論文
5-1-5

리눅스기반 인트라넷 환경에서 효율적인 RSIP 주소 변환기법 (A Efficient RSIP Address Translation Technique in Linux-based Intranet Environment)

이영택(Young-Taek Lee)[1] 김원(Won Kim)[2] 전문석(Moon-Seog Jun)[3]

요 약

인터넷의 급격한 보급과 신규 IP 주소의 수요가 급증하면서 IP 주소가 부족해지는 현상이 일어나고 있다. 이러한 문제점을 해결하고자 NAT(Network Address Translation)과 같은 주소변환 기술이 널리 사용되고 있다. NAT는 두 개의 연결된 네트워크에서 서로 다른 IP 주소영역을 사용할 수 있도록 해주는 아주 유용한 주소변환 기술이다. 하지만 인베디드된 IP주소를 가지거나 단대단 보안을 위해 IP 패킷을 암호화하는 IPsec과 같은 어플리케이션 환경 하에서는 주소변환에 이용할 수 없고 매번 주소 변환을 수행 하면서 전반적인 주소변환처리 성능이 상당히 떨어지는 문제점을 가지고 있다. RSIP (Realm Specific Internet Protocol)는 이러한 문제를 해결하기 위한 대안 프로토콜이다. NAT와 RSIP 모두 내부와 외부 주소영역 사이에서 동작하는데 NAT는 내부망과 외부망 사이에 주소변환을 수행하여 외부망과의 통신에 사용하지만 RSIP는 라우팅 가능한 공인주소를 미리 할당하여 사용한다. 본 논문에서는 NAT의 단점과 보완사항을 알아보고 그 대안을 충족시킬 수 있는 방식인 RSIP 프로토콜을 사용하여 리눅스 기반 인트라넷 환경에서 효율적인 주소변환 시스템을 제안 하고자 한다.

ABSTRACT

An IP address shortage problem is happening with a rapid propagation of the Internet and demands about a new IP address. Address translation technology as NAT is becoming use widely in order to solve these problems. NAT is an very useful IP address translation technique that allows two connected networks to use different and incompatible IP address schemes. But it is difficult to use NAT particularly for applications that embeded IP addresses in data payloads or encrypted IP packet to guarantee End-to-End Security such as IPSec. In addition to rewiting the source/destination IP address in the packet, NAT must modify IP checksum every time, which could lead to considerablely performance decrease of the overall system in the process of address translation. RSIP is an alternative to solve these disadvantages and address shortage problems of NAT. Both NAT and RSIP divide networks into inside and outside addressing realms. NAT translates addresses between internal network and external network, but RSIP uses a borrowed external address for outside communications. RSIP server assigns a routable, public address to an RSIP client temporaily to communicate with public network outside the private network. In this paper, I will analyze NAT and RSIP gateway system, and then I will propose the Linux-based RSIP gateway for more efficient IP Address Translation in Intranet environments based on RSIP standard of IETF.

논문접수 : 2004. 1. 2.
심사완료 : 2004. 1. 10.

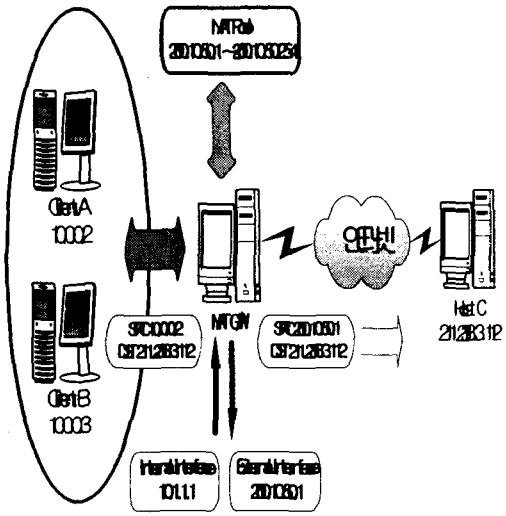
1) 정회원 : 롯데정보통신 롯데카드 IS사업
2) 정회원 : 전주기전여자대학
3) 정회원 : 숭실대학교

