통합 보안 관리 시스템 구축을 위한 효율적인 보안 솔루션 구조 설계

강민균*·한군희**·하경재***·김석수*

Efficient security solution structure design for enterprise security management system

Min-gyun Kang*·Kun-Hee Han*·Kyung-Jae*·HaSeok-soo Kim*

본 연구는 산업자원부 지역협력연구사업(R12-2003-004-03003-0)지원으로 수행되었음

요 약

과거 기업의 네트워크 보안 시스템은 단일보안솔루션이거나 여러 방식을 복합했지만 유기적인 연계가 되지못해 비효율적인 시스템이었다. 그러나 이제 통합보안관리 솔루션이등장하면서, 한층더 강한 보안 시스템을 구축하게 되었다. 통합보안관리 시스템(ESM)은 여러 가지 보안 솔루션을 관리 하기 편하게 하기 위하여 각 에이전트의 통합을 이루는 방식을 취한다. 즉, 기존 VPN, FireWall, IDS등의 시스템을 보안정책에 맞추어 통합적으로 연계, 관리를 이루는 시스템이다. ESM이 기존의 보안시스템에 비하여 더욱 발전된 보안시스템이기는 하나, 네트워크의 활용 및 기술의 발전 속도는 눈부신 속도로 증가 하고 있으며, 정보범죄 등의 역기능 또한 한층 그 수준을 높이고 있다. ESM 시스템도 많은 부분의 개선점이요구되고 있는데, 본 연구에서는 시스템 외부가 아닌 내부 보안에 대한 ESM의 취약점을 보완하고자 하였다. 보안정책의 기본이 되어지는 보안솔루션의 구조에 대해서 연구하여, 기존 보안시스템의 주 구성인 VPN, FireWall, IDS의 연계를 분석, 재구성하고 이를 통합하는 통합 보안 관리 시스템 자체의 보안을 강화 설계하였다. 가상의 침입자를 설정하여 Telnet Log analysys IDS를 기존의 ESM 시스템과 제안된 ESM시스템에 각각 적용한 접근 데이타를 비교, 분석하여 내부보안의 중요성과 제안된 시스템의 보안을 점검하였다.

ABSTRACT

Past corporation's network security system is single security solution, or mixed several ways, but there was inefficient system because doing not get into organic link. But, constructed more strong security system by ESM enterance on. ESM uses way to integrate of each agent to manage easily various kinds security solution. That is, it is system that connect system of existent VPN, FireWall, IDS and so on configurationally depending on security policy and manage. ESM is security system that is developed more than existent security system. But,practical use of network and the development speed of technology being increasing with the more faster speed, is heightening the level more as well as dysfunction of information crime and so on. Many improvements are required at ESM system, this research wished to make up for the weak-point in the ESM system about interior security. Studied on structure of security solution that is basis of security policy. VPN, FireWall, IDS's link that is main composition of existing security system analysis, reconstructed. And supplemented security of ESM system itself. Establish imaginary intrusion and comparative analysis access data that apply each Telnet Log analysys IDS existent ESM system and proposed ESM system comparative analysis. Confirm the importance of interior security and inspected security of proposed system.

키워드

ESM, 보안 솔루션, 통합관리, 기업 네트워크

* 한남대학교 멀티미디어학과
** 천안대학교 정보통신학부
*** 경남대학교 컴퓨터공학부

접수일자 : 2005. 2. 2

Ⅰ. 서 론

인터넷의 발전은 전자상거래(Electronic Commerce), 홈뱅킹(Home Banking) 등 네트워크를 이용한 서비스들이 다양하게 개발되어 사용자가 크게 증가하고, 인트라넷 구축을 통한 기업이나 교육기관 등 사회 전 분야에 걸쳐서 전자기록 및 자료 이용이 보편화됨에 따라 이를 악용하는 불건전 정보 유통 및 정보 범죄와 같은 정보화의 역기능 또한 크게 증가하고 있다[1].

정보범죄의 유형은 전산망 침해행위, 전자기록 위.변조, 각종 음란물 유통, 통신상의 명예훼손, 바이러스 제작 유포 등이 있으며, 특히 공공기관이나 기업체들이 외부에서 내부로부터 침입을 위주로 차단이 이루어 지고 있다[2].

현재 시스템의 보안을 침입차단시스템(Firewall)과 침입탐지시스템 IDS (Intrusion Detection System)가 대표적이다. 하지만 침입의 유형이 매우 다양화 되면서 침입에 대한 탐지 및 대응이 매우 복잡해지고 보안제품에 따라 기능 및 제어가 어려워지고 있다. 그로인해 다양한 보안솔루션에 대한 보안관리자들의 통합보안관리가 요구되었고 이러한 요구를 충족시키기 위하여 다양한 보안솔루션의 통합관리 시스템의 개발이 중요한 과제로 대두 되었다[3].

