IPSec과 L2TP를 이용한 VPN과 EDI 시스템의 연동

Interface of EDI System and VPN with IPSec and L2TP

최병훈* • 이건호**• 정병희***

* 시소닷넷 주식회사 보안사업부, choihuni@sysonet.co.kr
** 숭실대학교 산업·정보시스템공학과 부교수, ghlee@ssu.ac.kr
*** 숭실대학교 산업정·보시스템공학과 교수, bhchung@ssu.ac.kr

ABSTRACT

Electronic Data Interchange (EDI) between a number of companies goes on increasing on the internet. Although a conventional EDI system reduces business process efforts, time, resources, etc., important information is easily and frequently exposed by well trained hackers and crackers, which inflict a severe loss on the company and even put the company under a crisis. This study integrates the conventional EDI system and Virtual Private Net (VPN) to maximize an overall efficiency of speed and security in data transaction by the level of importance. The EDI system properly interfaced to IPSec and L2TP of VPN allows us to select two modes: the one focuses on a high speed with a low or a medium level security or the other does on a high level security with a low or a medium level speed. Both the company and the end users get a lot of tangible and intangible advantages by integrating the EDI system and VPN.

1.서론

네트워크를 이용한 기업간의 문서 및 정보 교환 으로 비용의 절감, 시간절약에 따른 내부 업무의 효율화 개선, 고객 서비스 향상, 거래당사자 간의 신뢰관계개선, 기업의 경쟁력의 강화 등의 효과와 이로 인한 매출액의 증가를 얻을 수 있다[4]. EDI(Electronic Data Interchange) 시스템은 컴퓨터 통신망을 통하여 상거래 및 은행 업무에 관련된 전자문서를 교환하는 과정에서 중요한 정보가 노출될 위험이 있다.

정보의 보호 서비스에 대한 요구는 증가되고 있으나 모 기업과 지사와 연동성에 있어서 많은 비용의 부담과 보안의 취약성으로 인하여 그 발전의 한계에 도달하고 있다.

EDI를 사용하기 위한 전용선 망의 사용빈도수에 비해서 높은 가격과 전용선 IP의 포화상태 임에도 통신사용수는 증가추세에 있다.

이에 대안으로 VPN(Virtual Private Network)과 IPV6가 있으나 아직 IPV6에 관련하여 안정적인 장비 및 실제 상용화 되어 있지 않기 때문에 VPN이 대안으로 많은 관심의 대상이 되고 있다.

EDI시스템의 적용에 대한 연구는 다양한 연구[1, 2, 3, 4]가 있었으나 EDI 시스템과 VPN 연동에 대한 실용적인 연구는 이루어지지 않았다. EDI와 VPN의 연동에 관해서는 이용의 가능성 제시하고 있으나 이에 대한 연구결과가 발표 되거나 사용단계에 있지 않다[10].

근래의 EDI 사용은 네트워크 통신망의 변화보다는 EDI 엔진 및 소프트웨어가 기존의 방식에서 xml을 이용한 xmlEDI의 방식을 사용하는 경우이다. 기존에 사용되고 있는 EDI의 방식보다는 안정성 및 보안성에는 보강되고 있으나 기존의 VAN(Value Aided Network)을 이용한 EDI방식을 모두 VAN과 xml을 이용한 방식으로 바꿈으로서 소요되는 시간과 안정화 되는데 시간이 소요되며, 보안에 취약한 단점이 있다[5].

이는 EDI 시스템이 보다 편리하고 안정적으로 발전은 하여야 하나 비용과 기술에 취약한 중소기업의 입장에서 보안의 강화와 데이터 전송속도의 융통성의 결여로 도입에 어려움이 있다.

따라서 본 연구에서는 기존의 IPV4에서 전용IP의 포화상태에 대한 하나의 해결책으로 보다 안정적이고 보안에 강력한 VPN과 EDI시스템의 연동 통하여 기존 방법들의 단점을 해소 하고자 한다.

보안에 취약한 기존 시스템을 보완하여 다음과 같이 시스템 설계하였다.

