

NGN 에서 세션기반 이동성 관리를 갖는 Mobile VPN

김양중^{1*}, 장철운^{**}, 정일영^{*}

* **한국의국어대학교 정보통신공학과

e-mail : {zeroplus, jcw21, iychong}@hufs.ac.kr

Mobile VPN Services with Session based Mobility Management in NGN

Yang-Jung Kim*, Chul-Woon Jang**, Il-Young Chong*

* **Dept. of Information and Communications, HanKuk University of Foreign Studies

요 약

Mobile VPN 은 ISP 또는 사업망으로 원격 작업자가 매체 독립적인 연결성을 제공하는 기술로써, 추가적인 장비 구입 비용 및 유지 비용을 줄 일 수 있는 효과적인 방안이다. NGN 에서 세션 기반의 이동성 관리를 할 수 있는 Mobile VPN 서비스를 위한 몇 가지 필요 요소 및 기술 방안을 제시함으로써 앞으로 차세대 인터넷에서의 향상된 VPN 서비스를 위한 효과적인 대응방안이 될 것이다.

1. 서론

Mobile VPN 은 원격 작업자가 매체 독립적으로 ISP 또는 사업망으로 접속하게 하는 기술을 말하며 추가적인 하부구조를 위한 비용을 줄일 수 있는 효과적인 방안으로 대두되고 있는 서비스다. NGN 에서 세션 기반의 이동성 관리를 통한 Mobile VPN 서비스를 위한 방안을 알아보고 구체적인 서비스 Call Flow 를 통하여 가능한 기술과 요구 사항을 살펴볼 것이다. 이를 위해서는 IMS 의 HSS 에 VPN 정보를 위한 요소가 필요하게 되며 NGN 에서 VPN Party 를 관리하기 위해를 위한 보다 효율적인 방안으로 볼 수 있다.

2. Mobile VPN 서비스

Mobile IP 기술은 망에서 이동성에 관계없이 고정 IP 주소를 할당하는 기술을 말한다. 모바일 네트워크가 점점 발달되고 사용되는 빈도가 많아지면서 바로 VPN 이란 서비스를 제외하고 생각할 수 없게 되었다. VPN 은 ISP 의 서비스 또는 모바일 작업자가 자신의

회사망의 자원을 이용하는데 추가적인 장비 및 기술 비용을 줄이는데 효과적인 기술이다. Mobile VPN 은 보안된 인증과 무선망 환경에서 네트워크를 위한 시스템을 위한 데이터 서비스를 제공한다.

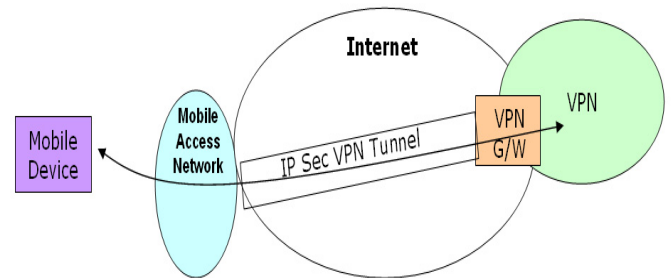


그림 1. Mobile VPN 서비스

¹ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성. 지원사업의 연구결과로 수행되었음

2.1 Mobile VPN Gateway 기능

Mobile VPN 서비스를 위해서 VPN gateway 는 터널링, 인증, 접속 제어, 보안, 라우팅과 다양한 정책결정 그리고 강력한 메커니즘을 제공한다. 세션 기반의 MVPN 서비스를 제공하기 위해서 MVPN gateway 에 추가적인 기능이 필요하며 요구되는 사항은 다음과 같다.

- Routing and Forwarding
- Buffer management
- Packet Scheduling, Marking and Metering
- Accounting and Performance Monitoring
- Lawful intercepting
- Various data mobility schemes
- Other typical wireless data networking functionalities

Mobile VPN gateway 의 주요 임무는 VPN client 와 사설망의 목적지사이의 이용자 데이터의 보안 전송과 안정성을 부여하는 것이다. 추가적으로 다른 네트워크 기술들과 VPN 형태들을 지원할 수 있을 정도로 다양한 기능이 구현되어야 한다.

