정보학연구 제7권 제4호 2004년 12월(pp.21-30)
The Journal of Information Technology. Vol.7. No.4

원격접속 VPN에 대한 성능분석

김지홍*

요 약

VPN은 공중망을 이용하여 전용선을 구축할 수 있는 기술로서, 전송되는 데이터에 대한 보안기능을 제공한다. 또한 권한을 가진 사용자만이 접근할 수 있도록 암호 및 보안 알고리즘을 사용한다. 본 논문에서는 IPsec 과 VPN에 관한 기술을 정리하고, 원격접속 VPN 성능분석을 위한 파이럿 시스템을 구축하였다. 그리고 단일사용자에 대한 원격접속 VPN의 성능을 분석하고, 5명의 사용자가 동시 사용하는 경우에 대하여 원격접속 VPN의 성능을 분석하였다.

Ⅰ. 서론

인터넷 프로토콜에서 네트워크 장비간의 접속 기능을 제공하는 계층은 네트워크 계층이다. 네트워크 계층에서 네트워크 장비간의 보안기능을 제공하는 대표적인 프로토콜은 IPsec으로서, 이와 관련된 장비들은 최근 전용선을 대신할 수 있는 기술로 대두되고 있다. 즉, 별도의 전용선을 설치하지 않아도 되므로 비용 절감효과와 더불어 보안기능을 제공한다. 예를 들어, 지사들의 근거리망을 모두 전용선으로 연결하여 사용을 하는 것보다는 공중망을 이용한 VPN을 사용하여 지사들의 근거리망을 연결한다면 비용의 절감을 가져올 수 있으며, 지사의 사용자들은 평상시와 동일한 방법으로 접근할 수 있으므로 투명성이 제공된다. 관리적인 측면에서도 적은 비용을 가지고 넓은 범위의 네트워크를 구성할 수 있으므로 아주 효율적인 방법이다[8].

* 세명대학교 정보보호학과 교수
본 논문은 2003년도 세명대학교 교내 학술연구비 지원에 의해 수행된 연구임

본 논문에서는 VPN을 이용한 터널링 형태인 원격접속(Remote Access) VPN을 구성하고, VPN 터널링을 설정하는 암호화 알고리즘 중에 현재 표준화된 Layer 2계층 프로토콜인 PPTP와 Layer 3계층 프로토콜인 IPsec을 이용한 원격접속 VPN 터널링을 구성하여, 터널을 이용하여 전송되는 데이터에 대한 전송속도와 소요시간 등을 알아본다.[1][2] 또한 다중사용자인 경우의 원격접속 VPN의 성능을 체크하기 위하여 라우터, VPN 전용장비(VPN Concentrator) 및 방화벽 장비(PIX 515E)와 각각 VPN 채널을 구성하여 5명의 사용자가 동시에 VPN을 사용하였을 경우에 대한 성능을 측정하였다.

1장에서는 IPsec 프로토콜의 구조와 Key 교환 과정을 다루고, 2장에서는 VPN에 관한 기본적인 개념, 기능, 구성과 방식, 종류 등을 다룬다. 그리고 3장에서는 원격접속 VPN의 성능을 실험하기 위한 테스트 베드를 구성하고, 먼저 단일 사용자인 경우, VPN을 사용하지 않은 경우와 제 2계층의 PPTP VPN을 사용한 경우, 및 제 3계층의 IPsec VPN을 사용한 경우에 대한 성능을 비교하였다. 또한 다중사용자인 경우에 대하여 원격

접속 사용자와 VPN 전용 장비간의 터널링 테스트 및 PIX 방화벽간의 전송 성능을 분석하였다. 마지막으로 결론에서는 이러한 분석결과를 논하고, 향후 전개되어야 할 연구 방향을 제시한다.

