정보산업 동향

K4E 방화벽의 보안기술

김 재 헌*, 조 자 영**

● 목 차 ●

1. 서 론

1.1 정보보안의 중요성

오늘날 우리는 정보화 혁명이라 칭해지는 거대한 변화의 시대를 살아가고 있다. 기업, 공공기관, 학교는 물론 가정에까지 컴퓨터와 인터넷이 널리 보급되었으며, 이를 운용하기 위한 사용환경은 사용자에게 친숙하게끔 쉬워지고 있다. 우리 주변의 생활양식이 컴퓨터와 네트워크에 밀접하게 연관될수록 이러한 변화의 역기능도 심각해지고 있다. 해킹을 비롯한 사이버 범죄가 매년 3배 이상 급격한 속도로 증가하고 있으며, 보안의 필요성에 대한 인식 역시 높아지고 있다.

물리적 보안에서도 가장 기본적이고 필수가 되는 것이 출입 통제에 관한 것처럼, 네트워크 보안에 있어서도 가장 기본이 되는 것이 전산 자원으로 유출입 되는 네트워크 플로우에 대한 제어권을 획득하는 것이다. 허가된 사용자 이외에는 모든 접근을 차단하고, 미리 정한 기준에 따라 네트워크에 대한 통제를 가능하게 하는 것, 바로 그것이 방화벽(Firewall) 제품의 기능이다.

* (주)유니와이드테크놀러지 수석연구원
** (주)유니와이드테크놀러지 솔루션 사업본부장

1.2 방화벽 인증평가제도

보안의 중요성이 대두됨에 따라 기업 및 공공 전산망에서의 정보보안 시스템이 도입되고 있다. 그러나 도입한 정보보안 시스템 자체에 보안 취약성이 내재되어 있을 가능성이 있기에 보안기능의 성능과 신뢰도에 대한 검증이 필요하게 되었다. 이를 해결하기 위한 방안으로 정보통신부에서는 정보통신망 침입차단시스템과의 평가기준 및 평가지침서를 고시하였으며 한국정보보호진흥원에서 1998. 2월 부터 침입차단시스템 평가를 시행하고 있다.

국가 정보원의 인증평가는 정보화촉진기본법 제15조를 근거로 하고 있으며, 평가등급은 K1등급을 최저단계로 하고, K2, K3, K4, K5, K6, 그리고 K7를 최고단계로 하여 총 7단계로 구분한다. 침입차단시스템 보안기능의 신뢰성을 확인하기 위한 보증요구사항은 개발과정, 시험과정, 형상관리, 운영환경, 설명서, 취약성의 6가지 사항으로 이루어진다.

기본적인 방화벽 제품의 성능에 부가된 비밀성 기능은 침입차단시스템을 통하여 전송되는 데이터가 인가되지 아니한 사용자에게 노출되었을 경우 그 내용이 알려지는 것을 방지하기 위하여 전송 데이터를 암호화할 수 있음을 의미한다. 비밀성에 대한 평가는 모든 등급에서 선택적으로 이루어질 수

있으며 비밀성 기능이 제공되는 경우에는 각 평가 등급에 E자를 붙여서 K1E, K2E, K3E, K4E, K5E, K6E, K7E로 표기한다.

네트워크 보안의 기본이자 필수라고 할 수 있는 방화벽 시장은 그 동안 외산 제품들이 주도해 왔다. 그러나 그 동안 국내에서 기술력을 다져온 여러 벤처기업에서 외산에 비해 결코 성능이 떨어지지 않는 제품들을 내놓기 시작했다. 상기에서 언급된 국가 정보원의 정보보안 평가인증은 국산 방화벽 제품을 선택하고자 하는 소비자들에게 중요한 지침으로 자리잡았다. 국가 정보원의 평가기준은 세계적 보안 평가기관의 평가기준에 준하여 인증을 발행하기 때문에, 공신력을 인정받고 있다.