보안시스템의 통합관리에 있어서 보안정책의 수립은 매우 중요한 영역을 차지하고 있다. 하지만 국내에서는 보안정책 수립에 대한 연구조차도 매우 드물게 이루어지고 있다. 이러한 보안정책의 기본이 되어지는 보안 솔루션의 구조에 대하여 연구하였다. 이를 위하여 기업 네트워크에서 활용하는 기존 보안 시스템 가상사설망(VPN, virtual private network), 침입차단 시스템(Firewall System), 침입탐지시스템(IDS, Intrusion Detection System)에 대한 구성 분석을 하고 이를 통합하는 통합보안관리(ESM, Enterprise Security Management)의 구조에 대해 분석하고 이를 구현하는데 있어서 좀 더 안전하게 할 수 있는 통합보안관리 구조 설계에 대해서 연구하였다.

Ⅱ. 인터넷 공격 절차

인터넷 공격절차는 3단계로 설명할 수 있는 데 1단계인 정보수집 단계에서는 공격대상이 되는 호스트에 대한 정보와 호스트가 수행하고 있는 서비스에 대한 정보를 파악하여 최종 공격 대상을 찾아내는 공격의 첫 번째 단계이다. 이 단계에서는 시스템 및 서비스 탐지, OS탐지, 토플로지/방화벽 필터링 규칙 탐지, 네트워크 서버의 정보 수집 등을 통해 정보를 파악하는 것이다. 먼저 시스템 및 서비스 탐지란 공격대상 네트워크에 시스템이 있는지를 파악하기 위해 일반적으로 Ping을 이용한 공격도구를 사용한다. 또한 DNS 서버를 조회해 어떠한 시스템이 있는지를 파악할 수 있다. 시스템의 존재여부에 대한 정보수집이 끝나면, 각 시스템이 어떠한 서비스를 제공하고 있는지를 점검하기 위해 열려진 포트를 점검하는 것이고 OS탐지는 좀 더 세밀한 공격을 위해 해당 시스템의 OS 버전에 대한 정보 수집을 수행한다. 토폴로지/방화벽 필터링 규칙 탐지에서 네트워크 토폴로지는 호스트간의 거리를 나타내는 'HOP Count'를 이용해 알아낼 수 있으며 'Traceroute' 프로그램을 응용한 공격도구를 이용한다. 또한 방화벽에 의해 보호되는 시스템에 대한 정보 및 방화벽 자체의 필터링 규칙정보를 수집하는 방법도 존재한다. 네트워크 서버의 정보수집은 DNS, SNMP, Sendmail, NetBIOS 등 일반 네트워크 서버가 제공하는 정보를 수집하여 공격에 유용하게 사용하는 것이며, DNS의 경우 'Zone Transfer' 또는 일반적인 질의를 통해 등록된 호스트의 정보를 알 수 있으며, 잘못 설정된 SNMP는 네트워크의 토폴로지 및 각종 네트워크 정보를 알려준다. 또한 라우터를 통해 중요한 정보를 알아낼 수 있는 방법도 존재한다.[4,5] 이러한 정보 수집 단계를 거쳐 2단계인 시스템 침입단계를 할 수 있는데 시스템 침입단계는 실제 개별 시스템에 침입하는 단계로, 정보수집단계에서 수집한 정보를 바탕으로 가장 취약한 부분을 공격하게 된다.[4,5] 마지막 단계인 공격 전이 단계는 1차적인 시스템 침입이후에 일어나는 침입을 말하는데, 1차적인 침입으로부터 얻은 정보 및 추가 작업을 통해 시스템 침입을 확대하고 다른 시스템에 침입하는 단계이다[4,5].

Ⅲ. 기업 네트워크의 보안 시스템

3.1. 가상사설망 (VPN, virtual private network)

VPN(Virtual Private Network)을 정의하기에 앞서

"가상"과 "사설" 각각의 의미에 대해 살펴본다. 가상이란 물리적으로 독립된 망 자원보다는 논리적으로 구분된 망 자원을 사용하는 것을 의미한다. 사설이란 통신에 참가하지 않은 장비는 통신 내용을 알 수 없을 뿐 아니라 통신에 참가하는 장비조차 알 수 없어야 함을 뜻한다.

사설의 또 다른 의미는 "공중"의 반대개념으로서, 공중 장비는 공개적으로 액세스될 수 있지만 사설 장비는 액세스의 제한을 받는다. 상기의 용어로 구성된 VPN은, 사전에 정의된 기업 또는 사용자만이 기업망에 연결되도록 액세스를 제어하며, 공통의 통신미디어를 분할하여 구축하는 통신 환경이라고 정의할 수 있다

상기와 같이 VPN에 대한 다양한 정의가 존재하지만 간단히 요약하면, VPN은 인터넷과 같은 공중망 하부구조에서 만들어진 사설망이라 할수 있다[6,7].

