L2TP tunneling 방법을 기반으로 한 가설 사설망의 보안 원격 접속 분석

Roja Kiran Basukala*· 최동유**· 한승조**

Analysis of Secure Remote Access to Virtual Private Home Network with L2TP Tunneling methods

Roja Kiran Basukala* · Dong-you Choi** · Seung-jo Han***

이 논문은 2007년도 조선대학교 학술연구비의 지원을 받아 연구되었음.

요 약

홈 네트워크는 전자적이고 전기적인 집의 여러 장치와 여러 이더넷과 같은 기술인 무선네트워크, 전화선 , 파워라인의통합인 인터넷과 연결된 게이트웨이와 통신을 한다. 이런 홈 네트워크는 인터넷에 기초를 두며 인터넷을 통해 모든 사람이 홈 네트워크에 접근을 할 수 있다. 홈 네트워크는 주거인이 편하고 안전한 삶을 위해 발전하며, 정보는 보안을 필요로 한다. 그러므로 홈 네트워크의 모든 리모트 접근은 믿을 수 있어야 한다. 이 논문은 홈 네트워크에 안전한 리모트 접근인 VPN에 기초를 둔 계획적이고 필수적인 두 가지 터널링 보안 방법인 L2TP을 분석 하였다.

ABSTRACT

Home network is the connection and communication of several electronic and electrical devices at home with the integration of several technologies like Ethernet, wireless, phone line and power-line at the residential gateway to the internet. This internet based home network can be accessed from any part of the world through any device by any person via internet. Since home network is developed for comfortable and safe life of home users, the information flow to/from home network needs to be private. Hence the remote access of the home network must be secured. This paper analyses two secure tunneling methods, voluntary and compulsory for L2TP(Layer Two Tunneling Protocol) based VPN (Virtual Private Network) for secure remote access of the home network.

키워드

Home Network, VPN, L2TP, Compulsory tunneling, Voluntary tunneling

* 조선대학교 정보통신공학과 석사과정
** 조선대학교 정보통신공학과 전임강사
*** 조선대학교 정보통신공학과 교수(교신저자)

접수일자 2008. 09. 29

Ⅰ. Introduction

Home network is inter-connection of several electrical and electronic home appliances for comfortable and daily life of home users. This is achieved by the integration of Ethernet, wireless, power line and phone line technologies at residential gateway at home. The residential gateway is connected to the outside world with the public internet in order to access internet from home and to access home network from outside. Since data flow in home network contain our daily life private information, the necessity of protecting incoming and outgoing traffic from the internet has greatly emerged. As the residential gateway separates the private home network from the public internet as shown in figure 1, securing incoming and outgoing traffic to the residential gateway should be secured.

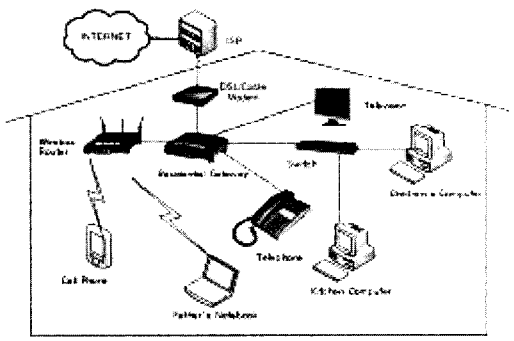

그림 1. 일반적인 홈 네트워크 구성
Fig. 1. General home network architecture

Remote access has become more popular since the increment of telecommutators and mobile users to access private networks. Similar concept can be utilized in home network [1]. VPNs allow home users working at office or on the road to remotely connect to home network services using the routing infrastructure provided by a public internet in a secure fashion. VPN is a point-to-point connection between the user's computer and a home network server. VPNs accomplish this by allowing the home user to tunnel through the Internet in a manner that provides the same security and features formerly available only in private home networks The nature of the intermediate inter-network is irrelevant to the home user because it appears as if the data is being sent over a dedicated private link to home network [2].

