이동 단말을 지원하는 VPN Gateway

관현천, 나재훈
한국전자통신연구원 IPv6 보안연구팀
{hckwon, jnahn}@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 음성을 지원하지 못하고 있다. 단말의 이동 시 단말은 새로운 IP 주소를 할당 받게 되는데, VPN 게이트웨이에는 단말이 초기에 할당된 IP 정보만 가지고 있기 때문에 이동한 단말이 전송하는 패킷을 받는 경우, source address 온도에 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 종료 없이 VPN 서비스를 제공해 주는 기능을 갖는다. 이를 위해 네트워크 계층에서 단말의 음성을 제공해 주기 위한 기법인 Mobile IPv6 기술과 VPN 기술을 통합하는 형태로 시스템을 설계하였다.


이동 단말인 MN(Mobile Node)이 다른 도메인으로 이동하면 방문하려는 프로그램에서 사용할 단말 소스 주소인 CoA(Care of Address)를 얻게 되며 이 주소를 자신의 홈 헛츠가(Home Agent)로 등록한다. CoA를 홈 에이전트로 등록한 후에 이동노드의 홈 주소를 목록화 하는 환경이 되면 포켓이 전달되며 HMAC와 함께 함께 있는 HA(Home Agent)로 전달된다. 홈 에이전트는 이 에이전트

[그림 1] Mobile IPv6의 동작

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

2. 설계 및 구현

2.1 설계

본 논문에서 설계한 VPN Gateway는 IPv6 기반으로 동작하도록 설계하였으며, IPv6 보안과의 연결성으로 고려하였다.

[그림 2] 이동 단말을 지원하는 VPN 서비스 개념도

[그림 3] 이동 단말을 지원하는 VPN 게이트웨이 구성도

[그림 4] MN의 이동 처리 과정

[그림 5] 네트워드 네트워크 환경

2.2 구현

일을 실행한 결과 생성된 SADB(Security Association Database)의 내용을 보여준다. [그림 6]은 3ffe:2e01:11::2/64를 주소로 갖고 있는 MN 이 3ffe:2e01:11::/64 도메인으로 이동한 경우, MGW6 의 Binding Cache의 내용을 보여준다.

```
pkey -A sp = s 3ffe:2e01:11::2 -d 3ffe:2e01:11::1 -T esp -S 0x1001 -p 62
pkey -A sp = s 3ffe:2e01:11::1 -d 3ffe:2e01:11::2 -T esp -S 0x1002 -p 62
pkey -A sp = s 3ffe:2e01:11::1 -d 3ffe:2e01:11::2 -T esp -S 0x1001 -p 62 --esp 3des-cbc --espkey 1234567890abcdef1234567890abedef
pkey -A sp = s 3ffe:2e01:11::2 -d 3ffe:2e01:11::1 -T esp -S 0x1002 -p 62 --esp 3des-cbc --espkey 1234567890abcdef1234567890abedef
```

[그림 6] 메뉴얼 SA 설정을 위한 script 파일

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

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

SPD:
```
src:3ffe:2e01:0001:0001:0000:0000:0000:0000/128 0
dst:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 0
protocol:62
lifetime=transport salesp:

dst:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 spi:0x1001

src:3ffe:2e01:0001:0001:0000:0000:0000:0001/128 0
protocol:62
lifetime=transport salesp:

dst:3ffe:2e01:0001:0001:0000:0000:0000:0002/128 spi:0x1002
```

[그림 7] 생성된 SADB

<table>
<thead>
<tr>
<th>Home Address</th>
<th>Care-of-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ffe:2e01:11::2</td>
<td>3ffe:2e01:11::4:204:75ff:fee2:3c02</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Type</td>
</tr>
<tr>
<td>992</td>
<td>2</td>
</tr>
</tbody>
</table>

[그림 8] 단말 이동 후, VPN Gateway의 Binding Cache

3. 결론

본 논문에서는 이동 단말을 지연하는 VPN 게이트웨이를 설계하고 구현하였다. 설계한 VPN 게이트웨이는 VPN 서비스를 받는 단말이 이동하는 경우에도 세션의 중단 없이 VPN 서비스를 제공할 수 있도록 설계하였다. 이를 위해 네트워크 계층에서 단말의 이동성을 제공해 주기 위한 기술인 Mobile IPv6 기술과 VPN 기술을 병합하는 형태로 시스템을 설계하였다.


4. 참고문헌