현재 VPN은 경제성의 이유로 전용선, FR 또는ATM을 사용하기보다는 인터넷에서 VPN을 제공하는 방안이 활발히 연구되고 있다. IP 망에서 VPN을 제공하기 위해 제안된 방법은 크게 VLL(Virtual Leased Lines), VPDN(Virtual Private Dialup Network), VPRN(Virtual Private Routed Networks)와 VPLS(Virtual Private LAN Segment)의 4가지로 나눌 수 있다. VLL은 가장 간단한 형태로서, IP 터널에 의해 VPN 양끝 단이 전용선처럼 연결된다. VPDN은 원격 사용자가 전용선을 사용하지 않고, 로컬 ISP의 NAS (Network Access Server) 에게 전화를 걸면, ISP가 인터넷을 경유하여 기업의 VPN 서버와 사용자 사이에 터널을 생성하는 방식이다. VPRN은 라우티드 WAN을 에뮬레이션하는 것으로서, ISP라우터 사이에 메쉬 형태의 IP 터널을 구성한다. 각 VPN라우터는 트래픽을 원하는 목적지로 포워딩할 수 있도록, 가상 사이트(물리적으로 하나의 사이트는 여러 VPN에 속할 수 있음)마다 VPN을 위한 라우팅 정보인 FT(Forwarding Table)을 가져야 한다. LANE(LAN Emulation)이 ATM상에서 LAN segment를 에뮬레이션하는것처럼, VPLS는 IP상에서 LAN segment를 에뮬레이션하는 방법이다. VPLS는 네트워크 계층의 포워딩이 아니라 링크계층 브릿징을 사용한다는 것을 제외하면, 망 토폴로지와 운용면에 있어서 VPRN과 유사하다.

현재 기업에서 VPN을 제공하기 위해 가장 널리 사용하고 있는 기술은 VPDN이라 할 수 있다[6].

그림 1은 VPN구조도를 나타낸 것으로 인터넷과 PSTN(public switched telephone network)을 이용하여 VPN을 구축한 구조도 이다. 여기에서 인터넷만을 또는 PSTN만을 사용해도 무방하며 구축환경에 따라 달라질 수 있다. 또한 VPN만을 적용할 수도 있고 VPN과 침입차단시스템을 함께 운용할 수도 있다[7].

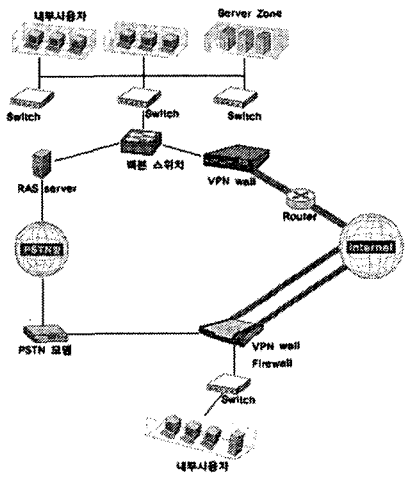

그림 1. VPN 구축 구조도
Fig. 1 VPN setup structure

3.2. 침입차단시스템 (Firewall System)

침입차단시스템의 원래의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는다는 뜻으로 이 의미를 인터넷에 적용한다면, 이는 네트워크의 보안 사고나 위협이 더 이상 확대되지 않도록 막고 격리하는 것이라고 할 수 있다. 이는 특히 어떤 기관의 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가하거나 인증된 트래픽만 허용하는 적극적인 방어대책이다. 침입차단시스템의 기본 목표는 네트워크 사용자에게 가능한 투명성을 보장하면서 위험지대를 줄이고자 하는 것이다. 침입차단시스템은 네트워크 게이트웨이 서버에 위치하고 있는 프로그램으로 다른 네트워크의 사용자들로부터 내부 사용자들의 자원을 보호하고 라우터프로그램과도 밀접하게 동작함으로써 모든 네트워크 패킷을 전달할 것인지 결정하기 위해 검사하여 여과시킨다. 침입차단시스템은 패킷 필터링방식과 프록시방식의 두 종류로 분류되며, 패킷필터링 방식은 네트워크를 통과하는 패킷

을 체크하여 허가되지 않은 패킷이 지나지 못하도록 하는 것이고, 프록시 방식은 외부와 내부 사이에 프록시서버를 설치하여 허가되지 않은 사용자의 접근을 막는 것이다. 침입차단시스템을 설치하면 네트워크 속도가 다소 떨어지게 되므로 속도 저하를 줄일 수 있는 대용량의 침입차단 시스템을 설치해야 한다[8,9].