1. 서 론

인터넷 기술의 성장과 사용인구의 증가에 의한 IP 주소부족 문제를 해결 하고자 사설 IP주소를 사용하는 방법이 널리 사용되고 있다. 현재 NAT(Network Address Translation)는 비공인 IP주소를 사용하여 인터넷을 사용할 수 있는 대표적인 기술로서 네트워크 주소변환을 위해 널리 사용 되고 있다. NAT는 사설 IP주소를 이용하여 서로 다른 IP 주소방식을 사용하는 두 개의 네트워크를 연결 시켜주는 역할을 수행하는데 사설 내부 네트워크상에 있는 호스트가 투명하게 외부 네트워크상의 호스트와 통신 할 수 있도록 연결 시켜 준다. 하지만 주소변환 과정을 매번 수행함으로서 네트워크 트래픽이 심해질수록 전반적인 성능이 현저하게 감소하는 경향이 있다. 또한 단대단 보안이 필요한 IPSec과 같은 어플리케이션 환경하에서 호환 되지 않는 문제점을 가지고 있다. RSIP(Realm Specific IP)는 NAT의 이러한 단점과 현재 사용되고 있는 IPv4 방식에서의 주소 부족 문제를 해결하기 위해 IETF에서 제안한 프로토콜이다. 본 논문에서는 NAT의 문제점과 보완사항을 알아보고 그 대안으로 활용 할 수 있는 방안으로 RSIP 프로토콜을 적용하여 사설 IP주소를 사용하는 인트라넷 환경에서 보다 효율적인 주소 변환 기법을 제안 하고자 한다. 본 논문의 구성은 다음과 같다. 제 2장에서는 NAT나 NAPT와 같은 기존 NAT 기술에 대한 설명과 이와 관련된 연구에 관한 내용을 설명하고 제 3장에서는 터널링을 사용한 주소변환 방식인 RSIP에 관련된 내용과 활용방안을 소개하고 제 4장에서는 RSIP 개념을 도입하여 인트라넷 환경에서 어떻게 효율적으로 네트워크 주소변환에 활용할 수 있는지 RSIP 게이트웨이의 설계 및 구현에 관한 내용을 제안 한다. 제 5장에서는 제안한 시스템에 관한 성능 평가와 활용방안에 대하여 분석 한다. 마지막으로 제 6장에서는 결론 및 향후 연구 방향을 제시 한다.

2. NAT

NAT는 사설망에서 공인 IP주소의 부족으로 인한 대처 방안으로 고안된 것이다. 사설 IP 체계를 가진 내부망에서 인터넷과 같은 글로벌 라우팅 네트웍에 접속하기 위해 필요시 사설 주소를 공인 주소로 변환시켜 준다. 즉, 사설 IP주소를 사용하는 내부망에 있는 사용자가 외부의 서비스 접속시 패킷이 마치 사설주소를 사용하는 로컬 시스템에서 보낸 것처럼 사설 IP주소를 공인 IP주소로 변환 시켜주는 기술이라고 할 수 있다[1,2].



[그림 1] Basic NAT에 의한 Global Addressing

[Fig. 1] Global Addressing by Basic NAT

[그림 1]은 Client A, B와 Host C 간의 데이터의 흐름을 보여주고 있다. 먼저 Client A는 목적지 주소(211.238.3.112)를 가지고 있는 패킷을 인트라넷으로 보낸다. 인트라넷의 라우팅에 의해 그 패킷은 NAT 라우터의 주소가 10.1.1.1인 내부 인터페이스에 도달하게 된다. NAT 라우터는 패킷이 주소 전환 테이블과 대응되는 접근 리스트에 맞는지 확인한 후 주소 변환을 요청하게 된다. NAT 라우터는 먼저 패킷이 출발지 또는 목적지에서 온 첫 번째 패킷인지를 확인하기 위하여 자신의 NAT 테이블을 확인한다. 만약 패킷이 이전에 전환된 주소와 같은 주소라면 NAT 테이블을 참조하여 전환된 주소로

수정하고 이전에 전환된 적이 없는 주소를 가진 첫번째 패킷일 경우 아래의 두 가지 방법 중 하나를 이용하여 새로운 주소로 전환한다.

- NAT Pool 에서 하나의 주소를 선택하여 출발지 주소(10.0.0.2)를 목적지 Host C로 가기 위한 주소(200.10.50.1)로 전환한다.
- NAT Pool 에서 정적 할당에 의해 미리 정의되어 있는 주소로 전환하여 목적지 Host C로 패킷을 전송한다.

Dynamic NAT의 경우에는 사용하지 않는 주소들 중에서 숫자가 낮은 주소를 먼저 할당한다. 새로 할당된 주소는 다음의 이어지는 패킷들을 위하여 NAT 테이블에 등록되며 라우팅 테이블과 라우팅 알고리즘에 의해 다음 홉이 결정된다. NAT의 과정이 일어나고 난 후에 라우터는 새로 만들어진 패킷을 어느 인터페이스로 보낼지 결정하고 결정된 인터페이스를 통하여 패킷을 전송한다. 목적지 Host C는 인터넷 라우팅을 통하여 Client A가 보낸 패킷을 받게 되며 A의 주소가 200.10.50.1 (10.0.0.2이 NAT에 의해 전환된 주소)이라고 생각하게 된다. A가 보낸 패킷에 대한 응답으로 Host C는 자신이 알고 있는 Client A의 주소인 200.10.50.1을 목적지 주소로 가진 패킷을 전송한다. 인터넷 라우팅에 의해 200.10.50.1을 목적지로 하는 패킷은 NAT 라우터의 외부 인터페이스에 도달하게 되고 NAT 라우터는 NAT 테이블을 참조하여 패킷의 주소를 다시 원래의 주소인 10.0.0.1로 변환하여 내부 인터페이스를 통해 패킷을 전송하고 결국 Client A는 Host C가 보낸 패킷을 받을 수 있게 된다.

2.1 NAPT (Network Address Port Translation)

NAPT는 NAT의 가장 큰 문제점인 IP 주소 이용률이 낮은 단점을 극복하기 위해 나온 네트워크 주소 변환 방법으로 현재 가장 많이 사용되고 있는 기법이다. NAPT는 IP 주소 하나를 로컬 네트워크의 여러 호스트가 공유하여 동시에 공인망과 통신할 수 있는 주소 변환 방법으로 TCP/UDP 계층의 포트 변환을 통해 하나의 공인 IP를 여러 대의 로컬 호스트가 공유할 수 있도록 N:1 바인딩을 지원한다.

