이동 단말을 지원하는 VPN Gateway

권혁찬 ° 나재훈
한국전자통신연구원 IPv6 보안연구팀
{hckwon°, jhnah}@etri.re.kr

The VPN Gateway Supporting Mobile Device

Hyeokchan Kwon° Jaehoon Nah
Electronics and Telecommunication Research Institute

요 약

현재의 VPN 제품들은 단말의 IP 이동성을 지원하지 못하고 있다. 단말의 이동 시 단말은 새로운 IP 주소를 할당 받게 되는데, VPN 게이트웨이는 단말이 초기에 등록한 IP 정보만을 가지고 있기 때문에 이동한 단말이 전송하는 패킷을 폐기하게 된다. 본 논문에서는 VPN 세션의 단절 없이 단말의 이동성을 지원하는 VPN 게이트웨이를 설계하고 구현하였다. 본 논문에서 설계한 VPN 게이트웨이는 IPv6 기반 네트워크에서 동작하며, 단말의 이동성을 지원하기 위해 Mobile IPv6 기술과 VPN 기술을 통합하는 구조를 갖는다.

1. 서 론

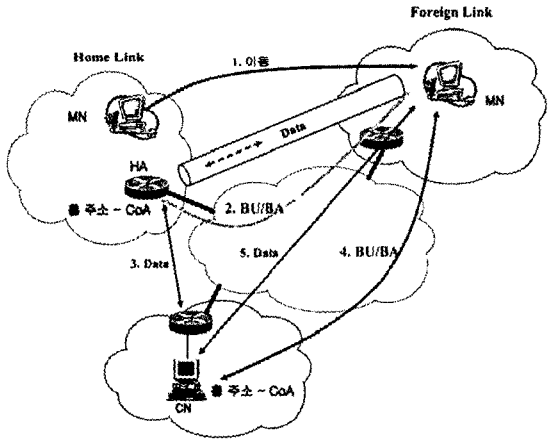
현재의 VPN 제품은 단말의 이동성을 지원하지 못하고 있다. 이는 단말의 새로운 주소를 인식하지 못하기 때문이다. IPv6 환경에서 단말이 이동하면 auto-configuration 방식에 따라 새로운 주소를 할당 받게 된다. VPN 게이트웨이는 단말이 초기에 등록한 IP 정보만을 알고 있기 때문에 이동한 단말이 전송하는 패킷을 받는 경우, source address 필드에 있는 주소를 인증하지 못하게 되며, 해당 패킷을 폐기하게 된다.

본 논문에서는 이동 단말을 지원하는 VPN 게이트웨이를 설계하고 구현하였다. 설계한 VPN 게이트웨이는 VPN 서비스를 받는 단말이 이동하는 경우에 세션의 끊김 없이 VPN 서비스를 제공해 주는 기능을 갖는다. 이를 위해 네트워크 계층에서 단말의 이동성을 제공해 주기 위한 기술인 Mobile IPv6 기술과 VPN 기술을 통합하는 형태로 시스템을 설계하였다.

Mobile IPv6 기술[1]은 IPv6 네트워크 계층(Layer 3)에서 단말의 핸드오프를 지원해 주는 기술이며, IETF Internet area 의 mip6 워킹그룹에서 표준화를 추진하고 있다. 올 해 6 월에 RFC 문서로 Mobile IPv6 기술이 등록되었다. Mobile IPv6 기술의 기본 동작은 [그림 1]과 같다.

이동 단말인 MN(Mobile Node)이 다른 도메인으로 이동하면 방문할 링크에서 사용할 임시 주소인 CoA(Care of Address)를 얻게 되며 이 주소를 자신의 홈 링크상에 위치한 HA(Home Agent)로 등록한다. CoA 를 홈 에이전트로 등록한 후에 이동노드의 홈 주소를 목적지로 하는 패킷이 전달되면 HA 가 이동 노드를 대신하여 패킷을 인터셉트 한다. 홈 에이전트는 이 패킷을 CoA 를 목적지로 터널링하여 이동 노드가 위치한 링크로 전달하며 이동 노드는 터널링 헤더를 제거하고 원래 패킷을 얻어낸다. 반대로 이동 노드가 상대 노드인 CN(Correspondent Node)으로 패킷을 전송할 경우 HA 로의 역터널링을 거쳐서 상대노드로 전달된다. 이 경우 MN 과 CN 은 항상 HA 를 거쳐서 통신을 하게 되며, CN 이 MN 의 새로운 위치를 바로 등록할 수 있도록 하기 위해서 RR(Return Routability)[1,3]이라는 프로토콜을 동작시킨다. RR 의 수행결과로 CN 은 MN 의 새로운 위치를 등록하게 되며, 이후로는 직접 통신을 하게 된다.