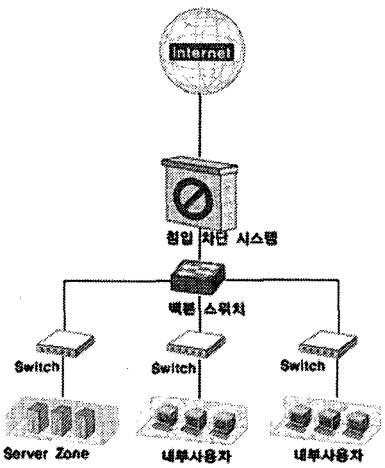

그림 2. 침입차단시스템 구축 구조도
Fig. 2 Firewall system setup structure

이러한 침입 차단 시스템은 5가지로 분류할 수 있는데, 먼저 패킷 필터링(Packet Filtering Firewall)방식은 네트워크 레벨의 시스템은 IP패킷의 발신지/수신지 주소와 포트에 의해 결정되며 단순한 라우터는 네트워크 레벨 침입차단시스템을 제공하는데, 이것은 패킷의 동작과 네트워크 경로를 판단해야하는 복잡한 규칙에 있어 판단하기 어렵고, 현재의 네트워크 레벨 침입차단 시스템은 매우 복잡해져서 접속이 허용된 상태와 데이터 내용 및 종류 등을 관리할 수 있다. 한 가지 구별되는 것은 네트워크 레벨 침입 차단 시스템이 라우터를 직접 제어할 수 있고 할당된 IP 블록을 정당하게 사용할 수 있도록 해주며 또한 빠르고 사용자에게 투명한 서비스를 보장한다. 응용 게이트웨이 방식(Application Gateway)은 2개의 네트워크 간에 직접적인 트래픽 차단 및 로그, Audit 기능 등이 지원되는 프락시(proxy)를 실행하는 기계를 말하며 프락시 응용은 침입차단시스템의 소프트웨어 부분이므로 많은 로그와 접근 제어 기능을 주는 것이 좋은 것이다. 응용레벨 침입차단시스템은 일반사용자에게 투명성이 없었으며 Client의 설정이 필요하였다. 최근의 응용레벨 침입탐지시스템은 투명성이 보장되고 상세한 Audit 보고와 네트워크 레벨 침입차단시스템보다 온전한 보안 모델을 제공한다. 특징은 Application layer에서 동작하고 해동 서비스별로 별도의 Gateway가 존재하며 패킷 필터링 및 패킷의 데이터 영역까지 제어가 가능한 방식이다. 서킷 게이트웨이 방식(Circuit Gateway)은 OSI네트워크 모델의 5계층에서 7계층 사이에 존재하며 어플리케이션 게이트웨이와는 달리 어느 어플리케이션도 이용할 수 있는 일반적인 프락시가 존재한다. 침입차단시스템을 통하여 내부네트워크로 접속하기 위해서는 먼저 클라이언트에 서킷프락시를 인식할 수 있는 수정된 클라이언트 프로그램이 필요하므로 수정된 클라이언트 프로그램이 설치되어있는 클라이언트만 circuit 형성이 가능한 단점이 있다. 상태검사 방식(Stateful Inspection) 기존 라우터에서 단일 패킷에 대한 정보 분석은 복잡한 서비스와 보다 높은 보안을 하기에 불충분하므로 새로운 접속요구 시 이것을 처리하기 위한 상태정보 분석이 필수적이다. 새로운 접속 시 과거 접속에 의해 파생된 정보들과 해당 어플리케이션에 의해 파생된 정보 분석은 새로운 접속에 대한 허용 및 거부에 대한 결정을 내리는 데 중요한 정보로 사용된다. 마지막으로 하이브리드 방식(Hybrid Type) 여러 유형의 방화벽들을 경우에 따라 복합적으로 구성할 수 있는 침입차단시스템으로 서비스 종류에 따라 사용자 편의성, 보안성 등을 고려한 기능을 선택적으로 부여할 수 있으나 서비스의 종류에 따라서 다양한 보안 정책을 부여함으로서 구축 및 관리하는데 어려움이 따를 수 있는 방식이다[10].

3.3. 침입탐지시스템 (Intrusion Detection system)

침입은 허가되지 않은 접근(unauthorized access)으로 컴퓨터 시스템의 보안요소를 침해하는 모든 행위를 말하며 이는 비밀번호 해킹을 통한 접근 및 실제적인 침입을 위한 포트 스캐닝(port scanning)등 그 종류는 다양하며 이러한 침입과 침입시도 등에 대해 보호하고자 하는 호스트나 네트워크에 대해 감시하고 발견 시 실시간 경고 및 대응하는 행위가 침입 탐지이다. 이 개념은 1980년 J.P Anderson에 의해 소개되었고 일반적인 침입탐지 절차는 정보수집 -> 정보가공 및 축약 -> 침입분석 및 탐지 -> 보고 및 조치로 이루어진다.

침입탐지시스템은 보호하고자 하는 시스템으로 부터 침입을 판단하기 위한 데이터를 수집하고 중복된 데이터나 쓸모없는 데이터를 필터링하고 탐지 기법을 사용해 침입을 탐지하고 그에 해당하는 응답을 하는 시스템으로 네트워크의 출입구에 위치하여 정해진 보안 정책에 따라 드나드는 패킷을 검사하여 규칙과 비교, 통과 여부를 결정하게 되는 시스템으로 침입차단 시스템과 다른 점이 있다면 침입탐지시스템은 네트워크를 출입하는 패킷을 포함하여 네트워크 내부에서 전달되는 모든 패킷을 검사한다. 그림 3은 침입탐지시스템을 구축 구조도이다.