이 글에선 인터넷 상의 보안 위협 요소와 그를 극복하기 위한 여러 대안, 그리고 유력한 대안으로 현재까지 인증받은 방화벽 제품 중 가장 강력한 기능을 제공하는 K4E 인증제품의 기능을 살펴보고자 한다.

2. 보안 위협요소 및 대책

2.1 네트워크 보안 위협 유형

정보의 흐름은 하나의 발신처 네트워크에서 목적지 네트워크로 이어지게 된다. 이와 같은 정상적인 정보의 흐름이 방해되거나 허가 없이 변조될 경우, 네트워크 보안에 문제가 발생하게 된다.

보안에 대한 위협 유형으로는

- 방해(Interruption) : 시스템의 일부가 파괴되거나 사용할 수 없게 되는 경우로 가용성에 대한 공격
- 가로채기(Interception) : 허가되지 않은 사용자가 도중에서 정보를 가로채어 비밀성을 침해하는 것
- 수정(Modification) : 허가되지 않은 주체가 시스템에 불법으로 접근하여 데이터를 변경함으로써 데이터의 무결성을 침해하는 것
- 위조(Fabrication) : 허가되지 않은 주체가 시스템에 거짓 정보를 삽입하는 것

등이 있다.

한편 인터넷에서의 일반적인 위협요소로는 허가되지 않은 자(시스템에 논리적 접근 권한이 없거나 시스템 정보를 사용할 권한이 없는 사용자)의 논리적 접근 시도, IP 패킷 스푸핑(허가되지 않은 사용자가 내부망에서 외부망으로 전송되는 패킷으로부터 발신처 IP를 도용하여 허가된 사용자인 것처럼 위장하여 시스템을 공격하는 것), 발신처 라우팅 공격(프로토콜 헤더에 있는 출발지 라우팅 정보를 수정하여, 패킷 필터링 규칙을 우회), 반복 공격(공격받고 있다는 사실을 전혀 인식하지 못하는 다양한 방법으로 네트워크를 계속적으로 공격), 허술한 감사 추적, 감사 추적 정보 파괴, 도청(도청의 방법으로는 네트워크 선을 직접적으로 태핑하는 와이어 태핑(wiretapping), 네트워크 상의 패킷을 소프트웨어를 이용하여 모니터링하는 스니퍼링(sniffering) 등), 신분위장, 서비스 거부 공격 등이 있다.

2.2 보안 위협에 대한 대책

이러한 위협에 대한 대책으로 다음과 같은 방법들이 사용된다.

첫째, 네트워크에 존재하는 서버들에 대한 자체 보안이다. 인터넷을 통하여 서비스를 제공하는 모든 네트워크 서버의 보안을 강화하여야 한다. 필요없는 모든 네트워크 서비스를 제거하여야 하며, 서버가 제공하는 보안기능을 충분히 활용하여야 한다.

둘째, 패킷필터링 라우터를 사용하여 IP레벨에서 적법한 패킷만 선별한다. 요즘 대부분 라우터는 패킷필터링 기능을 제공한다. 패킷필터링 기능을 이용하면 인터넷과 내부 네트워크로 오고 가는 네트워크 서비스의 종류(ftp, telnet 등), 프로토콜(TCP, UDP, ICMP 등), 시스템 또는 도메인 정보에 따라 패킷을 차단할 수 있다.

셋째, 여러 네트워크를 사용할 경우 내부 네트워크와 인터넷에 연결되는 네트워크를 분리하여 사용함으로써 보안을 향상시킬 수 있다. 단일 네트워크를 사용할 경우, 네트워크를 서브네팅하여 여러 개의 네트워크로 분리하여 사용할 수 있다.

마지막으로 침입차단 시스템을 사용하는 것이다. 침입차단시스템은 인터넷과 같은 위험한 네트워크로부터 내부 네트워크를 보호해주는 방패 역할을 하는 장치이다. 침입차단시스템이 없는 경우, 내부 네트워크는 안전하지 않은 네트워크 서비스, 그리고 취약점 스캐닝과 같은 공격에 매우 취약하며, 결국, 각 호스트 단위의 보안 해결책을 적용하여야 하는 높은 비효율성을 낳게 된다. 따라서 침입차단시스템은 네트워크 보안의 효율성을 증대시키며, 내부 네트워크를 많은 위협으로부터 보호할 수 있다.