RR 프로토콜은 이동단말과 통신중인 노드와 HA 를 거치지 않고 직접 통신을 가능하게 하기 위한 방식인데, VPN 서비스를 받기 위해서는 기본적으로 VPN 게이트웨이를 통해 VPN 도메인으로 접근을 해야 하기 때문에, 본 논문에서 설계한 시스템에서는 RR 프로토콜은 동작하지 않도록 하였다.



[그림 1] Mobile IPv6 의 동작

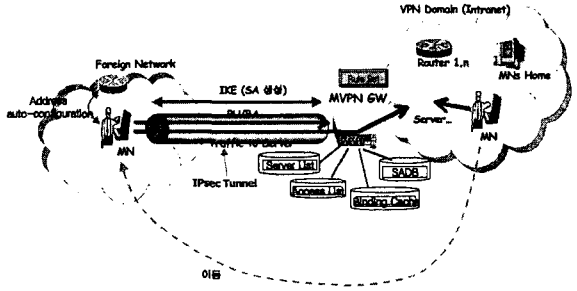
본 논문의 구성은 다음과 같다. 1 장 서론에서 설계한 시스템의 개요와 배경 지식을 기술하였고, 2 장에서 이동 단말을 지원하는 VPN 게이트웨이의 설계 및 구현에 대한 내용을 기술하였으며, 3 장에서 결론과 기존의 관련 연구와의 비교분석 내용이 설명된다.

2. 설계 및 구현

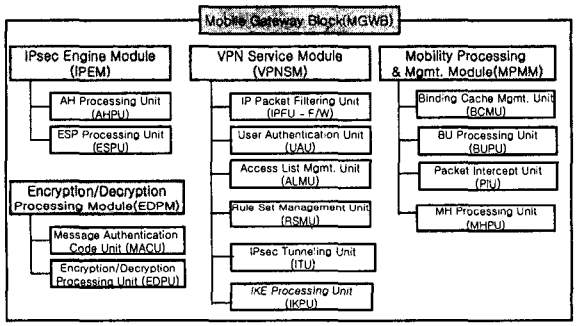
2.1 설계

본 논문에서 설계한 VPN Gateway 는 IPv6 기반으로 동작하도록 설계하였으며 Layer 3 IPsec VPN 을 대상으로 고려하였다.

또한 인증은 단말인증으로 사용자 인증을 대치하는 것으로 가정한다. 단말인증방법은 preshared key 를 이용한 IKE 를 사용하는 것으로 설계하였다. 설계한 VPN 게이트웨이의 개념도는 [그림 2]와 같으며, VPN 게이트웨이를 구성하는 블록들은 [그림 3]과 같다.



