IP 기반의 가상사설망에서의 효율적인 멀티캐스트 지원

백승진, 박종태
경북대학교 전자·전기공학부

Efficient Multicast for IP Based Virtual Private Network

Seung-Jin Baek, Jong-Tae Park
School of Electronic and Electrical Engineering, Kyungpook National University

요약

최근 인터넷 사용이 활성화됨에 따라 기존의 인터넷에서 사용하는 기술을 기업내에서 적용한 인트라넷이 보편화되고 있다. 또한 기존에 사내에서만 구축되던 것이 외부의 직원, 지사, 고객, 나아가 다른 기업들에게까지 확대한 엑스트라넷도 등장하고 있다. 이러한 추세에 발맞추어 IP 기반의 VPN이 각광받고 있다. IP-VPN은 인터넷과 같은 IP 기반의 공중망을 이용하여 가상 사설망을 구축하는 기술이다. 인트라넷 환경의 특성상 다양한 IP 기반의 멀티캐스트 응용들이 생겨나고 있으며, 사실상 많은 이러한 응용들이 IP-VPN 상에서 동작하게 된다. 그러나 현재의 IP-VPN 서비스 제공 플랫폼에서 효율적인 멀티캐스트 지원하지 않는다.

본 논문에서는 이러한 필요성에 따라 터널링을 이용한 IP-VPN 망에서 전달되는 IP 멀티캐스트 메시지를 효율적으로 지원하기 위해 요구사항을 분석하고, 그 구조를 제안한다.

Ⅰ. 서론

최근 인터넷 사용이 활성화되면서, 인터넷 기술을 기업내 통신 및 공동작업활동에 응용하는 인트라넷이 보편화되고 있다. 인트라넷을 더욱 확대하여 사내 정보의 이용범위를 관련업체 및 고객등 특정한 외부까지 확대한 엑스트라넷이 등장하고 있다[1]. 또한 근무의 위치가 사무실에 국한되지 않고 직원의 집이나 기업 외부와의 네트워크 구성을 필요로 하고 있다.

VPN기술은 기존의 전용선이나 VAN을 이용하여 기업간 정보제공을 위한 통신망을 구축하는 것이 아니라, 공중망을 통해 기업 외부에 있는 직원이나 고객이 기업망으로 접근하고, 공중망을 사용하여 지사와 본사 사이의 가상 통신망을 구축하는 기술이라 할 수 있다[2].

현재 VPN제공기술은 통신의 시작점과 끝점 즉, 본사와 지사 또는 본사와 직원의 PC에 터널링 프로토콜을 탑재하여, 이들 사이에 터널이라는 가상 통신 선로를 구축하는 방안이 널리 사용되고 있다. L2TP와 IPSec 등 터널링 프로토콜은 이미 거의 표준화 단계에 이르러 있다.

현재 인터넷/인트라넷 기술을 이용하여 많은 응용소프트웨어가 나오고 있으며, 인터넷폰, 화상회의 등 IP상에서 멀티 캐스트를 이용하는 응용도 많이 나오고 있다. 현재의 VPN을 포함한 기업의 사내망의 경우 IP에 기반한 인트라넷 기술을 사용하고 있어, VPN상에서도 이러한 멀티캐스트 기술이 시급히 요구되고 있다. 그러나 현재의 IP-VPN 기술은 1:1연결 및 전송을 중심으로 진행되어 왔다.

본 논문에서는 IP-VPN상에서 멀티캐스팅을 지원하기 위한 요구사항 및 구조를 제시한다. 특히 터널링 기술을 사용한 VPN상에서 동작하는 트래픽이 IP인 경우에 초점을 맞추도록 하겠다.

Ⅱ. 멀티캐스트 요구사항

멀티캐스트 지원을 위해서 요구되는 사항은 다음과 같다.