3. 방화벽 시스템 설계 동향

침입차단시스템의 구현 방식은 일반적으로 패킷 필터링 방식, 서킷 게이트웨이 방식, 어플리케이션 게이트웨이 방식, 하이브리드 방식으로 구분된다.

패킷필터링 방식(Packet Filtering Firewall)

네트워크 프로토콜 OSI 모델의 네트워크 층과 전송 층에서 패킷을 필터링하는 기능을 수행하며 패킷필터링 규칙을 사용하여 발신처 주소와 서비스 포트가 목적지 주소와 서비스 포트로 접근하는 것을 허용하거나 금지한다.

3.1 서킷 게이트웨이 방식(Circuit Gateway Firewall)

네트워크 프로토콜 OSI 모델의 전송 계층과 세션 계층에서 구현되며 TCP 프락시와 UDP 프락시가 존재하여 내부 망과 외부 망의 시스템이 직접 연결되는 것을 허용하지 않는다.

3.2 어플리케이션 게이트웨이 방식 (Application Gateway Firewall)

네트워크 프로토콜 OSI 모델의 응용 계층(제 7계층)에 구현되며 각 서비스별로 프락시 데몬이 있어

방 식	장 점	단 점
패킷필터링 방식	• 상대적으로 빠른 처리 속도 • 사용자의 투명성 보장 • 높은 유연성(새로운 서비스를 비교적 쉽게 부가) • 구축의 용이성 • 저렴한 가격 • 기존 응용 서비스 프로그램에 대한 수정 불필요	• 모든 정보 흐름을 패킷 형태로 처리 - 내부 망과 외부 망의 시스템이 직접 연결 • 데이터가 IP 수준에서 처리 - 데이터 내용 분석이 불가능 • IP헤더를 조작하는 IP spoofing 공격에 취약 • 일반적으로 로깅 기능을 제공하지 않으므로 내부 망이 침해 당했을 경우 인지하기 어려움 • 사용자 인증의 취약함 • 사용자별 접근 제어가 불가능
서킷 게이트웨이 방식	• 내부 망과 외부 망 간의 직접적인 연결 차단 • 비교적 단순하면서도 서비스 유연성이 높음	• 서킷 프로토콜을 사용한다면 사용자 프로그램의 수정이 반드시 필요
어플리케이션 게이트웨이 방식	• 내부 망과 외부 망간의 직접 연결을 어플리케이션 프락시를 이용하여 금지 - 외부의 공격으로부터 내부 망을 보호 • 기존 어플리케이션에 대한 수정 불필요 • 강력하고 포괄적인 로깅 기능과 감사 기록 기능을 제공 • 일회용 패스워드 등의 강력한 인증 기능을 포함가능 • 각 서비스별 접근 제어 및 서비스 이용시간 등 부가적인 기능 추가 용이	• 설치 시 네트워크 성능 저하 • 새로운 서비스를 추가하기 위해서 새로운 프락시가 추가되어야 하므로 새로운 서비스에 대한 유연성이 떨어짐
하이브리드 방식	• 보안성이 양호 • 새로운 서비스 부가가 용이	• 보안에 비례하여 구축이 복잡함 • 높은 가격 • 관리가 복잡함

내부 망의 시스템에 직접적인 접근을 막으며 서비스별 프락시가 서비스 요구자와 IP주소 및 포트를 기반으로 네트워크 접근을 제어한다.

3.3 하이브리드 방식 (Hybrid Firewall)

여러 유형의 침입차단시스템을 경우에 따라 복합적으로 구성한 형태이다.

아래의 표는 각각의 설계방식에 대한 장 단점을 표로 비교한 것이다.

