네트워크 주소 변환에 따른 보안 정책 협상

김건우[0] 나재훈 손승원
한국전자통신연구원
(kimgw[0], jhnah, swsohn)@etri.re.kr

SPS-ALG : Security Policy Negotiation through a NAT

Geon-Woo Kim[0] Jae-Hoon Nah Sung-Won Sohn
Dept. of Network Security, Electronics and Telecommunications Research Institute

요 약

IPsec 기술은 양단간 보안은 물론, 모드, 암호 프로토콜, 다양한 암호화 알고리즘들의 조합을 통하여 다양하고 계층적인 보안 서비스를 제공한다. 또한, 보안 정책 시스템은 패킷 처리에 관한 지침은 물론, IPsec의 핵심 요소인 Security Association을 협상하기 위한 보안 기반 규칙을 제공한다. 하지만 인터넷의 확장과 더불어 발생한 IP 주소 부족 문제를 해결하기 위한 NAT로 인하여 IPsec과 같은 단대단 통합 보안 서비스를 제공하는데 치명적인 장애가 발생하게 되었다. 또한 서로 다른 네트워크의 정책 서버간 보안 정책 협상도 NAT에 의한 주소 변환으로 인하여 불가능하게 되었다. 따라서 본 논문에서는 NAT 상에서의 효율적인 보안 정책 협상과 인증서 발급을 위한 SPS-ALG (Security Policy System-Application Level Gateway)를 제안한다.

1. 서론

인터넷상에서 전자상거래, VPN(Virtual Private Network) 서비스 등을 지원하기 위한 네트워크 보안 기술에 대한 연구가 활발히 진행되고 있다. 특히, 방화벽과 같은 보안 게이트웨이는 도메인의 경계부에 설치되어 메시지 인증, 접근 제어 및 IP 레벨의 보안(IPsec)과 Transport 레벨의 보안(TLS/SSL)과 같은 보안 프로토콜을 지원한다. 또한 인터넷 트래픽에 대해서 기밀성, 무결성 및 인증 서비스를 제공한다[1].

보안 정책은 효율적인 네트워크 보안 관리를 위한 해결 방안이지만 이에 대한 정의는 매우 다양하며[2] 서로 다른 환경에서의 네트워크를 제어하기 위한 규칙의 집합으로 규정할 수 있다[3].

보안 정책 시스템(SPS : Security Policy System)은 보안 정책 정보를 위한 분산 데이터베이스로서, 보안 도메인 내의 호스트들에 대한 보안 정책 정보를 접근을 허용한다. 보안 정책 프로토콜(SPP : Security Policy Protocol)은 클라이언트와 서버간에 정책 정보가 교환, 처리 및 보호되는 방법과 형식을 정의한다[5].

이러한 보안 정책 시스템은 패킷 처리에 관한 지침은 물론, IPsec의 핵심 요소인 SA(Security Association)을 협상하기 위한 기반 규칙을 제공한다. 하지만 인터넷의 확장과 더불어 네트워크 주소 변환 기술(NAT : Network Address Translation)이 널리 사용되고 있으며, 이로 인하여 IPsec과 같은 단대단 통합 보안 서비스를 제공하는데 치명적인 장애가 발생하였다. 또한 정책 서버간 협상 메커니즘에서도 Payload 내부에 IP 주소를 사용하는데, NAT 외부 IP 헤더의 주소만 변환할 뿐 Payload에 대해서는 접근은 허용되지 않는다.

이에, 외부 IP 헤더의 주소와 내부 Payload 주소의 불일치로 인하여 정상적인 정책 협상이 이루어지지 않는다. 따라서 본 논문에서는 NAT 환경에서의 효율적인 보안 정책 협상을 위한 SPS-ALG(Security Policy System-Application Level Gateway)를 제안한다.

제 2장에서는 SPS에 대해서 설명하고 제 3장에서는 NAT에 대해서 간단하게 설명한다. 제 4장에서는 NAT상에서의 정책 협상 메커니즘을 제공하는 SPS-ALG를 제안하고 제 5장에서 결론을 맺도록 한다.

