효율적인 기업 VPN 구축 및 운용을 통한 비용대비 성능향상 사례 연구

김성찬*, 이승민**, 전문석**
* EUKORAIL Co., Ltd., ** 숭실대학교 대학원 컴퓨터학과
e-mail : viper72@chol.com*,cowaboonga@hotmail.com**,mjun@computing.ssu.ac.kr**

A Case Study on Efficient Enterprise Virtual Private Network Implementation and Operation for a Performance Elevation against the Cost

Sung-Chan Kim*, Seung-Min Lee**, Mun-Seog Jun**
*Dept. of Information System, EUKORAIL, **Dept. of Computer Science, Soong-Sil University

요 약

정보통신 기술의 발달이 가져온 가장 큰 변화중의 하나로 글로벌 커뮤니케이션을 들 수 있을 것이다. 각 지역별 사업장을 운영하는 기업체들은 대부분 사업장들을 연결하는 광역 통신망을 구축하여 사용하고 있지만, 이를 운영하는데 드는 막대한 비용과 보안문제에 많은 어려움을 겪고 있는 실정이다. 본 논문에서는 사업장의 이동이 빈번한 기업의 광역 통신망을 구축함에 있어 비용 절감을 위해 재 활용된 개인용 컴퓨터를 이용하여 리눅스 기반의 VPN 게이트웨이를 만들어 사용하고 포트스캔 기술과 패킷 스니퍼를 이용한 네트워크의 모니터링을 통해 보다 안전하고 효율적으로 통신망을 운영한 사례를 제시하고자 한다.

1. 서론

오늘날 기업 활동에서 기업이 운영하는 네트워크가 차지하는 비중은 계속 증대되고 있다. 최근 들어 기업망은 공중 ATM 망 또는 프레임 릴레이 망을 근간으로 한 가상 사설망(VPN: Virtual Private Network)의 형태로 많이 구축되어 왔다. 더욱 최근에는 전 세계적으로 사용이 보편화된 인터넷 망을 기반으로 한 가상 사설망, 즉, IP 기반의 VPN 사용이 확산 되는 추세에 있다. 하지만 공중 인터넷 망은 보안에 매우 취약하여 기업에서 요구하는 보안성을 충족시키지 못한다. 본 논문에서는 보안에 취약한 VPN 망, 장비 교체 및 네트워크 구성에 따른 비용부담, 안정적인 회선 운용 미흡 이라는 3 가지 단점을 보완하여 기업 VPN 망을 구현한 사례를 보이고자 한다. 본 연구에서는 교체되어 재고로 남아있는 낮은 사양의 개인용 PC 와 리눅스 운영체제, 그리고 IPsec 보안프로토콜을 이용하여 각 지역 사무실에 설치될 VPN 장비를 구현하여 비용 및 보안문제를 해결하였고, 네트워크의 안정적인 운용을 위해 포트스캔 기술과 패킷 스니퍼를 이용한 네트워크 모니터 툴을 구현하였다. 본 논문의 구성은 2 장에서 VPN 구성의 핵심 프로토콜인 IPsec 과 그 솔루션인 Free S/WAN 에 대하여 설명하고, 3 장에서 VPN 망과 포트스캔, 패킷 스니퍼를 이용한 망 감시 기술에 대하여 설명한다. 4 장에서는 본 연구에서 구현한 시스템과 사용 결과에 대하여 기술하고, 5 장에서 시스템 사용 후 비용 대비 성능 향상 분석 결과를 보인 후, 6 장에서 결론을 맺는다.

2. Free S/WAN(Free Security Wide Area Network)

본 논문에서는 장비 교체 및 네트워크 구성에 따른 비용부담을 없애고 인터넷 망을 통신매체로 이용함으로써 발생할 수 있는 보안문제를 해결하기 위해 종단간의 데이터 통신을 모두 암호화 하는 IPsec 보안 프로토콜과 Secure OS 구성을 위한 리눅스, 재활용 된 개인 컴퓨터를 이용하여 VPN 게이트웨이를 구성하였다. 본 논문에서 사용한 IPsec 보안 프로토콜은 리눅스 기반의 VPN 솔루션을 개발하는 Free S/WAN 프로젝트를 사용하였으며, 이 프로젝트는 리눅스 게이트웨이를 이용한 터널링 기법을 사용하여 WAN 상에서의 네트워크 보안에 중점을 두어 개발하고 있는 공개 프로젝트이다. Free S/WAN 프로젝트는 현재 타 운영체제 등과의 호환성(Interoperability)을 지원하기 위한 작업을 수행 중이며 리눅스 상에서의 VPN 솔루션 구축을 목표로 하고 있다. Free S/WAN 은 사용자의 패킷 전체를 암호화 하여 상대방 게이트웨이를 목적지로

