Common Interface Component(CIC)를 이용한 IP-VPN 상호 호환성 개선방안 연구

한종철* 송주석
연세대학교 컴퓨터과학 산업시스템공학과
{cobi*, jssong}@emerald.yonsei.ac.kr

A Study of interoperability in IP-VPN with Common Interface Component(CIC)

Jongcheol Han* Jooseok Song
Department of Computer Science, Yonsei University

요 약

최근, VPN기술은 보안 통신을 위해 자주 사용되고 있다. 비록 IPsec이 표준화 되었지만 많은 Vender들의 구현은 아직까지 완전한 상호간의 호환성을 갖지는 못하고 있다. 본 논문은 IP-VPN에 있어 상호 호환성 문제를 연구했다. 연구결과, 서로 다른 IP-VPN 구현에 있어 상호 호환성을 지원할 수 있는 Common Interface Component(CIC)를 제안하게 되었다. CIC와 CIC-Manager는 다양한 IP-VPN 구현에 있어서 상호 호환성의 해결책을 제공한다. 또한 CIC를 이용하여 다양한 표준을 지원할 수 있다.

1. 서 론

인터넷 사용이 활성화되면서, 인터넷 기술을 기업 업무에 적용하는 인트라넷 (IntraNet)이 보편화되고 이를 특정 외부에까지 확대한 엑스트라넷(ExtraNet)이 등장하고 있다. 또한 근무의 위치가 사무실에 국한되지 않고 직원의 집이나 업무의 현장으로 확대되어 감에 따라 기업은 기업 내부에서의 정보 공유뿐 아니라 기업 외부와의 통신을 위한 네트워크 구성을 필요로 하고 있다. 이를 해결하기 위해 대두되고 있는 VPN(Virtual Private Network)기술 및 원격 접근기술은 누구에게나 개방되어 있는 공중망(Public Network)에서 안전한 통신을 하기 위해 개발되었다. VPN을 구현하기 위한 여러 방식이 있으나 그중 IPsec을 이용하여 구현하는 방법이 가장 널리 사용되고 있다. IPsec 은 Internet Engineering Task Force's (IETF)의 IP 보안 표준이다. 이는 Internet Key Exchange (IKE) 프로토콜을 포함하며 1998 년 11 월 RFC 로 발표되었지만 다양한 IPsec 구현으로 인해 서로 다른 업체간 상호 호환성의 문제가 발생했다. 상호 호환성 문제정을 극복하고자 정부 및 민간 단체에서 표준화 기구를 설립하고 각기 다른 상호 호환성 문제 해결을 위한 표준화 방안을 제시하고 있다. 각 표준화 기관에서 제시하고 있는 상호 호환성 해결 방안은 표준화 기관에 가입 후에 그 기관에서 정한 표준을 준수하여 IPsec VPN 을 구현하고 기관에서 제공하는 시험 과정을 거쳐 상호간 호환성을 검증하는 방법이 보편적인 방법으로 이용되고 있다. 이로 인해 여러 표준화기관의 표준 중에서 어떤 표준을 선택해야 하는지의 문제가 발생하였다. 이는 상호 호환성 해결을 위해 결성된 표준화 기관이 서로 상이한 표준을 제시함으로서 또 다른 상호 호환성의 혼란을 가져오는 결과를 초래했다. 따라서 표준화 기관에서 정한 표준을 따르지 않는 Vender 들 간의 IPsec VPN 구현과 서로 다른 표준기관의 표준을 준수하는 Vender 들 간의 IPsec VPN 구현으로 발생하는 상호 호환성 문제 해결을 위한 해결책이 필요하게 되었다. 본 논문에서는 해결 방안으로 Common Interface Component (CIC) 및 CIC-Manager 를 이용한 새로운 VPN 구조를 제시하고 있다. 이는 도메인간 발생하는 상호 호환성 문제를 극복하는 방안이 될 것이다.

