기업인프라보호를 위한 가상 사설망 VPN 구축 모델 개발

김수진*, 이승호*, 황도훈**, 강성효***, 전현호****
*대구가톨릭대학교 정보보호학과
**상명대학교 컴퓨터과학과
***세종대학교 정보통신학과
****KT 기업사업컨설팅본부
e-mail : hh.jeon@kt.com

Development of Virtual Private Network VPN Construction Model to Protect Enterprise Infrastructure

Su-Jin Kim*, Seung-Ho Lee*, Do-Hun Hwang**, Seong-Hyo Kang***, Hyun-Ho Jeon****
*Dept. of Information Security, Catholic University of Daegu
**Dept. of Computer Science, Sang-Myung University
***Dept. of Information and Communication, Se-Jong University
****Dept. of Enterprise business, KT

요 약

최근 급증하는 보안 침해 사고와 함께 보다 다양해지고 있는 해킹 기법들에 대한 대응책 마련이 논의되고 있다. 기업의 내부 인프라 자산 보호를 위해 조치를 취할 수 있는 기본적인 1 차 대응책으로 네트워크 계층에서의 방어에 대한 중요성이 대두되고 있다. 본 논문에서는 일반 공중망(Public Network)과 분리된 가상의 사설망(VPN: Virtual Private Network)을 구현함으로써 기존의 VPN 모델보다 보안성이 뛰어나며 저렴한 비용으로 외부에서의 접근 및 스누핑(Snooping)공격과 같은 보안위협에 대비할 수 있는 VPN 모델을 구축하여 실제 현업 망에서의 적용 가능성을 도출하고자 한다.

1. 서론

오늘날 네트워크 기술은 사물에 센서를 부착하여 실시간으로 데이터를 인터넷으로 주고 받는 사물인터넷(IoT, Internet of Things) 환경, 인간의 다양한 능력을 컴퓨터 프로그램으로 실현한 인공지능 기술 등 일상생활로 다양하게 영역을 넓혀가며 점점 더 진화를 거듭해가고 있다. 이와 동시에 보안 침해 사고와 관련한 해킹 기법들 역시 다양해지고 있다. 이러한 해킹 기법들에 대한 대응책 마련이 논의 되고 있으며 내부 인프라 자산 보호를 위해 보호 조치를 취할 수 있는 1 차 대응책으로 네트워크 계층에서부터의 방어가 중요해졌다. 이에 대응하여 외부에서의 접근 및 스누핑과 같은 외부공격으로부터 가상의 사설망을 이용하여 차단할 수 있다.

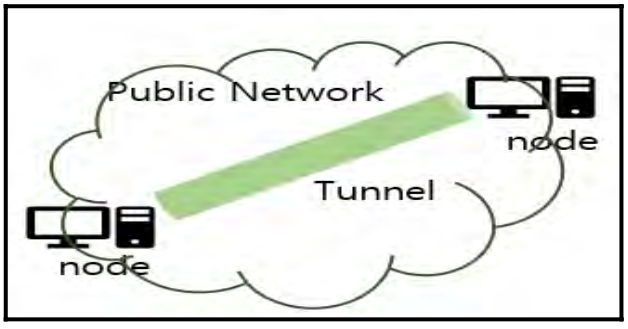
본 논문에서는 이러한 VPN 기술과 시장의 동향 그리고 VPN 을 실제로 도입 했을 때 어떠한 장단점이 있는지에 대해 알아보고, 가상솔루션인 GNS(Graphical Network Simulator)을 사용해 VPN 을 구현하여 그 결과와 기능을 도출하고자 한다.

2. 본론

2.1 VPN 동향에 대한 기술/시장 조사

(1) 터널링(Tunneling) 기술

공용 네트워크를 사설 네트워크처럼 사용할 수 있게 하는 핵심적인 기술인 터널링 기술은 공용 네트워크에 있는 두 노드 간 가상의 터널을 형성해 같은 네트워크에 속해 있는 제 3 의 사용자가 접근하지 못하도록 한다.



(그림 1) 터널링 기술의 구성

(그림 1)과 같이 공중망에 있는 두 노드 간의 통신 경로를 캡슐화(Encapsulation)와 디캡슐화(Decaps-ulation) 과정을 통해 논리적으로 단일 망을 형성한다[2].