3. 세션기반의 NGN 에서 Mobile VPN 서비스 구조

IMS 는 3GPP 에서 제안된 IP 기반의 멀티미디어 서비스를 제공하기 위한 표준이다. HSS(Home Subscriber Server)는 회선 교환망과 패킷 교환망의 가입자 정보를 유지하는 중요한 Entity 가 된다. HSS 는 HLR (Home Location Register)와 AuC (Authentication Center)를 포함하고 있으며 AuC 는 가입자의 인증키를 보관하고 보안된 데이터를 생성하게 한다. IMS 를 이용함으로써 IPsec 을 이용한 유선망의 VPN 에서 보다 안정된 인증 및 보안을 지원하고 가입자의 목적지까지 라우팅함에 있어서 필요한 대역폭과 코덱정보를 지원함으로써 세션기반의 Mobile VPN 서비스를 제공하는 중요한 메커니즘이 될 것이다.

따라서 세션 기반의 Mobile VPN 서비스 구조를 위해서 기존의 HSS 에 추가적인 기능이 있어야 한다. 추가적인 기능은 다음과 같다.

- VPN 서비스 등록 처리
- 가입자의 VPN ID, Session ID 관리
- 가입자의 다중 세션 관리
- 추가기능을 가진 Mobile VPN gateway 와 가입자 Profile 의 동기화 유지

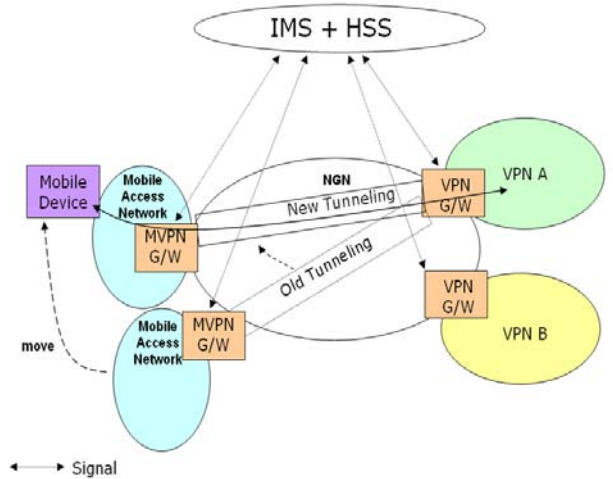


그림 2. 세션기반 Mobile VPN 에서 서비스 구조

세션기반의 Mobile VPN 서비스 구조는 그림 2 에서와 같은 형태가 된다. VPN 가입자가 VPN 서비스를 이용하기 위해서는 먼저 Mobile VPN gateway 를 통한 등록절차가 있어야 한다. Gateway 는 다시 이 등록정보를 HSS 로 등록하여 실제적인 VPN 정보를 조회하고 아울러 가입자가 이용할 서비스에 따른 대역폭 및 기타 필요한 사항에 대한 협의가 이뤄지도록 한다. HSS 는 VPN 가입자의 정보 즉, VPN ID, Session ID 등의 정보를 유지해야만 한다. 이것은 IMS 를 이용한 세션기반의 Mobile VPN 서비스를 위해서 필수사항이 된다. 해당 가입자에 대한 정보를 가지지 않는 HSS 의 경우 포워딩을 통해 정보를 가지는 HSS 로 보내 등록정보를 확인하는 과정을 진행하게 된다. 이 메커니즘은 VPN endpoint 를 찾는 과정에서 보다 안정적인 인증과 보안데이터를 무결성 전송을 지원하게 될 것이며 VPN party 로 참가 또는 탈퇴를 빈번히 반복하는 서비스에 대해 부하를 줄일 수 있는 효과적인 방안이라 볼 수 있다.