II. 본론

2.1. IPsec 프로토콜

IPSec 프로토콜은 네트워크 장비간의 보안채널을 제공하기 위한 네트워크 계층의 보안프로토콜로서, 호스트와 호스트간, 호스트와 보안 게이트웨이간, 보안 게이트웨이와 보안 게이트웨이간의 경로를 보호하기 위하여 사용하는 VPN(Virtual Private Network) 기능을 제공한다.[3]

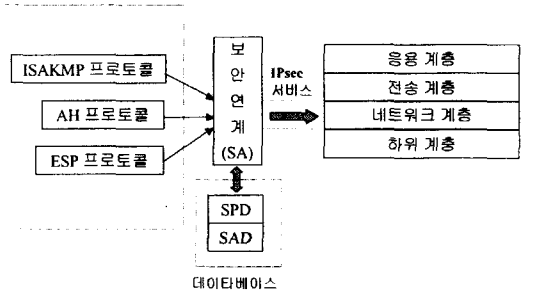
2.1.1. IPsec 프로토콜 구조

IPsec 구조는 (그림 1)과 같이 ESP (Encapsulation Security Payload), AH (Authentication Header) 및 ISAKMP (Internet Security Association and Key Management Protocol) 프로토콜 및 이들 프로토콜을 사용하여 보안연계(Security Association) 서비스를 제공한다. IPsec이 제공할 수 있는 주요 네트워크 보호 서비스는 접근제어와 무결서, 인증, 데이터 기밀성, 재전송 공격(Reply attack) 방지 등의 서비스를 제공한다.

ESP는 IPsec에서 제공되는 기본적인 서비스를 모두 지원할 뿐 아니라, 전송되는 데이터의 기밀성을 보호하기 위하여 표준 암호 알고리즘을 사용할 수 있다.

AH는 무결성과 인증기능을 제공한다. 다양한 표준 인증알고리즘을 지원하지만 암호화 프로토콜은 지원하지 않는다. 주로 Site to Site VPN 이나 원격접속 to VPN 에서 사용 할 때는 ESP를 많이 사용하며, Host 간의 IPsec를 사용할 경우 제한적으로 AH를 사용한다.

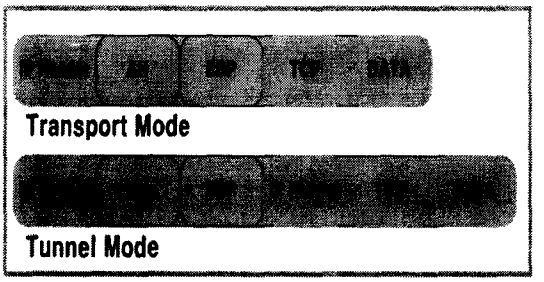
ISAKMP은 보안 협상과 그들의 암호화 키들을 관리하기 위해서 자동적으로 설정하는 방법을 제공한다. ISAKMP는 IKE(Internet Key Exchange)를 이용하여 AH와 ESP프로토콜에서 사용되는 암호 및 인증 알고리즘에서 사용되는 키를 교환하고 보안연계 협상(Security Association Negotiation)을 한다. IKE에서 사용 할 수 있는 인증알고리즘은 Pre-shared key와 공개키, 디지털 서명 등의 방식으로 나뉘어 진다. 공개키 기반방식은 공개키 기반시스템(Public Key Infrastructure)의 구축으로 보다 확장된 네트워크 보안기능을 지원하여준다. Pre-shared key 방식은 미리 설정된 키를 상호 안전하게 교환할 수 있게 하여주는 방식이다.



(그림 1) IPSec 구조

IPsec에서는 2가지의 모드가 존재하는데 주로 AH와 ESP가 Packet에서 어디에 위치하여 있느냐에 따라서 모드가 결정된다. 아래의 (그림 2)처럼 전송 모드와 터널 모드로 구성되는데, 전송모드는 단말(end point)과 단말에 위치한 두 호스트간에 이용되며, 패킷 헤더는 보호영역이 아니므로 헤더의 정보가 노출된다. 터널모드는 주로 두개의 보안장비 혹은 단말과 보안 장비간에