이 기법은 주소 변환을 위해 네트워크 계층의 목적지 주소 정보뿐만 아니라 트랜스포트 계층의 포트 정보를 이용해 IP 주소 이용률을 극대화한 시킨 방식이지만 IP 주소를 변환하기 위해 IP계층과 TCP/UDP 계층을 고려해야 하므로 처리가 복잡하고 처리속도도 느리다.

또한, 포트 번호에 민감한 서비스(Talk, RealPlayer)에 대해서 특별한 ALG(Application Level Gateway)를 사용하지 않으면 주소변환을 지원하지 못한다. 그리고 NAPT에서는 여러 개로 나뉘어 전달되는 패킷들을 하나의 완전한 패킷으로 만들기 위해 재조립해야 하는 등의 여러 문제점을 가지고 있다.

2.2 NAT의 한계 및 문제점

NAT 서비스는 IP 레이어와 TCP 레이어상에서 출발지, 목적지 등의 주소를 변경하여 IP 어드레스 부족 문제와 보안 문제를 동시에 해결할 수 있는 장점이 있는 반면 여러 문제점 또한 가지고 있다[1-3]. NAT는 1:1 바인딩으로 인한 IP주소 사용으로 효율성이 떨어진다. 반면 NAPT는 NAT의 단점을 보안, 포트 변환 방식을 통해 1:N 바인딩을 지원하므로 하나의 공인 IP주소에 여러 개의 로컬 호스트를 동시에 할당하여 IP주소 효율을 높일수 있다. 하지만 주소 변환시 포트까지 고려해야 하므로 변환 과정이 복잡하고 포트에 민감한 사용자 응용은 지원하지 못한다. 또한 매번 NAT 규칙을 적용하여 주소변환을 해야 하기 때문에 게이트웨이 단에서의 네트워크 트래픽이 증가하는 경우 전반적인 성능 감소로 이어 질 수 있다. 일반적인 TCP/IP 어플리케이션은 NAT 사용에 문제가 없으나 출발지와 목적지에 주소를 표시하지 않는 어플리케이션의 경우 NAT를 사용할 수 없다. 또한 일부 특별한 트래픽을 요구하거나 TCP/IP 헤더가 아닌 어플리케이션 레이어상에서 IP 정보를 전달하는 어플리케이션의 경우 NAT 사용에 제약이 생긴다. NAT는 TCP/IP에 관련된 헤더 정보의 조작만이 가능하다. 따라서 이러한 어플리케이션에서는 헤더 정보의 조작만으로 NAT를 사용한 주소 변환을 수행할 수가 없기 때문에 NAT 이외에 해당 어플리케이션에 해당하는 전용 프록시가 있어야 정상

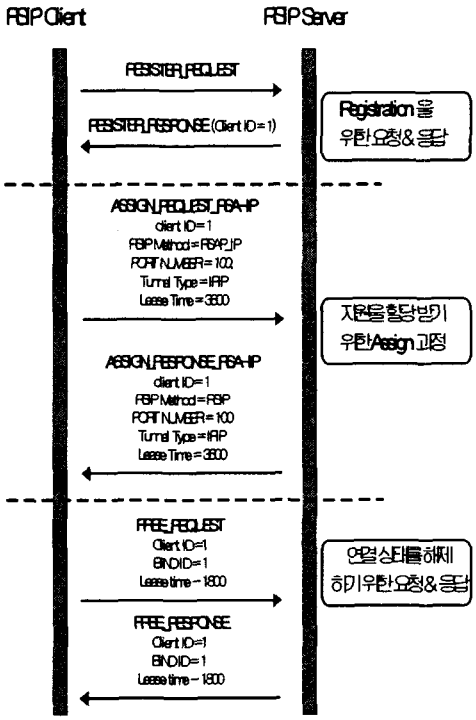
적인 서비스를 받는 것이 가능하다. 이러한 서비스의 대표적인 예로 IP 주소 자체를 암호화하는 IPSEC이나 멀티캐스트, 브로드캐스트를 필요로 하는 어플리케이션을 사용하는 경우 NAT 기능을 이용한 주소변환을 할 수가 없게 된다.

3. RSIP (Realm Specific IP)

RSIP는 기존 NAT/NAPT의 대안으로 출현한 터널을 이용한 주소변환 방법으로 클라이언트/서버 구조로 동작을 한다. 로컬 네트워크 내에서 라우팅을 위해 터널을 사용하며 다양한 터널 방식을 지원 할 수 있다. 기존의 IP 주소변환 방식에서 단대단 연결 제공과 보안 지원, 다양한 사용자 응용 프로그램을 지원하기 위해 많은 ALG가 필요하다는 단점을 극복하기 위해 나타난 새로운 IP 주소 변환 방식이다. RSIP는 서버와 로컬 네트워크의 호스트간에 자원을 할당하기 위한 협상을 초기에 수행해야 하며 외부 호스트와 통신하기 위해 필요한 터널 종류, 사용할 IP 혹은 IP와 포트번호, 사용시간 등의 여러 가지 정보를 할당 받은 후 공인 IP로 주소변환을 수행하게 된다. NAT와 RSIP는 네트워크의 영역을 내부와 외부 영역으로 나누는데 NAT가 이 두 영역 사이에서 주소 풀을 통해 주소를 변환 과정을 매번 수행 하는 반면 RSIP는 외부와 통신을 위한 공인 주소를 임대하는 형태로 사용한다. RSIP 클라이언트는 외부와의 통신을 할 때 외부 주소를 사용해야 할 필요를 인식 하고 있어야 하기 때문에 전용 클라이언트 프로그램이 필요하다[3,4].