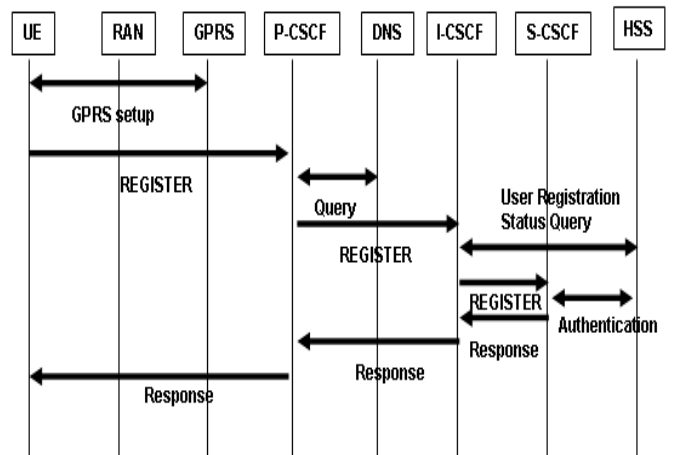


그림 3. Call flow of 3GPP IMS registering procedures without Mobile VPN gateway

Mobile VPN Gateway 가 없는 상황에서 3GPP IMS 등록 절차는 그림 3 과 같으면 메시지 흐름은 다음과 같다.

- 1. User Terminal connects with UMTS network.
- 2. Information data forwards to P-CSCF to register HSS.
- 3. P-CSCF query DNS server to lookup HSS.
- 4. Information data forwards I-CSCF to inform the subscriber profiles.
- 5. I-CSCF notifies the information of subscriber registration, authentication and user profiles, and get the S-CSCF address.
- 6. I-CSCF registers to S-CSCF using the obtained address.
- 7. S-CSCF query the subscriber to HSS for authentication.
- 8. S-CSCF sends response message to I-CSCF.
- 9. P-CSCF sends response message to UE.

Mobile VPN 에서 Gateway 의 역할은 위에서 언급한 것과 같이 터널링, 인증, 접속 제어, 무결성과 기밀성의 유지 및 관리가 된다. 세션 기반의 VPN Gateway 는 이것외에도 몇 가지 추가기능을 요구하며 요구되어지는 기능은 다음과 같다.

- Authenticated Endpoint Identifier from HSS
- Session Identification Management
- Bandwidth allocating and retrieving of authenticated sessions
- Table creation and management for VPN subscriber.
- Other typical wireless data networking functionalities.

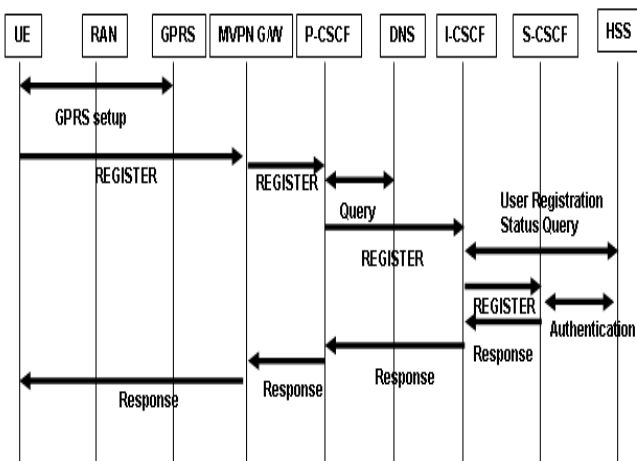


그림 4. 세션기반의 Mobile VPN Gateway 에서 Call Flow

그림 4 는 세션 기반의 Mobile VPN gateway 에서의 Call Flow 를 나타낸 그림으로써 Mobile VPN gateway 는 UMTS/GPRS 의 무선망에서 받아진 가입자 서비스 정보를 받아서 처리하는 Proxy 기능을 한다. 이는 여러 형태의 VPN 종류와 망특성에 따른 혼재한 트래픽을

다루는데 탄력적인 장비가 된다. 그림에 따른 메시지 플로의 상세한 절차는 다음과 같다.