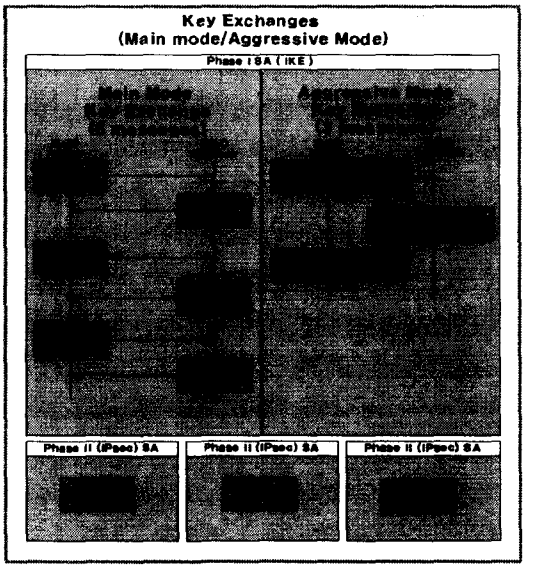
이용되며, 원래의 IP 패킷 전체를 보호영역으로 묶어두기 때문에 안전한 통신이 가능하다.



(그림 2) IPSec Mode

2.1.2. Key 교환 과정

터널을 구성하기 위한 과정인 키 교환 과정은 Phase1과 Phase2 과정으로 나뉘어 동작한다. Phase1은 메인모드(Main mode)와 집중모드(aggressive Mode)가 있는데 기본으로 메인모드를 선택하며, 아래의 (그림 3)처럼 메인모드의 경우 6번의 패킷교환을 통하여 세션과 SA의 키를 교환한다[6].



(그림 3) 키교환 과정

집중모드는 3개의 패킷을 통하여 세션과 SA (Security Association) 협상 및 키를 교환한다. 단계 1은 주로 ISAKMP(Internet Security Association and Key Management Protocol)에서 단계 2의 협상과정을 보호하기 위해 쓰일 SA를 보호하기 위한 동작 설정이며, 단계 2의 IPsec 키 교환은 퀵모드(Quick mode)로 동작되며 실제 보안 협상키를 구현하고 데이터의 암호화에 사용된다.

하나의 메인모드에서 세션을 맺으면 퀵모드가 다수 동작 된다.

2.2. VPN

VPN(Virtual Private Network)은 전송선망을 이용하지 않고, 공중망을 이용하여 제공되는 가설사설망 기술이다. 그러므로 VPN 기술은 사용자와 사용자간, 사용자와 자사의 네트워크간, 밀접한 관계가 있는 회사와 회사 간에 접속할 때에 보안기능을 제공할 뿐 아니라, 서비스 품질을 향상시킬 수 있으며, 또한 관리 면에서 우수한 전용선로 기술이다.

2.2.1. VPN 기능

일반적으로 VPN 기능은 기존의 전화망에서의 RAS(원격접속 Access Server) 서비스와 대비된다. RAS 서비스는 원격지 사용자가 전화망을 이용하여 내부 시스템으로 접속할 수 있는 방법으로서, 별도의 전용선, 전용선 사용료 및 RAS 장비 등을 필요로 한다. RAS 서비스는 사용자가 소수인 경우에는 적합하지만, 그룹 혹은 기업과 기업간 혹은 기업내의 다수의 조직원에 적용하기 위해서는 ISP 업체에서 제공하는 VPN 시스템을 이용하는 것이 가격 면에서 훨씬 저렴할 뿐 아니라, 다양한 보안서비스를 제공받을 수 있다. 다음은 VPN 시스템을 구성함으로서 다음과 같은 장

점을 가진다.

① 보안 및 정보보호 기능
② 서비스 품질(QoS: Quality of Service)
③ 규모(Scaling)
④ 관리(Management)
⑤ 다중서비스 공급자 지원
⑥ 다중방송(Multicast)

2.2.2. VPN 종류

VPN 종류는 크게 Site to Site VPN과 원격접속 Access VPN으로 구분될 수 있다. Site to Site VPN 이란 네트워크 장비에서 제공되는 기능을 이용하여 VPN을 구축하는 방법이며, 원격접속 Acces VPN은 원격 사용자가 VPN을 이용할 수 있도록 제공되는 기술이다.

