IPSec-VPN에서의 네트워크 중복 문제 해결을 위한 IPSec 네트워크 별칭 기법

박재성° 천준호 전문석
숭실대학교 대학원 컴퓨터학과
sestar@edunet4u.net, opendream@hanmail.net, mjun@comp.ssu.ac.kr

The Aliasing IPSec Network Mechanism for Solving an Overlapping Network Problem in the IPSec-VPN

Jaesung Park° Junho Chun Moon-Seog Jun
Dept. of Computing in Soong-sil University

요 약

IPSec Tunnel Mode를 이용하여 보안 네트워크를 구축 시, 네트워크 구성이 중복된 경우에는 중복되지 않도록 재구성해야 하는 문제가 있다. 본 논문에서는 IPSec Tunnel Mode 통신을 하고자 하는 두 네트워크가 중복된 경우, IPSec 네트워크 별칭 기법을 통하여, 이전 네트워크의 구성을 변경하지 않고 통신할 수 있는 방안을 제시한다.

1. 서 론

IPSec-VPN 시스템은 서로 다른 네트워크 또는 호스트 간에 가상 사설망을 구축하여 안전한 통신을 가능하게 한다. 따라서 임의의 두 네트워크 또는 호스트를 안전하게 연결하는 기능을 수행한다.

하지만 기존 네트워크 환경이 서로 중복되어 있는 경우, 네트워크 환경을 중복 되지 않도록 재구성해야 하는 문제가 있다.

본 논문에서는 IPSec 네트워크 별칭 기법을 사용하여 임의의 중복된 네트워크 환경에서 기존 네트워크 환경의 변경 없이, IPSec Tunnel Mode를 이용한 보안시스템을 구축할 수 있는 방안을 제시한다.

2. 관련 연구

2.1 IPSec Transport Mode

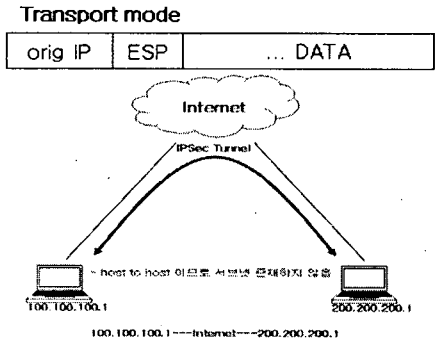

그림 1. IPSec Transport Mode Network

IPSec Transport Mode는 Host-to-host 간에 안전한 통신을 하고자 할 때 사용되며, 암호화 되지 않은 실제 IP 주소로 통신이 된다. 따라서 네트워크 중복이 일어나지 않는다.[2]

2.2 IPSec Tunnel Mode

IPSec Tunnel Mode는 Host-to-host 또는 Gateway-to-gateway 간에 안전한 통신을 하고자 할 때 사용되며, 실제 IP를 숨기고 통신이 된다.[3]

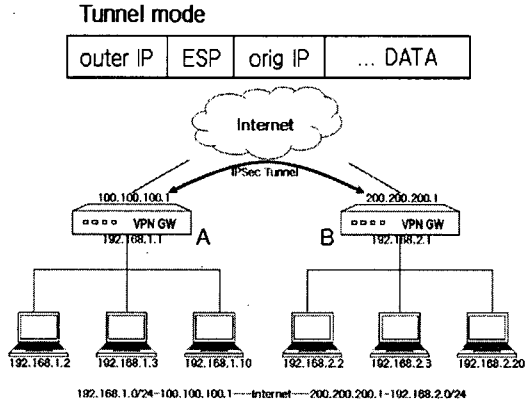

그림 2. IPSec Tunnel Mode Network

그림 2의 두 A, B 네트워크는 서로 중복된 네트워크 환경이 아니다. 따라서 기존 네트워크 환경의 변경 없이 IPSec-VPN 네트워크 환경을 구축할 수 있다.[4]