3.1 RSIP 동작 메카니즘

표면적으로 NAT에 비해서 RSIP는 상대적으로 변환과정이 간단하다. 사설 주소를 공인주소로 변환하는 대신 RSIP 서버는 라우팅 가능한 공인 주소를 외부와 통신을 하기 위해 RSIP 클라이언트에 임시로 할당한다. RSIP 클라이언트는 RSIP 세션이 이루어져 있는 동안 이 할당된 주소를 자신의 주소처럼 사용하게 된다. RSIP 클라이언트가 RSIP 서버로부터 임의의 공인 주소를 받게 되었을 때 RSIP 클라이언트는 IP 데이터그램의 데이터 패이로드안에 이 할당 받은 공인 주소를 외부와의 통신에 사용한다. 즉 임대한 공인주소는 터널링된 데이터그램의 어플리케이션 데이터 필드안에 인베디드 되어 사용하게 된다. 클라이언트의 주소변환 요청을 받은 RSIP 서버는 네트워크 트래픽이 사설 주소망을 통과하기 전에 내부 네트워크에서 사용되는 터널링된 데이터그램을 제거하고 터널링 되기전의 원래의 데이터그램을 외부로 통과 시키게 된다. 이러한 RSIP의 개념은 NAT에서는 불가능한 단대단 측면에서 장점을 살릴 수 있다.



[그림 2] RSIP 서버와 클라이언트의 메시지 흐름도

[Fig. 2] Message Flowchart of RSIP Server and Client

RSIP는 터널링을 통해 암호화된 데이터필드나 어플리케이션 데이터 상에서 인베디드된 IP 주소를 투명하게 통과 시킬 수 있지만 전통적인 NAT에서는 이러한 암호화를 통해 변경된 필드를 보유한 IP 데이터그램을 처리할 수 없다. 들어오는 데이터 플로우를 구별하기 위해 목적지 IP 주소, IP 프로토콜 타입, 목적지 TCP/UDP

포트, IPSEC의 SPI (Security Parameter Index)를 사용한다. [그림 2]는 RSIP 서버와 RSIP 클라이언트 사이에메시지 흐름을 보여주고 있다. 등록을 하기 위한 과정과 자원을 요청하여 할당받는 할당과정, 연결을 해제하여 자원할당을 해제하는 단계로 구분된다[3,4].

3.2 RSIP에서의 IPSec

RSIP의 가장 큰 잇점은 IP 주소 공유와 함께 IPSec과 같은 단대단 보안 솔루션과 연동이 가능하다는 것이다. IPSec에는 IKE (Internet Key Exchange)와 AH(Authentication Header), ESP(Encapsulating Security Payload) 등 세 가지 형태의 프로토콜이 있다. IKE 프로토콜은 자동화된 보안 연계협상, 키 생성, 분배 및 갱신을 담당하며, SA 협상과 생성으로 IKE 키가 생성되는 1단계와 IPSec SA 협상 및 생성으로 IPSec 키를 생성하는 2단계로 구성된다.

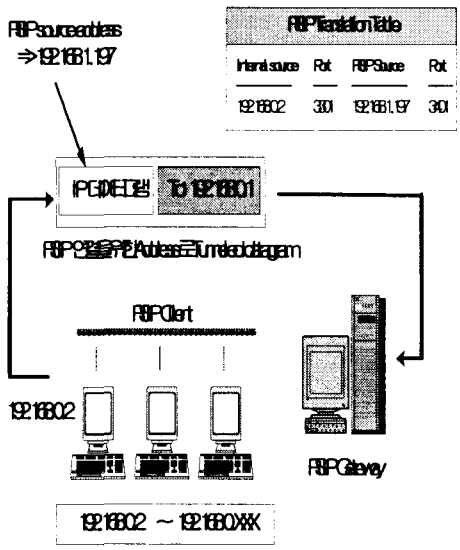
IPSec은 TCP/UDP 포트 번호을 암호화 하기 때문에 NAT 주소 변환과 혼용할 수 없다. IPSec으로 보호 되는 모든 패킷은 IP 헤더뒤에 AH 와 ESP 헤더를 삽입하여 IPSec SA 상에서 전송 된다. 이러한 헤더는 32 bit의 SPI 필드를 포함하고 있으며 이 값은 수신측에 따라 결정된다. SA 협상 과정 동안 RSIP 호스트는 특정 SPI 값을 사용하기 위해 public peer를 통보할 수 있다. 이 SPI 값은 할당된 IP 주소와 함께 RSIP 호스트에 패킷을 라우트하고 유일한 트래픽으로 구분하기 위해 RSIP 게이트웨이에 의해 사용 된다.