1) Site to Site VPN

① 인트라넷 VPN(Intranet VPN)

공중망을 통하여 기업 내 본사 네트워크와 원격지의 공장 혹은 지점의 네트워크간을 상호 연결한 VPN이다. 인트라넷 VPN을 구성하기 위해서는 기본적으로 데이터 보호를 위한 강력한 암호화기술이 요구된다. 기업내의 매출관리, 고객 데이터베이스 관리, 기밀 문서교환을 위한 ERP (Enterprise Resource Planning) 시스템 등이 사용된다.

② 익스트라넷 VPN(Extranet VPN)

공중망을 통하여 기업과 전략적인 업무파트너 기업간을 연결한 VPN이다. 소비자와 공급자 관계의 기업간에 네트워크 공유를 필요로 하는 경우에 사용된다. 기업간에 공유되어야 하는 여러 가지 솔루션은 상호 동작성을 보장하기 위하여 개방형 표준기반 해결방법(open standards-based solution)을 만족하여야 한다.

2) Site to Site VPN

원격접속 VPN(원격접속 Access VPN)이라고도 불리우며, 공중망을 통하여 기업 내 네트워크와 원격의 직원 혹은 이동중인 직원 간을 연결한 VPN이다. 원격접속 VPN 시스템은 원격사용자가 침입차단시스템을 경유하지 않고, 인터넷을 통하여 기업내의 네트워크로 접속하기 때문에, 기본적으로 원격의 사용자에 대한 강력한 사용자 인증 기술을 요구한다. 관리적 차원에서 원격접속 VPN 시스템에서는 VPN에 접속하는 사용자들에 대한 인증기능을 처리할 수 있는 중앙관리 시스템을 요구한다.

2.2.3 VPN 생성을 위한 보안프로토콜

인터넷 사용자들이 원격접속방식의 VPN을 사용하기 위해서는 제2계층의 기능을 이용한 PPTP 프로토콜과 제3계층의 기능을 이용한 IPsec 프로토콜이 사용된다.

1) L2TP 프로토콜

L2TP(Layer 2 tunneling protocol) 프로토콜은 제 2계층의 프로토콜로서, IETF 표준화 과정에서 발전된 PPTP와 L2F를 결합한 프로토콜이다. 성숙한 IETF 표준화 단계 프로토콜로서 광범위하게 구현되고 있고, IP, X.25, 프레임릴레이, 비동기 전송 모드(ATM) 네트워크를 통해 전송될 PPP(Point-to-Point Protocol) 프레임을 캡슐화하여 전송하는 방식이다.

2) IPsec 프로토콜

전 장에서 설명된 네트워크 계층의 보안프로토콜이다.

2.3. 원격접속 VPN 성능분석

VPN은 크게 VPN 기능을 가진 장비들을 이용한 보안터널링 기능을 제공하는 Site to Site VPN 방식과 원격 사용자 프로그램에 의해 보안 터널링 기능을 제공하는 원격접속 VPN 방식으로 구분된다. 본 논문에서는 원격접속 VPN 방식의 성능을 평가하기 위하여 VPN 전용장비, Fix 방화벽를 이용하여 파이럿 시스템을 구축하였다. 또한 원격접속 VPN 성능을 평가하기 위하여 Windows 시스템에 내장된 VPN 기능(PPTP 프로토콜)과 원격접속 VPN Client 프로그램을 사용하여 원격사용자가 VPN을 이용하는 구조로 시스템을 구축하여 원격접속 VPN의 성능을 평가하였다.

현재 IPsec을 지원하는 제품을 사용하였으며, 시스코사의 VPN3005와 pix firewall v6.2, Windows 2000 SP4 IPsec Policy를 사용하였다. 모든 장비에는 IPsec Acceleration Card는 미장착하여 고유의 CPU 성능을 기본으로 하고 있다.