2. Security Policy System

SPS에서 각 보안 도메인은 네트워크 자원(호스트, 서브넷, 네트워크, 정책 서버)과 정책을 통해서 도메인을 유일하게 정의하는 master file을 가진다. 이러한 정책은 로컬 데이터베이스에 저장되고, 정책 서버(PS : Policy Server)는 클라이언트 어플리케이션에게 정책 정보에 대한 접근을 허용한다. 정책 클라이언트(PC : Policy Client)는 PS와의 연동을 통해서 IPsec에 적용되는 보안 정책을 제공한다.

그림 1은 SPS를 구성하는 컴포넌트와 이들간의 연동을 보여주고 있다. 보안 정책 데이터베이스(SPDB)는 Local Policy Database, Cache Database 및 Security Domain Database로 구성되며, 이것은 어디까지나 논리적인 구분이며 구현에 종속적이다.

PC가 클라이언트 SPDB에서 해당 정책을 검색하여 IKE 서버에 제공하고 존재하지 않을 경우 PS에 요청한다.

PS는 서버 SPDB의 정책 정보를 PC에 제공하지만 PS도

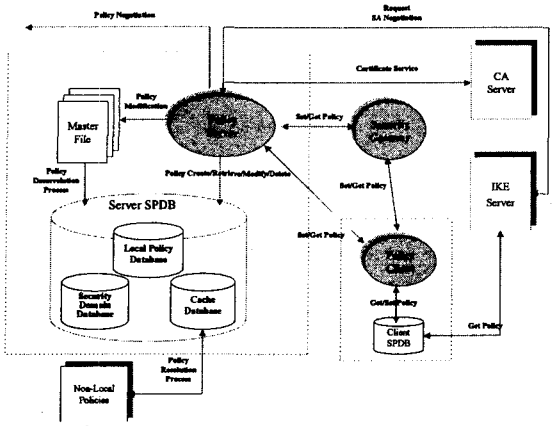

그림 1 SPS Components and Interactions

해당 정책 정보를 가지고 있지 않으면 해당 PS와 새로운 정책을 협상한다. 이러한 과정을 통해서 생성된 보안 정책 정보는 각 SPDB에 저장되고 IKE 서버에 제공된다.

3. NAT(Network Address Translation)

그림 2는 IP 주소 부족 문제를 해결하기 위해 로컬 네트워크 내의 통신에서는 로컬 IP를 사용하고, 인터넷과 같은 글로벌 네트워크와 통신을 할 경우 사용되는 NAT의 동작 방식과 흐름도를 기술한다.

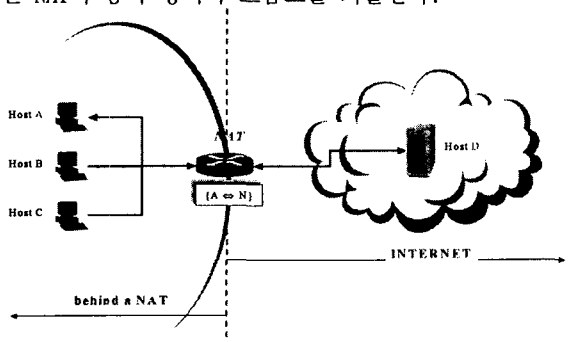

그림 2 Basic NAT의 네트워크 구조

NAT는 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 주소 변환 속도도 빠르고 인터넷에서 사용되는 다양한 서비스를 지원할 수 있다[6]. 하지만, NAT와 같은 인증된 중간 노드에 의한 IP 헤더의 수정을 허용하는 것은 일부 네트워크 환경에서는 불가피한 선택일수 있지만, IPsec, IKE 및 SPS와 같이 IP 주소를 기반으로 단대단 서비스를 제공하는 많은 시스템에 영향을 끼친다.

