초고속 IP 기반에서 GRE 터널링 기법을 이용한 접속 제어 연구

이재완* · 김형진** · 고남영*

A Study on Connection Control using GRE Tunneling Technique in High-speed IP Infrastructure

Jae-wan Lee* · Hyoung-jin Kim** · Nam-young Ko*

요 약

초고속 통신망에서 터널링 기법은 네트워크 인증 및 데이터의 보안 지원에 있다. 이를 위해 IPSec, SOCKS V5 및 GRE 터널링 프로토콜 등을 사용하고 있다. 본 논문은 초고속 통신망에서 특정 IP 대역에 대하여 라우팅 루트를 변경 시켜 유해 서비스 접속 차단 및 이용자 Needs에 따라 특정 서비스에 대한 라우팅 루트를 변경시켜 이용자가 원하는 선택적인 서비스 제공 기반을 구현하고자 하였다. 따라서 GRE 프로토콜을 이용하여 GRE의 동작 원리를 측정 · 분석하고, 그 결과를 접속 제어 및 인증 기반 서비스에 적용하고자 한다.

ABSTRACT

Tunneling technique does a role to network authentication or the preservation support of date at high-speed network. In order to this, IPSec, SOCKS V5 or GRE tunneling protocol have been using.

This paper embodies the offer base of communication service by changing routing route to special IP band for connection interception of harmful service and according to user's needs, by changing routing route to special service at high-speed network. So we measure and analysis action · principle of GRE with GRE protocol, the result apply to a service of connection control and authentication base.

키워드

초고속 통신망, Tunneling, GRE

Ⅰ. 서 론

최근 시스템 침해 사고가 급속히 증가함에 따라 다양한 인증 시스템이 도입 되고 있는 실정이지만, 실제로 인터넷 시스템에서 사용자 인증 자체가 취약성을 보이고 있다. 따라서 기존 초고속 인터넷 이용자의 다양한 욕구를 충족하고 네트워크의 신뢰성과 생존성을 위한 새로운 대안의 접속 제어 시스템의 중요성이 대두되고 있다.

따라서 본 논문에서는 유해 사이트 차단 및 사용자가 원하는 특정 서비스에 대한 접속 제어 기반의 서비스를 할 수 있는 터널링 기법을 활용하여 GRE의 동작 원리를 시험 · 분석 하고자 한다.

본 논문은 다음과 같이 구성된다. 2장에서는 터널링 (Tunneling) 및 GRE(Generic Routing Encapsulation) 프로

* 군산대학교 전자정보공학부
** 익산대학 정보통신과

접수일자 : 2006. 5. 26

토콜에 대해 기술하고, 3장에서는 시뮬레이션 환경을 설정·측정하고 그 결과를 분석한다. 4장에서 결론을 맺는다.

Ⅱ. 본 론

최근 초고속인터넷 환경에서 터널링 프로토콜을 사용해서 X.25, Frame Relay 및 PBX(Private Branch Exchange) 등 여러 가지 망을 통합할 수 있고 보안을 유지하며 네트워크 설치와 관리비용을 줄일 수 있는 망으로 정의되고 있다.

이를 구현하기 위한 기반 기술로는 크게 터널링 기술, 키관리 기술, VPN 관리 기술 등 3대 기술 요소가 있으며, 기반 기술 외에 VPN을 구현하기 위해서는 인증 및 암호화 기술이 필요하고, 부가적으로 라우터나 방화벽에서 제공하는 일부 보안기술도 병행하여 VPN을 구성할 수 있다.

현재 초고속 인터넷에서 제공하고 있는 부가서비스는 Clean-i, Timecodi 등 인증 기반의 유해차단 서비스 등이 있고, 이를 위해 L2TP 및 GRE 터널링 프로토콜을 사용하고 있다.

본 연구에서는 이에 Small 시험 망을 구성하여 GRE 터널링 프로토콜의 동작 원리 및 필요 Configuration을 측정·분석하고, 이를 토대로 초고속인터넷 환경에 적합한 부가서비스 제공 기반을 구현하고자한다.

2.1 터널링

터널링은 마치 송신자와 수신자 이외에는 누구도 사용할 수 없는 터널을 생성하는 것처럼 송신자가 보내는 데이터를 캡슐화 하여 수신자 이외에는 알 수 없도록 데이터를 전송하는데 사용된다.