- 1. User Terminal connects with UMTS network.
- 2. User Terminal registers to Mobile VPN gateway
- 3. Information data forwards to P-CSCF to register HSS.
- 4. Information data forwards I-CSCF to inform the subscriber profiles.
- 5. I-CSCF notifies the information of subscriber registration, authentication and user profiles, and get the S-CSCF address.
- 6. I-CSCF acknowledges subscriber registration and authentication, VPN ID, subscriber's profile to HSS .
- 7. I-CSCF registers to S-CSCF using the obtained address.
- 8. S-CSCF query the subscriber to HSS for authentication.
- 9. S-CSCF sends response message to I-CSCF.
- 10. P-CSCF sends response message to UE.
- 11. P-CSCF sends response message to Mobile VPN Gateway.
- 12. Mobile VPN Gateway sends response message to UE.

Mobile VPN gateway 가 없는 등록절차와 비슷하지만 게이트웨이 장비가 있음으로써 HSS 의 VPN 가입자 정보를 확인하는 Proxy 역할을 한다. 서로 다른 이기종망간의 Traffic 을 수렴하고 아울러 VPN 형태에 따른 다양성을 지닌 서비스에 따라 수용성을 높이기 위한 차원이다.

사용자 단말 장비는 GPRS/UMTS 망에 접속하고 사용자는 Mobile VPN Gateway 에 VPN 서비스 이용에 대한 등록절차를 따르게 된다. 이 사용자 등록 정보는 HSS 에 조회하기 위해서 P-CSCF 에 질의하게 되고 가입자 정보는 I-CSCF 에 전달되어 사용가능한 HSS 를 찾게 된다. 만일 이때 VPN 서비스에 대한 가입자 정보와 일치하지 않을 경우, 가능한 HSS 를 찾게 된다. 서비스 가능한 S-CSCF 를 질의받고 해당 HSS 에 VPN 서비스에 대한 가입자 인증절차를 거치고 다음으로 응답메세지를 등록했던 Entity 로 전달하면서 세션을 성립하는 것이 VPN gateway 를 이용하여 IMS 가입자 인증기반의 Mobile VPN 서비스의 간단한 메시지 흐름도가 된다.

4. Mobile VPN 을 위한 이동성 관리 프로토콜

VPN 을 적용하기 위한 기본 프로토콜로써는 IPsec, L2TP, MPLS 기반이 될 수 있으며 Mobile VPN 에서 고려하고자 하는 이동성 관리 프로토콜로써 Mobile IP 기반과 SIP 기반의 이동성 관리를 생각해 볼 수 있다.

먼저 Mobile IP 기반의 Mobile VPN 모델은 그림 5 에서 살펴 볼 수 있다.

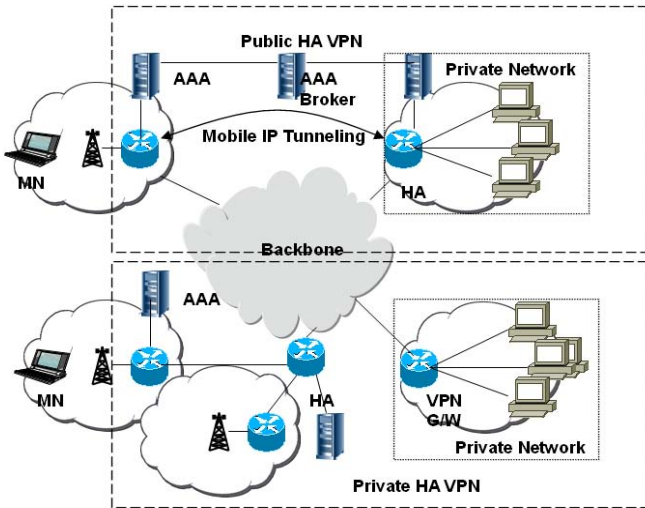


그림 5. Mobility for Mobile VPN (MIP)

HA의 위치에 따라 Public HA VPN과 Private HA VPN으로 나뉠 수 있으며 MN의 인증은 AAA 서버를 통해 Private Network의 서버로 접속하는데 양 Gateway 사이에 터널링이 만들어진다.