- 멀티캐스트 그룹 관리
- 동적인 그룹 가입/해지
- Reliable한 메시지 전달

동적인 그룹의 가입/해지는 실시간으로 그룹에 참여하

거나 해지하는 기능을 말하며, 이를 위해서는 멀티캐스트 그룹의 효율적인 관리가 필요하다. 또한 그룹에 가입한 호스트에 대해서는 정확한 메시지 전달과 에러 발생시 효율적인 복구가 필요하다.

IP-VPN의 경우 공중망을 통하여 패킷을 전송하게 된다. 멀티캐스트의 경우 대량의 데이터가 전송되게 되므로 공중망의 트래픽을 증가시키게 된다. 따라서 멀티캐스트로 인해 증가되는 공중망 트래픽 감소를 위한 방안이 요구된다.

Ⅲ. IP-VPN에서 멀티캐스트 지원

1. 구조 설계 : Security Gateway 기능 확장

본 논문에서는 효율적인 멀티캐스트 지원을 위해 Security Gateway를 확장했으며, 그 구조는 그림 1과 같다. IP-VPN에서 일반적으로 Router나 Firewall형태의 Security Gateway를 갖게 된다. Security Gateway는 인트라넷의 데이터를 공중망을 통해 전송하기 위해 암호화하는 기능을 갖고 있다. 그림 1은 Security Gateway를 중심으로 한 터널링 기반의 IP-VPN의 구성을 나타내고 있으며, 본 논문에서 사용되는 각 용어의 정의는 다음과 같다.

- Security Gateway : 공중망으로 나가는 데이터를 암호화하며, 또한 공중망으로부터 들어오는 암호화된 데이터를 복구한다[2].
- 도메인 : IP-VPN을 구성하는 경우 연결하게 되는 각각의 분리된 네트워크로 일반적으로 지리적으로 분산되어 있다.
- 터널 : L2TP 및 IPSec과 같은 터널링 프로토콜을 이용하여 두 양단간에 만든 가상의 경로이다[3,4,5].

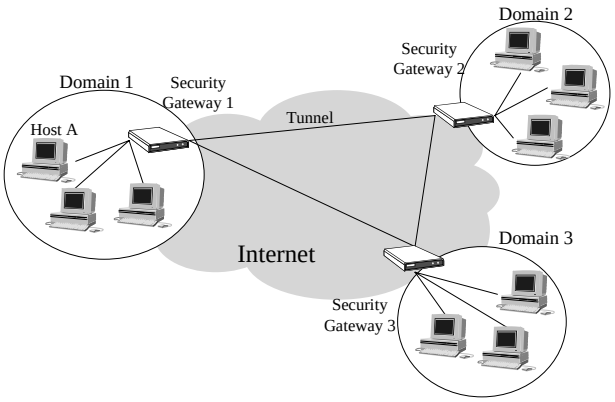

그림 1: 터널링 기반의 IP-VPN 구성

본 논문에서 가정한 것은 다음과 같다.

- 터널링 기술에 기반한 VPN만 고려한다.
- VPN상의 트래픽은 IP 트래픽에 한정한다.
- 한 도메인 내에는 하나의 Security Gateway가 존재한다.
- Security Gateway는 Join하고자 하는 Multicast Group에 관한 정보를 사전에 알고 있다.

기존의 IP망에서는 멀티캐스팅이 하나의 물리적으로 연결된 망에서 가능하였지만, VPN이라는 특수성을 고려할 때, Security Gateway를 이용하여 물리적으로 연결되지 않은 네트워크에서 멀티캐스팅을 구현한다.

멀티캐스팅을 위해서는 일반적으로 멀티캐스트 그룹에 속하는 호스트의 주소 목록을 만들게 된다. 그러나 그룹에 참여하는 호스트의 수가 많아질 경우, 하나의 Gateway에서 관리하기가 쉽지 않게 된다.

이에 대한 대안으로 여러 개의 Security Gateway에서 그 목록을 관리하는 방법이 있다. 각 Security Gateway는 자신이 속한 도메인 내에서 참여하는 호스트의 목록을 관리한다. 그리고 다른 도메인의 호스트 주소를 저장해두는 것이 아니라, 멀티캐스트 그룹에 참여하는 호스트가 있는 도메인의 Security Gateway의 주소만을 목록에 저장한다.