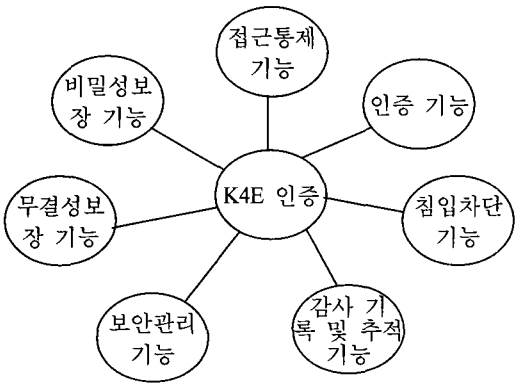
여기에 덧붙여 Stateful Inspection의 개념을 소개한다.

인스펙션 방식(Stateful Inspection)

스테이트풀 인스펙션은 패킷의 헤더, 발신지, 목적지, 포트번호의 문맥을 이용한 최첨단 접근통제 검사엔진으로 MAC 레이어와 IP 프로토콜 스택 사이에서 동작된다. SYN 패킷에 의해 만들어진 세션 테이블을 이용, 후속 패킷들에 대해 규칙테이블 검사 없이 고속으로 처리가 가능하며 패킷 절차가 맞지 않는 DOS 공격의 차단이 용이하고 UDP 패킷들에 대한 가상 세션을 형성 인바운드/아웃바운드 방향성 통제가 가능한 동적 패킷 필터링 엔진이다.

4. K4E 등급 방화벽 기능

이 글을 쓰는 시점까지 평가인증을 받은 제품 중 최상위 등급은 K4E였으며, 아래와 같은 기능에 대한 요구사항을 만족시켜야 한다.



4.1 접근통제기능

침입차단 시스템은 호스트에 대한 접근 통제 기능을 제공한다. 메일 서버나 공개 정보 서버와 같은 특정 호스트를 제외하고는 외부에서 내부 호스트에 접속하는 것을 금지하는 기능이 있다. 이러한 접근 통제는 패킷 필터링 규칙에 의해 가능하다. 패킷 필터링 규칙에 의거하여 패킷의 IP(Internet Protocol) 주소를 분석한 후 접근 허용여부를 결정하게 된다.

임의적 접근통제

임의적 접근통제 기능은 침입차단시스템을 통하여 이루어지는 모든 접속 및 데이터 패킷에 대하여 주체와 객체의 신분에 기초한 임의적 접근통제 규칙을 적용하여 접근을 통제하는 기능을 말한다. 이를 위해서는 주체 및 객체에 대한 정의가 되어야 하는데, 주체는 침입차단시스템을 통하여 객체에 접근하고자 하는 것으로 내부 또는 외부망의 사용자, 호스트, 호스트가 속해 있는 도메인이 될 수 있으며, 객체는 침입차단시스템을 통하여 접근을 요구받는 호스트나 도메인, 서비스 등이 될 수 있다. 또한 주체와 객체를 그룹화하여 편리하게 관리할 수 있다.

강제적 접근통제

강제적 접근통제는 주체의 보안레이블과 주체가 접근하고자 하는 객체의 보안레이블을 비교하여 보안 정책에 합당한 접근통제 규칙에 의해 접근통제를 하는 방법이다. 이때, 강제적 접근통제의 판단 기준이 되는 보안레이블은 접근 통제의 대상이 되는 주체 및 객체의 중요도를 나타내는 정보이다.

4.2 인증기능

전통적인 패스워드 시스템의 취약점을 방지하기

위하여 일회용 패스워드(S/Key)라는 강한 인증 기법을 사용한다. 로그인 과정마다 패스워드를 만들어 동일한 패스워드의 재사용을 막을 수 있다. 또한 인증기능을 이용하여 사용자의 신분을 확인할 수 있다. 침입차단 시스템에서 이와 같은 신분확인을 하는 목적은 첫째, 주체에 대해 식별 및 인증을 수행하여 침입차단시스템에 등록되지 않은 불법 사용자에 대해 일차적으로 접근을 통제하며 둘째, 침입차단시스템의 다른 보안기능 들이 올바로 동작할 수 있는 기본적인 역할을 제공하기 위함이다. 침입차단시스템에서 접근통제 시 신분확인 기능은 일차적인 필터링 역할을 하며, 침입차단시스템의 보안기능인 접근통제와 감사기록 및 추적이 제 기능을 할 수 있는 기반을 제공한다.