첫째, 기존에 사용하던 EDI 시스템의 분석을 통하여서 문서의 중요도를 파악하고 분석하였다. 문서의 중요도를 파악하므로 기존에 문서전송을 하기위한 소켓프로그램을 선택적으로 나눌 수 있는 방법을 제시하였다.

둘째, VPN장비의 IPSec와 L2TP를 이용하여 EDI시스템에서 전송되고자 하는 문서의 중요도를 파악한 후 선택적 프로토콜의 구분사용으로 신속성 및 보안성을 보다 효율적으로 제고하고자 한다.

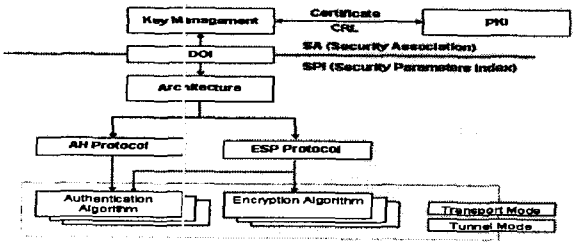
2. VPN과 IPSec

본 연구에서는 전통적인 EDI 방식과 VPN의 IPSec와 L2TP의 방식을 연동함으로써 관리가 용이하여 관리비용을 절감하고 기존의 네트워크 확장의 어려움을 해소하며 저 비용으로 서비스를 제공하고 정보의 보호와 업무에 따른 전송속도의 융통성을 부여하고자 한다.

IPSec은 IP 계층에서 보안 서비스를 제공하기 위한 IP 계층 보안 프로토콜과 키관리 프로토콜로 구성된다. 이 두 프로토콜은 서로 독립적으로 설계되어 있으며 SA(Security Association)를 매개로 하여 연결된다.

IP 보안표준은 IP 패킷의 발신지를 인증하고 패킷 내용이 불법으로 변조되었는지 확인하는 무결성 서비스를 제공하는 인증보안메커니즘(AH, Authentication Header)과 패킷의 데이터를 암호화함으로써 보안 서비스를 제공하는 암호화 보안 메커니즘(ESP, Encapsulated Security Payload)으로 구성되어 있다.

한편 키관리 메커니즘은 통신하는 양 호스트가 사용할 보안 메커니즘, 키 값, 키 유효기간 등 보안 연결 설정을 위해 필요한 내용을 협상하고 필요한 경우에 보안 연결을 해제한다[6].



<그림 1> IPSec의 구조

3. 시스템 설계

3.1 EDI 시스템 구성

EDI 시스템은 네트워크를 하여 EDI데이터를 전송할 수 있는 소켓부분과 VPN으로 부터 받은 EDI데이터를 처리할 수 있는 엔진부분과 EDI문서가 각 디렉토리별로 쌓이거나 폐기 될 수 있는 부분이 있다

데이터베이스에서 읽은 EDI문서의 중요도를 파악하는데 이때 반드시 송신측과 수신측의 IP Address를 알아 놓고 이 모든 송수신 측의 주소 또한 데이터베이스화 해놓아야만 생성된 소켓이 어느 IP address의 소켓을 생성할 것인가를 판단하여 보다 정확하고 데이터 손실률이 적은 회선에 시간적인 차이를 두고 보내줄 수 있게 된다.

3.2 VPN 망 시스템

3.2.1 L2TP(Layer Two Tunneling Protocol) 구성

VPN장비로 전송되어진 EDI문서는 트랜잭션ID의 값이 0인지 1인지를 확인한 후 IPSec와 L2TP 전송방식을 택한 후 상대편의 VPN장비로 EDI문서를 전송하게 된다.

L2TP 보안 프로토콜은 키 관리 측면에서 확장 가능하여야 한다. L2TP 보안 프로토콜은 제어 패킷들에 대해 인증, 무결성, 그리고 재사용 방지 기능을 제공하며 제어 패킷을 보호할 수 있어야 한다.

데이터 패킷에 대해서는 무결성과 재사용 방지 기능이 제공되어야 하며 암호 기능도 제공할 수 있어야 한다. 또한 L2TP 보안 프로토콜은 키 관리 기능과 이의 확장성을 갖고 있어야 한다.[7]

L2TP는 Microsoft사의 PPTP와 Cisco사의 L2F가 하나의 프로토콜로 함께 동작할 수 있도록 동의해서 표준화를 위해 IETF에 제시한 프로토콜이다.

