IPSec과 IMA를 이용한 인터넷과 내부 망 통합에 관한 연구

조 용 건*

요 약

이 연구는 인터넷 망과 조직이 자체보안을 위해 별도로 구축한 내부 망을 하나의 망으로 합쳐서 통합 체계를 구축하여 경제적이며 안전하게 인터넷과 내부 응용 서비스를 사용하는 방안을 제시하고자 한다. 기존에 일부에서 사용되고 있는 망 전환 장치는 기계적인 한계가 있으며 인터넷과 내부 망을 위한 별도의 네트워크를 구성해야 하는 문제점 때문에 연동성과 보안의 목표인 인증 및 암호화에 대한 대책이 부족하고 체계 구축 시 많은 비용이 소요되는 단점이 있다. 이에 ATM Forum 역 다중화 기술과 IPSec을 적용하여 네트워크 성능을 향상하고 구축비용을 절감하며 신뢰성 있는 이중 방어 체계의 구축 방안을 제안하고자 한다. 아울러 망 관리 기술을 이용한 Scanning 공격 기술과 SNMP, Spooler Port 등의 취약점을 집중 분석한 후 본 논문에서 제안한 이중 방어 체계 기반의 대응 방안을 제시하였다.

Study On Integrating Internet and Intranet based on IPSec and IMA Technology

Yong Gun Cho*

ABSTRACT

This research is on the study of integrating internet and intranet that was built for their own enterprise into one network system that promises a more economic and secure use. Compared to this system, the traditional network conversion device not only has its mechanical limits, but also requires a separate network set up. This raises both interoperability and security problems and results in a higher cost. Therefore, I propose dual defence system based on the inverse multiplexing of ATM Forum and IPSec to improve network ability and deliver enhanced system reliability while reducing cost. Furthermore, I also addressed some of the weaknesses of the Scanning Attacking Method, SNMP and Spooler Port and proposed counter measures that will deal with these weakness at the dual defence system.

Key words : TCP/IP, IP-SEC, IMA, FireWall

* 광운대학교 방위사업학과

1. 서 론

대부분의 경우 본사와 지사 간에 전용회선으로 연결하여 독자적으로 보호받는 내부 망을 구성하고 각 지사는 이 망을 통해 내부 응용 서비스를 제공 받고 있다. 이 때, 인터넷을 본사에 연결해서 각 지사에서도 내부 망을 통해 인터넷을 활용하고자 하는 요구가 있으나, 인터넷과 내부 망을 통합할 경우 보안의 취약성으로 인하여 많은 비용을 감수하더라도 별도의 망을 구축하거나, 별도의 망 전환 장치를 사용하게 된다.

인터넷을 통한 보안의 위협 요소에 대한 대책으로 통상적인 동일한 TCP/IP 기반의 망 전환 장치를 사용하기 보다는, 다양한 공격을 효과적으로 방어할 수 있는 적절한 보안 대책은 IPSec(Internet Protocol Security) 기반의 가상사설망(Virtual Private Network)과 인터넷 방화벽(FireWall)을 중심으로 하는 이중 방어 체계를 구축하는 것이 보안성을 높이고 경제적임을 보이고자 한다. 또한, 인터넷과 내부망 통합시 비용을 절감하기 위해 기존의 내부망 네트워크 자원을 사용해 인터넷을 활용하기 위한 방법으로 이중 방어 체계 하에서 인터넷용 착탈식 하드디스크의 사용을 제시하고, 네트워크 성능을 고려하여 지사에서 고속으로 인터넷에 접속하고자 하는 사용자 요구에 경제적으로 부합할 수 있는 ATM 역 다중화 방법의 적용을 제시한다.

본 논문에서 제안한 이중 방어 체계의 우수함을 보이기 위하여 내부 망에 존재하는 보안 위협 중에서 IPSec 보안 정책을 적용하기 어려운 ICMP와 TCP/IP 상의 SNMP 및 스풀러 포트 등의 세 가지 프로토콜에 대한 취약점을 분석하고, 제안된 이중 방어 체계 하에서 이를 통한 공격뿐만 아니라 다양한 보안 위협으로부터 내부 망을 효과적으로 보호할 수 있는 대책을 보이고자 한다.

