

Mobile IPv6 환경에서 방화벽 사용에 관한 문제점

하 동 주*, 엄 흥 열*

*순천향대학교 공과대학 정보보호학과

Mobile IPv6 Problem with Firewalls

Dong-Joo Ha*, Heung-Youl Youm*

Department of Information Security, SoonChunHyang University*

요 약

Mobile IPv6은 방화벽의 사용을 전혀 고려하지 않은 채 설계되었다. 그렇기 때문에 방화벽을 사용하는 네트워크에서는 정상적으로 동작하지 않는 문제가 생긴다. 본 논문에서는 일반적인 방화벽의 패킷 판단에 사용되는 상태테이블에 관하여 설명하고, Mobile IPv6 환경에서 방화벽을 사용함으로써 생기는 문제점을 알아본 뒤 향후 Mobile IPv6 환경에서의 방화벽 사용에 관한 연구의 방향을 제안한다.

I. 서 론

Mobile IPv6로 인하여 Mobile 환경에서도 IPv6의 혜택을 받으면서 편리하고 안전하게 네트워크 환경을 구축할 수 있게 되었다. 하지만 Mobile IPv6는 기존의 방화벽을 전혀 고려하지 않고 설계되었기 때문에 방화벽이 존재하는 네트워크에서는 정상적으로 사용할 수 없다. 그렇기 때문에 지금 시점에서 Mobile IPv6 네트워크를 구축하려면 해당 네트워크에 방화벽을 설치할 수 없을뿐더러 방화벽 없이 네트워크 환경을 구축한다고

해도 외부와의 통신 역시 방화벽이 존재하지 않은 곳에 존재하는 단말과의 통신만 가능한 문제가 생긴다. 이러한 문제는 Mobile IPv6를 도입하기 어려운 이유 중 큰 몫을 차지하고 있기 때문에 개선이 시급하다.

본 논문의 구성은 다음과 같다. II장에서는 Mobile IPv6과 방화벽을 함께 사용함으로써 생기는 문제점들의 언급에 앞서, 확실한 이해를 돕기 위하여 각각의 문제점들의 근본적인 원인인, 방화벽의 내부적인 패킷 처리 방식을 설명한다. III장에서는 지금까지 알려진 Mobile IPv6 환경에서의 방화벽 사

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음

III. 방화벽으로 인한 문제점

Mobile IPv6 환경에서 방화벽으로 인하여 발생하는 문제점들은 크게 두 가지로 나뉜다. 첫 번째는 IPsec의 사용으로 인하여 발생한다. Mobile IPv6는 안전한 통신을 위하여 IPsec을 사용하는데 대부분의 방화벽의 기본 설정으로는 IPsec ESP 패킷들을 제대로 인식하지 못하여 차단한다. 두 번째는 HA(Home Agent)와 MN(Mobile Node), CN(Correspondent Node) 사이에서 발생하는 주소의 변화를 방화벽이 인식하지 못하기 때문에 발생한다. 경로 최적화가 이루어지기 전이나 진행 중인 경우의 통신은 HA에게 가로채어지고, 방화벽은 이와 같은 과정을 알 수 없기 때문에 상태테이블을 갱신할 수 없는 문제가 발생한다.

위의 문제들이 발생하는 경우를 정리하면 다음과 같다.

3.1 MN이 방화벽 뒤에 위치할 경우

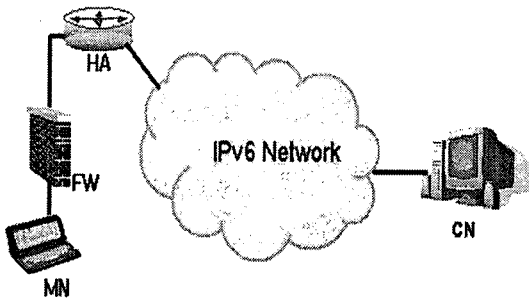


그림 4. 방화벽이 존재하는 네트워크의 MN

1. MN이 CoA(Care of Address)를 획득하기 위하여 바인딩 업데이트를 요청 할 때 IPsec ESP를 사용하기 때문에 방화벽이 인식하지 못함

2. CN과 MN이 통신을 할 때 HA에 의해 가로채어져서 통신하기 때문에 방화벽의 상

태테이블의 정보와 일치하지 않음

3. 경로 최적화를 진행할 때 IPsec ESP이 사용되므로 방화벽이 인식하지 못함

4. MN이 방화벽을 사용 중인 다른 네트워크로 이동했을 때 그곳의 방화벽의 상태테이블에는 이미 연결이 성립된 MN의 통신에 대한 정보가 없음

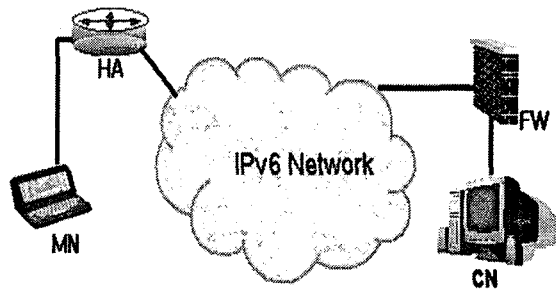


그림 3. 방화벽이 존재하는 네트워크의 CN

3.2 CN이 방화벽 뒤에 위치할 경우

1. 경로 최적화를 진행할 때 MN이 CN에게 CoTI 메시지를 보낼 때 Source Address를 CoA로 보내기 때문에 방화벽의 상태테이블의 정보와 일치하지 않음