L2F의 배경로는 layer2의 전송 패킷을 위한 암호화헤더를 정의하고, L2F 터널링은 IP에 속해있지 않고 다른 물리적 방식으로 동작 할 수 있게 한다.

L2TP는 터널이 한개 이상의 연결을 지원하도록 한다. 사용자에 대한 인증된 정보는 첫번째, 터널을 설치하기에 앞서 ISP에 대해 인증하고, 두번째, 연결이 공통의 VPN장비에서 설치될 때 2 level이 있다.

PPTP처럼 인터넷을 통해 목적지에 tunnel될 수 있는 dialup access를 제공하기 위해 PPP의 기능을 이용한다[8].

3.2.2 IPSec 구성

IPSec(Internet Protocol Security)방식을 사용하여 전송되는 EDI문서는 AH 또는 ESP를 요구하게 된다. AH 패킷과 ESP 패킷 처리순서는 다음과 같다.

-AH 패킷 처리순서

AH의 outbound 패킷 처리의 순서는 SA 검색을 한다.

(가) AH를 처리하기 위한 SA를 찾는다.

(나) ICV 계산을 한다.

(다) Inbound 패킷 처리의 순서는 먼저 재조립되는 부분(Reassembly)으로 AH를 처리하기 전에 IP 절단 및 분열된 패킷인 경우에 패킷을 재조립한다.

-ESP 패킷 처리순서

ESP의 Outbound 패킷 처리의 순서는 SA 검색이 있다.

(가) ESP를 처리하기 위한 SA를 찾는다.

(나) 정보를 ESP Payload내에 암호화 하고 필요한 자료의 처음과 ESP Trailer를 추가한 후 결과를 암호화한다.

(다) ESP Header와 ESP Payload에 대한 ICV를 계산한다.

SA 검색은 수신된 IP 패킷의 목적지 IP 주소와 SPI(Security Parameters Index)값을 이용하여 사용할 SA를 결정한다. 만약 사용할 SA가 없는 경우에는 IP 패킷을 버리게 된다.

AH ESP에서 받은 패킷은 ISAKMP(인터넷 보안키 관리 메커니즘, Internet Security Association and Key Management Protocol)로 패킷 처리를 하게 된다.

키 관리 메커니즘에 사용되는 ISAKMP 패킷의 송수신 구조를 설명한다. ISAKMP 프로토콜은 UDP(User Datagram Protocol) 500번 포트를 사용하며, 보안정책에 따른 제어 없이 직접 보안 호스트 체크를 통해 로컬 처리할 패킷과 직접 통과시킬 패킷을 구분한다.

ISAKMP의 Outbound 패킷 처리는 다음과 같다,

ISAKMP 모듈에서 전송하는 패킷은 소켓(socket) API를 사용하지 않고 가공되지 않은 소켓을 사용하며, 보안정책에 따른 필터링 모듈의 제어를 받지 않고 바로 전송한다. 보안호스트 체크는 ipsec_filter에서 이미 된 상태이다.

Inbound 패킷 처리는 수신된 ISAKMP 패킷은 필터링 모듈에 의해 바로 IP 커널에 전달된다. 단, 보안정책의 제어없이 보안호스트 체크(isakmp_filter)만으로 ISAKMP 모듈에서 처리할 패킷과 바이패스해야 할 패킷이 결정된다. 단, Center NAT (Network Address Translation) 기능이 작동된 경우는 바로 바이패스하지 않고 보안정책에 따라 처리한다. 수신 ISAKMP(인터넷 보안키 관리 메커니즘) 패킷 중 보안호스트로 오는 패킷은 VPN보안장비가 직접 처리해야 하므로, Inbound ISAKMP 패킷에 대한 보안호스트 체크가 필요하다.