2. 기존 방법을 이용한 인터넷과 내부망 통합의 문제점 분석

인터넷과 내부 망 통합에 사용되는 방법은 LAN의 경우 통상적으로 망 전환 장치가 사용되고 있다. 그러나, 망 전환 장치는 인터넷을 통한 보안 위협에 대한 대책으로 잘못 인식되고 있고 PC 구매 비용의 절감 효과도 과대 평가되고 있다. 또한, WAN의 경우 기존의 본사와 지사 간의 전용회선 상에서 ATM 또는 프레임 릴레이 다중화 기술이 사용되고 있으나 고속 접속에 대한 사용자 요구를 제대로 수용하지 못하고 있다.

2.1 망전환 장치를 이용한 통합

인터넷 PC를 따로 설치할 경우 사무 공간이 협소해 지고 경제적인 낭비를 초래하게 된다. 이 때, 망 전환 장치를 사용함으로써 인터넷 PC를 별도로 구매할 필요가 없어 구매 비용을 상당부분 절감할 수 있어서 여러 조직에서 사용하고 있는 실정이다.

망 전환 장치는 한 대의 PC로 인터넷과 내부 망을 물리적으로 분리하여 운용할 수 있는 장치로서, PC 한 대에 네트워크 인터페이스와 하드디스크를 각각 한 개 이상씩 추가하고 전자 계전기(Relay) 변환 방식의 전환 버튼에 의해 자동으로 망 전환 및 하드디스크 전환을 처리한다. 그러나 전자 계전기는 누설 전류에 의한 On/Off 동작 지연 등의 오동작 및 고장 발생 시 망 전환 및 하드디스크 전환이 올바르게 이루어지지 않을 수 있는 가능성이 있다. 또한, 여전히 인터넷을 위한 LAN과 내부 망을 위한 LAN을 별도로 설치해야 하는 근본적인 문제를 여전히 갖고 있어서 두 개의 망을 구성할 수밖에 없는 경제적인 취약점이 있다.

2.2 ATM 다중화 기술을 이용한 통합

필자가 근무했던 국방부에서는 백본망에 ATM

교환기를 도입하여 사용하고 있는데, 인터넷과 내부 망의 분리된 트래픽을 하나의 전송 선로를 통해 전송하기 위해 ATM 다중화 기술을 이용함으로써 회선 비용을 절감할 수 있다.

ATM은 연결형 채널을 통한 가상 회선 교환(Virtual Circuit Switching) 기술이며, 53바이트 고정 길이의 셀(Cell)을 비동기식, 즉 비주기적으로 각 채널에 할당하고 헤더의 레이블(Label)로 각 셀을 구분하는 레이블 다중화(Label Multiplexing)에 의해 다양한 대역폭과 다중 접속(Multiple Access) 기능을 제공한다. 또한, ATM은 프레임 릴레이 연동(Frame Relay over ATM) 및 전용회선 대행(Circuit Emulation) 서비스를 제공한다. 그러나 급격히 증가하고 있는 인터넷과 내부 망의 트래픽을 한 개의 전용 DS1/E1 또는 DS3 회선으로 다중화하는 것은 효율적이지 못하다.

3. 새로운 방법을 이용한 인터넷과 내부 망 통합 방안의 고찰

인터넷과 내부 망 통합에 있어서 고려되어야 할 요소는 다음 세 가지로 요약할 수 있다.

- 내부 망 트래픽을 안전하게 보호한다.
- 네트워크 자원을 공유하여 사용한다.
- 적절한 대역폭을 선택하여 사용한다.

첫 번째와 두 번째 고려사항을 만족시키기 위한 방법으로 이중 방어 체계를 제안한다. 이중 방어 체계는 IETF 표준 인터넷 보안 프로토콜(IPSec)과 인터넷 방화벽 기술을 연동하여 내부 망을 공용 망과 IPSec 기반의 내부 망으로 나눈다. 그리고 한 대의 PC에 인터넷용 착탈식 하드디스크를 추가하여 동일한 네트워크 인터페이스를 사용함으로써, 공용 망을 통해 인터넷에 접속할 수 있을 뿐만 아니라 공용 망을 통해 내부 망의 서버에 안전하게 접속할 수 있다. 또한, 공용 망의 프린터, 라우터 및 선로 등의 자원을 공유하여 사용할 수 있게 된다. 세 번째 고려사항은 ATM FORUM역 다중화 방법을 적용함으로써 충족할 수 있음을 보이고자 한다.