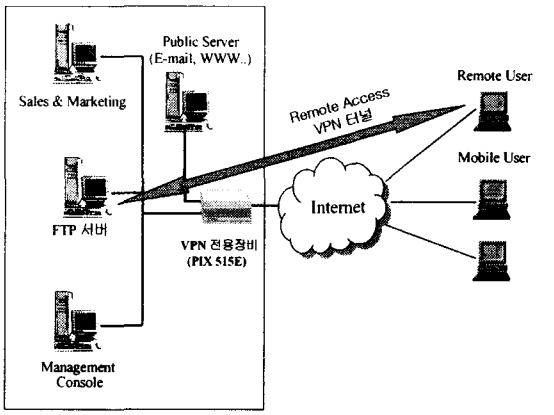
2.3.1. 원격접속 VPN 구성

원격접속 VPN을 구성하기 위해서 (그림 2)와 같이 구성하기 위하여 <표 1>과 같은 테스트베드를 사용하여 아래와 같은 기술하였다.

〈표 1〉 테스트 디바이스 목록

제품명	IP Address	Version
Cisco Pix 515E	Ext:192.168.135.243 Int:10.10.1.1/24 Client:10.10.1.2	6.2
Cisco VPN 3005	Ext:192.168.135.244 Int:10.10.4.1/24 Client:10.10.4.2	2.5.1
Windows2000 IPsec Polic	Ext:192.168.135.41 Int:10.10.5.1/24 Client:10.10.5.2 P4-1.7G/256	SP 4 팬티엄 4(1.7G)

- 암호 프로토콜 : 3DES, MD5, DH1
- 키교환 및 암호화 엔진 : IKE, AH, ESP
- 터널링/암호화 구현 기술 : IPSec, PPTP



(그림 4) 원격접속 VPN 테스트 환경

2.3.2 단일 사용자 원격접속 VPN 성능테스트

(그림 4)와 같이 원격접속 VPN 구성은 원격지에서 자사의 네트워크에 접속을 하거나 이동중인 직원들이 신뢰성을 기반으로 한 일정한 보안된 네트워크에 접속하기 위하여 사용할 수 있는 방법이다. 여기에서 CISCO VPN 전용장비인 VPN 전용장비를 이용하여 원격접속 VPN을 구성하고, 원격접속자인 Window 시스템에서 L2기반의 PPTP와 L3기반의 IPSec을 사용하여 각각의 클라이언트로 VPN 전용장비와 터널링을 구성하였다.

〈표 2〉 일반 시스템에서의 데이터 전송

	Throughput (Up Link)		Throughput (Down Link)	
	시간	전송속도	시간	전송속도
1	1:46s	0.94 MB/s	1:19s	1.26 Mbp
3	1:46s	0.94 MB/s	1:19s	1.26 Mbps
4	1:47s	0.93 MB/s	1:18s	1.27 Mbps
5	1:46s	0.94 MB/s	1:18s	1.27 Mbps

<표 2>는 VPN을 사용하지 않은 경우의 일반 시스템에서의 파일전송 프로그램을 이용하여 측

정된 데이터 전송성능을 보인다. 이에 반면에 <표 3>은 Cisco 클라이언트에서 지원되는 L3 레이어에서 IPsec 암호화 구현 기술을 이용하여 VPN 전용장비와의 터널링을 설정하고 데이터의 업로드와 다운로드를 한 경우에 데이터 전송속도를 나타내고 있다.

전용장비의 CLF(CPU LOAD FACTOR)가 거의 풀로 차고, 업로드와 다운로드에서 약간의 속도 차이를 보이고 있으나 거의 비슷한 속도를 보여준다.

〈표 3〉 IPSec 터널링 (Single)

	Throughput (Up Link)		Throughput (Down Link)	
	시간	전송속도	시간	전송속도
1	4:20s	0.38 MB/s	4:02s	0.41 Mbps
2	4:20s	0.38 MB/s	4:02s	0.41 Mbps
3	4:20s	0.38 MB/s	4:02s	0.41 Mbps
4	4:19s	0.39 MB/s	4:02s	0.41 Mbps
5	4:20s	0.38 MB/s	4:02s	0.41 Mbps

<표 4>는 Window 2000 Server에서 지원되는 L2 레이어 PPTP를 이용하여 VPN 전용장비와 터널링으로 연결하여 데이터의 업로드와 다운로드를 테스트한 결과이다. VPN 전용장비의 속도면에서 역시 약간의 차이가 있으나 비슷함을 알 수 있다.