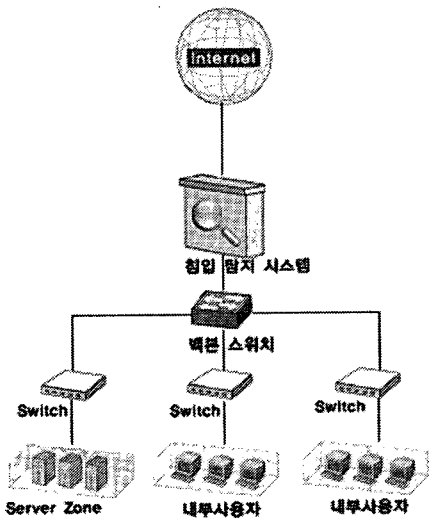

그림 3. 침입탐지시스템(IDS) 구축 구조도
Fig. 3 IDS setup structure

침입탐지시스템은 두 가지 정도로 분류할 수 있는데 첫 번째로 데이터 소스 기반 분류는 호스트 기반 침입탐지시스템과 네트워크 기반 침입탐지시스템이 있는데 먼저 호스트 기반 침입탐지시스템은 호스트 기반 IDS는 단일 호스트에서 침입을 탐지하는 것으로 그 호스트의 감시(audit) 기록이나 들어오는 패킷 등을 검사하여 침입을 탐지하며 호스트에 login 프로세스를 감시하고 root 사용자의 행동을 감시하며, 파일 시스템 감시들을 통해 침입을 발견하게 된다.

호스트 기반 IDS는 강력한 도구로 침입자 공격시 로그리스트를 통해 공격된 자료를 역 추적할 수 있고 네트워크 기반IDS 보다 탐지성이 월등하다. 호스트 기반 IDS의 단점으로는 우선 IDS를 타겟 호스트에 설치해야 하므로 해당 호스트의 성능이 저하되고 데이터를 얻기 위해 로깅 등에 대한 설정이 번거롭고 타겟 호스트가 있든 네트워크 내의 다른 호스트들이 공격을 당해도 알 수가 없다는 단점이 있으며 또한 호스트 기반 침입탐지시스템에는 여러개의 호스트에서 침입을 탐지하는 다중호스트 기반시스템도 존재한다. 다음으로 네트워크 기반 침입탐지시스템은 네트워크 기반 침입탐지시스템은 네트워크의 모든 트래픽에 대해 패킷을 수신하고 분석하여 침입을 발견하는 것을 자동으로 처리하며 특히 권한 없이 접근하거나 권한을 초과하는 접근에 대한 탐지에 뛰어나고 네트워크내의 호스트나 서버의 별도의 설정 없이 사용 가능하며 오류 발생 시에 큰 피해를 주지 않는다.

반면 서명 분석(signature analysis)이 많아 일반적인 알려진 공격을 탐지 하는데는 뛰어나나 복잡한 정보를 가진 위협요소에 대한 공격은 탐지하기가 어렵고 또한 분석을 통해 엄청난 양의 데이터 교환을 필요로 하며 이를 위해 분석을 위한 데이터의 축약 과정을 통해 필터링하므로 패킷 분석이 정확하고 침입탐지가 정확하다. 두 번째로 침입탐지 모델 기반의 분류는 비정상 행위 탐지(Anomaly Detection)와 오용 탐지(Misuse Detection)의 두 가지로 나누어 볼 수 있으며 비정상 행위 탐지는 알려지지 않은 새로운 공격기법도 탐지가 가능하다는 장점이 있지만 그에 앞서 정상적인 행위에 대한 프로파일을 구축해야 하기 때문에 다량의 데이터의 분석을 필요로 한다. 때문에 상대적으로 구현 비용이 큰 편이고 어렵기 때문에 상용 제품에서는 오용탐지를 주로 사용하고 비정상 행위 탐지는 보조하는 측면에서 많이 사용되고 있다[9].

3.4. 통합 보안 관리 시스템 개념

통합 보안관리 시스템(ESM : Enterprise Security Management)이란 침입 차단 시스템, 침입 탐지 시스템, 가상 사설망 등 이 기종 보안 솔루션을 중앙에서 통합관리하는 시스템으로 솔루션 간 상호 연동을 통해 전체 IT 시스템에 대한 보안 정책 수립이 가능한 시스템이다[11].

통합 보안 관리 기술 수준은 현재 자사 제품에 대한 모니터링 기능이 구현되어 있지만, 앞으로는 보안 프

로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전할 것이며, 수집된 자료를 분석하여 보안 사건에 대한 리포팅 기능과 함께 각 보안시스템에 대한 세부 정책관리 기능이 가능한 단계로 발전할 것으로 예상되고 있다. 통합 보안 관리를 위한 보안 표준 프로토콜로는 체크포인트사의 Firewall-1/VPN을 중심으로 컨텐츠 보안, 인증 및 권한 관리, 침입탐지시스템, 사건 분석 및 리포팅, 디렉토리 서버분야의 프레임워크 파트너를 구성하는 OPSEC과 IETF의 침입탐지시스템 상호연동 메시지 표준을 구축하고 있는 IDWG 워킹그룹이 대표적이다.

ESM은 워크플로우에 따라 사용자 및 정책 관리자와 취약성 및 위협 평가로 분류할 수 있다[3].