프락시 인증

일반 서비스 프락시가 인증 상태 정보를 요구할 때, 인증 프락시는 인증 서버에게 인증 결과를 요구한다. 인증 상태 정보를 요구하는 프락시는 FTP, Telnet, HTTP, SMTP 가 있다.이 프락시는 서비스를 수행하는 당시 해당 사용자에 대한 인증 정보를 체계로부터 받고, 인증 절차를 거치지 않은 세션이라면 인증 프락시에게 인증 절차를 거치도록 요청한다. 인증 절차에 의해 인가된 사용자라고 판단되면 프락시 서비스를 진행한다.

4.3 비밀성 보장 기능

침입차단시스템에서 요구되는 비밀성이란 보호하고자 하는 데이터에 인가되지 않은 자가 접근하여 그 내용을 보지 못하도록 하는 제반 수단, 절차, 방법을 의미하는데, 암호화 기법이 주로 사용된다. 개인 프라이버시를 위해 통신할 때 , 암호화하여 전송하거나 중요한 데이터를 암호화하여 저장함으로써 비밀을 유지한다. 또한, 통신 선로 이외의 시스템에서의 중요한 자료의 보안을 위해 파일 암호를 지원한다. 침입차단 시스템의 보안규칙 파일인 정책 파일은 하드 디스크에 저장될 때, 데이터 변경 감지 기능인 무결성 체크와 데이터의 암호화를 통해 안전하게 저장된다. 침입차단 시스템이 시작하게 되면 정책 파일을 로드하기 위하여 암호화된 정책 파일을 복호화한 후, 무결성 확인을 거치게 된다. 정책 파일이 무결성에 위배되지 않았다면, 보안규칙 정보를 로드한 후, 무결성/비밀성 키를 이용하여 정책 파일에 대한 해쉬 생성 및 정책 파일을 암호화하여 저장하게 된다.

4.4 무결성 보장 기능

침입차단시스템은 각 보안기능이 정상적으로 동작하기 위한 정보를 저장하는데 이러한 정보들에 대해 인가되지 않은 사용자가 임의적인 변경을 하거나 삭제를 하게 되는 경우에 정보보호시스템의 보안기능은 제 역할을 할 수 없게 된다. 또한, 침입차단시스템을 통하여 전송되는 데이터들은 네트워크 중간에서 가로채기에 의한 변경 후 재전송되는 위협이 있을 수 있다. 무결성 기능은 시스템 내부의 데이터에 대한 변경 및 시스템을 통하여 전송되는 데이터들에 대하여 인가되지 않은 변경이 발생하는 경우 이를 감지하여 적절한 조치를 취할 수 있음을 의미한다. 보안기능과 연관된 데이터에 대한 무결성을 제공하기 위해서 시스템은 무결성 대상 데이터들을 정의하고, 정의된 데이터에 대하여 변경을 감지한다.

무결성 체크를 위한 검사값 생성 및 관리

일반적으로 무결성 검사값 생성을 위해서는 해쉬함수가 많이 이용된다. 해쉬함수는 키를 사용하는 해쉬함수인 MAC(Message Authentication Code)과 정수론 등 수학적 분야에 기초한 일방향 함수를 이용하고 키를 사용하지 않는 해쉬함수가 있다. 해쉬함수를 통해 발생된 무결성 검사값을 무결성 대상 데이터베이스에 저장하여 관리하게 되는데, 인가된 관리자의 데이터에 대한 변경 시 해당 무결성

검사값도 함께 변경이 되어야 한다.