In this paper section 2 focuses VPN technology and compares several VPN protocols to be used in home network, L2TP tunneling protocol to be used in our home network is described in brief in section 3. Section 4 compares the tunneling modes of L2TP protocol. Then Section 5 describes the simulation analysis of compulsory and voluntary tunneling modes of L2TP based virtual private home network. Finally Section 6 mentions the conclusion of the analysis and the future works.

Ⅱ. Virtual Private Home Network

A VPN secures traffic over an insecure medium like internet by emulating a point-to-point private link over a shared or public network. Hence VPN can be used to provide remote access to home network resources over the public Internet, while maintaining privacy of information. This is done by encapsulating packets with a new header at the network layer to create tunnels (logical paths) and encrypting data for confidentiality. Using the connection to the local ISP, the VPN software creates a virtual private network between the remote user and the home network VPN server across the Internet [3]. Figure 2 shows a VPN used to connect a remote user to a home network.

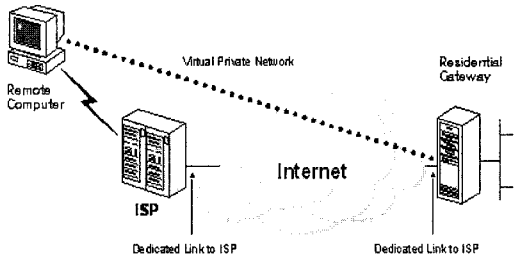

그림 2. 사설 홈 네트워크의 원격 접속을 위한 VPN을 사용하기
Fig. 2. Using a VPN to connect a remote client to a private home network

VPNs must be implemented using some form of tunneling mechanism. Tunneling is creating a transparent virtual network link between two network nodes that is unaffected by physical network links and devices. It provides routable transport for un-routable packets. Tunneling can be achieved by any of four primary tunneling protocols L2F, PPTP, L2TP and IPSec [4]. These protocols can be used as the key components used to construct our implementation of a virtual private Home network to provide home network security[3].

Layer two forwarding was designed for traffic tunneling from mobile users to their corporate server.

PPTP uses Point-to-Point Protocol (PPP) to provide remote access that can be tunneled through the Internet to a desired site. Tunneling allows senders to encapsulate their data in IP packets that hide the routing and switching infrastructure of the Internet from both senders and receivers to ensure data security against unwanted viewers, or hackers. As described in [2], PPTP uses a TCP connection for tunnel maintenance and generic routing encapsulation (GRE) encapsulated PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be compressed. But an overhead of 6 bytes of data compression takes place upon compression. However, PPTP can support only a single tunnel between end points. Another limitation is that PPTR requires IP internetwork for tunneling.

L2TP is a network protocol that encapsulates PPP frames to be sent over IP, X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) networks. L2TP was based on L2F protocol and PPTP. L2TP uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The payloads of encapsulated PPP frames can also be compressed with 4 bytes of overhead only. L2TP allows for the use of multiple tunnels between end points. L2TP provides for tunnel authentication, while PPTP does not.

IPSec uses data encryption standard (DES) and other algorithms for encrypting data, public-key cryptography to guarantee the identities of the two parties to avoid man-in-the-middle attack, and digital certificates for validating public keys. Both client and server negotiates the encryption technique and the key before data is transferred. The encrypted payload is then encapsulated again with a plain-text IP header and sent on the internetwork for delivery to the tunnel server. Upon receipt of this datagram, the tunnel server processes and discards the plain-text IP header, and then decrypts its contents to retrieve the original payload IP packet and routes to its destination.

The following table 1 compares three tunneling protocols in several features. Comparing the three tunneling protocols PPTP, L2TP and IPSec, it is found that L2TP consists of more features as L2TP is the combination of L2F and PPTP. So we propose to implement L2TP VPN tunneling in home network.