2. 본 론

2.1 Common Interface Component (CIC)의 개요

업체간 서로 상이한 IPsec VPN 구현에서 발생하는 상호 호환성 문제를 극복하고자 NIST 의 IPsec-WIT[2], VPN Consortium 의 Documentation Profiles for IPsec Interoperability[3], ICSA 의 VPN lab.[4], ITSEC 등에서 각기 다른 표준을 제시하고 있다. CIC 는 상이한 구현을 갖는 Vender 들의 IPsec VPN 구현 및 여러 표준화 기구에서 정한 표준을 각 Vender 들이 VPN 을 이용한 통신 이전에 CIC 협상후에 CIC 를 통한 하나의 표준으로 VPN 통신 방법을 설정함으로서 상호 호환성을 극복할 수 있게 하는 공통 인터페이스 표준이다. CIC 는 각각의 Vender 들의 IPsec VPN 구현을 위한 Driver 와 Application 상위에서 동작하며 협의된 표준으로 VPN 통신 방법을 변환시켜 줄 수 있도록 각각의 Vender 들에

의해 구현되어야 한다. 따라서 Vender 들은 상호 호환성을 유지하고자 하는 표준에 맞은 CIC 를 구현해야 한다. 또한 구현된 CIC 를 이용한 VPN 통신으로 각각의 표준화 기관에서 정한 시험을 거쳐야 한다. CIC 는 Gateway 와 통신 할 수 있는 CIC-Manager 에 의해 분배된다. 여기서는 편의를 위해 Domain 을 동일 IPsec VPN 이 호환되는 영역으로 정의하며 시험을 위한 기본 단위로 사용 하고자 한다.

2.2 모드별 협상과정 및 분배구조

2.2.1 조건

- Domain 내의 Gateway 는 CIC 를 지원할 수 있다.
- 각 Domain 은 ICSA CIC 를 반드시 지원해야한다.
- 각 Domain 내에서는 상호 호환이 되는 VPN 구조를 갖는다.
- 각 Vender 들이 구현한 CIC 는 Domain 내의 repository 에 저장되어 있어야 한다.
- CIC 는 VPN 을 이용한 통신 이전에 CIC-Manager 간의 통신을 통한 표준 CIC 협상 후에 선택된 CIC 가 Gateway 에 분배된다.

2.2.2 Tunnel mode for Gateway-to-Gateway

그림[1]과 같이 각각의 Domain 에 있는 Gateway 를 통해 상호 호환성 있는 VPN 통신을 하고자 할 경우이다. CIC-Manager 간의 CIC 협상후에 선택된 CIC 는 각각의 Domain 에 있는 Gateway 에 전달된다. 각 Domain 은 각 Vender 에서 지원하는 CIC 표준들을 CIC-Manager 와 통신할 수 있는 repository 에 저장해 두어야 한다. 협상의 진행은 아래와 같은 다섯 단계의 절차를 거치게 된다. 이는 Domain 대 Domain 간의 Gateway 를 통한 상호 호환성 있는 VPN 통신을 하고자 할 경우에 유용한 방법이다. 각각의 Domain 내의 Gateway 가 여러 표준의 CIC 를 갖는 것보다는 CIC-Manager 가 CIC 들을 관리함으로서 새로운 CIC 나 변경된 CIC 의 분배시에 유리하다. 다음은 Gateway 간 통신을 위한 Tunnel mode 생성시의 그림[1]에 대한 설명이다.

(1)서로 상이한 VPN 구현을 갖고 있는 Domain1 과 Domain2 가 상호간 통신을 하고자 한다.

(2) Domain1 의 CIC Manager 와 Domain2 의 CIC Manager 가 어떤 표준으로 상호간 통신을 할 것인지 협상한다. 협상에 의해 ICSA 표준을 사용하기로 협상되었다면,

(3) Domain1 의 Gateway 는 Domain1 의 CIC Manager 로부터 ICSA CIC 를 전달받고 설치한다.

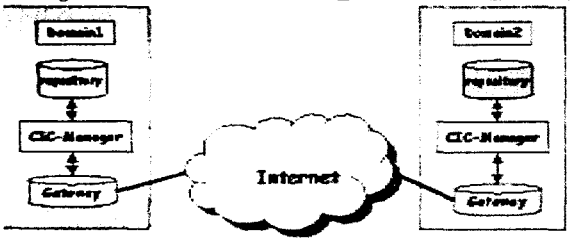

그림 1) Gateway간 통신을 위한 Tunnel mode

(4) Domain2 의 Gateway 는 Domain2 의 CIC Manager 로부터 ICSA CIC 를 전달받고 설치한다.