〈표 4〉 PPTP 터널링

	Throughput (Up Link)		Throughput (Down Link)	
	시간	전송속도	시간	전송속도
1	1:00s	1.67 MB/s	53s	1.89 Mbps
2	1:00s	1.67 MB/s	52s	1.92 Mbps
3	1:00s	1.67 MB/s	52s	1.92 Mbps
4	1:00s	1.67 MB/s	52s	1.92 Mbps
5	1:00s	1.67 MB/s	55s	1.82 Mbps

<표 3>과 <표 4>와 같이 속도 면에서 L3 IPsec을 이용한 Cisco 클라이언트보다 L2 레이어 PPTP를 이용한 Window 2000 Server 클라이언트가 속도 면에서 살펴보면 초당 전송속도에서 약 4배라는 많은 차이를 보임을 알 수 있다. 원격접속 VPN은 개인사용자가 사용하는 것보다는 관리 자적인 측면에서 사용한다고 볼 수 있으므로 L2, L3 프로토콜 중에 어느 것을 사용할 것인가를 결정하는 경우 적절한 선택을 하는 것이 중요하다.

2.3.3 다중 사용자 원격접속 VPN 성능테스트

1) VPN 3000을 이용한 원격접속 VPN 성능 테스트

<표 4>와 <표 5>는 (그림 2)에서 5명의 원격 사용자가 동시에 VPN 3000 전용장비를 이용하여 원격접속 VPN으로 터널링을 구성하고, 100 Mbyte의 데이터를 업로드 및 다운로드한 테스트 결과이다.

〈표 4〉 VPN 전용장비를 이용한 원격접속 VPN (5 Clients Upload)

	CPU load factor	Throughput (단위 : s, bps)				
		Client1	Client2	Client3	Client4	Client5
1	90%	15:04s 0.11M	20:14s 84.35K	20:05s 84.98K	20:07s 84.84K	20:09s 84.70K
2	90%	15:32s 0.11M	19:58s 85.48K	20:02s 85.19K	19:55s 85.69K	19:57s 85.55K
3	90%	15:11s 0.11M	20:02s 85.19K	19:58s 85.48K	20:03s 85.12K	19:48s 86.19K
4	90%	15:09s 0.11M	19:59s 85.40K	20:02s 85.19K	20:08s 84.77K	19:54s 85.76K
5	90%	15:01s 0.11M	20:02s 85.19K	20:06s 84.91K	20:05s 84.98K	20:09s 84.70K

위 실험결과에서 100Mbyte의 데이터를 VPN 전용장비를 이용한 터널링을 구성하여 데이터의 업로드와 다운로드에서 전송시간 및 데이터양이 터널링을 사용하지 않았을 경우의 전송시간 및 데이터양보다 많은 차이를 가지고 있음을 알 수 있다. 암호화를 통한 보안성에서는 뛰어나지만

아직까지 부하 증가를 가지고 온다는 점에서 좀도 개선해야 할 문제를 가지고 있다는 것을 알 수 있다.

〈표 5〉 VPN 전용장비를 이용한 원격접속 VPN (5 Clients Download)

	CPU load factor	Throughput (단위 : s, bps)				
		Client1	Client2	Client3	Client4	Client5
1	90%	11:54s 0.14M	21:29s 79.44K	21:31s 79.32K	21:32s 79.26K	21:44s 78.53K
2	90%	14:34s 0.11M	21:29s 79.44K	21:28s 79.50K	21:33s 79.20K	21:43s 78.59K
3	90%	14:47s 0.11M	21:27s 79.56K	21:28s 79.50K	21:35s 79.07K	21:31s 79.32K
4	90%	14:11s 0.12M	21:27s 79.56K	19:06s 79.20K	21:31s 79.32K	21:27s 79.56K
5	90%	13:48s 0.12M	9:58s 0.17M	19:06s 89.35K	19:08s 89.20K	19:11s 88.97K

2) 방화벽(PIX 515E)를 이용한 원격접속 VPN 성능 테스트

<표 6>과 <표 7>은 (그림 2)에서 VPN 3000 전용장비 장비 대신에 PIX 장비로 구성하여, 원격사용자가 PIX 장비를 통하여 원격접속 VPN으로 터널을 구성하고, 100 Mbyte의 데이터를 업로드 및 다운로드한 테스트 결과이다.