3.1 이중 방어 체계를 갖춘 망 통합

3.1.1 이중 방어 체계의 구성 요소

(1) IETF 표준 인터넷 보안 프로토콜

IPSec(Internet Protocol Security)은 IP계층에서 인증 및 암호화 보안 서비스를 제공함으로써 상위의 어떠한 프로토콜 또는 하위의 어떠한 매체라도 모두 동일하게 보호하며, 백그라운드 수행으로 사용자에 대한 영향을 보이지 않는 투명성(Transparency)을 제공하는 기술이다.

IPSec은 보안 정책(Security Policy)에 따른 패킷 필터링(Packet Filtering)과 보안 서비스를 제공하기 위한 AH(Authentication Header), ESP(Encapsulation Security Payload)의 두 가지 보안 프로토콜을 사용하는 커널 모드와, 안전한 키 관리를 위한 IKE(Internet Key Exchange) 키 교환 프로토콜을 사용하는 사용자 모드로 나뉘어 수행된다.

보안 프로토콜은 모두 인증 서비스를 제공한다. ESP는 암호화 서비스를 제공하며, Null 암호화로 인증 서비스만 제공할 수도 있다.

IKE는 SA(Security Association) 협상을 위한 ISAKMP(Internet Security Association and Key Management Protocol) 프레임워크에 Diffie-Hellman 기반의 Oakley Key Distribution Protocol을 결합한 표준 키 교환 프로토콜이다.

IPSec은 호스트와 게이트웨이(Gateway)에서 구현되며, 전송 모드(Transport Mode) 또는 터널 모드(Tunnel Mode)로 운영된다. 전송 모드, 터널 모드의 패킷 헤더 구조는 각각(IP, ESP, TCP, data), (IP, ESP, IP, TCP, data)와 같다. 터널 모드의, 바깥쪽 IP 헤더의 IP 주소는 IPSec 게이트웨이를 나타내며 안쪽 IP 헤더의 주소와는 다르게 되어 게이트웨이 사이에서 터널을 만들어 주게된다.

IKE는 UDP 500번 포트를 사용한다. 또한, ESP, AH는 IP헤더의 다음 헤더(Next Header) 필드 값이 각각 프로토콜 50번, 51번이며, ESP헤더의 다음 헤더(Next Header) 필드는 암호화되어 트래픽 분석이 어려우나 AH헤더는 공격자에게 보이게 된다.

(2) 인터넷 방화벽(FireWall)

방화벽은 내부 망과 인터넷 간 접근을 제한하는 구성 요소의 집합으로서, 패킷 필터링(Packet Filtering) 방식과 프락시(Proxy) 방식으로 크게 나뉘어 발전되어 왔다.

패킷 필터링 방식은 패킷 헤더 정보를 가지고 접근 통제를 하는 방식으로 패킷 변조에 대한 취약점이 있고, 프락시 방식은 특정 서비스를 사용자 또는 IP 주소별로 상세한 접근 통제를 하는 방식으로 속도가 느리다.

패킷 필터링 방식은 이러한 단점을 보강하여 상태 감시(Stateful Inspection) 방식으로 발전되었고, 이 방식은 허용된 패킷의 Communication-derived State, Application-derived State 및 Context Information 등을 조합한 후 동적으로 상태 테이블(State Table)에 저장하고 보안 규칙을 적용함으로써 패킷 변조에 효과적으로 대응할 수 있고 빠르게 처리할 수 있는 방식이다. 또한, 프락시 방식에는 SOCKS 범용 프락시를 사용하는 서킷 게이트웨이(Circuit Gateway)와 응용 게이트웨이(Application Gateway) 방식이 있다.

방화벽의 구조는 인터넷 접속점을 가지는 배스천 호스트(Bastion Host)와 스크린 즉, 패킷 필터 라우터의 결합된 형태에 따라 다음과 같이 세 가지 구조로 크게 구분된다.