그림 3의 C, D 두 네트워크는 중복된 네트워크 환경이다. 따라서 Gateway에서는 적합한 라우팅을 할 수 없다. C 또는 D 네트워크 환경을 서로 중복되지 않도록 변경해야 통신이 가능하다.[1]

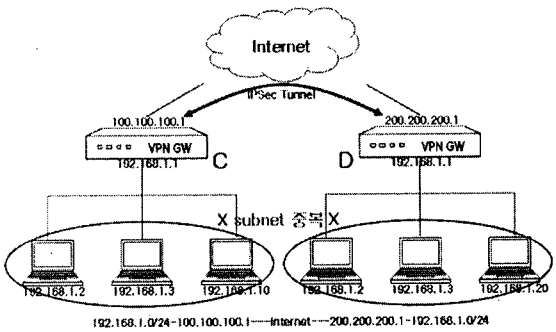

그림 3. IPSec-VPN에서의 중복된 네트워크 구성

3. IPSec 네트워크 별칭 기법

3.1 IPSec 네트워크 별칭 기법 모듈

IPSec 네트워크 별칭 기법은 다음과 같이 두 가지 모듈로 구성되어 있다.

첫 번째 모듈은 IPSec 네트워크 별칭 테이블을 구성하는 모듈이고, 두 번째 모듈은 IPSec 네트워크 별칭 테이블에 따라, ESP 패킷안의 Original Source IP와 Original Destination IP를 변경하는 모듈이다.

표 1. IPSec 네트워크 별칭 테이블

	Outer Source IP	Outer Destination IP	Original Source IP	Original Destination IP
GW A	A_IP	B_IP	A_Sub_IP'	B_Sub_IP'
GW B	B_IP	A_IP	B_Sub_IP'	A_Sub_IP'

IPSec 네트워크 별칭 테이블 구성 모듈은, 표 1과 같이 두 네트워크 간에 IPSec Tunnel Mode 설정 시, 네트워크 별칭 테이블을 구성한다. A_IP 와 B_IP는 각각의 Gateway의 IP이고, A_Sub_IP' 와 B_Sub_IP'는 네트워크 중복을 방지하기 위한 네트워크 호스트의 별칭 IP이다.

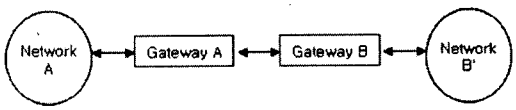

그림 4. A 네트워크에서의 별칭 네트워크 구성

그림 4는 A 네트워크에서의 별칭 네트워크 구성을 나타낸다. 즉, 중복된 네트워크를 방지하기 위하여, B 네트워크를 임의의 별칭 네트워크로 구성한다.

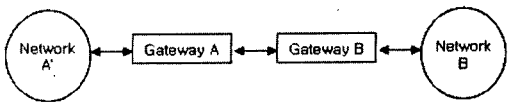

그림 5. B 네트워크에서의 별칭 네트워크 구성

그림 5는 B 네트워크에서의 별칭 네트워크 구성을 나타낸다. 즉, 중복된 네트워크를 방지하기 위하여, A 네트워크를 임의의 별칭 네트워크로 구성한다.

두 번째 모듈은 그림 6과 같이 Gateway에서 패킷을 송수신 할 때, ESP 패킷안의 Original Source IP와 Orignal Destination IP를 변환한다. 네트워크 A, B 각각의 IP 변환 과정은 그림 7, 8과 같다.