〈표 6〉 PIX 방화벽을 이용한 원격접속 VPN (5 Clients Upload)

	CPU load factor	Throughput (단위 : s, bps)				
		Client1	Client2	Client3	Client4	Client5
1	90%	1:02s 1.59M	1:06s 1.52M	1:18s 1.28M	1:16s 1.32M	1:13s 1.37M
2	90%	1:07s 1.49M	1:19s 1.27M	1:21s 1.23M	1:22s 1.22M	1:12s 1.39M
3	90%	1:01s 1.63M	1:17s 1.30M	1:20s 1.25M	1:21s 1.23M	1:18s 1.28M
4	90%	1:08s 1.45M	1:18s 1.28M	1:21s 1.23M	1:23s 1.20M	1:18s 1.28M
5	90%	1:07s 1.48M	1:13s 1.37M	1:18s 1.28M	1:15s 1.33M	1:12s 1.39M

위 실험결과에서 100Mbyte의 데이터를 PIX 장비를 이용하여 터널링을 구성하여 데이터의 업로드와 다운로드를 한 결과를 보여주고 있다. 전용장비를 사용하였을 경우보다 빠른 데이터의 전송속도를 보여주고 있다. 하지만 이것은 장비의 CPU 처리속도와 같은 장비의 차이 때문에 생기는 속도 차이를 나타낸다. 전용장비라 할지라도 터널링을 위해 최적화되지 않은 장비라면 PIX와 같은 장비기반의 VPN보다 성능이 저하되는 것을 알 수 있다. 또한 데이터 전송시간 및 데이터양이 터널링을 사용하지 않았을 경우의 전송시간 및 데이터양보다 상당히 많이 떨어지는 것을 알 수 있다. 터널링 암호화를 통해 데이터의 보안에는 뛰어난 장점을 가지지만 데이터 전송율이 떨어진다는 단점을 가지고 있으므로 더욱더 최적화된 네트워크 구성을 위해서는 터널링을 이용하면서 데이터 전송률도 고려를 해야 할 것이다.

〈표 7〉 PIX 방화벽을 이용한 원격접속 VPN (5 Clients Download)

	CPU load factor	Throughput (단위 : s, bps)				
		Client1	Client2	Client3	Client4	Client5
1	90%	1:30s 1.10M	1:41s 0.99M	1:41s 0.99M	1:39s 1.01M	1:30s 1.11M
2	90%	1:32s 1.08M	1:40s 1.00M	1:41s 0.99M	1:41s 0.99M	1:29s 1.12M
3	90%	1:34s 1.06M	1:37s 1.03M	1:39s 1.01M	1:42s 0.98M	1:31s 1.10M
4	90%	1:32s 1.09M	1:41s 0.99M	1:41s 0.99M	1:42s 0.98M	1:31s 1.10M
5	90%	1:28s 1.12M	1:37s 1.03M	1:29s 1.12M	1:39s 1.01M	1:29s 1.12M

Ⅲ. 결론

본 논문에서는 먼저 IPsec과 VPN에 대한 기본적인 개념을 다루고, 원격접속 VPN의 성능을 측정하기 위하여 단일사용자의 경우에는 VPN을 사용하지 않은 경우와 L2 계층의 VPN(PPTP 방식)을 구성한 경우, L3 계층의 VPN(IPsec 방식)

을 구성한 경우를 각각 나누어 실험하고 결과를 비교하였다.