첫째, 이중 네트워크 호스트(Dual-homed Host) 구조는 두 개 이상의 네트워크 인터페이스를 가지고 인터넷과 내부 망에 동시 접속되는 호스트를 중심으로 구축되고, 프락시 서비스를 제공하게 된다.

둘째, 스크린 호스트(Screened Host) 구조는 배스천 호스트를 내부 망에 두고 스크린 라우터의 패킷 필터링으로 오직 배스천 호스트 만을 접속하도록 설정된다. 이 구조는 프락시 서비스를 선택적으로 사용하는 유용성과 보다 더 나은 보안을 제공한다.

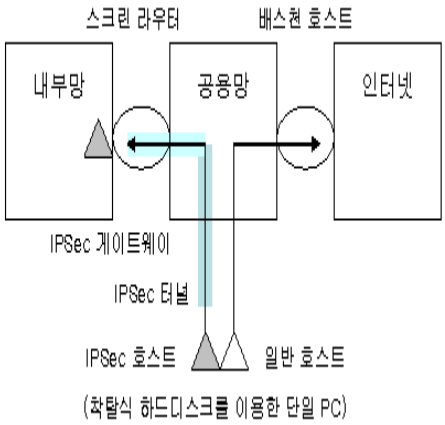
셋째, 스크린 서브넷(Screened Subnet) 구조는 스크린 호스트 구조의 변형으로 배스천 호스트에 대한 침입의 영향을 줄이기 위해 내부 망에 스크린 라우터를 설치하여 DMZ(De-Militarized Zone, 비무장지대)라고 불리우는 경계선 네트워크(Perimeter Network)를 추가함으로써 내부 망을 보다 더 격리시킨다. 그러나 방화벽은 방화벽을 통과하지 않는 트래픽이나 내부 사용자의 불법 행위에 대해서는 막을 수 없고, 실행 파일 형식의 바이러스의 침투에 대해서도 효과적으로 막지 못하는 문제점이 있다.

3.1.2 이중 방어 체계의 구조와 보안 정책

(1) 이중 방어 체계의 구조

(그림 1)과 같이 이중 방어 체계는 방화벽의 이중 네트워크 호스트와 스크린 서브넷의 혼합된 구조를 구축함으로써 인터넷, 경계선 네트워크 및 내부 네트워크로 구분하여 보안도를 증가시키고, 이들은 각각 주소 변환 기술인 NAT(Network Address Translation)와 정적 라우팅(Static Routing)으로 연결된다.

이 때, 경계선 네트워크는 네트워크 자원을 공유하여 사용하는 영역인 공용 망이 되고, 공용 망은 별도의 네트워크 구성없이 내부망과 인터넷 접속에 모두 이용된다. 또한, 공용 망을 지나는 내부망 트래픽은 IPSec 터널을 통하여 안전하게 전송된다. 따라서 기존의 망 전환 장치를 사용하는 것에 비해 보안도가 심대히 증가한 반면 구축비용은 대폭 감소된다.



(그림 1) 이중 방어 체계의 구조

때문에, 이러한 접근을 필요로 하는 어플리케이션들은 하부의 네트워크 카드(NIC)와 그 위에 놓이는 WIN32 어플리케이션 사이에 인터페이스로서 제공되는 가상 장치 드라이버(VxD)를 사용해야 한다. 이러한 기본 구조는 (그림 2)와 같다.

(2) 이중 방어 체계의 보안 정책

이중 방어 체계의 보안 정책은 거부가 기본값(Default Deny)으로 설정되고, 다음 표와 같이 허용되는 서비스를 결정하게 된다. 이 보안 정책은 네트워크 레벨에서 수행된다.

〈표 1〉 이중 방어 체계의 보안 정책

구 분	보안 요소	보안 정책
인터넷	배스천 호스트	Outgoing 접속 허용
		Outgoing UDP 500번 포트 거부 Outgoing 50번, 51번 프로토콜 거부
공용망	스크린 라우터	UDP 500번 포트 허용 50번, 51번 프로토콜 허용
내부망	IPSec 게이트웨이, 호스트	All IPSec Apply

스크린 라우터의 공용 망 접속점에서 수행되는 패킷 필터링에 의해 IPSec 트래픽 만을 허용함으로써 방화벽을 통과하지 않거나 공용 망을 통해 이루어지는 공격과 바이러스의 침투에 대해 효과적으로 방어할 수 있다.