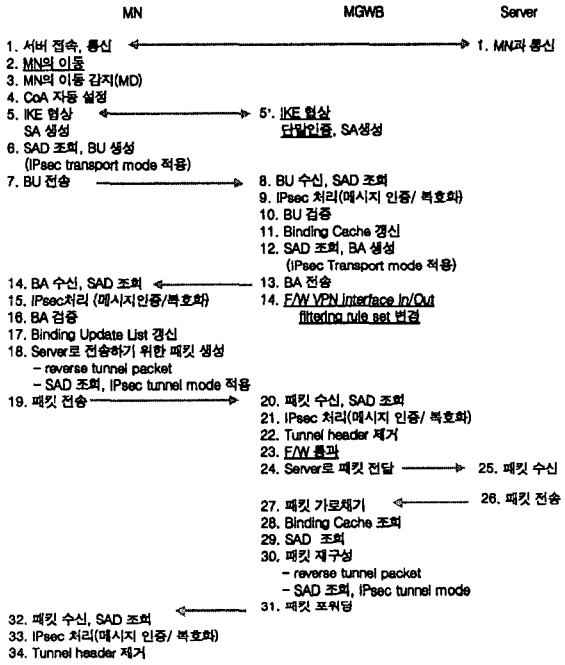
[그림 2] 이동 단말을 지원하는 VPN 서비스 개념도



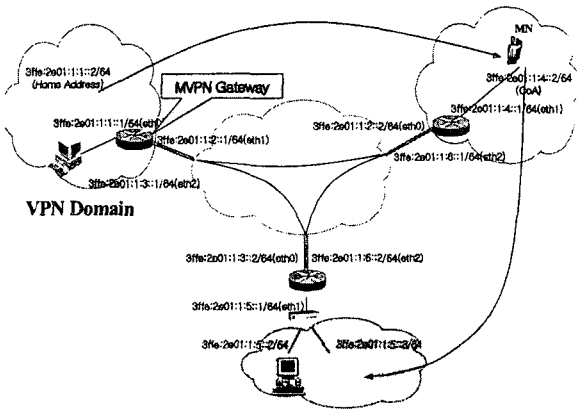
[그림 3] 이동 단말을 지원하는 VPN 게이트웨이 구성블록

[그림 2]에서 MVPN GW 는 Mobile VPN Gateway 를 표현한 것으로 기존의 VPN 게이트웨이와 HA 의 기능을 통합시킨 구조를 갖는다. MVPN GW 는 자신이 관리하는 VPN 도메인을 보호하기 위해 IPv6 기반 firewall 기능을 포함하며, firewall 의 패킷 필터링 규칙을 정의한 Rule Set 을 관리한다. Rule Set 은 인증된 단말의 위치 정보를 저장하고 있으며 외부로부터 패킷이 도착하면 MVPN GW 의 firewall 모듈은 Rule Set 을 참조하여 패킷을 통과시킬 것인지를 결정한다.

단말의 이동성을 제공하기 위해서는 Rule Set 이 실시간으로 갱신될 필요가 있다. 또한 이동 단말을 인증하고 그 위치를 관리하는 메커니즘이 필요하다. 이러한 기능은 Mobile IPv6 의 HA 의 기능과 유사하며, [그림 3]의 Mobility Processing&Mgmt. Module(MPMM)이 이러한 기능을 담당한다. 이동한 단말은 먼저 MVPN GW 와 사전 공유한 preshared key 를 이용하여 IKE 협상을 수행한다(IKPU). 협상 과정에서 단말의 인증 작업이 함께 수행된다. 다음으로 이동단말은 MVPN GW 로 자신의 새로운 위치를 등록하기 위한 BU(Binding Update) 패킷을 전송하게 되는데 이 패킷은 IKE 협상을 통해 생성한 SA 를 이용하여 IPsec tunnel mode 로 보호된다(ITU, IPEM, EDPM). BU 패킷을 수신한 MVPN GW 는 BU 패킷을 검증한 후 이동단말로 BA(Binding Acknowledgement) 패킷을 전송한다(BUPM). 동시에 자신의 Binding Cache 에 이동 단말의 홈 주소와 이동 후 할당 받은 CoA 주소를 저장하고 (BCMU), 이 정보를 VPNSM 의 Rule Set Management Unit(RSMU)으로 알리고, RSMU 는 이 정보를 기초로 Rule Set 을 변경하여 줌으로 새로운 위치로 이동한 이동 단말의 패킷을 VPN 도메인으로 전달해 줄 수 있도록 준비시켜 준다. 이 모든 과정이 네트워크 계층에서 처리되기 때문에 세션은 계속 살아있게 된다. [그림 4]에서는 MN 의 이동에 대한 처리 과정을 보여준다.



[그림 4] MN 의 이동 처리 과정



[그림 5] 테스트베드 네트워크 환경

2.2 구현

본 논문에서 설계한 VPN Gateway 는 IPv6 네트워크 환경에서 그리고 Linux 2.4.21 kernel 기반으로 구현이 진행중이다. 보안 정책과 SA 협상 부분은 현재는 manual 로 설정하는 구조로 구현이 되었으며, IKE 기능을 추가로 구현할 예정이다. 보안 정책과 SA 설정 방법은 pfkey interface 를 이용하여 구현하였다. [그림 5]는 테스트베드 네트워크 환경을, [그림 6]은 SA 를 설정하기 위한 script 파일을, [그림 7]은 [그림 6]의 script 파

일을 실행한 결과 생성된 SADB(Security Association Database)의 내용을 보여준다. [그림 8]은 3ffe:2e01:1:1::2/64 홈 주소를 갖고 있는 MN 이 3ffe:2e01:1:4::/64 도메인으로 이동한 경우, MGWB 의 Binding Cache 의 내용을 보여준다.

```
pfkey -A sp -s 3ffe:2e01:1:1::2 -d 3ffe:2e01:1:1::1 -T
    esp -S 0x1001 -p 62
pfkey -A sp -s 3ffe:2e01:1:1::1 -d 3ffe:2e01:1:1::2 -T
    esp -S 0x1002 -p 62
pfkey -A sa -s 3ffe:2e01:1:1::2 -d 3ffe:2e01:1:1::1 -T
    esp -S 0x1001 -p 62 --esp 3des-cbc --espkey
    1234567890abcdef1234567890abcdef
pfkey -A sa -s 3ffe:2e01:1:1::1 -d 3ffe:2e01:1:1::2 -T
    esp -S 0x1002 -p 62 --esp 3des-cbc --espkey
    1234567890abcdef1234567890abcdef
```