표 1. 터널링 프로토콜의 비교
Table 1. Comparisons of tunneling protocols

Comparisons	PPTP	L2TP	IPSec
Authentication Tunnels		√	√
Compression	√	√	√
Smart Cards	√	√	
Address Allocation	√	√	
Multiprotocol	√	√	
Encryption			√
Flow Control		√	
Requires Server	√	√	

Ⅲ. Layer 2 Tunneling Protocol

L2TP is a network protocol that encapsulates PPP frames to be sent over IP, X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) networks. L2TP was based on Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The payloads of encapsulated PPP frames can be encrypted and/or compressed. The L2TP packet format in IP networks is illustrated in figure 3.

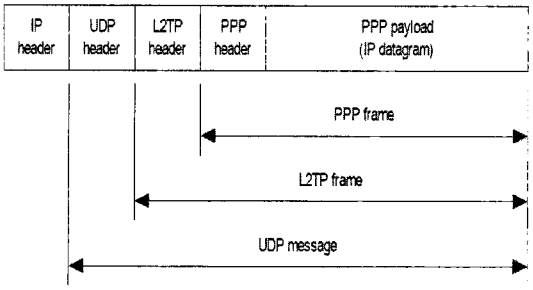

그림 3. L2TP 패킷 형식
Fig. 3. L2TP packet format

The L2TP access concentrator (LAC) and the L2TP network server (LNS) are two key components of L2TP and act as the L2TP tunnel endpoints. LAC tunnels the PPP connection across the Internet to the LNS. In our implementation we use enable L2TP network server service in the residential gateway. The Home Network may then perform services as if the user were connected to a network access server directly.

IV. Tunneling Modes

VPN tunnels can be either voluntary or compulsory. In voluntary tunneling, the user initiates the tunnel, typically by use of a tunneling client while in compulsory tunneling the tunnel is created without any action by the user who has no control over the tunnel [3]. The major pronounced differences between these to tunneling mechanisms are enlisted in the table 2.

From the above comparison it is found that voluntary tunneling can be used for home network for secure remote service. Also voluntary tunneling can benefit from reusing the existing authentication and address assignment mechanisms used by PPP without modification [3]. However voluntary tunneling requires VPN enabled software to initiate VPN tunnel.

표 2. 터널링 노드 비교
Table 2. Comparisons of tunneling nodes

Voluntary Tunneling	Compulsory Tunnel
Tunneling is initiated by end-user.	Tunneling is created by Network Access Server(NAS) or Router
Requires client software on remote device.	Requires support required on NAS or Router.
Works with any Network device.	Works with any client but NAS must support same tunneling method.
Tunneling transparent to leaf and intermediate devices.	Tunneling transparent to intermediate routers.
User must have tunneling client compatible with Server.	User traffic can travel only through the tunnel.
Simultaneous access to the internet and intranet is possible.	Internet access possible.
Tunneling overhead to the remote client and the private network.	Tunneling overhead to ISP only.

V. Simulation and Analysis

The simulation setup was performed for VPN tunneling using opnet version 10 [5] as shown in figure 4. Ethernet, wireless and wired connection was connected to the residential gateway for basic home network setup. The residential gateway is then connected with ADSL link(1.5Mbps downlink/ 384kbps uplink) provided by ISP. The real-time applications, video conferencing and VoIP were used in the home network devices and the remote VPN client. The residential gateway is considered as LNS for tunneling in our home network.

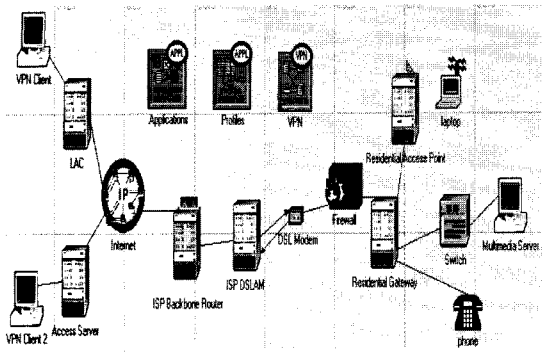

그림 4. 시뮬레이션 모델
Fig. 4. Simulation model

The two remote VPN clients try to connect to the home network from different places via LAC and the access server respectively. Assuming, the authentication is performed, two L2TP Tunnels are created from LAC and access server to the residential gateway. The simulation was performed in two scenarios named compulsory and voluntary. In compulsory tunneling, the VPN parameters were configured as shown in figure 5. For the next scenario, operation mode was modified to voluntary mode in both tunnels to observe the traffic in voluntary tunneling mode.