데이터 무결성 체크 대상

데이터의 무결성을 제공하기 위해서는 먼저 무결성 대상 데이터를 정의하고, 데이터의 변경을 감지하기 위해 원래의 데이터로부터 유일하게 구분되는 값을 생성하고 보관하는 방법이 제공되어야 한다. 무결성 확인 프로세스는 관리자의 요청이나 주기적인 검사로 동작이 되며 대상 데이터에 대하여 무결성 검사값을 생성하고 무결성 대상 데이터베이스의 검사값과 비교하여 무결성을 확인하게 된다. 보안기능과 관련된 데이터로는 신분확인에서의 인증 데이터, 임의적 접근통제 규칙, 강제적 접근통제 규칙, 보안레이블, 감사기록 및 추적에서의 감사기록 대상사건, 무결성 기능에서의 무결성 대상 목록, 무결성 대상 데이터베이스 등이 될 수 있다.

4.5 침입차단기능

침입을 차단하기 위한 방법으로 패킷 필터링, Stateful Inspection, 프락시 서비스, 응용서비스통제 등이 존재한다.

패킷 필터링

패킷 필터링 방식의 방화벽은 OSI 모델에서 네트워크층(IP 프로토콜)과 전송층(TCP 프로토콜)에서 패킷의 출발지 및 목적지 IP 주소 정보, 각 서비스에 port 번호, TCP Sync 비트를 이용한 접속제어를 한다. 침입차단기능이 OSI 7 모델에서 제 3, 4계층에서 처리되기 때문에 다른 방식에 비해 처리속도가 빠르며, 사용자에게 투명성을 제공한다. 또한 기존에 사용하고 있는 응용 서비스 및 새로운 서비스에 대해서 쉽게 연동할 수 있는 유연성이 있다.

Stateful Inspection(상태정밀검사방식)

스테이트풀 인스펙션은 클라이언트/서버 모델을 유지시키면서 모든 어플리케이션층의 전후상황에 대한 문맥 데이터를 제공함으로서 이전의 세 가지 접근 (패킷 필터링과 어플리케이션 게이트웨이 및 하이브리드 방식)의 한계를 극복한다. 스테이트풀 인스펙션에서 패킷은 방화벽 패킷 필터링의 위치에서 인터셉트되며 인스펙션 엔진이 그 다음 임무를 수행한다. 인스펙션 엔진은 모든 어플리케이션층으로부터의 보안결정을 위해 요구되어지는 상태관련 정보를 추출해낸다. 그리고 이러한 정보는 뒤따르는 커넥션 시도를 평가하기 위해 동적인 상태정보 테이블 안에서 관리 유지되어 진다. 이것은 매우 높은 보안을 제공하며 최대의 성능과 범용성과 확장성을 지닌 솔루션을 제공한다.

프락시 서비스

프락시 시스템은 사용자에게 직접 이중 네트워크 호스트에 접속하도록 하는 대신 모든 접속을 배후에서 처리해주면서 사용의 투명성을 제공한다. 사용자는 이중 네트워크 호스트와의 접속을 의식하지 않고 외부망 호스트에 접근할 수 있으며, 모든 접속은 프락시 서버의 보안기능에 의해 제어되므로 허가되지 않은 사용자나 호스트의 접속을 막을 수 있다. Telnet, FTP, HTTP, SMTP 등 특정 프로토콜을 위한 프락시 서버가 작동함으로써 클라이언트 프로그램을 경유하여 실제 목적지 서버에 접속하는 대신 프락시 서버에 접속하고, 프락시 서버는 클라이언트의 요구를 검증한 후, 접근을 허용해 줄 것인지 아닌지를 결정한다. 만약 요구가 받아들여지면 프락시 서버는 클라이언트를 대신해 실제 서버에 접속하여 클라이언트의 요구를 실제 서버에 전달하고 실제 서버의 응답을 클라이언트에게 전달한다. 프락시 서버는 접근 허용 여부를 결정하기 위해 사용되는 프로토콜을 이해하고, 해석할 수 있어야 하며, 이것은 통신상에 많은 부하를 줄 수 있다.