RSIP 호스트는 각각 공인 주소에 대하여 유일한 SPI 값을 사용해야 하므로 IP 주소와 포트 쌍과 함께 RSIP 서버는 호스트에 대해서 유일한 SPI 값을 할당해야 한다. IPSec의 SA 협상은 IKE 프로토콜을 사용하는데 IKE는 포트 500번을 사용하도록 지정되어 있다. 만약 두 개 이상의 RSIP 호스트가 출발지 포트가 500번인 IKE에서 운영 되고 있다면 그들은 서로 IKE 패이로드의 첫 번째 8바이트를 수정하여 다른 초기 쿠키를 가지고 있어야만 한다. RSIP 게이트웨이는 들어오는 IKE 패킷에 대하여 이러한 초기 쿠키값을 기반으로 적당한 호스트로 라우팅 하게 된다. 초기 쿠키는 SPI 값과 같이 협상될 수 있으나 동시에 같은 초기 쿠키를 사용하면서 동일한 IP 주소를 할당받은 두 개의 호스트가 존재 할 수 있기 때문에 RSIP 게이트웨이는 이미 사용중에 있는 쿠키값으로 IKE 패킷을 드롭 시켜 쿠키가 유일하도록 보장 하게 된다[3,5].

4. 인트라넷 환경에서의 효율적인 네트워크 주소 변환 기법 설계 및 구현

본 장에서는 리눅스 기반에서 효율적인 주소 변환을 수행하기 위한 RSIP 게이트웨이의 설계 및 구현에 관한 내용을 설명한다. RSIP 기반 주소변환을 위해서 필요한 클라이언트와 RSIP 게이트웨이 간 터널링 방법으로는 IPIP 터널링 방법을 사용 하였다.

4.1 제안한 RSIP 게이트웨이 기본 구조



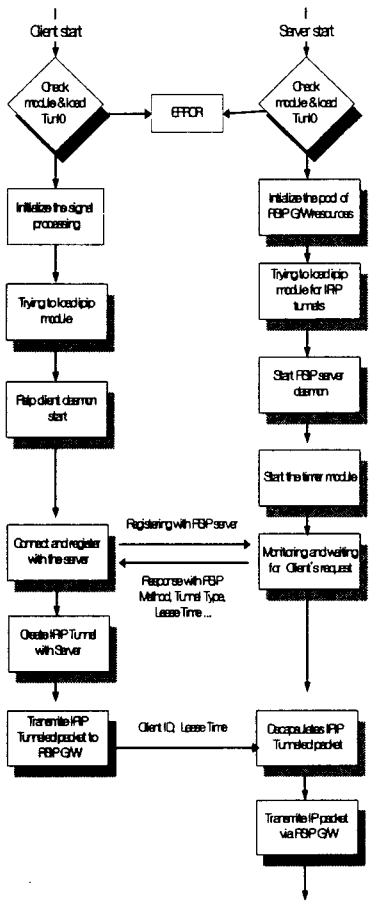
[그림 3] IPIP 터널 데이터를 가지는 RSIP 구조

[Fig. 3] RSIP Structure to have IPIP Tunneled Datagram

리눅스 상에서 IPIP 터널링을 사용하기 위해서는 커널 컴파일을 통해 해당 옵션을 지원 하게 해야 한다. IPIP 터널링은 IP 헤더를 중복시

키는 형태의 IP 캡슐화기법으로 데이터그램을 처리하여 보내면 목적 호스트로 터널 전달이 이루어 지고 이를 받은 서버는 역캡슐화 를 처리하여 최종 목적 호스트에게 데이타그램을 전달한다.

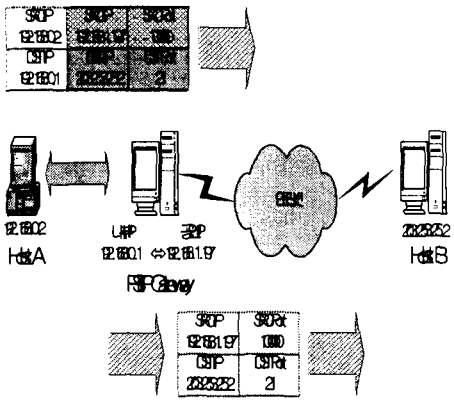
[그림 3]을 보면 RSIP 연결을 위한 IP주소 (192.168.0.1)로 터널링된 데이터그램안에는 RSIP 서버와의 협상과정을 통해 이미 할당 받은 공인 IP주소 (192.168.1.197)가 출발지주소로 지정 되어 있는 데이터그램을 포함하고 있다. RSIP 게이트웨이는 RSIP 변환 테이블을 참조하여 데이터그램을 역 캡슐화한 후 외부의 목적지에 전달하게 된다. [그림 4]는 RSIP 클라이언트와 RSIP 게이트웨이가 리눅스에서 동작하기 위한 일련의 과정을 순서도로 나타낸 것으로 크게 터널링 모듈을 사용하여 가상 인터페이스를 로드 할 수 있는지 검사하는 부분과 RSIP 클라이언트와 RSIP 서버 데몬을 시작하여 등록을 수행하여 초기화 하는 과정, IPIP 터널을 생성하여 보낸 패킷을 역 캡슐화하여 외부로 보내는 과정으로 구분 할 수 있다.