먼저 사용자 및 정책관리는 보안 또는 관리정책에 따라 사용자 및 Access 관리에 무게 중심을 둔 범주이다. 이 범주에는 인증이나 Single Sign-On의 기능을 포함하는 경우가 많고, 초기 ESM 모습이 많이 반영되어 보안적 측면보다는 시스템 관리적 측면의 성격이 강하다. 취약성 및 위협 평가 네트워크 및 시스템의 취약점, 위협 요소들을 분석하고 모니터링하는 관리도구의 형태를 취하며 제품에 따라 분석 또는 정책관리, 모니터링 및 경보(Alert) 등 어느 쪽에 초점을 두느냐에 따라 특성이 약간씩 다르다. 최근 ESM 기술의 주류를 이루고 있으며 기존 보안 제품들과의 통합(Integration)이 활발히 진행되는 범주이다.

ESM의 일반적인 구조는 논리적이 3계층 또는 4계층으로 나눌 수 있으며 3계층 구조는 Agent part, Manager part, Console part로 나눌 수 있다. 또한 4계층 구조는 Agent part Sub (Local) Manager part Master (Global) -Manager part Console로 분리된 구조로 나줄 수 있는데 각각의 계층이 하는 역할은 다음과 같다[3].

Ⅳ. 효율적인 통합 보안관리 시스템구축을 위한 보안 시스템 구조

보안 관리의 중요성이 강조되면서 점차 도입하는 기업이 늘고 있는 통합 보안 관리(ESM) 솔루션은 다양한 이기종 보안 솔루션을 중앙 집중 관리하고, 보안 솔루션 이벤트의 상호간 연관성 분석을 통해 오 탐지를 최소화하는 방향으로 발전하고 있다. 자원 낭비를 줄이고 효율적인 중앙 집중 관리를 가능하게 한다.

비즈니스의 활성화와 더불어 정보시스템은 내·외부자에 의해 노출되고 있다. 이에 따라 기업의 신뢰도와 서비스 가용성이 더불어 위협받고 있는 게 사실이다.

최근 정보통신부가 조사한 '정보보호 실태조사'에 따르면 국내 기관들의 정보보호 투자비율은 선진국에 비해 크게 부족하다. 특히 보안 솔루션의 도입 패턴을 두고 볼 때, 통합 보안 관리와 취약점 분석 등 침해 사고에 대한 예방 부분에 있어서는 그 준비가 매우 저조한 것으로 나타났다. 올해 초에 발생했던 1.25 인터넷 대란이나 복합적인 사이버 침해 사고들의 원인이 관리자가 시의 적절하게 대응하지 못했기 때문이라는 사실을 감안하면 심각한 문제가 아닐 수 없다.

하지만 현실적으로 각 보안 솔루션들을 운영하면서 상호연관성 분석을 통해 이상 징후를 찾아낼 수 있는 수준의 정보보호 전담조직 및 전문인력을 갖추기란 쉽지 않다. 방화벽, 침입탐지시스템(IDS), 가상사설망(VPN), 안티 바이러스와 같은 다양하고 전문화된 보안 솔루션의 도입은 증가하는 반면, 보안 솔루션에 대한 전문지식 보유 인력은 여전히 부족하기 때문이다. 그렇다고 보안만 전담하는 관리자를 두면 사전 방지 및 대응 조치가 가능한 것도 아니다. 각 보안 솔루션이 처리하는 방대한 양의 보안 이벤트와 분석 작업은 결코 수작업으로 처리할 성질의 것이 아니다.

또한 기업의 보안 관리자들이 행하는 단순하고 반복적인 업무(모니터링/로그 분석, 보고서 산출)의 자동화로 정보보호정책 및 지침 수립 등의 중요도 높은 업무에 집중할 수 있게 도와 기업의 비즈니스 연속성을 확보한다.[12]

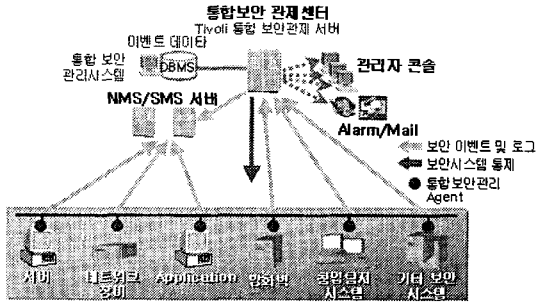

그림 4. 통합보안관리시스템 구조도
Fig. 4 ESM structure

하지만 이러한 통합 보안 시스템을 보면 그림 4와 같이 트리 구조를 이루고 있다. 이 구조를 볼 때 앞에서 말한 것과 같이 내외부적으로 보안을 이루어야 하는데 있어서 현재 구축되어지는 통합 보안 시스템은 외부적으로는 기업에 맞는(네트워크 속도, 보안의 중요도) 보안 정책을 수립할 수 있지만 내부적으로는 상당한 위험에 노출 되어져 있다. 이러한 내부적 노출을 방지하기 위하여 내부 서버에 한 번 더 보안 시스템을 구축하는 구조를 이루어야 한다. 외부적인 침입에 의해서만 보안이 철저하고 내부 침입에 대비하지 않는다면 기업 내 구성원의 해킹이나 구성원의 사소한 실수로 인하여 구성원 컴퓨터가 노출이 되어 진다면 외부적으로 철저히 보안을 이루어도 무용지물이 된다. 이를 구조도로 표현한다면 다음과 같은 구조를 형성할 것이다.