하는 보안 정책으로 패킷을 암호화하여 TCP 포트 50 번으로 전송하는 구조를 갖고 있다. 암호화에서 가장 중요한 키 분배는 리눅스 콘솔에서 수동으로 키를 직접 정의하여 동작시킬 수 있고, 또는 키 교환 프로토콜(IKE) 등을 이용하여 관리자가 정의한 보안 알고리즘들로 협상하고 알고리즘을 선택하며 키를 교환한다.

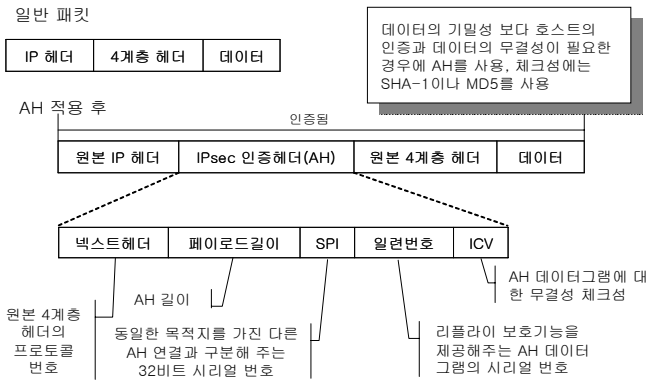

그림 1 AH 모드

그림 1 은 종단간의 암호화된 통신 터널을 만들기 전에 종단간의 인증 과정을 수행하는 IPsec AH 모드에 대하여 설명한 것이다[2].

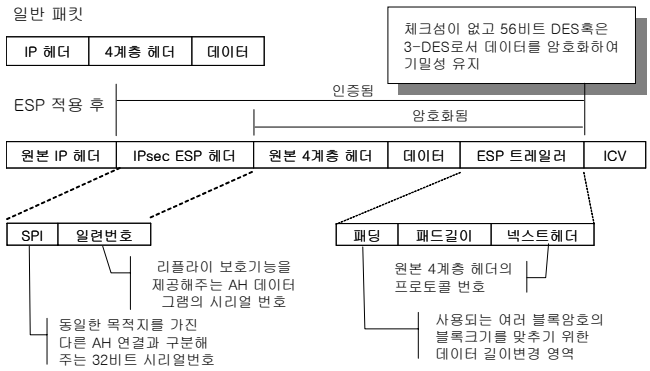

그림 2 ESP 모드

그림 2 는 인증 과정이 완료된 후 실제 데이터를 암호화해서 보내는 IPsec ESP 모드에 대하여 설명한 것이다. 본 연구의 VPN 게이트웨이에서는 보안에 취약한 인터넷 망을 이용하기 때문에 Free S/WAN 프로젝트의 IPsec 보안 프로토콜을 이용함으로써 사용자의 주소 및 포트 번호를 암호화 한다[3].

3. VPN(Virtual Private Network)과 망 감시 기술

가상사설망(Virtual Private Network)이란 기업의 네트워크를 구성할 때 전용 임대선 대신에 인터넷과 같은 공중망을 이용하여 이것을 사설망처럼 이용한다는 기술이다. 기업의 근무 환경이 많은 정보를 공유하는 방향으로 변화하게 됨에 따라 사용자들이 주어진 시간에 처리할 수 있는 업무가 확대되거나 근무 위치가 사무실에 국한되지 않고 집이나 업무 현장으로 까지 넓혀짐으로 인하여 재택 근무자 또는 이동근무자가 늘게 되었다. 이러한 변화로 인하여 기업은 기업 내부에서의 정보 공유를 위한 근거리 망의 구성에서 벗어나 기업 네트워크를 확대하기 위해 외부와의 네트워크 구성이 필요하게 된 것이다. 따라서 기업은 외부와의 연결된 네트워크 사이에서 자신의 정보를 안전하게 전송하기 위하여 사설망을 구성하게 되는데, 네트워크 구성에 막대한 시설 투자비용이 요구되고 네트워크 운영과 관리에 많은 인적, 금전적 요소가 요구되는 등의 문제점이 발생하게 된다. 이 같은 문제점들을 해결하고 공중망과 사설망의 단점을 해소하기 위해 가상 사설망기술이 발전하게 되었다[4].