(5) Domain1 와 Domain2 는 Gateway 에 설치된 ICSA CIC 를 통해 VPN 통신이 가능하다.

2.3 CIC 구조

CIC Manager 로부터 다운받은 CIC 는 그림[2]과 같이 Driver 와 Application 상위에 위치한다. 업체들의 서로 상이한 VPN 구현 및 표준은 CIC 를 통해서 협의된 표준기관의 표준으로 통신이 가능하게 된다.

2.3.1 CIC 전송 프로토콜

CIC Manager 가 CIC 를 전달할 때 ftp 와 같은 일반 파일 전송 프로토콜을 이용하여 별도의 인증 과정 없이 관련 CIC 를 전달한다.

2.3.2 CIC 를 이용한 통신

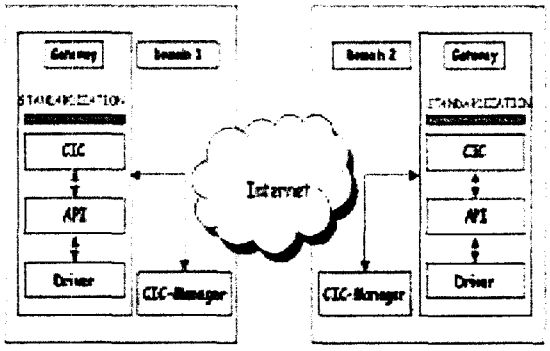

그림 2) CIC 를 위한 Gateway

CIC를 이용한 Gateway간 통신은 그림[2]에서와 같다. CIC를 이용한 Gateway간 통신은 CIC를 설치하는 주체가 Gateway가 된다. 먼저 Domain 1 과 Domain 2가 CIC-Manager를 통해 CIC표준 협상절차를 거친 후에 전달되어진 CIC를 각 Gateway들의 Driver와 Application상위에 설치하게 된다. 결국 CIC협상 후에 전달 후 설치된 CIC를 통해 상호간 호환성 있는 VPN통신을 할 수 있는 방법이 만들어지는 것이다. 따라서 서로 다른 IPsec VPN 구현이나 상이한 표준을 갖고 있는 Domain 1과 Domain 2의 Gateway들은 협상된 CIC를 통해 특정 표준 형식으로 상호 호환성 있는 VPN통신을 할 수 있다.

2.3.3 Message 교환

2.3.3.1 Gateway 간 CIC 협상을 위한 Message 교환

Gateway 간 CIC-Manager 를 이용한 Message 교환시에는 그림[3]과 같이 메시지를 교환하게 된다. 교환되는 메시지는 아래와 같다.

(1) Domain1 의 Gateway 가 Domain1 의 CIC-Manager 에 Domain 2 와의 통신 요청

(2) Domain1 의 CIC-Manager 는 Domain1 의 Gateway 에 메시지 수신에 대한 응답 보냄

(3) Domain1 의 CIC-Manager 는 Domain2 의 CIC-Manager 에 CIC-List 보냄

(4) Domain2 의 CIC-Manager 는 자신의 Gateway 에 선택된 CIC 전달

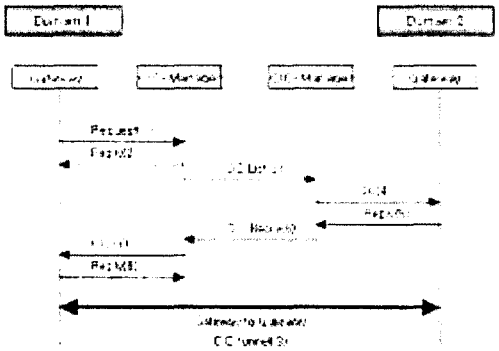

그림 3) Tunnel Mode에서 CIC 협상을 위한 Message교환

(5) Domain2 의 Gateway 는 CIC 를 받은 것에 대하여 CIC-Manager 에 응답

(6) Domain2 의 CIC-Manager 는 Domain1 의 CIC-Manager 에 선택된 CIC 를 응답 (CIC-Reply)

(7) Domain1 의 CIC-Manager 는 선택된 표준 CIC 를 Gateway 에 전달

(8) Domain1의 Gateway는 CIC를 받은 것을 CIC-Manager에게 알림

(9) Domain1 의 Gateway 와 Domain2 의 Gateway 는 CIC-tunnel 생성

위와 같은 메시지 교환을 통해 Domain1 과 Domain2 의 Gateway 는 CIC-Manager 를 통한 CIC 협상 후에 CIC 를 전달받아 각각의 Gateway 에 설치하게 된다. 결국 상호 호환성 있는 IPsec VPN 통신을 위한 CIC tunnel 이 생성된다.