다음은 그림 6에서와 같이 SIP 기반의 Mobile VPN 모델을 고려할 수 있다. Mobile IP는 이동을 하게 되면 새로운 IP를 부여 및 등록과정으로 세션이 끊기게 되지만, SIP로 이동성 관리의 Mobile VPN에서는 Visited Network과 Home Network에 SIP 서버를 두고 MN이 동시 re-INVITE 메시지로 세션을 연결해줌으로써 seamless 핸드오프 할 수 있게 된다.

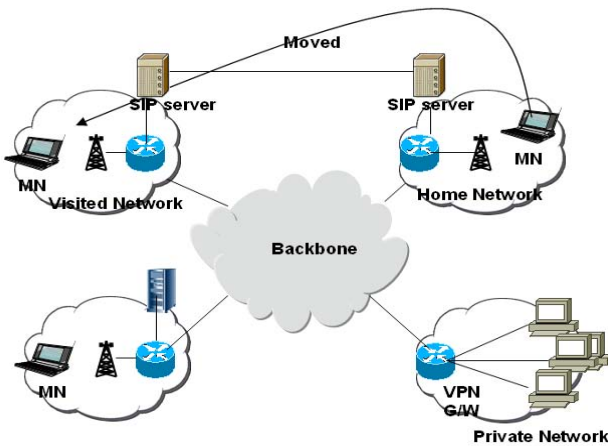


그림 6. Mobility for Mobile VPN (SIP)

5. 결론 및 향후 계획

Mobile Network이 점점 발달되고 사용자 단말 사용이 증가됨에 따라서 인프라를 위한 추가적인 장비 구입 및 유지를 위한 추가 비용을 줄이면서 어떤 이동 환경에서도 Mobile Worker로서 작업할 수 있는 장점을 지닌 것이 바로 Mobile VPN이라고 할 수 있다. 하

지만 전통적인 VPN 형태로서 보안 및 인증에 대한 추가적인 보완사항이 필요하고 아울러 VPN endpoint로의 견고한 라우팅을 하기 위한 문제점을 갖는다. NGN에서 세션기반의 이동성 관리를 갖는 Mobile VPN은 이런 다양한 차세대 네트워크의 VPN 형태에 따른 가입자 서비스를 충족시킬 수 있는 중요한 기술이라고 볼 수 있으며, IMS의 중요한 Entity인 HSS의 추가적인 VPN 가입자 정보를 등록하고 이기종 트래픽을 수렴할 수 있는 Mobile VPN gateway에 서비스에 따른 기능을 추가함으로써 Mobile 상에서 얻을 수 있는 잇점을 최대한 이용할 수 있는 기술이 될 것이다.

향후 추가적인 기능을 더욱 세분화하고 그에 따른 요구사항을 분석해야 할 것이며 여러 서비스 시나리오에 충족할 수 있는 모델에 대한 견고한 메커니즘을 설계해야 한다. 추가적으로 Mobile VPN에서 이동성 관리를 위한 SIP 기반 Seamless Handoff의 연구가 이뤄져야 할 것이다.

참고문헌

- [1] C. Perkins, "IP Mobility Support", RFC 2002
- [2] G. Montenegro, "Reverse Tunneling for Mobile IP", RFC 2344
- [3] P. Calhoun, C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794
- [4] C. Perkins, "IP Mobility Support for IPv4", RFC 3220
- [5] 3GPP TS, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228
- [6] 3GPP TS, "customized Applications for Mobile network Enhanced Logic (CAMEL)", 3GPP TS 23.278
- [7] 3GPP TS, "Impacts of speech-enabled services on IMS, PS and CS domains", 3GPP TS 23.878
- [8] ITU-T Recommendation Y.1311 (2001), IP VPNs - Generic Architecture and Service Requirements
- [9] ITU-T Recommendation Y.1311.1 (2001), Network Based IP VPN over MPLS Architecture