터널링 기술의 가장 보편적인 형태는 네트워크 프로토콜(IP, IPX)을 PPP에 캡슐화한 다음 그 패킷을 다시 터널링 프로토콜에 캡슐화 한다. 이 접근 방법은 터널링 프로토콜이 계층 2 프로토콜을 전송하므로 계층 2 터널링(L2T:Layer 2 Tunneling)이라고 한다.

또 다른 방법은 네트워크 프로토콜로서 직접 터널링 프로토콜로 캡슐화 하는 방법으로서, 이 방법은 계층 3 터널링(L3T:Layer 3 Tunneling)이라고 한다.

이러한 터널링 프로토콜의 계층 2에서는 MAC Layer에서 Tunnel을 형성하여 패킷 데이터를 전달하는 PPTP (Point-to-Point Protocol), L2P(Layer 2 Forwarding Protocol), L2TP(Layer 2 Tunneling Protocol) 등이 있고, 계층 3에서는 IP Layer에서 tunnel을 형성하여 데이터를 전달하는 프로토콜로 IPSec, SOCKS V5 및 GRE 등이 있다[1,2,3,8].

GRE 터널링 기법은 하나의 프로토콜 기반에서 다른 프로토콜로 Encapsulation하는 많은 방법들(RFC 1234, RFC 1226)이 제안되었다[3-6]. GRE는 이런 다른 프로토콜과 비슷하지만 위의 제안들보다 좀 더 일반적인 프로토콜이다.

그 결과 특정한 프로토콜 상에서의 정확한 동작에는 효과적이지 못했다. 위의 문제점들을 보안하고 좀 더 단순하고 일반적인 메커니즘의 Encapsulation방법이 GRE이다. 이것은 Encapsulation을 위한 간단하면서도 일반적인 메커니즘을 제공한다.

2.2 Encapsulation의 종류

터널링 기술에 쓰이는 Encapsulation의 종류는 다음과 같다.

① IP in IP encapsulation

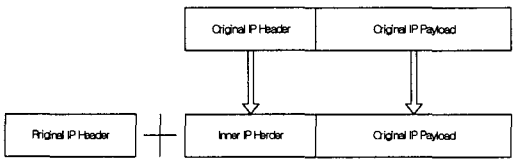


그림 1. IP in IP encapsulation 구성도
Fig.1 IP in IP encapsulation construction

그림 1은 IP in IP encapsulation 기술로 가장 단순한 형태의 IP Encapsulation 방법이다. 따라서 단순히 내부헤더 바로위에 IP 표준 외부헤더를 덧붙이는 기법이다.

② Minimal Encapsulation

IP in IP Encapsulation은 내부 헤더의 여러 가지 정보를 단지 복사만 하는 부분이 많기 때문에 그런 리던던시를 줄이기 위해 내부 헤더와 외부헤더가 중복되는 부분은 외부 헤더로 다 옮기고 최소한의 정보만으로 내부헤더를 구성한다. 그리고 터널의 End point에서 다시 Decapsulation 될 때 내부헤더를 복구한다.

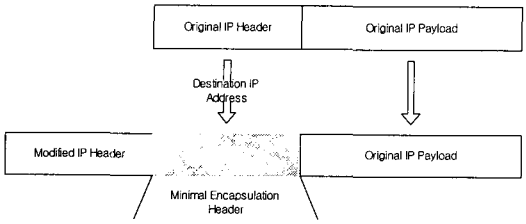


그림 2. Minimal Encapsulation 구성도
Fig. 2 The Construction of Minimal Encapsulation

③ GRE(Generic Routing Encapsulation)

위 두 가지 Encapsulation은 단지 IP Protocol에서만 사용이 가능하지만 GRE는 다른 네트워크 레이어의 Protocol에서도 자유롭게 사용이 가능하다. 다음 그림 3에서와 같이 Original Packet 전체를 Payload로 보고 따로 GRE 헤더와 지금 사용할 Protocol의 헤더를 붙인다.