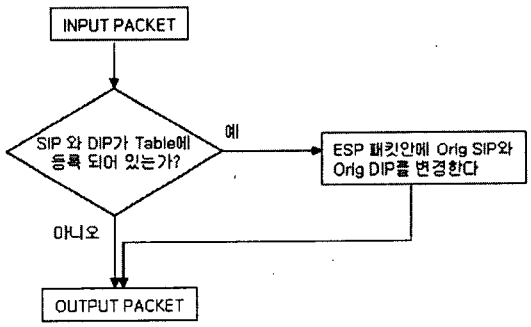

그림 6. IPSec 네트워크 별칭 테이블 변환 과정

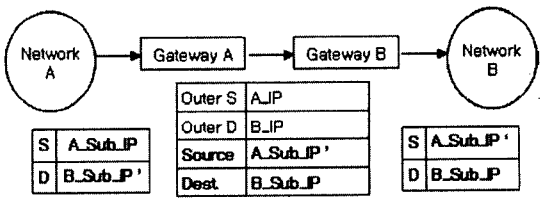

그림 7. A에서 B로 통신 시, IP 변환 과정

그림 7에서 보는 바와 같이, Gateway A에서 Gateway B로 패킷 전송 시에는, 자신의 네트워크 IP인 A_Sub_IP는 별칭 A_Sub_IP' 로 변환하고, 상대방 네트워크 IP는 실제 B_Sub_IP로 변환한다.

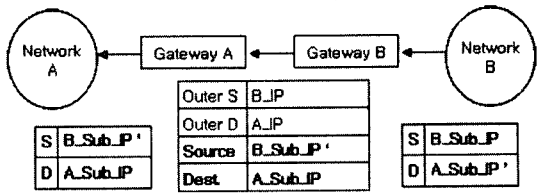

그림 8. B에서 A로 통신 시, IP 변환 과정

그림 8에서 보는 바와 같이, Gateway B에서 Gateway A로 패킷 전송 시에는, 자신의 네트워크 IP인 B_Sub_IP는 별칭 B_Sub_IP' 로 변환하고, 상대방 네트워크 IP는 실제 A_Sub_IP로 변환한다.

3.2 IPSec 네트워크 별칭 기법 프로세스

IPSec 네트워크 별칭 기법의 2가지 모듈을 이용하여, 임의의 중복된 네트워크 환경에서 IPSec-VPN을 적용하는 6가지 프로세스가 있다.

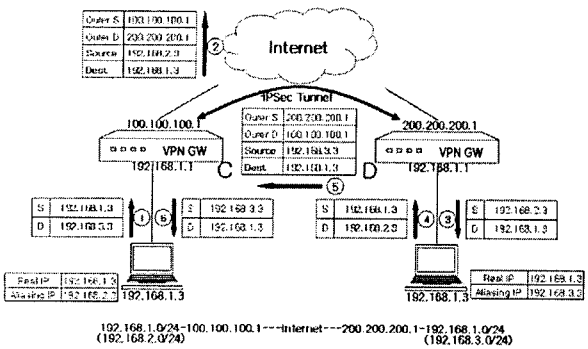

그림 9. IPSec 네트워크 별칭 기법을 이용한 IPSec-VPN 적용

그림 9는 두 VPN Gateway가 터널 협상을 할 때, 기존의 네트워크와 중복되지 않는 임의의 별칭 네트워크를 생성한다. C의 실제 네트워크는 192.168.1.0/24 이고, 별칭 네트워크는 192.168.2.0/24 이다. D의 실제 네트워크는 192.168.1.0/24 이고, 별칭 네트워크는 192.168.3.0/24 이다.

IPSec 네트워크 별칭 기법은 중복된 네트워크 환경에서 다음과 같은 6가지 프로세스로 IPSec-VPN을 구축할 수 있다.

① C 네트워크의 Host에서 D 네트워크의 Host 에게 패킷을 전송하는 과정이다. C 네트워크의 Host 입장에서 볼 때, 자신의 IP는 192.168.1.3 이고, D 네트워크의 Host의 IP는 192.168.3.3 이다.