⊟ VPN Configuration	(...)
├ rows	2
⊟ row 0	
├ Tunnel Source Name	LAC
├ Tunnel Destination Name	Residential Gateway
⊞ Delay Information	(...)
├ Operation Mode	Compulsory
⊟ Remote Client List	(...)
├ rows	1
⊟ row 0	
└ Client Node Name	VPN Client
⊟ row 1	
├ Tunnel Source Name	Access Server
├ Tunnel Destination Name	Residential Gateway
⊞ Delay Information	None
├ Operation Mode	Compulsory
⊟ Remote Client List	(...)
├ rows	1
⊟ row 0	
└ Client Node Name	VPN Client 2

그림 5. VPN 터널링 파라미터
Fig. 5. Parameters for VPN tunneling

The voice, video and VPN tunnel traffic were observed to explore the better VPN tunneling method. From the simulation results shown in figures 6 and 7, it was found that voluntary tunneling performed better with higher voice and video traffic.

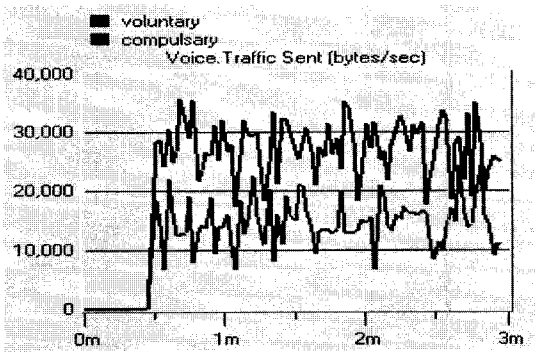

그림 6. 터널에서 음성 트래픽 전송
Fig. 6. Voice Traffic sent in the tunnel

The increase in tunnel traffic and information flow traffic is due to no load in ISP in VPN tunneling mode. With an L2TP compulsory tunnel, the remote client initiates a connection to its ISP. The ISP then establishes an L2TP connection between the remote VPN client and the home network. The ISP must support LT2P because it must control and monitor all the traffic flow from LAC to LNS. Thus there is an overhead to the ISP and hence less traffic flows as obtained in figure 6 and 7.

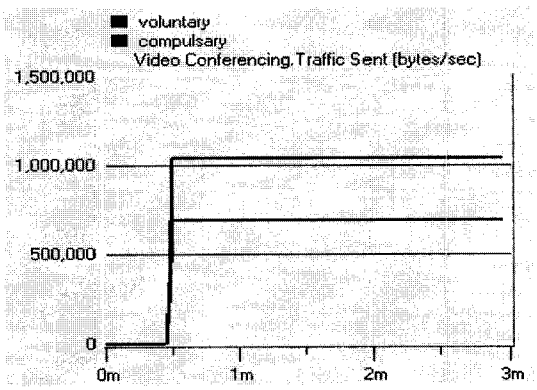

그림 7. 터널에서 영상 트래픽 전송
Fig. 7. Video traffic sent in the tunnel

However, with an L2TP voluntary tunnel, the connection is created by the remote VPN client. As a result, the remote client sends L2TP packets to its ISP which forwards them on to the home network. With a voluntary tunnel, the ISP does not need to support L2TP. Due to no overhead of tunneled traffic in ISP, more tunneled traffic flows through ISP as shown in figure 6 and 7.