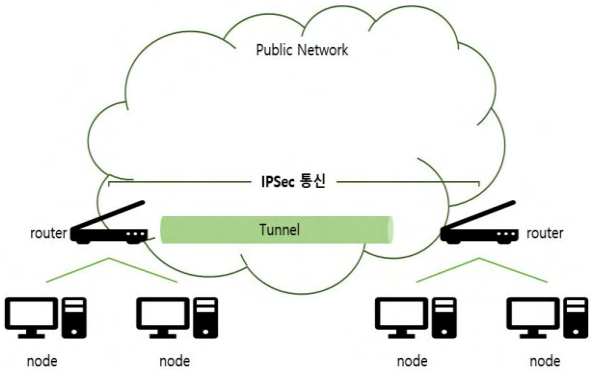
(2) 암호화(Encryption) 기술

터널링 기술을 사용함에 있어 악의적인 제 3 의 사용자가 중간에서 패킷(Packet)을 가로채더라도 그 내용을 알 수 없도록 만드는 암호화 기술이 사용된다.

IPSec(Internet Protocol Security) VPN 에서 사용되는 데이터의 인증 및 암호화인 ESP(Encapsulation Security Payload)[2]의 암호화와 복호화를 위해 일반적으로 사용되는 암호 알고리즘으로는 DES, Triple-DES, AES, AIRA, SEED 가 있다. 이 중 AES 알고리즘은 국제 표준으로 지정된 대칭 키 암호화 알고리즘으로 128, 192, 256 비트의 키 길이와 128 비트 크기의 블록을 사용한다.

(3) IPSec 을 이용한 VPN [3]

3 계층인 Network Layer 에서는 보안 표준인 IPSec[2]을 사용하여 추가 헤더와 프로토콜을 이용해 네트워크 패킷을 보호한다. 추가되는 헤더와 프로토콜로는 데이터 송신자의 인증을 처리하는 인증 헤더 AH(Authentication Header)와, 송신자의 인증과 더불어 데이터 암호화도 함께 처리하는 ESP(Encaps-ulation Security Payload), 키 교환에 사용되는 IKE 프로토콜[2]등을 이용해 보안 서비스를 제공한다. 또한, IPSec 은 개별 사용자 컴퓨터의 어떠한 변경 없이 보안에 관한 문제를 처리할 수 있다.



(그림 2) IPSec VPN 통신 흐름

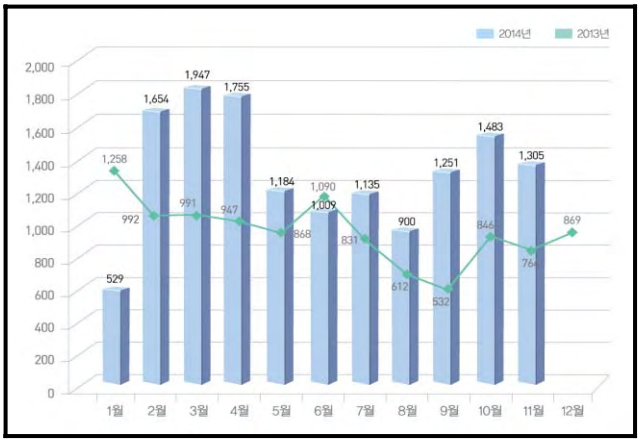
(4) VPN 시장의 동향

VPN 은 다양한 방법으로 구현될 수 있다. 그 종류로는 PVC 나 SVC 등을 통해 구현한 VPN, L2TP 나 PPTP, IPSec 을 이용해 터널링 기술을 기반으로 한 CPE(Customer Premise Equipment) 기반의 VPN, VOIP 기반의 VPN, SSL VPN 이 있다. 다양한 VPN 의 종류 중 현재 가장 널리 사용되고 있는 것은 단연 IPSec 기반의 VPN 이다. (그림 2)는 IPsec VPN 의 대표기능인 터널링 기술을 나타낸 그림이다. IPSec 기반의 VPN 은 공중망에서 터널링 기술과 AH 와 ESP[2]를 이용한 인증 및 데이터 암호화를 사용하며, 이를 사용해 안전하게 가상 사설망을 구현할 수 있다.

2.2 VPN 도입 가능성 연구

(그림 3)에서 보듯이 최근 나날이 고도화되고 변칙적인 해킹기법으로 보안침해사고가 급증함에 따라 내부 인프라 자산을 보호하기 위한 네트워크 보안의 중요성이 증가하고 있다.

본 연구에서는 상용망에 VPN 을 도입하였을 경우 어떠한 장점과 단점이 있는지 알아보고 이를 토대로 실제 상용망에서의 VPN 도입 가능성에 대해 분석하고자 한다. VPN 은 공중망을 사설망처럼 사용하기 위한 기술로 2 장에서 언급한 터널링 기술을 이용하여 기밀성 및 무결성을 보장한다[4].