구분	L2TP	IPSec
장점	-단순함(Simplicity) -End-To-End 압축 및 암호화 -시간적 절약	- 확장성 우수 - 보안성 우수 - 신뢰성 우수
단점	-확장성, 보안성, 신뢰성 미비 -PPP Payload 형식만 지원	-보안화 암호화에 따른 시간소요

<표 1> L2TP와 IPSec의 장단점

4. 기능설계

대부분의 EDI업무는 전문과 같이 중요도가 높은 것과 통보 및 조회 등의 중요도가 낮은 업무가 있다. 업무의 중요도 보다 조회 등 빠른 시간적인 작업을 요구할 경우에 암호화, 인증화의 과정을 거쳐는 시간의 지체보다는 빠른 대응이 업무의 효율성을 높일 수 있다.

이때 중요도가 높고 낮음을 판단할 때는 양사간의 전문 포멧을 추가 또는 수정 시에 내용 등의 동의를 얻어서 나누어 중요도에 따라서 전문의 공통부 부분을 데이터베이스화 한다.

전문의 발송 시 전문의 헤더부에 따라서 IPSec 전송방식으로 보낼 것인지 L2TP방식으로 전송할 것 인지를 판단, 시간과 보안적인 측면 두가지로 구분한다.

또한 EDI문서의 트랜잭션ID의 값이 1이면 조회 등 중요도가 낮은 문서로 인식하여 L2TP기반의 구성된 터널로 인하여 수신측의 VPN장비로 데이터를 전송하게 된다. 이때 트랜잭션ID의 값에 0 또는 1의 값이 함께 전송되어지는데 TCP/IP기반의 소켓 프로그램에서 부과가 된다.

5. 구현 및 분석평가

5.1 시스템 분석

100개의 EDI 데이터를 전송, 데이터베이스에서 EDI시스템으로의 TCP소켓 접속가능 여부와 전송되어진 EDI데이터의 전송시간, 실패확률, 패킷 등을 분석하였다.

EDI데이터의 중요도를 데이터베이스화하여 각 EDI전송 PC에서 VPN보안장비로의 접속여부를 확인, 이때 L2TP를 이용한 방식과 IPSec의 전송방식중 시간과 보안의 중요도를 파악한다. 이때 전송이 실패된 EDI데이터의 패킷을 캡쳐하여 분석한 후 패킷의 차이점을 비교하였다.

5.2 소켓접속 결과

EDI전송 PC에서 VPN보안장비로의 접속여부는 데이터를 전송하기 전 접속이 한번 이루어진 상태에서 EDI데이터를 전송하므로 무리 없이 접속되었다.

기존의 전용선 사용비용을 경감하여 EDI데이터의 처리시간의 이점을 얻을 수 있다.

전용선에 비해 상대적으로 저렴한 사용료임에도 회선의 품질 및 안정성에 대해서는 기업전용선에 전혀 뒤떨어지지 않기 때문에 VPN 전용선 사용은 증가추세에 있다. 특히 한국의 경우 2003년 중반 이후에 400개 중소, 벤처기업의 패턴을 분석해 보면 200 여 회사가 기존의 전용선 방식에서 VPN 전용선으로 전환하여 사용하고 있다[9].

하지만 자료나 문서가 EDI 시스템을 벗어나 네트워크 통신망을 통과하는 과정에서는 보안의 많은 문제점이 있다.

5.3 기존의 시스템과의 비교평가

기존의 EDI 전송방식과의 차이점은 비용 부분에서 현저히 절감 할 수 있다. 또한 전송오류가 발생할 시에는 기존의 방식으로는 X.25회선에서만 패킷을 볼 수 있었으나 이 또한 별도의 분석 장비를 가지고 확인할 수 있으므로 비효율적이며 비용 또한 이중으로 사용됨을 볼 수 있

다. 이에 VPN 보안호스트를 사용하므로 자체적으로 분석과 원인을 할 수 있으므로 보다 빠르고 안정적인 대책을 세울 수 있다.

네트워크 상황에서 기존방식으로는 TCP/IP 및 X.25, SNA방식을 함께 사용하고 있으며 VAN업체 통하여 전송되어지므로 이에 따른 비용 또한 적지 않게 들어가고 있다.

이에 VPN호스트를 사용하므로 TCP/IP방식의 ADSL회선을 사용가능하므로 X.25, SNA, VAN업체에 들어가는 비용을 ADSL사용료만 지급하므로 최대한 줄일 수 있음을 나타내고 있다.