3. 결 론

급속한 인터넷의 보급과 더불어 기업에서도 Intranet, Extranet, Remote Access 등의 방법으로 기업내부의 네트웍과 기업외부의 네트웍을 안전하게 연결하는 방법을 모색하게 되었다. 이런 방법을 제시한 것이 VPN 기술이다. VPN 을 위한 여러 구현 방법중에서 IPsec 을 이용한 VPN 이 가장 널리 사용되고 있다. IETF 에서는 IPsec 구현을 위한 표준화 문서를 제시하였지만 문서 해석 등의 어려움 등으로 인해 각각의 업체는 서로 상이한 VPN 구현을 하게 되었다. 상이한 구현에 의해 발생한 상호 호환성 문제가 VPN 의 대중화에 QoS 문제와 더불어 큰 장벽이 되었다. VPN 상호간 호환성 문제 해결은 VPN 대중화를 이루기 위해 시급히 해결되어야할 문제이다.

본 논문에서는 CIC 와 CIC-Manager 를 이용한 IPsec VPN 상호 호환성 해결 방안을 제시하였다. CIC-Manager 는 각 도메인에서 CIC 호환성 협상 및 분배를 담당한다. 서로 다른 VPN 구현 및 표준에 상관없이 CIC-Manager 를 통해 협의된 CIC 는 각 Gateway 에 분배 후 설치됨으로서 VPN 상호 호환성을 극복할 수 있다. 이 방법은 구현상의 상호 호환성 문제뿐만 아니라 여러 표준을 준수하는데서 발생할 수 있는 도메인간의 상호 호환성 문제 또한 해결 할 수 있다. 이를 위해 각 Vender 에서는 여러 표준의 CIC 를 구현해야 하며 CIC 협상을 위한 추가적인 Message 교환시간이 필요한 문제점이 있다. 이런 몇 가지 단점을 제외하면 제시한 방법은 위에서 제시한 상이한 구현과 여러 표준화 기구에 의해 발생할 수 있는 문제를 해결할 수 있는 좋은 해결책이 될 수 있을 것이다. 또한 VPN 의 효율적 관리를 위해 연구되고 있는 Policy 서버와 본 논문에 제시된 CIC 구조를 결합함으로서 각 도메인의 상이한 Policy 에 의한 상호 호환성 문제와 IPsec VPN 호환성을 함께 해결함으로서 보다 향상된 상호 호환성 구조를 제시할 수 있을 것이다. Policy 서버와의 연동 구조 및 CIC 협상을 위해 교환되는 메시지 형식은 향후에 추가적인 연구가 필요할 것이다.

4. 참고문헌

[1] Ruixi Yuan, W. Timothy Strayer, "Virtual Private Networks", Addison-Wesley, April 2001.

[2] http://ipsec-wit.antd.nist.gov/newindex.html, NIST

[3] http://www.vpnc.org/InteropProfiles/,VPN Consortium

[4] http://w4ww.icsalabs.com/html/communities/ipsec/index.shtml, ICSA Lab.

[5] http://www.ietf.org/html.charters/ipsec-charter.html

[6] William Yurcik, David Doss, "A Planning Framework for Implementing Virtual Private Networks", IEEE Communication Magazine, pp.41-44, June 2001

[7] Jeremy De Clercq, Oliver Paridaens, Alcatel, "Scalability Implications of Virtual Private Networks", IEEE Communication Magazine, pp.151-157, May 2002.

[8] Seung-Jin Baek, Moon-Sang Jeong, Jong-Tae park, "Policy-based Hybrid Management Architecture for IP-based VPN", Proceeding of the IEEE/IFIP Network Operations and Management Symposium, Honolulu, Hawaii, pp.989~990, April 2000.