본 연구에서 가상사설망의 안정적인 운용을 위해 네트워크 모니터에 사용할 기술은 패킷 분석과 포트 스캔을 이용한 네트워크 감시 기술이다. 본 기술의 본래 목적은 네트워크 내에서 침입자에 의한 오용행위 탐지나 비정상행위 탐지를 위한 것이지만, 기업체에서 메일 서버나 기타 데이터베이스 서비스를 사용자들에게 제공할 경우, 관리자는 각 서버들이 제대로 동작하는지 어플리케이션 서비스 포트 스캔을 통해 감시 할 수 있다. 뿐만 아니라 가상사설망을 구성하고 있는 각 지역 사무실을 연결한 가상사설망 서킷이 안정적인지 불안정적인지 상태 감시와 함께 사용자들의 데이터 송수신에 따른 네트워크 부하 량도 측정할 수 있어 문제가 발생하였을 경우, 즉각적인 원인 분석과 함께 조치를 취할 수 있다. 본 연구에서 구현한 네트워크 모니터 시스템은 서비스 포트 관제를 위한 “NMONITOR” 라는 포트 스캐너와 패킷 분석을 위한 “Packet Sniffer” 를 이용하여 구현 하였다[5][6].

4. VPN 망과 네트워크 감시 시스템

본 연구에서 구현한 가상 사설망과 네트워크 감시 시스템의 구성도는 그림 3 과 같다. 가상 사설망에서 구현한 네트워크는 서울 본사 네트워크에 연결되는 12 개의 지방 사무실 네트워크로 본사에 위치한 서버에 VPN 게이트웨이 종단간 터널링 통신을 통해 업무용 어플리케이션을 이용 할 수 있다.

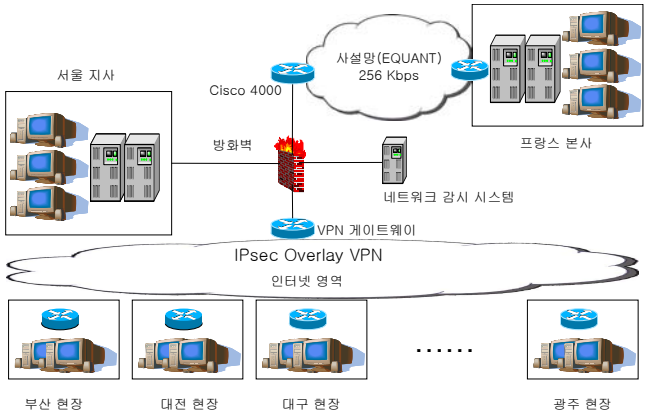

그림 3 가상 사설망 구성도

VPN 망은 재활용된 개인용 컴퓨터에 리눅스 운영체제를 설치하고 IPsec 프로토콜 설치 프로그램인 Free S/WAN 1.92 버전[1]을 리눅스 커널 컴파일을 이용해 포팅 시킨 후 종단간 터널링을 통한 사설망을 구현하

도록 한다. 이때 서울 본사에 위치한 VPN 게이트웨이에 지방 사무실의 VPN 게이트웨이가 연결되는 1:N 의 구성을 유지하도록 한다. 표 1 은 VPN 게이트웨이의 구현 사양이다. VPN 게이트웨이를 구현할 때 중요한 것은 외부로부터의 공격을 받지 않도록 모든 서비스 포트를 닫아야 한다[7].