응용서비스 통제

네트워크 접속 정책에 따라 특정 필드나 프로토콜을 필터링하는 것은 네트워크 접속의 허용이나 접근 서비스 유형을 결정하는 작업이다. Telnet 서비스의 23번 포트를 비롯하여 몇몇 서비스들은 본질적으로 취약점이 많고, 침입자에 의해 자주 악용되곤 한다. 이러한 서비스들이 내부망에 접속하고자 할 때, 침입차단시스템에서 반드시 필터링되어야 한다.

내용검색 및 필터링

패킷의 내용을 검색하여 필터링 한 후 대상 호스트에 전달해 줌으로써 바이러스 체크, Java/ActiveX 애플릿 차단, 유해 URL 통제기능, SPAM메일 차단, 통제 내용의 키워드 검색기능, FTP 명령어 차단 등을 지원한다.

4.6 보안관리기능

보안관리는 침입차단시스템의 보안기능을 안전하게 수행하기 위하여 관리자만이 수행하는 기능으로써, 침입차단시스템의 보안기능과 관련된 데이터에 대한 설정, 조회, 변경 및 삭제할 수 있는 관리자 인터페이스를 제공하고, 침입차단시스템의 보안기능이 올바로 동작하는가를 확인할 수 있는 기능을 의미한다. 보안관리 기능은 보안관리 프로세스를 통하여 관리자가 직접 설정 및 변경해 주어야 하는 모든 보안 관련 데이터들을 관리할 수 있는 인터페이스를 제공하는데 이때, 보안관리 프로세스는 보안정책에 위배되는 설정에 대해서는 관리자에게 경고하여 보안정책에 합당한 올바른 설정이 이루어 질 수 있다. 보안정책 설정 검증기는 관리자가 설정한 보안정책으로 모의시험을 거쳐서 설정된 정책들 간에 모순점이 없는지를 검증한다. 보안관리기능은 안전성을 위해 관리자가 침입차단시스템 로컬에서 해당 프로그램을 직접 수행할 수 있고, 네트워크를 통해 보안관리 프로세스를 접속하여 관리할 수 있다. 이때 , 보안관리 프로그램에 접속하기 위해서는 관리자의 신분이 확인되어져야 하며, 보안관리에서 발생되는 모든 사건 들은 감사기록 되어진다.

4.7 감사기록 및 추적기능

감사기록 및 추적이란 침입차단시스템과 관련한 보안관련 활동들에 대해 기록하고, 기록된 자료를 분석하여 침입차단시스템을 통한 침입의 예방, 탐지 및 불법적인 행위를 추적하는 것이다. 침입차단시스템에서 제공되어지는 보안기능이나 주체 및 객체의 모든 활동 및 접근에 대하여 감사기록을 수행함으로써 생성된 감사자료를 이용하여 불법적인 침입에 대한 허점을 보완할 수 있고, 실시간 침입탐지 기법을 적용하여 불법침입에 대한 예방을 하는데, 이 때 E-mail이나 핸드폰의 단문메시지 서비스 등을 이용하여 실시간으로 경보를 처리해 주는 기능이 있다. 여기에 더하여 오프라인으로 감사 자료를 분석함으로써 불법적인 침입에 대한 책임소재 파악에 도움을 줄 수 있다. 감사기록 및 추적의 기능들이 효과적으로 수행이 되기 위해서는 기본적으로 신분확인을 통한 주체의 식별자가 올바로 확인이 되어야 한다. 또한 침입차단시스템 보안관련 사건에 대한 감사 자료는 매우 중요하기 때문에 감사 자료에 대한 접근 통제가 함께 이루어야 한다. 감사 자료의 보안을 위해 앞서 설명되어진 비밀성, 무결성 기능을 이용한다.