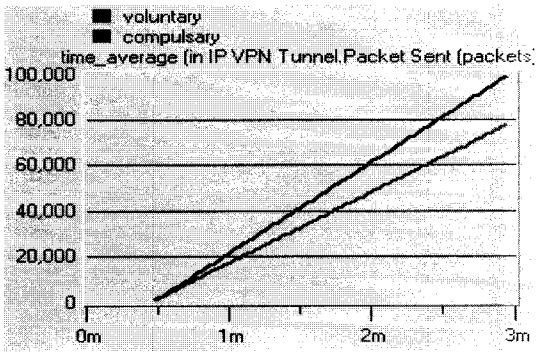

그림 8. VPN 터널 패킷 전송
Fig. 8. VPN tunnel packets sent

Also the VPN tunnel packets sent in voluntary tunneling was also increased by almost 20% compared to compulsory tunneling 'as shown in figure 8. With compulsary tunneling, same tunnel is shared by remote multiple clients whereas in separate tunnel exists for separate remote clients. So more traffic flows in voluntary tunneling via separate tunnels. The VPN client can hence securely connect to the home network anytime with voluntary tunneling method without giving any tunneling overhead to the ISP.

VI. Conclusion and Future Works

Hence in this paper we have discussed about importance of VPN in-home network for home network. Then a comparison between the VPN protocols was performed and L2TP was chosen to be used for virtual private home network. After that tunneling method to use in L2TP were compared to explore that voluntary tunneling is better than compulsory tunneling for home network. From the simulation analysis also it was found that voluntary tunneling performs better performance with high data traffic and VPN traffic. In future we would like to integrate IPSec with L2TP to provide more security to virtual private home network along with the remote wireless devices.

References

[1] Richard Shea, L2TP Implemenation and Operation, The Addision-Wesley Networking, Basic Series, 1999

[2] "Virtual Private Networking: An Overview" Microsoft Windows 2000 Server, Microsoft Corporation, 1999

[3] Lynne Genik, Matthew Kellett, Peter C. Mason,Mazda Salmanian and Vahid Aftahi, "Virtual Private Wireless Local Area Networking" Defence R&D Canada - Ottawa, Technical Memorandum, DRDC Ottawa TM 2006-124, July 2006

[4] Binod Vaidya, Jong Woo Kim, Jae-Young Pyun, Jong An Park, Seung Jo Han "Framework for Secure Audio Streaming to Wireless Access Network"

[5] OPNET Modeler Simulation Software, http://www.opnet.com

※ This study was supported by research funds from chosun university, 2007.

저자소개

Roja Kiran Basukala

2007년 Tribhuvan University, Institute of Engineering, Pulchowk Campus (학사)
2008년 조선대학교 정보통신학과 (석사 입학)

※관심분야 : home network, information security, WLAN

최동유 (Dong-you Choi)

1999년 2월 : 조선대학교 전자공학과 졸업 (공학사)
2001년 2월 : 조선대학교 대학원 전자공학과 졸업 (공학석사)
2004년 8월 : 조선대학교 대학원 전자공학과 졸업 (공학박사)
2004년 9월 ~ 2005년 6월 : 에너지 자원신기술연구소 전임연구원
2006년 3월 ~ 2007년 2월 : 청주대학교 이공대학 전자정보공학부 전임강사
2007년 3월 ~ 현재 : 조선대학교 전자정보공과대학 정보통신공학부 전임강사
※관심분야 : 전파전파, 이동통신, 통신 및 회로시스템

한승조 (Seung-jo Han)

1980년 조선대학교 전자공학과 (학사)
1982년 조선대학교 전자공학과 (공학석사)
1994년 충북대학교 전자계산학과(공학박사)
1986년 6월~1987년 3월 : 뉴올리언즈대학 객원교수
1995년 2월~1996년 1월 : 택사스대학 객원교수
2000년 12월~2002년 3월 : 버클리대학 객원교수
1998년 3월~현재 : 조선대학교 전자정보통신공학부 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제방지 시스템, ASIC 설계