표 1 VPN 게이트웨이 구현 사양

Hardware	Pentium 500M Hz
Operating System	Red Hat Linux 7.2
Security Protocol	Free S/WAN 1.92 (IPsec)
Programming Language	C
Open Service Port	ALL CLOSE

종단간 VPN 게이트웨이간의 터널이 형성되면 패킷을 암호화 하여 통신을 할 수 있는데, 이를 확인하기 위하여 일반적인 TCP/IP 를 이용한 통신과 IPsec 프로토콜을 이용하여 통신한 내용을 패킷 분석을 통하여 분석한 결과는 그림 4 와 그림 5 와 같다.

```
0x0000   4500 0030 8da2 40b9 4001 ce03 0aba 63fd        E..0..@.@.....c.
0x0010   0aba 64fd c0c1 c2c3 c4c5 c6c7 c8c9 cacb        ..d.............
0x0020   cccd cecf d0d1 d2d3 d4d5 d6d7 d8d9 dadb        ................
16:05:05.914044 10.186.99.253 > 10.186.100.253: icmp: echo request (frag 36258:1
480@0+)
0x0000   4500 05dc 8da2 2000 ff01 [illegible]           E..... ..[illegible]
0x0010   0aba 64fd 0800 29da 9f0b 0700 2148 7c3d        ..d...)..... !H|=
0x0020   c2f2 0d00 0809 0a0b 0c0d 0e0f 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        ............ !"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435                                          45
16:05:05.914044 10.186.100.253 > 10.186.99.253: (frag 52758:28@1480)
0x0000   4500 0030 ce16 00b9 ff01 0e8f 0aba 64fd        E..0..........d.
0x0010   0aba 63fd c0c1 c2c3 c4c5 c6c7 c8c9 cacb        ..c.............
0x0020   cccd cecf d0d1 d2d3 d4d5 d6d7 d8d9 dadb        ................
16:05:05.914044 10.186.100.253 > 10.186.99.253: icmp: echo reply (frag 52758:148
0@0+)
0x0000   4500 05dc ce16 2000 ff01 e99b 0aba 64fd        E..... .....d.
0x0010   0aba 63fd 0000 31da 9f0b 0700 2148 7c3d        ..c...1..... !H|=
0x0020   c2f2 0d00 0809 0a0b 0c0d 0e0f 1011 1213        ................
0x0030   1415 1617 1819 1a1b 1c1d 1e1f 2021 2223        ............ !"#
0x0040   2425 2627 2829 2a2b 2c2d 2e2f 3031 3233        $%&'()*+,-./0123
0x0050   3435                                          45
```

그림 4 TCP/IP 프로토콜을 이용한 통신의 패킷

```
0x0000   4500 0068 8d19 00b9 4032 1169 3d48 3058        E..h....@2.i=H0X
0x0010   3d48 3041 b4b0 b932 94c6 dee7 53a2 54e9        =H0A...2....S.T.
0x0020   791e 1be4 c431 6bc1 8b82 4685 2b85 9cbd        y....1k...F.+...
0x0030   c561 8555 8efb 5560 7f42 6f5c 096f e2e5        .a.U..U`.Bo\.o..
0x0040   a0a5 ff14 9d16 0604 a2cf f05e ed39 278a        ...........^.9'.
0x0050   5dfd                                          ].
16:02:22.034044 61.72.48.65 > 61.72.48.88: ESP(spi=0xb24d5953,seq=0x80) (frag 52
492:1480@0+)
0x0000   4500 05dc cd0c 2000 [illegible]                E..... ..[illegible]
0x0010   3d48 3058 b24d 5953 0000 0080 14ad 0cc3        =H0X.MYS........
0x0020   08ab 1ca2 fcd7 4283 deaa 16e0 9a21 94ba        ......B......!..
0x0030   4649 4d46 4095 c4db 0036 659d b51d ba0f        FIMF@....6e.....
0x0040   3d68 0440 bb93 0da5 4fd3 fe3b c9cd fe1b        =h.@....O..;....
0x0050   66a3                                          f.
16:02:22.034044 61.72.48.65 > 61.72.48.88: (frag 52492:84@1480)
0x0000   4500 0068 cd0c 00b9 4032 d175 3d48 3041        E..h....@2.u=H0A
0x0010   3d48 3058 6791 1e3a 0b24 7d91 fd5b aead        =H0Xg..:.$}..[..
0x0020   2ec3 d298 7de9 691c 55bb 9758 475d b3ed        ....}.i.U..XG]..
0x0030   1b2f 6b0f b5a8 644d 6c01 6ea6 de82 645b        ./k...dMl.n...d[
0x0040   9dd2 d31d 2b6b 7edc d526 60c7 01ba c0ff        ....+k~..&`.....
0x0050   1dea                                          ..
16:02:23.034044 61.72.48.88 > 61.72.48.65: ESP(spi=0x095fe6bb,seq=0x81) (frag 36
122:1480@0+)
```