또한, 방화벽에서 인터넷으로부터의 모든 접속을 허용하지 않고 공용 망을 추가하여 내부 망을 격리시킴으로써 내부 망의 트래픽을 볼 수 없게 하는 상호 보완 관계를 가진다.

3.2 ATM Forum 역 다중화 방법을 이용한 통합 방안

일반적으로 다중화(Multiplexing)는 다수의 저속 트래픽을 하나의 고속 링크로 전송하는 것을 의미하고 역 다중화(Inverse Multiplexing)는 상대적으로 고속의 트래픽을 다수의 저속 링크를 통해 보다 효율적으로 전송하는 것을 의미한다.

1997년에 ATM FORUM에서 정의한 표준 프로토콜인 IMA(Inverse Multiplexing for Asynchronous Transfer Mode)는 여러 개의 전용 DS1/E1 회선 등의 물리 링크를 묶어 큰 대역폭의 단일 ATM 링크 번들로 IMA 링크 그룹을 형성하고, 이 그룹 상에서 ATM(프레임 릴레이 연동, 전용회선 대행 포함) 인터페이스의 셀(Cell) 트래픽을 분배하여 전송한 후 원격지 종단에서 본래의 ATM 계층의 셀 스트림으로 결합하여 주는 기술이다.

IMA는 물리 계층에서 구현되며, ATM 계층과 IMA 간 상호작용을 담당하는 Transmission Convertgence Sublayer와 물리 링크 상의 IMA 프레임 전송을 위한 Physical Medium Dependent Sublayer로 나뉘어 진다.

인터넷과 내부 망을 통합할 경우 부가적인 대역폭 소요가 발생하게 된다. 이 때, 역 다중화 방법인 IMA 기술을 적용하여 DS1/E1과 DS3의 중간 대역폭을 선택하여 사용함으로써 저비용으로 고속 접속의 요구를 충족할 수 있다.

이 때, 전용회선 대행 인터페이스를 사용할 경우에는 고정 대역폭 적합을 위한 AAL1(ATM Adaptation Layer 1) 헤더 및 ATM 셀의 5Byte 헤더와 같은 부가적인 오버헤드(약 25%) 때문에 IMA 링크 그룹의 대역폭은 ATM 인터페이스 대역폭의 합보다 커야 한다.

따라서, 인터넷에 프레임 릴레이 연동 인터페이스, 내부 망에 전용회선 대행 인터페이스를 혼합하여 두 개 이상의 전용 E1 회선으로 IMA 프레임을 전송할 수 있다.

4. 제안된 이중 방어 체계의 보안 능력 분석

IPSec 보안 정책을 적용하기 어려운 ICMP, SNMP와 같은 망 관리 프로토콜과 공용 망의 네트워크 프린터를 공유하여 사용하기 위한 스풀러 서비스에 대해 살펴본 후, 본고에서 제안한 이중 방어 체계의 보안 능력을 분석해 본다.

4.1 ICMP를 사용하는 스캐닝 공격 기술

ICMP(Internet Control Message Protocol)는 포트를 가지지 않고 IP 헤더의 다음 헤더(Next Header) 필드 값이 프로토콜 1번이다. ICMP는 질의 또는 에러 형태(Type) 및 코드(Code) 메시지를 사용하여 네트워크와 서비스에 대한 스캐닝(Scanning)을 할 수 있다.

호스트 탐지를 위해 일부 조각이 빠진 단편화(Fragmentation)된 데이터그램을 전송하는 것은 열린 포트일 경우 ICMP Fragment Reassembly Time Exceeded에러 메시지가 되돌아오고, 닫힌 포트일 경우 UDP 패킷은 ICMP Port Unreachable에러 메시지가 되돌아오며 TCP handshake 패킷은 연결을 재설정하라는 TCP RST 패킷이 되돌아온다. 또한, 응답이 없을 경우에는 트래픽이 필터 된다는 것을 나타낸다.