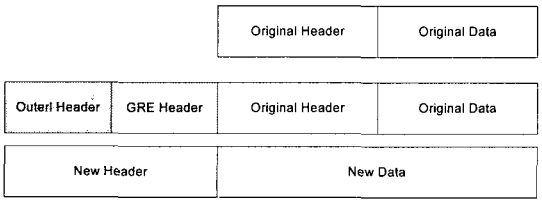


그림 3. GRE 기술 구성도
Fig. 3 The Construction of GRE Technique

2.3 GRE 동작원리

그림 4에서 GRE의 동작원리는 일반적인 메커니즘을 그대로 사용하여 관련된 Flag를 검사하고, 정당한 정보를 가지고 있는지 조사한다. 그리고 Routing Present Bit이 Setting되어 있으면 SRE(Source Route Entry)정보를 검사하여 Semantic 적합성을 검사하고, SRE과정이 완료되면 GRE Header를 없애고 Payload Packet만 남긴다.

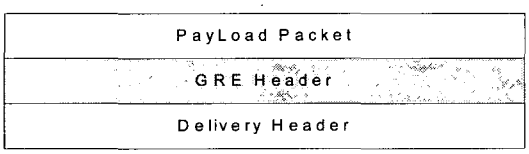


그림 4. GRE 패킷 포맷
Fig. 4 GRE Packet Format

다음 그림 5에서는 GRE 터널링을 이용한 특정 유해사이트차단 흐름도이다.

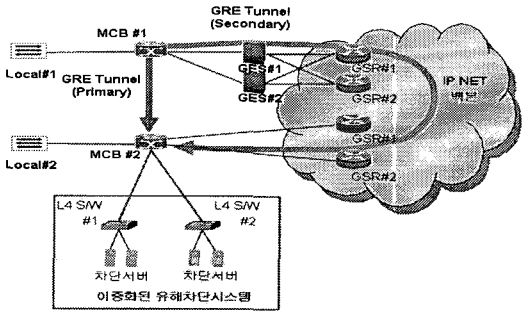


그림 5. GRE 터널링 구성도
Fig. 5 The Construction of GRE Tunneling

이는 GRE 터널을 이용하여 사용자가 할당 받은 특정 IP 대역에 대하여 라우팅 루트를 변경시켜 유해사이트의 접속을 차단하는 접속 제어(인증) 기반 서비스이다. 또 SER (Service Edge Router)에서 사용자의 환경에 따라 특정 서비스에 대한 라우팅 루트를 변경시켜 사용자가 원하는 선택적인 서비스를 제공한다.

Ⅲ. 실험 및 결과

3.1 GRE 시뮬레이션 환경

GRE 터널링 프로토콜을 Small 시험 망에 적용·구현하고, 구현된 시험 망에서 트래픽을 발생하여 Routing 경로를 측정·분석한다.

사용된 장비는 Cisco 2500(2대), Cisco 2600(2대), Cisco 3600(1대), S/W 등 이다.

3.2 실험 및 결과

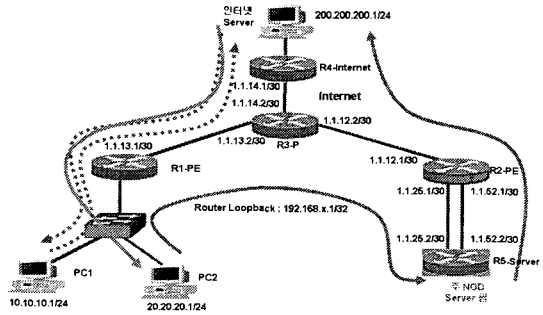


그림 6. GRE 패킷 흐름도
Fig. 6 The Flow of GRE Packet

① 그림 6과 같이 Router별 Interface Configuration 작업을 한다.
② Routing Protocol(ISIS,BGP,Static)을 적용 한다.
③ 구성 완료 후 패킷 라우팅을 측정한다.
④ GRE Tunnel 생성작업(Router R1, R2)을 한다.
⑤ Tunneling을 이용한 트래픽 흐름을 측정 한다.
⑥ 시뮬레이션 작업 후 결과를 확인 · 분석한다.