그림 5 IPsec 프로토콜을 이용한 통신패킷

보안 프로토콜을 사용하지 않을 경우 그림 4 에서와 같이 ICMP 라는 패킷 내용과 발신지와 목적지의 IP 주소를 모두 볼 수 있다. 하지만 그림 5 에서는 발신지와 목적지의 IP 주소가 아닌 경유 되는 IP 주소만 볼 수 있으며 패킷 내용도 ESP 프로토콜로 암호화 되어 전송됨을 볼 수 있다.

인터넷 기반의 패킷 중첩을 통한 인증 VPN 의 경우 전송 매체로 ADSL 을 많이 이용하기 때문에 회선을 얼마나 안정적으로 운영하는가가 매우 중요하다. 회선을 안정적으로 운영하기 위해서는 항상 회선의 상태가 어떠한가를 감시해야 하는데, 인터넷 ADSL 은 연결 보장형 서비스가 아니기 때문에 항상 연결 상태를 감시하여 서킷이 끊어졌을 경우 신속하게 대처해야 한다. 네트워크 상태를 감시하는 또 다른 이유는 내부 사용자의 데이터 전송이 비정상적이거나 잘못된 사용으로 인해 네트워크의 전송 성능을 저하 시킬 수 있는 가능성이 있으므로 사용자들의 데이터 전송상태도 항상 감시 되어야 하며, 비정상적인 데이터 전송의 경우 패킷 차단을 통한 즉각적인 대처를 해야 한다.

EUKORAIL Network Monitor - Last check: Jan 5 11:35 - See network statistics

Service	Details	Status	Alarm	Remarks
[VPN BOX] OSONG_CAT_(vpn1)	10.186.101.253:icmp			0% loss, avg=18.816ms
[VPN BOX] TAEJUNAS_(vpn1)	10.186.103.253:icmp			0% loss, avg=8.833ms
[VPN BOX] YONGIN_(vpn2)	10.186.105.62:icmp			0% loss, avg=36.615ms
[VPN BOX] PUSANRS_(vpn1)	10.186.102.253:icmp			0% loss, avg=49.253ms
[VPN BOX] PUSANAS_(vpn1)	10.186.105.193:icmp			0% loss, avg=18.708ms
[VPN BOX] PUSANASINSP_(vpn1)	10.186.105.1:icmp			0% loss, avg=20.330ms
[VPN BOX] KOYANGRS_(vpn1)	10.186.108.253:icmp			0% loss, avg=6.562ms
[VPN BOX] KOYANG_RSENG_(vpn1)	10.186.109.253:icmp			0% loss, avg=20.411ms
[VPN BOX] KOYANGAS_(vpn1)	10.186.105.65:icmp			0% loss, avg=8.952ms
[VPN BOX] KOYANGWH1_(vpn2)	10.186.105.97:icmp			0% loss, avg=40.205ms
[VPN BOX] KOYANGWH2_(vpn2)	10.186.105.161:icmp			0% loss, avg=36.695ms
[VPN BOX] NAMSEOUL_CTC_(vpn1)	10.186.105.129:icmp			0% loss, avg=0.064ms
[SERVICE] Lotus_SMTP	10.186.97.8:25/tcp			open
[SERVICE] Lotus_Notes	10.186.97.8:1352/tcp			open
[SERVICE] Scala_MSSQL	10.186.97.8:1433/tcp			open
[SERVICE] Sibelius_Oracle	10.186.97.3:1521/tcp			open
[SERVICE] Sibelius_Sibwind	10.186.97.3:4267/tcp			open
[SERVICE] HMServer_Oracle	10.186.97.4:1521/tcp			open
[MACHINE] Seoul9_file_server	10.186.96.3:icmp			0% loss, avg=0.538ms
[MACHINE] Koyang1_file_server	10.186.108.3:icmp			0% loss, avg=16.850ms
[MACHINE] Koyang2_file_server	10.186.109.3:icmp			0% loss, avg=18.737ms
[MACHINE] Pusan1_file_server	10.186.102.3:icmp			0% loss, avg=45.262ms
[MACHINE] Detail_DesignServer	10.186.97.5:icmp			0% loss, avg=0.324ms
[MACHINE] Seoul5_SUS	10.186.96.4:icmp			0% loss, avg=0.722ms