본 연구의 L2TP를 이용하여 데이터를 전송 시에는 전송시간을 단축 할 수 있다. 즉, 단순 계좌조회 및 데이터의 처리결과 조회 등은 EDI문서의 중요도가 낮으므로 L2TP통신방법을 이용하여 보냄으로 수신측에서 보다 신속한 결과를 받는 것이 효율적일 것이다.

IPSec를 이용한 EDI데이터 전송방식은 신속함 보다는 안전한 방식으로 암호화와 인증화의 과정을 거치도록 한다.

단위 : 분

구 분		기 존 방 식		본 연구
		VAN EDI방식	기존 VPN EDI	
데이터 전송	1	37	38	37
	2	37	39	38
	3	36	38	36
	4	37	37	36
	5	37	38	36
	6	38	38	36
	7	36	38	35

<표 2> 데이터 전송시간 비교

즉, 계좌이체 및 비밀번호 등과 같은 중요한 데이터의 문서는 IPSec통신을 이용하여 시간은 다소 소요되지만 보다 안전한 암호화와 인증화 과정을 거치므로 안전한 데이터 전송이 이루어지고 있다.

공중망의 보안성을 VPN을 통하여 획득함으로서 무역 및 은행업무 등 네트워크를 통해서 이루어지는 많은 자료의 공유 및 전송에 관련된 직, 간접적인 비용절감 효과를 기대 할 수 있다.

6. 결론

인터넷은 개방성과 정보 공유라는 강점을 가지고 있는 반면에, 정보의 유출, 파괴, 변조 등의 각종 해킹과 바이러스 침해에 취약한 구조를 가지고 있다. 이에 대한 안전성과 신뢰성을 제공하는 정보 보호 시스템이 인터넷 기반의 정보 인프라 구축의 필수 요소가 되고 있다.

이에 따라 문서와 데이터는 그 중요도에 따라 속도 및 보안의 정도가 결정되어야 한다. 보안에 철저해야 하는 문서는 데이터를 무조건 빠르게 전송하기 보다는 보안에 치중하여야 하고 빨리 처리해야 하는 문서이면 보안적인 면보다는 속도를 우선적으로 처리하여야 할 것이다.

따라서 전송속도 및 보안은 상황에 따라 꼭 필요한 부분의 네트워크 정보를 적절히 사용한다면 보다 효율적일 것이다.

이에 EDI 시스템에서 VPN장비로 상황에 따라 적절히 접속하여 보안에 관련된 정책 등을 효율적으로 처리함으로서 처리속도와 보안에서 개선될 수 있다.

참고문헌

[1] 조홍익, "XML기술에 의한 EDI 및 ERP사이의 인터페이스 구현", 건국대학교 정보통신대학원 석사학위논문, 2003.

[2] 김우현, "전자서명 알고리즘을 적용한 암호화된 XML/EDI 구현", 대구대학교 대학원 석사학위논문, 2000.

[3] Reija Korhonen, Airi Salminen, "Visualization of EDI messages: facing the problems in the use of XML", ACM Press, 2003.

[4] Karen Ketler, John Willems, Vicki Hampton, "The EDI implementation decision: a small business perspective", ACM Press, 1997.

[5] 이진화, "무역 EDI의 활용 현황 및 효율성 제고방안", 전북대학교 대학원석사학위논문, 2002.

[6] 퓨처 시스템"VPN보호기술 세미나", 퓨처 시스템, 2004.

[7] Townsley, A,Valencia, A,Rubens, G,Pall, G,Zorn, and Palter, "Layer Two Tunneling Protocol L2TP", Network Working Group, RFC2661, August 1999.

[8] 고은주, "VPN을 위한 IPSec의 기밀성 및 인증모듈구현", 호남대학교 대학원 석사학위논문, 2001.

[9] K. Muthukrishnan, "A core MPLS IP VPN architecture", Work in progress, RFC 2917, July 2001.

[10] Turban, Efraim "Introduction to E-Commerce", Prentice Hall, pp.273-280, August 2002.