따라서 Security Gateway는 다음과 같은 기능이 확장되어야 한다.

- 호스트 그룹 리스트 및 Security Gateway 리스트 관리
- 오류발생시 재전송을 위한 버퍼
- ACK 취합 및 전송

이러한 구조를 통해 얻을 수 있는 장점은 다음과 같다.

- IP-VPN상에서 멀티캐스트 구현
- 멀티캐스트 그룹의 호스트 수보다 작은 수의 패킷이 공중망을 통과하게 된다. 트래픽 감소시킬 수 있다.
- 로컬에서 도메인내에 참여하는 호스트를 관리하므로 이미 다른 호스트가 그룹에 참여하고 있을 경우 가입 및 해지에 걸리는 지연시간을 감소할 수 있다.

2. 동작과정

IP-VPN 상에서 멀티캐스트 메시지의 전달 및 확인, 멀티캐스트 그룹에 가입/해지 등의 과정은 다음과 같이 이루어진다.

- Send Messages
  한 호스트에서 멀티캐스트 메시지를 전송하게 되면, 해당 호스트가 속한 도메인의 Security Gateway는 도메인 내의 다른 그룹에 참여하는 호스트에게 메시지를 전달하게 되고, 이어서 그룹에 등록되어 있는 다른 도메인의 Security Gateway에게도 메시지를 전달하게 된다. 메시지를 전달받은 다른 도메인의 Security Gateway들도 자신들의 도메인 내에 있는 호스트에게

메시지를 전달하여 멀티캐스팅을 수행하게 된다.
그림 2는 IP-VPN 상에서 멀티캐스트 메시지가 전달되는 과정을 보여주고 있다. 즉, 공중망에 통과하는 패킷의 수는 그룹에 가입한 호스트의 수가 아니라 Security Gateway의 수와 같게 된다.

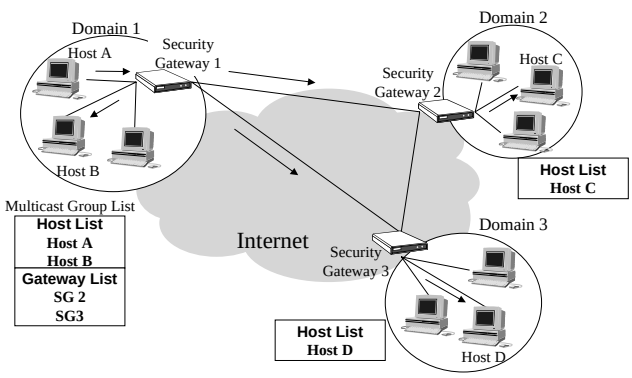

그림 2: 멀티캐스트 메시지의 전달과정

- ACK

일반적인 멀티캐스트의 경우 멀티캐스트 메시지를 보낸 호스트에게 메시지를 받은 호스트가 ACK/NAK를 보내게 된다. 그러나 본 논문에서 제안하는 구조에서는 메시지를 보내는 호스트는 메시지를 받는 대상이 모르는 상태에서 메시지를 보내기 때문에 그 의미가 없다. 이 경우 ACK/NAK는 해당 도메인의 Security Gateway가 담당하게 된다. 즉 Security Gateway는 자신의 도메인의 호스트들의 ACK를 다 모은 후 하나의 ACK만을 원래 메시지를 전송한 Security Gateway에게 전송하게 된다. 메시지를 처음보낸 Security Gateway 역시 자신의 도메인 내의 ACK와 다른 도메인의 Security Gateway의 ACK를 다 모아서 메시지를 전송한 호스트에게 되돌려준다. ACK가 전달되는 경로는 그림 2의 화살표의 반대방향과 같다.