같은 조건에서의 동일한 VPN 전용장비와 세션을 맺은 후 100Mbyte의 데이터를 전송한 결과 두 알고리즘 모두 투명성을 보이지만 속도 면에서 많은 차이가 나타나는 것을 알 수 있었다. 실험결과에 의하면 IPsec 방식에 비하여 PPTP 방식이 4배 정도의 성능차가 나타나는 것으로 나타났다. 이처럼 원격접속 VPN에서 IPsec을 이용한 방법은 PPTP 방식에 비하여 부가적인 기능으로 인하여 성능이 떨어짐을 알 수 있다. 그러나 IPsec 방식은 일반 사용자보다 관리자적인 측면에서 사용하는 것이 적절하며, 사용자로서는 L2, L3 프로토콜 중에 어느 것을 사용할 것인가를 사용 목적에 따라 적절한 선택을 하는 것이 중요하다.

또한 다중사용자에 대한 VPN 전용장비와 방화벽을 이용하여 각각 원격접속 VPN을 구성하고 데이터의 전송을 통해 VPN의 성능을 실험해 본 결과, 방화벽장비가 VPN 전용장비에 비하여 성능이 우수한 것으로 나타났다. 이러한 결과는 실제 장비의 CPU 처리속도와 처리능력의 차이에 의해 나타날 수도 있다. 그러나 터널링 암호화를 통해 데이터의 보안에는 뛰어난 장점을 가지지만, 데이터 전송율이 떨어진다는 단점을 가지고 있으므로 더욱 더 최적화된 네트워크 구성을 위해서는 터널링을 이용하면서 데이터 전송률도 고려해야 할 것이다.

마지막으로 본 시스템에서 실험에 사용된 장비가 보급형 수준의 장비이며, VPN 가속기 등을 설치하지 않은 상태이므로 VPN 동작 시에 시스템 성능에 많은 부하를 줌으로서, VPN 기능과 시스템 성능 간에는 상반된 결과가 나타난 것으로 보인다. 그러나 만일 고성능의 장비를 사용하였다 하더라도 다중 사용자를 이용한 원격접속 VPN 방식의 경우에는 사용자수가 증가함에 따라 시스템의 성능에 영향을 줄 것으로 예상된다.

향후 VPN의 우수한 성능을 유지하면서 시스템에 커다란 영향을 미치지 않을 수 있는 QoS 기능을 이용한 VPN 설정등과 같은 방법 등에 대한 연구가 수행되어야 할 것으로 사료된다.

참고문헌

[1] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, *Layer two tunneling protocol(L2TP)*, RFC 2661, 2003.

[2] W. Lai, D. McDysan, *Network hierarchy and multilayer survivability*, RFC 3386, 2002 [3] IP Security Protocol(ipsec). IETF, http://www.ietf.org/html.charters/

[4] D. Piper, *The internet IO security domain of interpretation for ISAKMP*, RFC2407, 1998.

[5] D. Harkins, D. Carrel, *The internet key exchange(IKE)*, RFC 2409, 1998.

[6] *Products for Remote Access VPNs*, http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns125/networking_solutions_package.html

[7] 이만영, 김지홍, 염흥렬, 송유진, 이임영, "인터넷 정보 보안", 생능출판사, 2002.

[8] RFC 문서

- IP Authentication Header (RFC 2402)
- IP Encapsulating Security Payload (ESP) (RFC 2406)
- Internet Security Association and Key Management Protocol(ISAKMP) (RFC 2408)

- The Internet Key Exchange (IKE) (RFC 2409)
- A Core MPLS IP VPN Architecture (RFC 2917)
- Virtual Private Networks Identifier (RFC 2685)
- A Framework for IP Based Virtual Private Networks (RFC 2764)

The Performance Analysis on Remote Access VPN

Ji-Hong Kim*

Abstract

A VPN(Virtual Private Network) is constructed using public wires to connect nodes. It can be used like the dedicated line and maintain the security of the data on the VPN. And It uses encryption and other security mechanisms to ensure that only authorized users can access the network.

In this paper we summarize IPsec and VPN technology and construct pilot VPN system for analyzing the performance of remote access VPN.

Then we analyze the performance of remote VPN system using VPN concentrator in case of single user and in case of multi users.

Key words : VPN, IPsec, VPN system

* Professor, Department of Information Security, Semyung University