to4 를 지원해야 한다. 이 방식은 IPv6 와 IPv4 간의 연동과 관련된 방식으로 일반적인 IPv4 네트워크의 NAT 에 적용하기에는 무리가 따르며 단시간에 구현, 적용하기가 어렵다.

본 논문에서 제안하는 방식은 IPsec 패킷을 전송하는 호스트가 변환될 주소를 미리 인지하여 이를 기반으로 한 암호 알고리즘을 적용하는 것이다. 이는 기존의 IPsec 과 NAT 시나리오를 그대로 적용하기에 가장 적합한 방법이다. 별도의 프로토콜을 사용하지 않는 것도 장점이다. IPsec 패킷을 전송하기 전에 생성되는 IKE 협상 패킷을 Request 메시지로 사용하므로 시스템과 네트워크에 오버헤드가 없고 실시간으로 변환 주소 정보를 인지할 수 있다.

## 참고문헌

[1] Chien-Lung Wu, "IPsec/PHIL(packet header information list): design, implementation, and evaluation", IEEE/IEE Computer Communications and Networks, 2001

[2] IETF RFC 2401 "Security Architecture for Internet Protocol"

[3] IETF <draft-ietf-ipsec-nat-reqts-02.txt> "IPsec-NAT Compatibility Requirements"

[4] IETF RFC 3022 "Traditional IP Network Address Translator (Traditional NAT)"

[5] 정보통신연구원 간행물, 전우직, 이광희 "IP 주소 변환 기술에 관한 연구 동향"

[6] IETF RFC 3056 " Connection of IPv6 Domains via IPv4 Clouds"