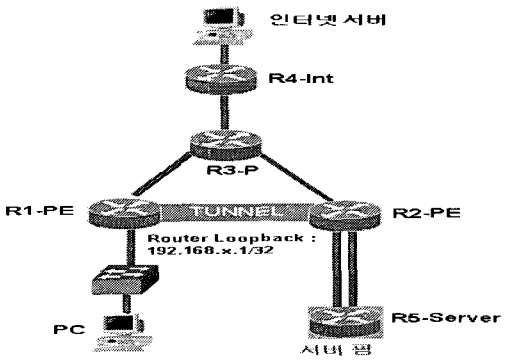


그림 7. GRE 시스템 구성도
Fig. 7 GRE System Construction

그림 6의 GRE 패킷 흐름 메커니즘을 이용하여 그림 7에서와 같이 5 가지로 나누어 라우팅 루틴을 설정하였다. 각 루틴에서 Interface별 IP을 등록하고, 라우팅 경로에 따라 ISIS 및 BGP Routing Protocol을 적용하였다. 또 Tunneling Interface, ACL 및 PBR을 생성하고, 라우팅 측정 결과는 다음과 같다.

① R1-PE 라우팅 측정 결과

• Interface별 IP 등록 및 확인

```
R1-PE(config)# int e0/0
R1-PE(config-if)# ip address 10.10.10.2
        255.255.255.0
R1-PE(config-if)# ip address 20.20.20.2
        255.255.255.0 sec
R1-PE(config)# int s1/1
R1-PE(config-if)# ip address 1.1.13.1
        255.255.255.252
R1-PE(config)# int loopback 0
R1-PE(config-if)# ip address 192.168.1.1
        255.255.255.255
```

• Routing Protocol 적용 (ISIS, BGP)

* isis 는 R3와 동일, s1/1 ip router isis 등록 *

```
R3-P(config)# router isis
R3-P(config-router)#net 49.0001.0000.0000.0003.00
R3-P(config-router)# passive-interface Loopback0
R3-P(config-router)# is-type level-2-only
R1-PE(config)# router bgp 4766
R1-PE(config-router)# no synchronization
R1-PE(config-router)# neighbor 192.168.3.1
        remote-as 4766
R1-PE(config-router)# neighbor 192.168.3.1
        update-source Loopback0
R1-PE(config-router)# network 10.10.10.0 mask
        255.255.255.0
R1-PE(config-router)# network 20.20.20.0 mask
        255.255.255.0
R1-PE(config-router)# no auto-summary
```

• Tunneling Interface 생성

```
R1-PE(config-if)# int tunnel 0
R1-PE(config-if)# ip address 192.168.11.1
        255.255.255.0
R1-PE(config-if)# tunnel sourec loopback 0
R1-PE(config-if)# tunnel destination 192.168.2.1
```

• ACL, PBR 생성 및 적용

```
R1-PE(config)# access-list 101 permit ip 20.20.20.0
        0.0.0.255 any
R1-PE(config)# route-map SERVER
R1-PE(config-route-map)# match ip address 101
R1-PE(config-route-map)# set interface Tunnel0
R1-PE(config)# int e0/0
R1-PE(config-if# ip policy route-map SERVER
```

② R2-PE 라우팅 측정 결과

• Interface별 IP 등록 및 확인

```
R2-PE(config)# int s1/0
R2-PE(config-if)# ip address 1.1.25.1
        255.255.255.252
R2-PE(config)# int s1/1
R2-PE(config-if)# ip address 1.1.52.1
        255.255.255.252
R2-PE(config)# int s1/2
R2-PE(config-if)# ip address 1.1.23.1
        255.255.255.252
R2-PE(config)# int loopback 0
R2-PE(config-if)# ip address 192.168.2.1
        255.255.255.255
```

• Routing Protocol 적용 (ISIS, BGP)

```
R2-PE(config)# router isis
R2-PE(config-router)#net 49.0001.0000.0000.0002.00
```

R2-PE(config-router)# passive-interface Loopback0
R2-PE(config-router)# is-type level-2-only
* s1/2 ip router isis 등록 *
• **Tunneling Interface 생성**
R2-PE(config-if)# **int tunnel 0**
R2-PE(config-if)# ip address 192.168.11.2
255.255.255.0
R2-PE(config-if)# tunnel sourec loopback 0
R2-PE(config-if)# tunnel destination 192.168.1.1
• **ACL, PBR 생성 및 적용**
R2-PE(config)# access-list 101 permit ip any any
R2-PE(config)# **route-map Tunnel**
R2-PE(config-route-map)# match ip address 101
R2-PE(config-route-map)# set interface serial1/2
R2-PE(config)# int s1/1
R2-PE(config-if# **ip policy route-map Tunnel**