그림 6 포트 스캐닝을 이용한 망 감시

EUKORAIL Network Monitor
Detail for IP 10.186.105.162 - Daily statistics today - Last update: Mon Feb 28 15:25:00 2005

IP Source	IP Destination	Protocol	Port	Bytes in	Bytes out	Packets in	Packets out	Remarks
10.186.105.162	10.186.96.3	tcp	nbsession	864343	225306	1662	1608	
10.186.105.162	10.186.97.8	tcp	lotus	39821476	8559254	36371	25832	Lotus Notes: Gyung-Nyun HA/O=EUKORAIL
10.186.105.162	10.186.96.3	udp	nbdatagram	0	13378	0	51	
10.186.105.162	10.3.1.8	udp	domain	193	59	1	1	
10.186.105.162	10.186.96.3	icmp	0	0	420	0	7	

그림 7 패킷스니퍼를 이용한 패킷 모니터

그림 6 은 포트 스캔을 이용하여 네트워크 상태를 실시간 감시하는 네트워크 모니터 시스템이다. 가상 사설망을 구성하는 각 종단 네트워크의 디폴트 게이트웨이를 ICMP 포트 스캔을 하여 응답이 돌아올 경우

파란색으로 표시하도록 한다. 응답이 없으면 붉은색으로 표시 되고, 관리자에게 전자우편을 발송하여 즉각적인 조치를 할 수 있도록 한다. 네트워크 모니터 시스템에서 포트 스캔 기술이 유용한 이유는 서버에서 운용되는 어플리케이션에 대한 동작 유무도 각 서비스 포트스캔을 통하여 파악 할 수 있기 때문이다.

본 연구에서 구현한 네트워크 모니터 시스템은 각 종단 네트워크에서 송, 수신되는 패킷을 패킷 스니퍼로 분석하여 네트워크 사용자들의 오용 행위가 없는지 감시 할 수 있도록 하였다. 그림 7 은 한 호스트에서 송, 수신된 내용의 예로써 전체 데이터그램의 크기와 프로토콜의 종류, 송신된 패킷과 수신된 패킷의 크기 등의 상세한 정보를 얻을 수 있다. 따라서 호스트 및 네트워크 별 송, 수신되는 패킷의 양을 감시함으로써 네트워크에 부하가 발생하는 것을 미연에 방지하고 네트워크의 오용에 기인한 과부하 현상을 방지해 네트워크를 안정적으로 운용 할 수 있도록 한다.

5. 시스템 성능평가

본 연구에서 구현한 가상 사설망은 지역 사무실의 이동이 빈번하거나 영구적으로 운용되지 않을 경우 네트워크 장비구매 비용 및 운용 비용이 많이 지출되는 사설 통신망을 운용하기 어렵기 때문에 그에 대한 대안으로써 월 유지 비용이 적은 인터넷 ADSL 과 IPsec 보안 프로토콜을 이용하여 가상 사설망을 구축한 기업 네트워크 구축 사례이다.

그림 8 은 128K bps 전용선을 이용하여 사설망을 구축할 경우 필요한 월 유지비용을 접속되는 종단 네트워크 수의 증가에 따라 필요한 금액과 인터넷 ADSL 을 전송매체로 하여 VPN 망을 구축하였을 경우 증가되는 종단 네트워크 수에 따라 필요한 금액을 비교한 결과다.