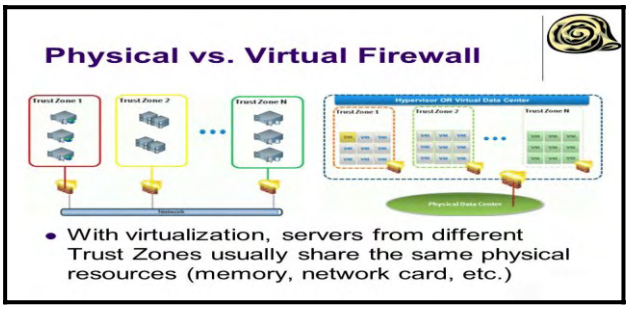


(그림 3) 2013 - 2014 년도 해킹사고 접수처리 건수 추이

일부 개방형 무선 네트워크 상에 웹 트래픽에 사용자가 원하지 않는 추적 기능을 포함한 광고가 삽입되어 있거나 특정 패킷을 도청하는 경우가 있다. 이 경우 VPN 을 활용하면 이러한 추적이나 도청을 피하는데 유용하다. 또한 물리적 방화벽과 VPN 을 이용한 가상 방화벽의 비용적인 측면을 비교해 봤을 때, 보통 중소기업에서 사용할 정도의 물리적 방화벽을 도입 한다면 실제 고가의 방화벽 장비를 구입해야 하지만 VPN 을 이용한 가상 방화벽을 도입한다면 장비를 구입할 필요가 없다.

개인이나 중소기업에서 방화벽을 도입하는 것은 고가의 비용으로 인해 쉽지않다. 기업에서 VPN 방화벽을 도입한다면 이러한 비용 문제를 해결하면서 물리적 방화벽과 같은 효과의 방화벽을 구축할 수 있다.

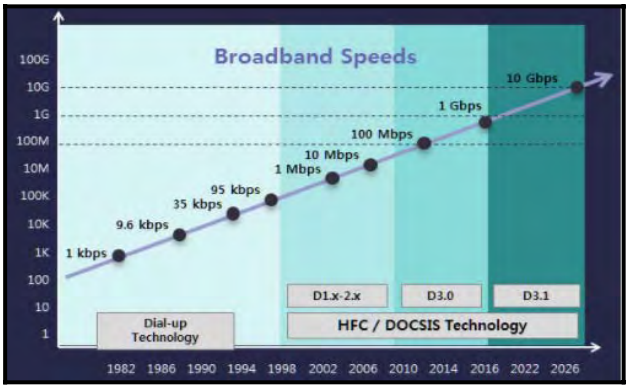
또한 VPN 방화벽을 사용할 경우 물리적 방화벽과는 다르게 네트워크 내의 자원을 공유한다는 면과 논리적으로 구성이 간편하다는 점이 있다[3].



(그림 4) 물리적 방화벽과 가상 방화벽의 비교

첫 번째로, 자원을 공유함으로써 VPN 을 사용하는 사용자는 특정 지역에 국한되지 않고 업무를 수행 할 수 있다는 장점이 있다. 예를 들어, 회사 내부망에서 하던 업무를 퇴근 후 집에서도 이어서 할 수 있고 출장을 가더라도 VPN 을 통해 회사 내부망에 접속한다면 회사 밖에서도 안전하게 업무를 수행 할 수 있다.

그러나 자원을 공유함으로 VPN 을 여러 사람이 동시에 사용할 경우 통신 속도가 저하 될 수 있다는 단점이 있다. 그러나 최근 네트워크 통신 속도가 전보다 크게 발전해 많은 동시 사용자를 감당할 수 있어 중소기업이나 소규모 단체가 사용하기엔 크게 무리가 없는 수준이다[5].