③ R3-P 라우팅 측정 결과

• Interface별 IP 등록 및 확인
R3-P(config)# int s1/1
R3-P(config-if)# ip address 1.1.13.2 255.255.255.252
R3-P(config)# int s1/2
R3-P(config-if)# ip address 1.1.23.2 255.255.255.252
R3-P(config)# int s1/3
R3-P(config-if)# ip address 1.1.34.2 255.255.255.252
R3-P(config)# int loopback 0
R3-P(config-if)# ip address 192.168.3.1
255.255.255.255
• **Routing Protocol 적용 (ISIS, BGP)**
R3-P(config)# **router isis**
R3-P(config-router)#net 49.0001.0000.0000.0003.00
R3-P(config-router)# passive-interface Loopback0
R3-P(config-router)# is-type level-2-only
R3-P(config)# **router bgp 4766**
R3-P(config-router)# no synchronization
R3-P(config-router)# neighbor 192.168.1.1
remote-as 4766
R3-P(config-router)# neighbor 192.168.1.1
update-source Loopback0
R3-P(config-router)# neighbor 192.168.1.1
route-reflector-client
R3-P(config-router)# neighbor 192.168.4.1
remote-as 4766
R3-P(config-router)# neighbor 192.168.4.1
update-source Loopback0
R3-P(config-router)# neighbor 192.168.4.1
route-reflector-client
R3-P(config-router)# no auto-summary
* s1/1, s1/2, s1/3 ip router isis 등록 *
• **Routing table 생성 확인**
R3-P#sh ip ro

④ R4-Int 라우팅 측정 결과

• **Interface별 IP 등록 및 확인**
R4-int(config)# **int s0**
R4-int(config-if)# ip address 1.1.34.1
255.255.255.252
R4-int(config)# int e0
R4-int(config-if)# ip address 200.200.200.2
255.255.255.0
R4-int(config)# int loopback 0
R4-int(config-if)# ip address 192.168.4.1
255.255.255.255
• **Routing Protocol 적용 (ISIS, BGP)**
R4-int(config)# **router bgp 4766**
R4-int(config-router)# no synchronization
R4-int(config-router)# neighbor 192.168.3.1
remote-as 4766
R4-int(config-router)# neighbor 192.168.3.1
update-source Loopback0
R4-int(config-router)# network 200.200.200.0 mask
255.255.255.0
R4-int(config-router)# no auto-summary
* isis 는 R3와 동일, s1/1 ip router isis 등록 *

⑤ R5-Server 라우팅 측정 결과

• **Interface별 IP 등록 및 확인**
R5-Server(config)# int s0
R5-Server(config-if)# ip address 1.1.25.2
255.255.255.252
R5-Server(config)# int s1
R5-Server(config-if)# ip address 1.1.52.2
255.255.255.252
R5-Server(config)# int loopback 0
R5-Server(config-if)# ip address 192.168.5.1
255.255.255.255
• **Routing Protocol 적용 (static)**
R2-PE(config)# ip route 0.0.0.0 0.0.0.0 serial 1

다음은 PC1, PC2에서 실제 트래픽을 발생시켜 패킷 흐름을 측정하고 경로를 분석하였다.