- NAK

NAK의 경우도 ACK와 같이 1차적인 처리는 해당 도메인의 Security Gateway에서 한다. Security Gateway는 멀티캐스트를 위한 별도의 버퍼를 마련해두고, 메시지를 임시 저장하게 된다. 자신의 도메인으로부터 모든 ACK가 도착한 경우 버퍼에서 해당 메시지를 삭제하고, NAK가 들어올 경우 버퍼에 담기있는 메시지를 재전송하게 된다.

- Join

한 호스트가 멀티캐스팅 그룹에 가입할 경우 도메인의 Security Gateway에게 가입 신호를 보내게 된다. Security Gateway가 이미 멀티캐스트 그룹에 가입되어 있는 경우 간단히 자신이 관리하는 호스트 목록에 해당 호스트를 추가함으로써 가입과정이 끝나게 된다.
만약 Security Gateway가 그룹에 속하지 않는 경우 Security Gateway는 Primary Security Gateway 및 다른 Gateway들에게 자신을 등록시킨후 자신도 역시 가입요청을 한 호스트를 새로 생성한 그룹 목록에 추가한다. 그림 3은 호스트가 그룹에 가입할 때 신호의 흐름을 나타내고 있다.

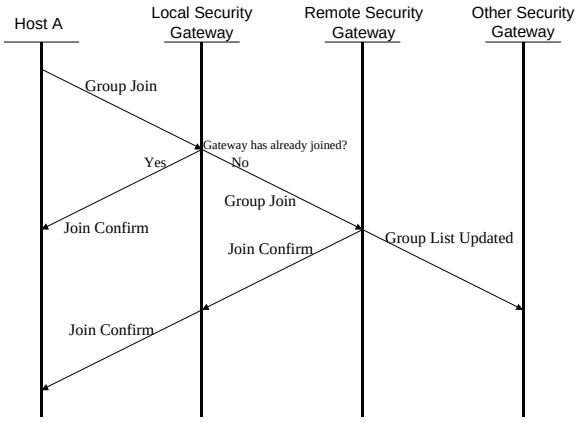

그림 3: 그룹 가입 신호 전달

- Remove

도메인 내의 호스트는 멀티캐스트 그룹에서 가입을 해지할 수도 있다. 요청을 받은 Gateway는 우선 호스트를 그룹 목록에서 삭제한다. 그리고 더 이상 목록에 호스트가 있지 않을 경우 다른 Gateway들에게 자신이 더 이상 그룹에 속하지 않음을 알리게 되어 더 이상의 멀티캐스트 메시지를 받지 않게 된다.

Ⅳ. 결론

본 논문에서는 멀티캐스트 그룹을 관리하도록 Security Gateway의 기능을 확장하여 IP-VPN 망에서 멀티캐스트 지원을 위한 구조를 제안하였다. Security Gateway에 터널 생성 및 암호화 등의 기능외에도, 멀티캐스트 그룹 관리, 에러 발생시 재전송 기능 등을 포함하였다.

그러나, Securiry Gateway에 과부하가 걸리는 등 몇가지 문제점을 안고 있다. 향후 Security Gateway의 부하를 분산하고, 도메인 내에 2개 이상의 Security Gateway가 있을 경우의 그룹 목록 관리 문제를 연구할 계획이다.

참고 문헌

[1] "The new world of virtual private networking services," Cisco whitepaper, 1998.

[2] Bryan Gleeson, Arthur Lin, Juha Heinanen, Grenville Armitage, Andrew Malis, "A framework for IP based Virtual Private Networks," Internet Draft, 1999.

[3] "Layer 2 Tunneling Protocol," Cisco whitepaper, 1998.

[4] W. M. Townsley, A. Valencia, A. Rubens, G. S. Pall, G. Zorn, B. Palter, "Layer Two Tunneling Protocol L2TP," Internet Draft, 1999.

[5] R. Thayer, N. Doraswamy, R. Glenn, "IP Security Document Roadmap," RFC 2411, 1998.