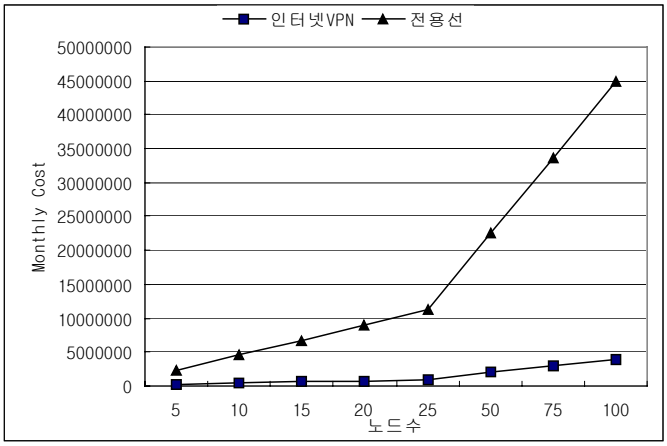

그림 8 노드 수 증가에 따른 비용차이 비교

기업 사설망에 접속되는 종단 네트워크의 수가 많아질수록 월 유지비용의 차이는 급격하게 커지게 된다. 또한 본 연구에서 구현한 가상 사설망의 전송매체인 인터넷 ADSL 의 전송 성능은 128K bps 의 전용선과 비교하였을 때 훨씬 좋은 성능을 보임을 알 수 있다.

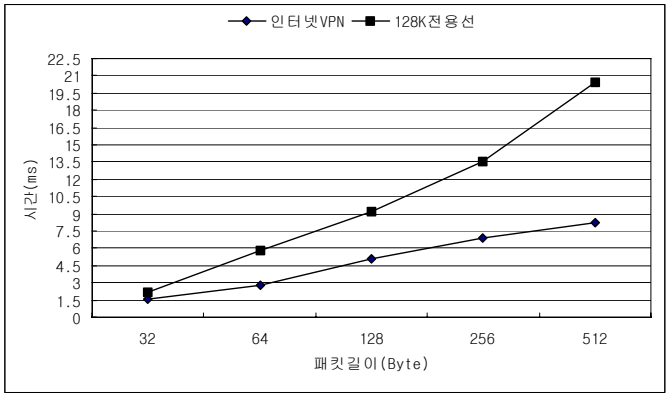

그림 9 패킷 전송 크기에 따른 응답시간 비교

그림 9 는 ICMP 패킷의 크기를 32 바이트에서 512 바이트까지 변화를 주면서 전송하였을 경우 목적지에서 echo 응답이 되돌아 오는 응답 반응 시간을 비교한 결과이다. 처음 32 바이트 길이의 패킷에서는 응답시간에 대한 차이가 거의 없지만, 패킷의 크기가 증가할수록 128K 전용선의 응답시간이 늦어 지며, 응답시간의 차이가 2 배 이상 커짐을 볼 수 있다.

6. 결론

본 논문에서는 구현한 기업 가상사설망 시스템은 보안에 취약한 VPN 망, 장비 교체 및 네트워크 구성에 따른 비용부담, 안정적인 회선 운용 미흡이라는 3 가지 단점을 보완하여 기업 가상 사설망을 구현한 사례이다. 본 논문에서 구현한 가상 사설망 시스템은 현재에도 사용 중이며 실제 사용 결과도 ATM 이나 프레임 릴레이로 구현한 사설망에 비해서 회선 연결성 및 안정성도 손색이 없었으며, 회선 운영비는 1/10 으로 줄어든 반면, 데이터 전송능력은 128K 전용선을 사용하였을 때와 비교해 5 배정도 증가하였다. 본 논문에서 구현한 시스템은 종단 네트워크에서 종단 네트워크로의 가상 사설망 시스템을 구현한 것으로서 향후 타 운영체제와의 호환성을 보강하여 종단 호스트에서 종단 네트워크로의 가상 사설망 접속 시스템으로 확장 발전 시킬 계획이다.

참고문헌

[1] Free S/WAN 홈페이지 “http://www.freeswan.org”.
[2] IETF RFC 2402 “IP Authentication Header (AH)”.
[3] IETF RFC 2406 “IP Encapsulating Security Payload (ESP)”.
[4] Dave Kosiur, “Building and Managing Virtual Private Networks,” John Wiley & Sons, 1998.
[5] 김창배, 박성준, “IPsec 을 이용한 가상 사설망 구현,” 한국 멀티미디어학회, 1999.
[6] 오승희, 채기준,” 다양한 트래픽을 이용한 VPN 프로토콜 성능평가,” 정보처리학회 논문지 C, 2001.
[7] 이동춘, 김점구,” VPN 의 데이터 무결성 평가를 위한 VIES 설계 및 구현,” 정보처리학회 논문지 C 2002.