네트워크 매핑을 위해 사용되는 Microsoft Windows 계열의 Tracert 유틸리티는 IP 헤더의 TTL(Time To Live) 필드 값을 하나씩 증가시키면서 한번에 세 개의 ICMP Echo 메시지를 목적지 호스트로 보낸다. 라우터는 패킷을 포워딩하기 전에 TTL 필드 값을 감소시키고, 이 값이 0 또는 그 이하일 경우에는 ICMP TTL exceeded in transit 에러 메시지를 되돌려 보낸다. 따라서 TTL 필드 값을 1부터 증가시키면서 패킷을 보냄으로써 목적지 호스트에 이르는 경로상의 모든 라우터를 알 수 있게 된다.

UNIX 계열의 Traceroute 유틸리티는 UDP 포트 33434번에서 대략 33633번까지 사용하며 목적지 포트 번호를 하나씩 증가시키면서 한번에 세 개의 UDP 패킷을 보내며, 닫힌 포트일 경우 ICMP Port Unreachable 에러 메시지를 되돌려 받는다. 또한, 열린 포트일 경우 UDP 포트는 Listening 상태에 있게 되어 응답이 없다.

운영체제 식별을 위해 잘못된 코드 값을 가진 ICMP 데이터그램을 사용할 경우 UNIX 계열은 그대로 응답하고 Microsoft Windows 계열은 올바른 코드 값으로 바꿔 응답한다.

4.2 TCP/IP 상의 SNMP 및 Spooler Port 취약점 분석

4.2.1 SNMP 취약점 분석

네트워크 관리 프로토콜인 SNMP(Simple Network Management Protocol)는 관리자(Manager)에서 각 에이전트(Agent)의 MIB(Management Information Base) 정보 분석 및 처리를 위해 사용되는 통신 프로토콜이다.

SNMP는 관리자와 에이전트 간의 통신 방법으로 폴링(Polling)과 트랩(Trap)을 사용하며, 폴링은 관리자가 에이전트의 UDP 161번 포트로 GetRequest, GetNextRequest 및 SetRequest PDU(Protocol

Data Unit) 형태의 요청 메시지를 전송하고 에이전트로부터 GetResponse PDU 형태의 응답 메시지을 받는 방식이다. 또한 트랩은 에이전트가 관리자의 UDP 162번 포트로 에이전트의 특정 이벤트를 알리는 Trap PDU 형태의 메시지를 전송하는 방식이다.

SNMPv1의 SMI(Structure of Management Information)는 Counter32(32-bit unsigned integer)를 사용하여 단지 IP 네트워크 주소만 나타낼 수 있도록 표준화 되어 IP 네트워크에서만 사용되며, Agent는 MIB 정보에 대한 Manager의 접근 권한을 확인하기 위해 평문(Cleartext)의 Community String을 사용하여 쉽게 노출될 수 있고, GetNextRequest 메시지를 통한 커다란 테이블 조회는 수많은 테이블 행의 검색과 패킷 전송이 반복되어 트래픽에 영향을 주게 된다.

SNMPv2의 SMI는 SNMPv1의 SMI를 포함하며, Counter64(64-bit unsigned integer)를 사용하여 계층적 네트워크 주소인 OSI NsapAddress(Network Service Access Point Address)를 나타냄으로써 다중프로토콜을 지원하고, 인증과 데이터 무결성을 위해 메시지 다이제스트(Message Digest) 알고리즘과 이의 수행에 필요한 인증키 분배에 공개키 알고리즘 및 재전송 공격(Replay Attack) 방지용 타임스탬프(Timestamp)를 사용하며, 메시지 암호화를 위해 DES(Data Encryption Standard) 알고리즘을 사용할 수 있다. 또한, 한번의 요청으로 여러 값들을 읽어와 불필요한 대역폭을 줄일 수 있는 GetBulkRequest PDU 형태와 Manager 간 통신을 통해 계층 및 분산 관리가 가능한 InformRequest PDU 형태가 정의되었다. 그러나 SNMPv1의 비정상적인 폴링과 트랩 메시지에 의해 시스템이 다운되거나, 기본적으로 브로드캐스팅 패킷을 모두 허용함으로써 접근 통제가 이루어지지 않을 수 있고, SNMPv2에서도 이와 유사한 문제가 발생할 수 있다는 것이 OUSPG(Oulu University Secure Programming Group)를 통해 밝혀졌다[7].