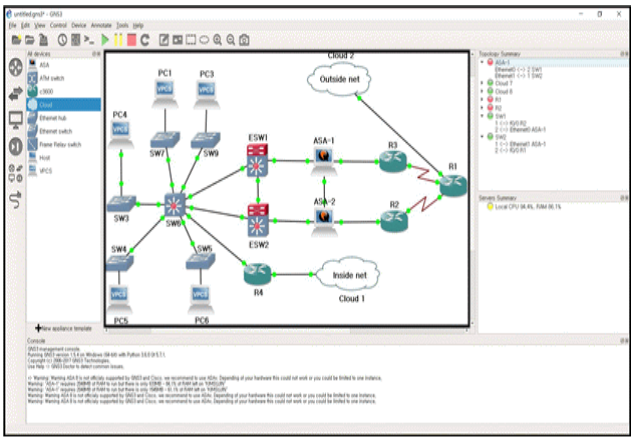
(그림 5) 연도별 광대역인터넷 속도 측정/예상 수치

두 번째로, 가상 사설망 VPN 환경은 일반 물리적인 네트워크 환경을 구성할 때 보다 더욱 간편하고 수월하게 할 수 있다는 장점이 있다. 물리적인 환경을 구성할 때는 직접 손으로 장비를 확인하고 작업해야하는 번거로운 작업들이 많지만 VPN 을 통한 네트워크 환경을 구성할 때는 이러한 번거로움에서 벗어나 논리적으로 손쉽고 간편하게 네트워크 환경 구성이 가능해 관리 및 유지보수가 쉽다는 장점이 있다.

2.3 가상화솔루션(GNS)을 활용한 VPN 구축

(1) 가상 네트워크 환경 구축

GNS(Graphical Network Simulator)는 실제 네트워크 장비들을 가상 장비로 구현할 수 있는 네트워크 소프트웨어 에뮬레이터이다. (그림 1)과 같이 GNS 는 Cisco 의 Packet Tracer 처럼 GUI(Graphic User Interface) 환경에서 사용할 수 있으며 Virtual box, VMWare 와 같은 가상 컴퓨터와 스위치, 라우터를 상호 연동할 수 있다[6].



(그림 6) GNS3 를 이용한 예상 토폴로지 구성

(2) 작품 기능

구현하고자 하는 작품의 기능을 아래 <표 1>와 같이 S/W 와 H/W 부분으로 구분하였다. S/W 주요기능으로는 (그림 6)에서 언급한 GNS 에뮬레이터를 이용하여 가상 라우터(Router) 장비 및 방화벽 장비 ASA(Adaptive Security Appliance)를 드래그 앤 드랍(Drag & Drop)으로 생성 가능하다.

<표 1>의 GNS-02 기능으로 가상 장비들(Router, Switch, ASA) 간 포트(Port)연결을 해주며 GNS-03 기능인 콘솔(Console)기능을 이용하여 가상 장비에 IP 주소 및 보안정책(ACL : Access Control List)을 설정할 수 있다.

• H/W 주요 기능

데이터가 이동하는 경로를 지정하고 전송해주는 라우터는 크게 4 가지 기능이 있다. Router-01 기능은 라우터 장비에 IP 주소를 할당하여 다른 장비들과 통신을 가능하게 해주는 역할을 한다. Router-02 기능은 다른 장비에서 Ping 을 보냈을 때 보안정책을 설정하여 원하는 데이터만 수신이 가능하다. Router-03 의 기능을 통해 최단 경로를 탐색하며 모든 기능은 Router-04 의 콘솔기능으로 라우터 장비에 명령을 내릴 수 있다.

• S/W 주요 기능

Cisco 사 전용 방화벽 장비인 ASA(Adaptive Security Appliance)는 ASA-01 기능인 영역별 IP 주소를 할당해주며 라우터와 마찬가지로 보안정책을 설

정하여 영역 간 특정 트래픽(Traffic)을 차단 및 허용할 수 있는 방화벽 역할을 하며 모든 기능은 콘솔 기능을 통해 가상 ASA 장비에 명령을 내릴 수 있다.

<표 1>S/W, H/W 전체 기능 목록

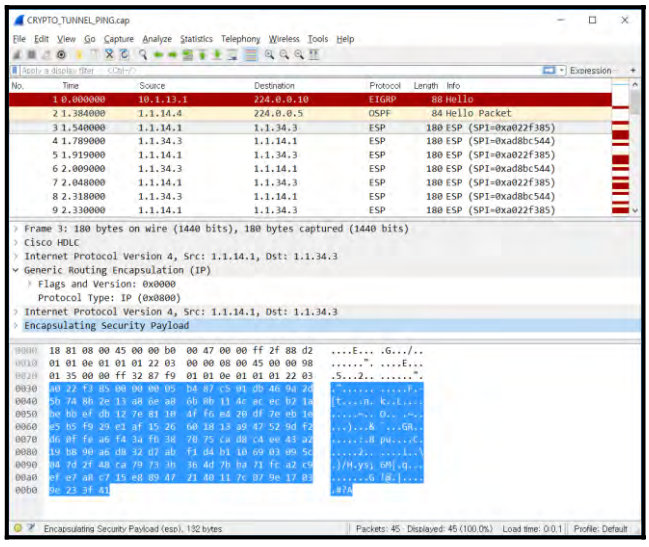
구분	기능	설명	현재진척도(%)
S/W	GNS-01-01	라우터 생성	100%
	GNS-01-02	방화벽 생성	100%
	GNS-02-01	장비들 간 연결	80%
	GNS-02-02	장비들 간 실행	80%
	GNS-03	콘솔(Console)기능	100%
H/W	Router-01	IP 주소 할당	100%
	Router-02	보안정책(ACL, Access Control List)설정	80%
	Router-03	최단 경로 탐색	100%
	Router-04	콘솔(Console) 기능	100%
	ASA-01-01	Inside(내부)영역 IP 주소 할당	100%
	ASA-01-02	Outside(외부)영역 IP 주소 할당	100%
	ASA-01-03	DMZ(중립)영역 IP 주소 할당	100%
	ASA-02	보안정책 설정	80%
	ASA-03	영역 간 특정 트래픽 차단 및 허용	100%
	ASA-04	콘솔 기능	100%