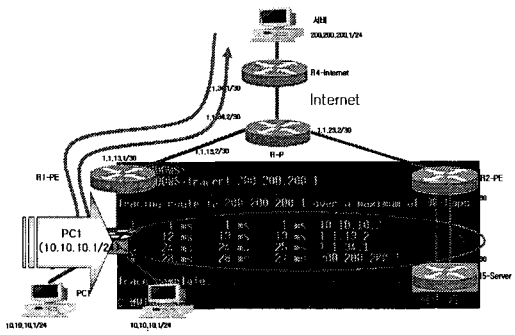


그림 8. PC1 패킷 흐름 결과
Fig. 8 The Packet Flow Result in PC1

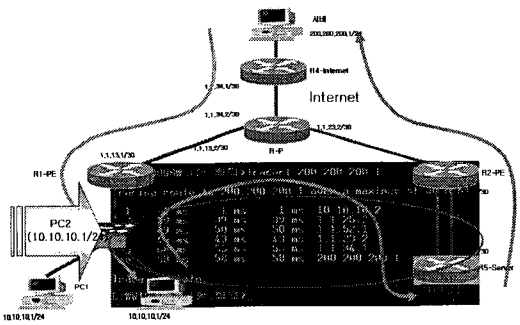


그림 9. PC2 패킷 흐름 결과
Fig. 9 The Packet Flow Result in PC2

그림 8과 그림 9에서 PC1, PC2의 패킷 흐름은 양호한 것으로 나타났다. 따라서 Small 시험 망에서 측정한 라우팅 변경 및 루틴별 패킷 흐름에서 패킷 손실이 없는 것으로 나타나, GRE를 활용한 최적의 서비스 제공 기반을 구현할 수 있음을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 초고속 통신망에서 인터넷 부가서비스 제공 기반을 구현하기 위해서 GRE 터널링 기법을 이용한 접속 제어 방안을 모색했다.

시뮬레이션을 위해 Small 시험 망을 구성, 패킷 흐름을 측정·분석하였으며, 그 결과는 다음과 같다.

첫째, 특정 IP 대역의 라우팅 루트를 변경 시켜 유해 서비스 접속 차단 등 접근 제어 기반을 구축했다.

둘째, 이용자 Needs에 따라 특정 서비스에 대한 라우팅 루트를 변경시켜 이용자가 원하는 서비스 제공 기반을 구축했다.

셋째, 접근 제어 및 서비스 제공 기반에서 PC1, PC2의 패킷 흐름은 양호 한 것으로 나타났다.

따라서 초고속 IP 환경에서 GRE 터널링 프로토콜을 이용한 접근 제어 기반의 선택적 서비스 제공이 용이함을 알 수 있다.

향후 Source IP 기반의 VRF Selection 기능을 이용한 인터넷 부가서비스의 제공 기반을 모색한다.

참고문헌

[1] Hamzeh K., et al, "Point-to-Point Tunneling Protocol," draft-ietf-pppext-12tp-16.txt,Apr. 1999.

[2] Townsley, W., et al, "Layer Two Tunneling Protocol," draft-ietf-pppext-l2tp-16.txt,Jun. 1999.

[3] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," RFC 1825, Jul. 1998.

[4] B. Gleeson, et al, "A framework for IP based Virtual Private Network," RFC2764, Feb. 2000.

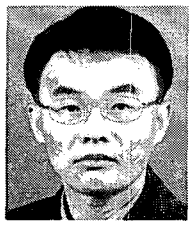
[5] C. Perkins, D. Johnson, "Route Optimization in Mobile IP," Internet Draft, draft-ietf-mobileip-optim-09.txt, Feb. 2000.

[6] P. Calhoun외, "Diameter Base Protocol", RFC3588, September 2003.

[7] Perkins, C., Editor, "IP Mobility Support", RFC 2002, October 1996.

[8] W. Townsley외, "Layer Two Tunneling Protocol L2TP", RFC2661, August 1999.

저자소개



이 재 완(Jae-wan Lee)

1989년 전북대학교 공학사
1996년 군산대학교 공학석사
2004년 군산대학교 공학박사

※ 관심분야:초고속인터넷 응용, 유 · 무선 네트워크, 북한통신

김 형 진(Hyoung-Jin Kim)

1997년 호원대학교 이학사
1999년 군산대학교 공학석사
2004년 군산대학교 공학박사
2004. 9~2005 군산대학교 전자정보공학부 계약교수
2005. 4~현재 익산대학 정보통신과 전임강사

※ 관심분야 : 멀티미디어 DBMS, 멀티미디어 시스템, 유 · 무선 네트워크.

고 남 영(Nam-young Ko)

1973년 광운대학교 공학사
1980년 건국대학교 공학석사
1995년 국민대학교 통신행정학박사
1996년 Pacific Western Univ. - Com_ (Ph. D Com_)
1992년 7월~현재:군산대학교 전자정보공학부 교수

※ 관심분야:유 · 무선통신, 통신정책, 북한통신.