그림 5에서 기업에 맞는 보안정책에 따라 선택적으로 VPN, 침입탐지시스템, 침입차단 시스템중 선택을 하거나 내부적으로 침입탐지시스템 또는 침입차단시스템을 필요에 따라 선택을 하여 구축을 할 수는 있지만 ESM agent를 기점으로 하여 ESM agent 안의 시스템은 모두 구축을 하는 것이 내외부적으로 보안에 안전하다는 것을 알 수 있다.

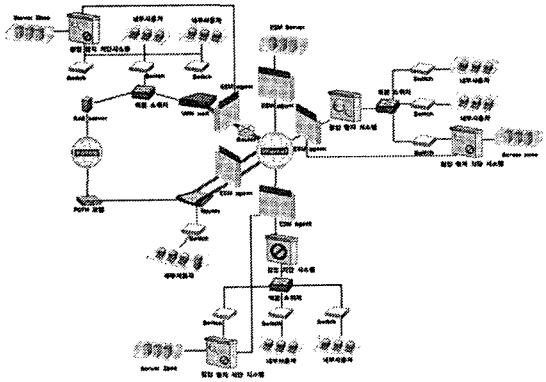

그림 5. 제안된 통합보안관리 시스템 구축 구조도
Fig. 5 ESM structure to be proposed

이 시스템에 있어서 보안에 대한 안정성 평가는 사용하는 보안 시스템과 통합 보안 관리에 따른 보안 정책에 따라 달라질 것이다. 이를 확인하기 위하여 침입을 탐지할 수 있는 로그 분석과 탐지된 서버를 차단하는 Telnet Log analysis IDS를 기본 통합보안관리 시스템 방식으로 설치한 시스템 A와 제안된 통합보안관리 시스템으로 구축한 시스템 B를 텔넷을 이용한 테스트를 통하여 다음과 같은 데이터를 얻었다.

표 1. 시스템 별 접근 결과 데이터
Table. 1 access data to accrodingly system

A 시스템		B 시스템	
ID	Telnet log	ID	Telnet log
total	158	total	158
root	28	root	45
test1	23	test1	20
test2	31	test2	35
test3	17	test3	23
test4	13	test4	14
test5	20	test5	21

표 1. 은 이 두 시스템을 테스트하기 위하여 시도한 접근 ID별 접근 결과이다. 이러한 데이터를 기반으로 다음과 같은 그래프를 작성하였다.

그림 6은 표 1.의 A 시스템의 데이터를 토대로 실시한 결과로써 이 그래프에서 lose 데이터가 상당히 많은 것을 알 수 있다. 이 lose 데이터는 시스템 인트라넷 안에서 테스트를 한 데이터로 A시스템에서는 검출이 불가능한 데이터이다.

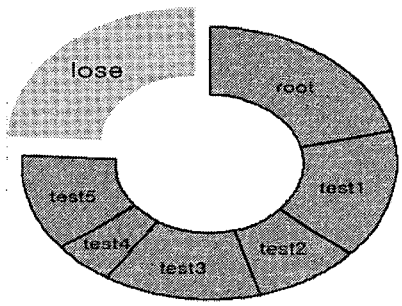

그림 6. A 시스템 처리 결과
Fig. 6 A system process result

그림 7은 Telnet Log analysis IDS를 제안된 통합 보안관리 시스템에 접목시킨 후 표 1. 의 B 시스템 접근 데이터를 통한 결과를 그래프로 표현한 그림이다. 이 그림은 손실된 데이터가 없고 내·외부적으로 탐지한 데이터를 표시하고 있다.

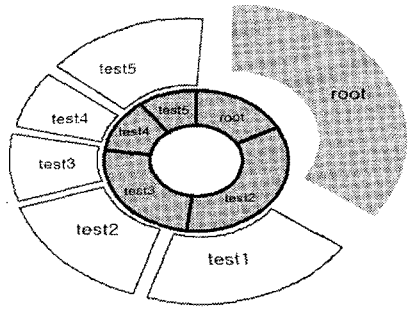

그림 7. B 시스템 처리 결과
Fig 7. B system process result

V. 결 론

정보화 사회로의 발달로 인간들이 만들어낸 인터넷은 인간들의 삶에 편리함과 즐거움을 제공하지만 다른 한편으로는 악의적 마음을 가진 사람들 혹은 호기심을 가진 사람들에 의해 많은 사람에게 피해를 주고 있으며 그 피해 또한 계속 증가하고 있다.