3.3 HA가 방화벽 뒤에 위치할 경우

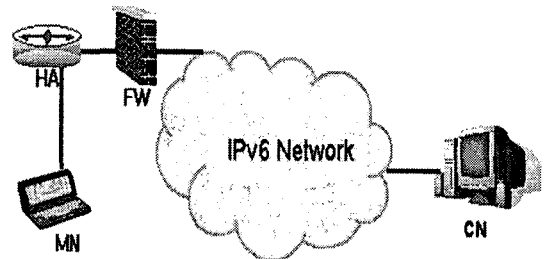


그림 5. 방화벽이 존재하는 네트워크의 HA

1. 바인딩 업데이트나 경로 최적화 시의 HoT 등, IPsec ESP에 의해 보호되어야 하는 메시지들을 방화벽이 인식하지 못함

2. 방화벽이 stateful inspection packet filters 같은 트래픽을 차단할 경우, CN으로부터 요청된 연결 및 MN으로부터 전송되는 패킷은 차단됨

3.4 MN이 방화벽이 있는 네트워크로 이동한 경우

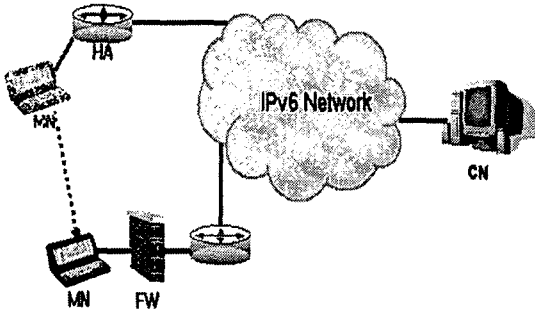


그림 6. 방화벽이 존재하는 네트워크로 이동

1. MN이 CoA를 획득하기 위하여 바인딩 업데이트를 요청 할 때 IPsec ESP를 사용하기 때문에 방화벽이 인식하지 못함

2. 방화벽이 있는 네트워크로 이동하기 전에 연결이 성립되었거나 연결을 진행하는 중에 이동하였을 경우 방화벽의 상태테이블에 관련된 정보가 존재하지 않음

3. 경로 최적화를 진행할 때 IPsec ESP이 사용되므로 방화벽이 인식하지 못함

4. 바인딩 업데이트에 성공했다고 가정할 경우, MN은 실질적으로 CoA를 사용하여 통신하기 때문에 방화벽의 상태테이블에 관련된 정보가 존재하지 않음

IV. 결론

본 논문에서는 방화벽의 패킷 차단 기준을 살펴본 뒤, Mobile IPv6 네트워크 환경에서 방화벽을 사용할 때 발생하는 문제점을 알아보았다. 첫 번째 문제인 방화벽이 IPsec

ESP를 인식하지 못하는 것인데, 이 문제점은 Mobile IPv6 뿐만 아니라 모든 IPsec ESP을 사용하는 통신의 공통적인 문제이고, 방화벽의 설정을 통하여 해결할 수도 있다. 하지만 현실적으로, 존재하는 모든 네트워크의 방화벽의 설정을 바꾸기가 불가능하다. 또한, 두 번째 문제인 상태테이블의 인식에 관한 문제는 기존의 방화벽의 패킷 판단 정보만으로는 해결할 수 없으며, HA 혹은 MN, CN등과 방화벽사이의 직접, 혹은 간접적인 의사소통이 필요하다. 이 문제점의 해결 방법 역시, 방화벽을 변경해야 하는 방식으로 한다면 모든 네트워크의 방화벽을 수정해야 하기 때문에 Mobile IPv6 네트워크는 제한적일 수밖에 없다. Mobile IPv6의 보다 편리하게 사용하려면, 위의 문제점들을 해결할 수 있으면서도 기존의 방화벽의 변경 없이 가능한 해결 방법을 찾아야 할 것이다.

[참고문헌]

- [1] F. Le, S. Faccin, B. Patil, H. Tschofenig "Mobile IPv6 and Firewalls: Problem Statement", RFC 4487, May 2006
- [2] D. Johnson, C. Perkins, J. Arkko "Mobility Support in IPv6", RFC 3775, June 2004
- [3] J. Arkko, V. Devarapalli, F. Dupont "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004