[그림 4] RSIP Client, G/W 동작 순서도

[Fig. 4] RSIP Client, G/W Operation Flowchart

4.2 RSIP 게이트웨이 데이터 흐름도

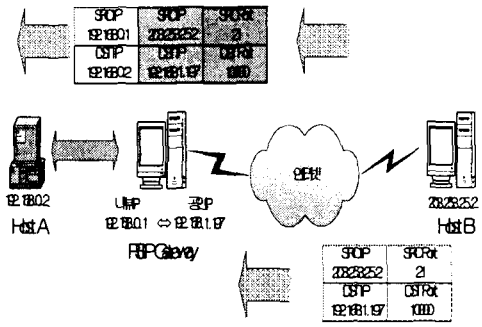


[그림 5] RSIP Outgoing 데이터 흐름도

[Fig. 5] RSIP Outgoing Data Flowchart

[그림 5]는 RSIP 서버를 통해 외부로 향하는 패킷의 흐름을 보여 주고 있다. 그 동작 과정을 살펴보면 다음과 같다.

1. 호스트 A(IP 192.168.0.2)는 RSIP 프로토콜을 이용해 서버로부터 Global 네트워크의 호스트와 통신할 때 사용될 다양한 파라미터(공인 IP주소, 포트번호, 터널 타입, 사용시간)를 얻는다.
2. 서버는 호스트 A의 로컬 주소와 할당된 다양한 파라미터 값을 바인딩하여 테이블에 기록한다.
3. 호스트 A는 서버로부터 할당받은 파라미터를 이용해 터널을 생성, 데이터 패킷을 목적지인 B로 전송한다.



[그림 6] RSIP Inbound 데이터 흐름도

[Fig. 6] RSIP Inbound Data Flowchart

[그림 6]은 RSIP 서버를 통해 내부 네트워크로 향하는 패킷의 흐름을 보여 주고 있다. 그 동작 과정을 살펴보면 다음과 같다.

1. 호스트 B (IP 주소: 203.253.25.2)는 RSIP 서버를 목적지로 하는 패킷 (IP주소 : 192.168.1.197)을 전송한다.
2. RSIP 서버는 Incomming 트래픽을 바인딩 정보에 따라 분류하고 호스트 A로 생성된 터널을 이용해 IPIP 터널을 생성하여 데이터 패킷을 전송한다.

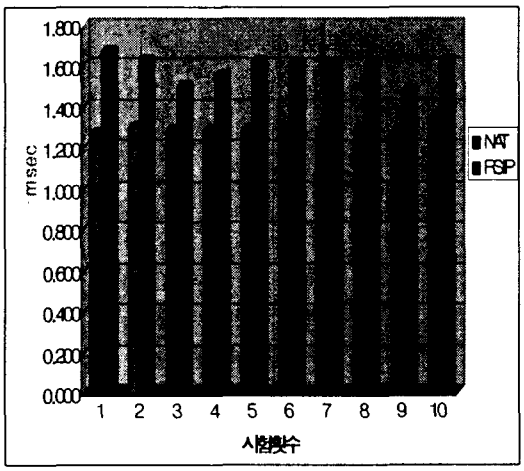
5. 성능 분석 및 평가

이 장에서는 앞에서 제안한 요구사항과 개념을 적용하여 구현된 RSIP 기반 리눅스 게이트웨이와 기존 NAT 게이트웨이와의 성능을 비교 분석하였다.

5.1 응답 시간 측정

주소변환 시스템의 외부 호스트가 얼마나 빠른 응답을 하는지를 알아보기 위해 RTT 값을 측정 해 봄으로서 두 시스템 의 응답시간을 비교해 보았다. 실험은 리눅스 서버 상에서 NAT와 RSIP가 동작 할 수 있도록 각각 설정 한 후 동일하게 제시한 실험조건과 시험 환경에서 내부 클라이언트에서 외부망 서버 호스트 B (192.168.1.189)로 ping 테스트를 수행 하였다. 클라이언트에서 NAT, RSIP 게이트웨이상에서

주소변환 과정을 거친 후 외부 서버인 호스트 B 까지의 RTT average 값을 측정 하였다. 시험의 정확성을 위해 같은 테스트를 10번 수행하여 평균값을 산출하여 비교 해 보았다. [그림 7]은 NAT와 RSIP의 Ronnd trip 지연시간의 RTT average 값의 평균값을 결과를 나타낸 비교한 그래프이다. 테스트 결과 전체적으로 NAT가 RSIP 보다 지연시간 단축을 보여 주고 있음을 알 수 있다.



[그림 7] NAT와 RSIP의 RTT 비교 그래프

[Fig. 7] A RTT Comparative Graph of NAT and RSIP

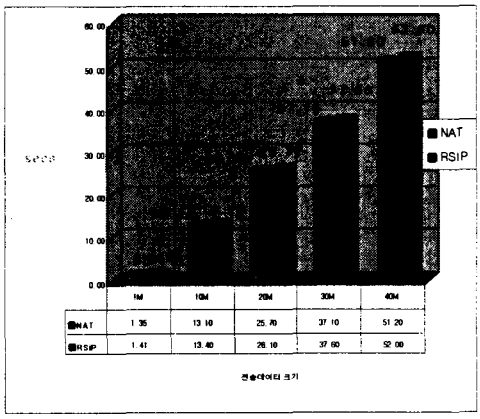
5.2 데이터 전송처리 시간 측정

아래에 주어진 실험조건[A-D]에 따라 주소변환에 사용되는 테스트 서버에 대용량 데이터 전송 트래픽을 유발 시켜 트래픽 정도에 따라 NAT과 RSIP의 각 클라이언트에서 파일 전송처리 속도를 측정하여 성능을 비교 분석 하였다.