본 논문에서는 침입차단시스템에서 침입탐지시스템을 거쳐 통합 보안 관리시스템 구조로 발전해 나가는 보안 시스템에 대하여 발전 과정과 발전 방향을 분석하였으며 보안 시스템의 가장 근본적인 목표인 내외부적 보안을 강화하고 보안 시스템 구축을 최종점인 통합 보안 관리 시스템 구축에 있어서 효율적이며 기업에게 맞는 어떠한 보안정책에도 적용할 수 있는 보안 시스템 체계 구조도를 제시하였다. 향후 침입차단방법은 급격히 발전하는 해킹 및 바이러스에 대해 실시간 차단 및 침입정보의 철저한 분석으로 비슷한 유형의 패킷이나 침입에 대해 정보를 미리 파악하여 침입을 차단할 수 있어야 하며 대용량 데이터 처리 시 네트워크속도가 현저히 저하되지 않도록 트래픽양을 분산시킬 수 있는 침입차단 방법을 구성해야 할 것이다. 그러나 보안 시스템의 추가로 인하여 비용이 증가하는 단점이 발생할 수 있으며 서버의 네트워크 속도의 저하가 있을 수도 있다. 하지만 이러한 것은 기업의 보안정책에 의해서 해결이 가능할 것이다.

향후 침입차단방법은 급격히 발전하는 해킹 및 바이러스에 대해 실시간 차단 및 침입정보의 철저한 분석으로 비슷한 유형의 패킷이나 침입에 대해 정보를 미리 파악하여 침입을 방해하거나 침입한 상대를 공격할 수도 있도록 해야 할 것이다. 또한 대용량 데이터 처리 시 네트워크속도가 현저히 저하되지 않도록 트래픽량을 분산시킬 수 있는 침입차단 방법을 구성해야 할 것이다.

참고문헌

[1] 김병구,정태명,"침입탐지 기술의 현황과 전망", 정보과학회지 제 18권 제 1호, 2000.1
[2] 김익수, 김명호, "실시간 침입탐지 및 차단을 위한 시스템", 정보과학회지, Vol.29 No.1, 2002.4
[3] 손우용, "통합보안관리 시스템에서 우선순위 기반의 보안정책 수립 모델 " 박사 학위 논문, 2004.7.
[4] 한국정보보호진흥원, "2003년 5월 해킹바이러스 통계 및 분석 월보," 정보보호뉴스 2003년 5월호
[5] 한국정보보호학회, "인터넷 정보 보안", 한국정보보호진흥원, 2002. 11
[6] 정태명, "가상사설망(VPN)",제6회 정보통신망 정보보호 워크숍 발표집, 1999.5.
[7] 정윤희, 최희숙, 손승원, "인터넷에서 VPN 제공기술 및 동향에 대한 연구", 주간기술동향, 한국전자통신연구원, 1999.05.
[8] 김재현, 조자영, "K4E 방화벽의 보안기술", 한국정보처리학회지, Vol.9, No.1, 2002.1
[9] 이주영, "네트워크 기반 프로토콜 공격에 대한 침입탐지 시스템의 설계", 석사학위 논문, 2002.4
[10] 이상훈, 도경화, 정경원, 정문석, "악의적인 내부 네트워크 사용을 방지하는 침입 차단 시스템을 위한 패킷 필터링 모듈 설계", 정보과학회지, Vol.29, No.2, 2002.10
[11] 최현희 ,정태명, "통합보안관리시스템을 위한 보안정책 일반화에 관한 연구", 정보처리 학회 논문지 제 9-C권 제 6호, 2002.12.
[12] 김현아, "[정보보호전문업체 신 4인방 출사표] 한국IBM", 아이뉴스24 2002년 10월

저자소개

강민균(Min-gyun Kang)

2003년 8월 한남대학교 컴퓨터 공학과 공학사
2003년 8월~현재 한남대학교 대학원 공학석사
※관심분야 : 정보보호, 컴퓨터 네트워크, XML

한군희(Kun-Hee Han)

1989년 2월 : 충북대학교 컴퓨터공학과(공학사)
1994년 8월 :경남대학교 컴퓨터공학(공학석사)
2000년 8월 :충북대학교 컴퓨터공학과(공학박사)
1989년 1월 ~ 1994년 12월 : 대우정보시스템 연구원
1995년 3월 ~ 2000년 12월 : 대천대학 전기전자컴퓨터학부 교수
2001년 3월 ~ 현재 : 천안대학교 정보통신학부 교수
※관심분야 : 정보보호, 컴퓨터 네트워크, XML

하경재(Kyung-Jae Ha)

1980년 2월 성균관대학교 전기공학과 학사
1982년 2월 성균관대학교 대학원 전기공학과 석사
1989년 2월 성균관대학교 대학원 전기공학과 박사
1997년 미국 Wayne 주립대학 visiting scholar
1984년~ 현재, 경남대학교 컴퓨터공학부 교수
※관심분야 : 지능시스템, 소프트컴퓨팅

김석수(Seok-soo Kim)

1991년 2월 성균관대학교 대학원 공학석사
1991년 2월 ~ 1996년 5월 정풍물산(주) 중앙연구소 주임연구원
1997년 4월 ~ 1998년 1월 (주)한국탑웨어 책임연구원
2002년 2월 성균관대학교 대학원 공학박사
1998년 3월 ~ 2000년 2월 경남도립거창전문대학 교수
2000년 3월 ~ 2003년 2월 동양대학교 컴퓨터공학부 교수
2003년 3월 ~ 현재 한남대학교 정보통신멀티미디어학부 교수
※관심분야 : 멀티미디어, 정보통신, 웹솔루션, 정보보호, 원격교육 플랫폼 및 컨텐츠