[그림 6] 매뉴얼 SA 설정을 위한 script 파일

```
SADB:
------------------------------------------
src:3ffe:2e01:0001:0001:0000:0000:0000:0002/128 0
dst:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 0
protocol:62
ipsec_proto:esp spi:0x1001 auth:none esp:3des-cbc
lifetime(alloc/byte/add/use)     s:0/0/0/0     h:0/0/0/0
    c:0/0/1321/0
state:mature

src:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 0
dst:3ffe:2e01:0001:0001:0000:0000:0000:0002/128 0
protocol:62
ipsec_proto:esp spi:0x1002 auth:none esp:3des-cbc
lifetime(alloc/byte/add/use)     s:0/0/0/0     h:0/0/0/0
    c:0/0/1321/0
state:mature

SPD:
------------------------------------------
src:3ffe:2e01:0001:0001:0000:0000:0000:0002/128 0
dst:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 0
protocol:62          mode:tranport
sa(esp)
    dst:3ffe:2e01:0001:0001:0000:0000:0000:0001/128
    spi:0x1001
src:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 0
dst:3ffe:2e01:0001:0001:0000:0000:0000:0002/128 0
protocol:62          mode:tranport
sa(esp)
    dst:3ffe:2e01:0001:0001:0000:0000:0000:0002/128
    spi:0x1002
```

[그림 7] 생성된 SADB

Home Address	Care-of-Address
3ffe:2e01:1:1::2	3ffe:2e01::1:4:204:75ff:fee2:c302
Lifetime	Type
992	2

[그림 8] 단말 이동 후, VPN Gateway 의 Binding Cache

3. 결 론

본 논문에서는 이동 단말을 지원하는 VPN 게이트웨이를 설계하고 구현하였다. 설계한 VPN 게이트웨이는 VPN 서비스를 받는 단말이 이동하는 경우에 세션의 끊김 없이 VPN 서비스를 제공해 주는 기능을 갖는다. 이를 위해 네트워크 계층에서 단말의 이동성을 제공해 주기 위한 기술인 Mobile IPv6 기술과 VPN 기술을 통합하는 형태로 시스템을 설계하였다.

기존의 유사한 관련연구로서 [2]에서는 IPv4 네트워크를 대상으로 VPN 도메인 내부에 HA 를 두고 외부에 추가의 external-HA 를 두는 방식을 제안하였다. MN 이 이동하면 미리 VPN 게이트웨이와 안전한 채널이 형성되어 있는 external-HA 로 위치 등록을 하면, external HA 가 MN 의 패킷을 터널링하여 VPN 게이트웨이를 통과시켜 주는 방식이다. [4]의 IPv6 기반의 방식도 [2]번의 방식과 유사한 구조를 갖는다. 그러한 이러한 방식들에는 몇 가지 문제점들이 존재한다. 먼저 HA 가 중복되어 존재하는 오버헤드가 있으며, 단말이 이동 한 경우 패킷이 전달 되는 경로가 매번 외부의 HA, VPN GW, 내부의 HA, VPN 서버를 거쳐야 하므로 성능상의 저하문제도 발생한다. 반면 본 논문에서 제안한 방식은 기존의 고정 단말에 대한 VPN 서비스를 제공하는 경우와 동일한 패킷 전송 경로를 갖는다. 단, 이동 단말이 많은 경우 또는 단말의 이동이 매우 빈번하게 발생하는 경우 VPN 게이트웨이에 많은 부담을 주게 되고 이로 인한 성능 저하의 가능성도 존재한다. 향후 과제로서 성능 측면에서 설계한 구조를 검증하는 과정이 필요할 것이다.

4. 참고문헌

[1] D.Johnson, C.Perkins, J.Arkko, " Mobililty Support in IPv6," IETF RFC 3775

[2] S.Vaarala, Mobile IPv4 Traversal Across IPsec-based VPN Gateways, IETF internet draft, draft-ietf-mobileip-vpn-problem-solution-03, 2003. 9.

[3] 권혁찬, 나재훈, 정교일, " Mobile IPv6 표준화 및 기술동향," IITA, 주간기술동향 1146 호, 2004. 5.

[4] H. Ohnishi, K.Suzuki and Y.Takagi, " Mobile IPv6 VPN using Gateway Home Agent," IETF Internet draft, draft-ohnishi-mobileip-v6vpngateway-01.txt, 2002. 10.