- 실험 조건 A : 데이터 전송 트래픽이 없을 경우
- 실험 조건 B : 67M 데이터 전송 트래픽을 발생 했을 경우
- 실험 조건 C : 107M 데이터 전송 트래픽을 발생 했을 경우
- 실험 조건 D : 214M 데이터 전송 트래픽을 발생 했을 경우

5.2.1 실험 조건 A에서의 데이터 전송처리 시간 측정

실험 조건 A에서 클라이언트에서 전송 데이터 크기에 따라 수신하는데 필요한 전송 속도를 측정 하였다. [그림 8]은 데이터 전송 트래픽을 발생 하지 않았을 경우 클라이언트에서 데이터 크기에 따른 전송 시간을 측정한 결과로 전반적으로 NAT가 RSIP 보다 좀 더 나은 성능을 보이고 있다.

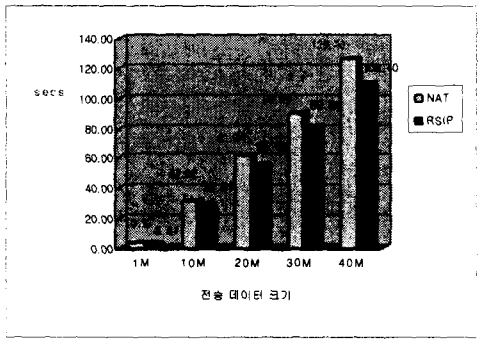


[그림 8] 실험 조건 A에서의 데이터 전송처리 시간 비교 그래프

[Fig. 8] Data Transmission Processing Time Comparative Graph in Experiment Condition A

5.2.2 실험 조건 D 에서의 데이터 전송처리 시간 측정

실험 조건 D에서 클라이언트에서 전송 데이터 크기에 따라 수신하는데 필요한 전송 속도를 측정 하였다. [그림 9]는 RSIP와 NAT의 클라이언트 단에서 1 M에서 40M까지 데이터를 전송하는데 필요한 시간을 측정한 결과로 실험 조건 A의 경우에 NAT가 RSIP에 비해 다소 우수한 성능을 보인 실험 결과와 비교해 볼 때 서버 트래픽이 증가된 경우인 실험 조건 D의 경우 RSIP가 NAT 보다 더 빠른 전송 시간을 보여 주고 있음을 알 수 있다.



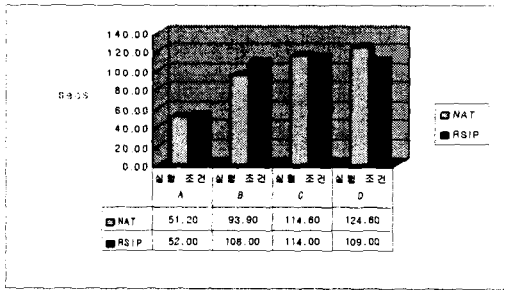
[그림 9] 실험 조건 D에서의 데이터 전송시간 비교 그래프

[Fig. 9] Data Transmission Time Comparative Graph in Experiment Condition D

또한 NAT에 비해 RSIP가 전송 데이터 크기가 1M인 경우 약 4.5%, 10M인 경우 약 10.3% 정도 더 빠른 전송 시간을 보인 반면 40M 데이터 전송인 경우에는 대략 13% 의 향상된 전송 시간을 보이고 있다. 즉 고용량의 데이터 전송 일수록 RSIP의 성능이 NAT에 비해 우수한 성능을 보인다는 것을 알 수 있다.

5.2.3 실험 조건 [A-D] 에서의 데이터 전송처리 시간 측정

실험 조건 [A-D]에 따라 클라이언트가 40 M byte의 데이터를 외부 서버에서 전송 받을 경우 전송 데이터 시간과 속도를 비교해 보았다. [그림 10]은 실험조건 [A-D]에 따라 NAT와 RSIP의 데이터 전송 시간을 그래프로 나타낸 화면이다.



[그림 10] 실험 조건에 따른 데이터 전송처리 시간 비교 그래프

[Fig. 10] Data Transmission Processing Time Comparative Graph in Experiment Conditions

성능 측정 결과를 분석 해 보면 실험 조건 B까지 NAT가 더 빠른 전송시간을 보이고 있지만 데이터 전송 트래픽 부하 정도가 더 심해진 실험조건[C-D]를 적용 했을 경우 RSIP가 NAT에 비해 보다 더 우수한 성능을 보이고 있음을 알 수 있다.

이 결과를 통해 RSIP가 주소변환 게이트웨이 상에서 서버 부하 및 네트워크 트래픽에 덜 민감하게 동작 한다는 것을 알 수 있고 고용량의 데이터 전송 일수록 NAT에 비해 보다 우수한 성능을 보인다는 것을 알 수 있다.