(3) 가상 VPN 환경 구축

가상 방화벽 장비 ASA 는 기본적으로 Inside, Outside, DMZ 영역으로 구분된다. Security-level 이 가장 높은 Inside 영역에서 DMZ, Outside 영역으로 접근이 가능하지만 Inside 영역으로 접근할 수 없다. 영역간의 프로토콜 종류별, 출발지 주소(Source Address) 혹은 목적지 주소(Destination Address)에 따라 데이터 패킷을 차단하거나 통과시켜주는 역할을 한다. 예외적으로 보안정책으로 인하여 Outside 영역에서 Inside 영역으로 접근이 가능하다. 본 논문에서는 (그림 6)에서 언급한 최종토폴로지의 일부분인 가상 라우터 두 개와 가상 방화벽 장비 ASA 간 ACL 정책을 통해 ICMP 프로토콜을 이용하여 허가된 영역에 Ping 을 이용한 통신이 가능하도록 설정하였다.

- ASA 장비 VPN 통신 확인

가상 방화벽 장비 ASA 를 통해 적용한 정책이 정상적으로 구현이 되는지 여부는 통신 패킷 미러링 툴인 Wireshark 를 통해 확인 할 수 있었다.



(그림 6) Wireshark 를 통한 VPN 통신 확인

(그림 6)상의 Payload 부분인 ESP 헤더 영역이 암호화되어 데이터가 알아볼 수 없는 상태임을 확인할 수 있다

3. 결론

시간이 지날수록 네트워크 기술은 진화를 거듭하고 있다. 이에 상응하여 해킹기법들이 나날이 새로워지고 지능화되고 있으며 그에 따른 보안 침해사고 역시 증가하고있는 추세이다. 그렇기 때문에 정보 보안의 중요성을 인지하고 그에 따른 보안 기술에 대한 연구가 활발하게 진행되고 있다.

본 논문에서는 인터넷과 같은 공중망에서 송수신되는 정보를 보호해주는 암호기술인 VPN 을 선정하였고 이에 대한 조사를 진행하였다. 이를 기반으로 가상솔루션인 GNS 를 이용하여 가상 네트워크 환경과 가상 VPN 을 구현하였다. 결과적으로 가상 장비들간에 Ping 을 보내는 테스트를 진행하였을 때 정보를 담은 패킷이 출발지에서부터 목적지까지 전달되는 과정에서 보안 정책에 따른 전달 여부를 확인할 수 있었다.

또한 VPN 방화벽 모델은 가상화 기반으로 구현을 하였기 때문에 기존의 방화벽과 차별성을 두어 공간적인 제약을 해소하며, 구축을 위한 소요시간이 줄어드는 장점이 있다. 중소기업에서는 방화벽을 구축하기 위해 많은 구축비용이 들게 되는데 VPN 방화벽을 이용하여 보다 저렴한 가격으로 보안 환경을 구축할 수 있다.

향후 연구에서는 네트워크 트래픽을 크게 설정한 Congestion 상태와 현재 성행하고 있는 실제 해킹기술 도입할 경우 등과 같이 다양한 환경에서 테스트를 진행하여 보안정책으로 적절한 VPN 모델역할을 하는지 검증해나갈 계획이다.

"본 논문은 2017 년 한이음 ICT 멘토링 프로젝트의 결과물 입니다."

참고문헌

[1] H. S. Yoon "Mobile VPN architecture for smart work environment"
[2] J. H. Yoon "IPSec VPNs vs. SSL VPNs"
[3] Merilyn Oliver "Virtualization and Cloud Computing"
[4] KISA, "암호 이용 안내서"
[5] Cisco Korea Blog, "빠르고 빠른 기가인터넷 세상"
[6] J. P. Jeong "Accelerated VPN Encryption using AES-NI"