② C 네트워크의 Host에서 보내온 패킷을 암호화 하여, D 네트워크의 호스트에게 전송하는 과정이다. C 네트워크의 Host에서 보내온 패킷을 D 네트워크의 Host에게 보내는 패킷이므로, 암호화를 하기 때문에 Outer IP가 추가된다. 그리고 별칭 네트워크가 구성되어 있으므로, D 네트워크에서 발신지와 목적지를 제대로 알 수 있도록 Source IP를 별칭 IP로 변환하고, Destination IP를 실제 IP로 변환한다. ESP 패킷안의 IP를 변경하므로, 실제 라우팅 테이블에는 영향을 미치지 않는다.[1]

③ C 네트워크의 VPN Gateway에서 보내온 패킷을 D 네트워크의 VPN Gateway에서 복호화 하여, D 네트워크의 Host에게 전송하는 과정이다. C 네트워크의 VPN Gateway에서, D 네트워크에서 구별할 수 있도록, Source IP는 별칭 IP로 변환하고, Destination IP는 실제 IP로 변환하여 보내왔기 때문에, 추가 변환 작업이 필요 없다. 따라서 D 네트워크의 VPN Gateway에서는 복호화만 하여 D 네트워크의 Host로 패킷을 전송한다. 따라서 D 네트워크의 Host는 Source IP가 192.168.2.3 이고, Destination IP가 192.168.1.3 인 패킷을 전송 받는다.

④ D 네트워크의 Host에서 C 네트워크의 Host에게 응답 패킷을 보내는 과정이다. D 네트워크의 호스트 입장에서 볼 때, 자신의 IP는 192.168.1.3 이고, C 네트워크의 호스트의 IP는 192.168.2.3 이다.

⑤ D 네트워크의 Host에서 보내온 패킷을 암호화 하여, C 네트워크의 호스트에게 전송하는 과정이다. D 네트워크의 Host에서 보내온 패킷을 C 네트워크의 Host에게 보내는 패킷이므로, 암호화를 하기 때문에 Outer IP가 추가된다. 그리고 별칭 네트워크가 구성되어 있으므로, C 네트워크에서 발신지와 목적지를 제대로 알 수 있도록 Source IP를 별칭 IP로 변환하고, Destination IP를 실제 IP로 변환 한다.

⑥ D 네트워크의 VPN Gateway에서 보내온 패킷을 C 네트워크의 VPN Gateway에서 복호화 하여, C 네트워크의 Host에게 전송하는 과정이다. D 네트워크의 VPN Gateway에서, C 네트워크에서 구별할 수 있도록, Source IP는 Aliasing IP로 변환하고, Destination IP는 Real IP로 변환하여 보내왔기 때문에, 추가 변환 작업이 필요 없다. 따라서 C 네트워크의 VPN Gateway에서는 복호화만 하여 C 네트워크의 Host로 패킷을 전송한다. 따라서 C 네트워크의 Host는 Source IP가 192.168.3.3 이고, Destination IP가 192.168.1.3 인 패킷을 전송 받는다.

4. 결 론

본 논문에서는 IPSec Tunnel Mode를 이용하여 보안 네트워크를 구축 시에, 서로 중복된 두 네트워크 환경에서도, 네트워크 구성의 변경 없이 IPSec-VPN 네트워크를 구성할 수 있는, IPSec 네트워크 별칭 기법을 제안하였다.

IPSec 네트워크 별칭 기법은 임의의 환경을 가진 네트워크와 IPSec을 이용한 안전한 통신을 할 수 있는 방법을 제시한다. 이는 네트워크 구성의 변동이 많은 Mobile Network에서 유용하게 쓰일 수 있다.[5][6]

5. 참고문헌

[1] J. Moy, "OSPF Version 2" RFC1583, IETF, 1994
[2] J. Touch, "Use of IPsec Transport Mode for Dynamic Routing" RFC3884, IETF, 2004
[3] P. Srisuresh, "Security Model with Tunnel-mode IPsec for NAT Domains" RFC2709, IETF, 1999
[4] S. Kent, "IP Encapsulating Security Payload (ESP)" RFC2406, IETF, 1998
[5] T. Kivinen, "Design of the MOBIKE Protocol" draft-ietf-mobike-design-02.txt, IETF, 2005
[6] 홍기훈, 정수환, 이계상, "IETF IPSEC 관련 그룹 및 MSEC 그룹 표준화 동향," 정보보호학회지, vol. 14,no. 2, pp. 38-45, April 2004.