성능 분석을 통해 NAT 방식이 ICMP 메시지 처리나 네트워크 트래픽이 적은 경우등 비교적 서버 부하가 적은 환경에서는 RSIP 보다 우수한 성능을 보였지만 고용량 데이터 전송시나 네트워크 트래픽이 심한 경우에는 RSIP 방식이 NAT에 비해 우수한 성능을 보인다는 것을 알 수 있었다. RSIP는 출발지나 목적지 주소의 변환이나 TCP 포트할당, 체크섬 필드의 재계산 등을 요구하지 않기 때문에 매번 주소변환과정을 거쳐야 하는 전통적인 NAT 보다 트래픽이 심한 경우에 더 좋은 성능을 보여 준다. 즉, 주소를 리스 받기 위한 초기화가 이루어 진 후 RSIP 게이트웨이의 성능은 NAT에 비해 RSIP가 초래하는 일련의 지연보다 더 효율적이라고 볼 수 있다. RSIP는 실질적으로 NAT에 비해서 게이트웨이 단에서 처리해야만 하는 작업이 상대적으로 적기 때문에 대용량 데이터를 처리 해야 하는 파일 서버나 네트워크 트래픽이 빈번한 환경에서 주소변환시스템으로 사용된다면 보다 우수한 성능을 보일 것이다.

6. 결 론

본 논문에서는 인트라넷 환경에서 터널링을 사용하여 주소변환 시스템으로 활용 할 수 있는 리눅스 기반 RSIP 게이트웨이를 제안하였다. 기존 리눅스 기반 NAT 게이트웨이와 성능 분석 및 비교를 통해 RSIP를 적용한 시스템이 네트워크 트래픽 증가나 고용량 데이터 전송시에

NAT 보다 우수한 성능을 가진다는 것을 알 수 있었다. NAT는 매번 주소 변환이라는 과정을 게이트웨이 단에서 거치면서 TCP 포트할당, 체크섬 필드의 재계산등 복잡한 연산을 수행 해야 하기 때문에 네트워크 트래픽 증가시 성능이 다소 떨어지는 문제점을 가지고 있다. 이에 비해 RSIP는 주소변환 과정에서 출발지와 목적지주소 변환이나 NAT를 위해 필요한 일련의 복잡한 연산등을 요구하지 않고 단지 터널링에 사용된 IP 패이로드만을 제거 하기 때문에 전통적인 NAT 보다 네트워크 트래픽이 심한 경우나 고용량 데이터 전송시에 보다 더 우수한 성능을 보여 준다.

RSIP 서버는 공인 주소와 사설 주소 영역사이에서 주소를 변환 하는 것이 아니라 단지 RSIP 클라이언트에 인베디드 되어 있는 데이터그램에서 터널링에 사용된 IP 패이로드만을 제거하고 외부 네트워크로 포워딩 한다. 따라서 외부 네트워크로 포워딩 하는 과정에 IP 데이터그램에 대한 어떠한 변경이 없기 때문에 인베디드된 데이터가 암호화 되어 있더라도 전송할 수가 있다. 아직 RSIP 프로토콜을 사용한 시스템이 실제로 적용된 사례가 적기 때문에 응용분야나 활용방안에 대한 구체적인 검증이 미흡하다. 하지만 앞으로 네트워크 트래픽 부하에 우수한 성능을 가지면서 단대단 보안환경에서 IP 주소 변환이 가능하다는 잇점을 살릴 수 있는 연구가 이루어진다면 NAT를 보완 하는 유용한 네트워크 주소변환 기술로서 널리 사용 될 것으로 보인다.

참 고 문 헌

[1] Bill Ducher, "The NAT Handbook", WILEY, May 2001.

[2] P. Srisuresh and M. Holdrege, "IP network address translator (NAT) terminology and considerations'', Internet RFC 2663, Aug. 1999.

[3] M. Borella and J. Lo, "Realm Specific IP: Framework", RFC 3102, October 2001.

[4] M. Borella, D. Grabelsky, J. Lo, "Realm Specific IP: Protocol Specification", RFC 3103, October 2001.

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

이영택

2000년 숭실대학교 컴퓨터학부(학사)
2003년 숭실대학교 컴퓨터학과(석사)
2003년 ~ 현재 롯데정보통신
관심분야 : 컴퓨터보안, 네트워크

김 원

1988년 숭실대학교 전자계산학과(학사)
1993년 숭실대학교 전자계산학과(석사)
1997년 숭실대학교 전자계산학과(박사)
1995년~현재 전주기전여자대학 실용예술학부 조교수
관심분야 : 멀티미디어 통신, 멀티미디어 보안, 저작권 보호

전문석

1980년 숭실대학교 전자계산학과 졸업(학사)

1996년 University of Maryland 전산과 졸업(석사)

1989년 University of Maryland 전산과 졸업(박사)

1989년 Morgan State University 전산수학과 조교수

1989년~1991년 New Mexico State University 부설 Physical Science Lab. 책임연구원

1991년~현재 숭실대학교 정보과학대학 부교수

관심분야 : 컴퓨터 알고리즘, 병렬처리, VLSI 설계, 암호학