4.2.2 Spooler Port 취약점 분석

TCP 515번 스풀러 포트를 사용하는 네트워크를 통한 원격 인쇄 작업은 평문으로 전송된다. 또한, 네트워크 프린터를 사용하는 경우에는 스풀러 포트를 사용하여 PC로 접속하려는 트래픽은 발생하지 않을 것이다.

4.3 이중 방어 체계 기반의 대응 방안

이중 방어 체계는 공용망의 네트워크 자원을 안전하게 사용하기 위해 다음 표와 같은 보안 정책이 추가로 설정되며 거부가 기본값(Default Deny)이다.

〈표 2〉 이중 방어 체계의 보안 정책 확장

구 분	보안 요소	보안 정책
인터넷	배스천 호스트	Outgoing 1번 프로토콜 거부 Outgoing UDP 161번, 162번 목적 포트 거부 Outgoing TCP 515번 포트 거부
공용망	스크린 라우터	1번 프로토콜 허용
내부망	IPSec 게이트웨이, 호스트	1번 프로토콜 IPSec Bypass Outgoing TCP 515번 포트 IPSec Bypass

배스천 호스트에서는 ICMP 메시지들은 모두 거부 되어야 하나, 최소한 네트워크 테스트를 위한 도구인 Ping에 의해 사용되는 8번 형태의 Echo와 0번 형태의 Echo reply 메시지는 허용될 수 있다. 스크린 라우터와 IPSec 호스트에서는 IPSec 트래픽만을 허용하여 UDP 스캔 등의 공격이 필터되기 때문에 ICMP 메시지를 허용할 수 있다.

또한, TCP/IP 상의 SNMP 프로토콜을 이용하는 모든 통신은 금지되며, 스풀러 포트를 사용하여 PC로 접속하려는 트래픽은 모두 차단하여야 한다.

5. 결 론

본 논문에서는 이중 방어 체계를 구축하여 내부 망의 트래픽을 안전하게 보호하며, 별도의 네트워크 구성 없이도 내부 망을 통해 인터넷을 활용함으로써 비용을 절감하고, ATM Forum 역 다중화 방법을 적용하여 본사와 지사 간에 적절한 대역폭의 회선을 선택하여 통신함으로써 저비용으로 네트워크 성능을 향상시킬 수 있음을 보였다. 또한 네트워크 자원을 공유하여 자원 활용을 극대화하였고, 아울러 공유로 인한 취약점에 대해 분석해 보고 이를 이중 방어 체계 하에서 네트워크 레벨의 보안 정책 수행으로 적절히 해결할 수 있었음을 보였다.

하지만 IPSec 프로토콜과 이와 관계된 알고리즘들은 구현 자체에 의해 상당한 영향을 받게 된다. 예를 들어 운영체제 보안에서의 결점이나, 저질의 난수 발생 초기 값들은 IPSec에서 제공되는 보안이 저하될 수 있다. 더욱이 네트워크 보안은 여러 가지 요인들에 의해 영향을 받는다.

끝으로, 이중 방어 체계의 구성 요소인 IPSec을 IP 네트워크 뿐만 아니라 다른 모든 네트워크에 확장 적용할 수 있는 네트워크 계층의 다중 프로토콜 지원 방안에 대한 연구가 계속 이루어져야 할 것이다.

참 고 문 헌

[1] William Stallings, “Cryptography and Network Security 4’th edition”, Prentice Hall pp. 483-516, 2006.
[2] Nortel Networks, Inverse Multiplexing for ATM Guide.
[3] 조용건, 하경찬, 손민승, “인터넷 보안 프로토콜 기반 군 통합망 설계에 관한 연구”, 제5차 통신전자정보화 학술대회, 2001.
[4] 박호영외1명 역, “인터넷 방화벽 구축하기”, 한빛미디어, 2001.
[5] 정중기 역, “인터넷 프로토콜 핵심 가이드”, 한빛미디어, 2000.
[6] Ofir Arkin, “ICMP Usage in Scanning”, 2000.
[7] Allan Leinwand, Karen Fang Conroy, “Network Management”, Addison-Wesley.

조 용 건

1982년 육군사관학교 전자공학과(이학사)
1988년 국방대학교 전산학과(공학석사)
1998년 KAIST 전산학과(공학박사)
2007년~현재 광운대학교 방위사업학과 교수