4. SPS-ALG

SPS는 새로운 정책을 협상하기 위해서 SPP(Security Policy Protocol)을 사용한다. SPP 메시지는 IPsec이나 다른 보안 알고리즘에 의해서 인증되어야 하면 무결성을 보장할 수 있어야 한다.

4.1 SPP(Security Policy Protocol)

SPP 메시지는 다음과 같은 6가지 메시지로 구성된다.

- Query Message
  특정 정책 정보를 요청하는 메시지
- Reply Message
  Query Message에 대한 정책을 포함하는 메시지
- Policy Message
  PS로 정책을 upload/download하기 위한 메시지
- Policy Acknowledgement Message
  Policy Message에 대한 Ack 메시지
- Transfer Message
  PS간 정책 정보를 교환하기 위한 메시지
- Keep-Alive Message
  보안 게이트웨이나 다른 모니터링 장치에 서버의 상태를 알려주는 메시지

4.2 SPS Negotiation through a NAT

그림 3은 NAT상에서 보안 정책을 협상할 때 발생하는 주소 불일치 과정을 보여주고 있다.

외부 IP 헤더의 주소는 NAT에 의해서 글로벌 주소인 129.254.12.12로 변환되어 호스트 B로 라우팅 되지만 메시지 내부의 IP 주소는 호스트 A의 로컬 주소인 129.254.12.1을 그대로 가진다. 이러한 불일치로 인하여 인증이 실패하게 되어 패킷이 폐기되면 정책 협상이 이루어 지지 않으므로 IPsec 서비스는 제공할 수 없다.

또한 인증서를 발급 받기 위해서는 IP 주소를 통해서 인증할 수 있어야 하지만 로컬 주소를 사용하기 때문에 문제가 발생할 수 밖에 없다.

이러한 주소 불일치와 인증서 문제를 해결하기 위해서는 NAT가 설치되어 있는 라우터에서 보안 정책 패킷에 대해서 추가적인 작업이 필요하다

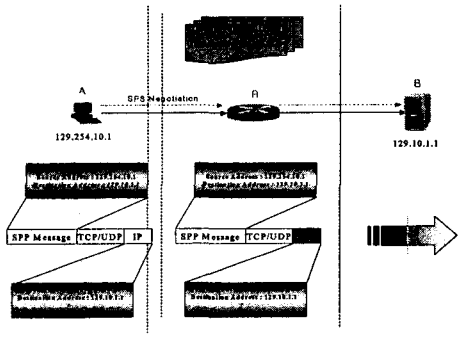

그림 3 NAT상의 SPS Negotiation

4.3 SPS-ALG(Security Policy System-Application Level Gateway)

SPS-ALG는 DNS나 ftp와 마찬가지로 라우터에서 어플리케이션 정보에 대한 접근을 허용한다.

LDAP을 통해서 인증서를 발급받거나 SPP를 통해서 새로운 정책을 협상하는 과정에서, NAT에 설치된 SPS-ALG과의 연동을 통해서 변환될 주소 정보를 습득한다.

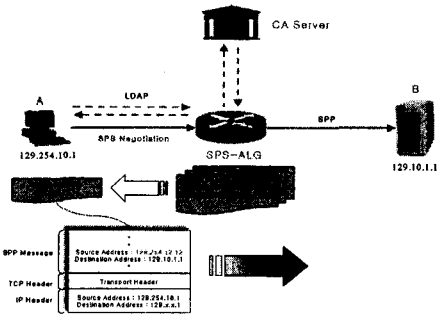

그림 4 SPS-ALG

그림 4에서 보는 바와 같이 SPP나 LDAP 프로토콜을 사용하면 NAT 주소 정보를 수신한다. 호스트 A로부터 외부로 향하는 패킷이 통과하기 전에 NAT는 주소 매핑 정보를 설정하지 않는다. 따라서 호스트 A는 외부 글로벌 네트워크로 ICMP와 같은 패킷을 보내면, SPS-ALG가 이 패킷에 의해서 Triggering되어 캐쉬 데이터베이스의 주소 매핑 정보를 호스트 A로 전송한다.

이런 정보를 바탕으로 Payload를 구성하는데 자신의 로컬 주소가 아닌 매핑 주소를 사용한다. 습득된 인증서 역시 매핑 주소에 대한 인증 정보를 포함하고 있다.

5. 결론

보안 정책은 서로 다른 환경에서의 네트워크를 제어하기 위한 규칙의 집합으로, 보안 정책 시스템(SPS : Security Policy System)은 보안 정책 정보를 위한 분산 데이터베이스로 규정할 수 있다. 또한 인터넷의 급속한 확산으로 인하여 발생하는 IP 주소 부족 문제를 해결하기 위해서 NAT와 같은 주소 변환 기술에 관한 연구가 활발히 진행되고 있다.

하지만 보안 정책 시스템의 SPP 메시지에서 사용하는 IP 주소에 대해서는 NAT의 접근이 허용되지 않기 때문에 외부 IP주소와 메시지 내의 IP 주소의 불일치로 인하여 정책 협상 과정에서 심각한 문제가 발생할 수 있다.

IPsec과 IKE와 마찬가지로 SPS도 IP 주소를 기반으로 호스트 인증과 chain-of-trust 기법을 사용하므로, IP 주소의 변환은 곧 인증 실패로 연결된다.

이러한 문제점을 해결하기 위해서 본 논문에서 제안한 방식이 SPS-ALG를 사용하는 것이다. ALG를 사용하는 다른 어플리케이션들과 마찬가지로 어플리케이션 레벨의 데이터에 대한 접근을 허용한다.

즉, 호스트는 SPS-ALG와의 연동을 통해서 정책 패킷을 전송하기 전에 이미 NAT에서 매핑될 주소 정보를 획득하여 이를 메시지의 주소 영역에 직접 반영한다. 또한 CA 서버로부터 획득한 인증서도 자신의 글로벌 IP 주소에 해당한다. 주소 매핑 정소를 취득하기 위해서 ICMP와 같은 제어 패킷을 사용할 수 있다. LDAP이나 SPP프로토콜을 사용하기 전에 외부 글로벌 네트워크로 ICMP 패킷을 전송하면 NAT에서 주소가 변환되고 이는 곧 호스트도 다시 재전송된다.

SPS-ALG를 사용함으로써 NAT상에서 효율적으로 보안 정책 서비스를 제공할 수 있을 뿐만 아니라 기존 네트워크에 적은 오버헤드로 쉽게 설치되어 NAT에 의한 문제를 쉽게 해결할 수 있다.

Reference

1. Zao J, Sanchez L, Condell M, Lynn C, Fredette M, Helinek P, Krishnan P, Jackson A, Mankins D, Shepard M, Kent S, "Domain Basd Internet Security Policy Management", Proceedings DARPA Information Survivability Conference and Exposition, DISCEX'00, IEEE Comput, Soc, Part vol.1, 1999, pp.41-53 vol.1, Las Alamitos, CA, USA.
2. Young-Ju Lee, Nam-Kyung Um, Ji-In Lee, Sang-Ho Lee, Geon-Woo Kim, "Design of A Working Mechanism for Hierachical Security Policy", Proceedings of The 12'th KISS Fall Conference, vol.1, 2000, pp.36-40, Taejon, KOREA.
3. Baltatu M, Lioy A, Mazzicchi D, "Security policy system: status and perspective" Proceedings IEEE International Conference on Networks 2000 (ICON 2000), Networking Trends and Challenges in the New Millennium. IEEE Comput, Soc, 2000, pp.278-284, Los Alamitos, CA, USA.
4. L.A. Sanchez, M.N. Condell, "Security Policy System", Internet Draft, Network Working Group, IETF, November 18, 1998.
5. L.A. Sanchez, M.N. Condell, "Security Policy Protocol", Internet Draft, Network Working Group, IETF, July 17, 2000.
6. 정보통신연구원 간행물, 전우직, 이광희 "IP 주소 변환 기술에 관한 연구 동향"