5. 침입차단 시스템 구축 시 장점

침입차단시스템은 크게 네트워크 보안을 증가시키고 불안전한 서비스를 원천적으로 필터링함으로써 서브네트 상에 있는 호스트에 대한 위험을 감소시킨다. 선택된 프로토콜만이 방화벽을 통과할 수 있기 때문에 내부 네트워크 환경은 위험에 덜 노출된다. 또한 침입차단 시스템은 호스트 시스템으로

의 액세스를 컨트롤할 수 있고, 일관된 네트워크 액세스 정책을 실행할 수 있다. 인터넷 안팎으로 모든 액세스가 침입차단시스템을 통과한다면, 침입차단시스템은 액세스 정보를 기록할 수 있고, 네트워크 사용에 관한 유용한 통계자료를 제공한다. 의심스러운 활동이 있을 때 적당한 알람 기능을 가진 침입차단시스템은 침입 시도를 받고 있는지 또는 침입 되었는지에 대한 세부사항을 제공해 준다. 대부분의 수정된 소프트웨어와 추가되는 보안 소프트웨어를 많은 호스트에 분산시키지 않고 침입차단시스템에 설치할 수 있어서 경제적이다. 그리고 설치될 곳의 네트워크 환경에 따라 서브네트(Subnet : 내부 네트워크를 필요와 용도에 맞게 나누어서 사용), NAT(Network Address Translation : 주소변환 기능으로 적은 수의 공인 IP를 많은 내부 자원이 활용할 수 있게함), LNA(Local Network Adapted : 설치에 있어서 별도의 IP 구성에 변경이 필요없음), NCF(Network Configuration Free : IP 구성에 있어서 물리적인 배치에 무관하게 적용할 수 있음) 등의 다양한 설치 모드를 지원함으로써 운영의 편리성을 도모하고, 부족한 IP 자원의 문제를 해결해 주어 TCO(총 소유비용)를 절감할 수 있어 효율적이다.

6. 결 론

국내의 컴퓨팅이나 통신환경의 보급에 비해서, 보안에 대한 인식이나 준비가 부족한 것이 사실이다. 조직의 진정한 자산은 방범 인력이 경비업무를 수행하는 물리적 실체가 아닌, 전산자원 속에 보관되어 있는 지적 산출물에 있음을 인식할 필요가 있다. 이러한 귀중한 자산에 대한 최소한의 보호조차 되어 있지 않은 곳이 너무나 많다.

방화벽 제품이 보안의 만병통치약은 아니다. 하지만 방화벽 없이 보안을 논한다는 것은 어불성설이다. 즉, 네트워크 보안의 필수 요소이자 기본적인 첫 출발점은 바로 방화벽이다. 지금 보안 솔루션 도입을 위해 고심 중인 조직이 있다면, 단연 가장 강력한 성능의 K4인증 방화벽을 추천한다.

내부망 만이 아니라 본사와 지사 내지는 여러 지점 간의 원격지 통신을 필요로 한다면, 통신 선로상에서 허가되지 않은 자에 의해 통신 내용이 도청되거나 변조되지 않도록 비밀성 기능이 보장되어야 한다. 원격지 간의 통신은 전용회선을 설치하기엔 너무나 비용이 많이 들어서 대개의 경우 기존의 상용회선을 사용하되 전용회선의 효과를 얻을 수 있는 VPN(Virtual Private Network, 가상사설망) 장비를 사용하게 된다. K4E 이상의 인증을 획득한 방화벽 제품에는 체계 대 체계의 VPN 기능이 지원되어 통신의 비밀성을 획득할 수 있다.

공공 통신 환경에서의 비밀성 획득을 위해 VPN과 함께 PKI(Public Key Infrastructure, 공공키 기반) 제품이 널리 쓰이고 있고, 국가정보원에서도 이 제품들을 CC(Common Criteria, 세계적인 보안 공통

항 목	내 용
평가 등급	- K4E
차단 방식	Hybrid Type - Stateful Inspection 기능 구현
Data 보호	- VPN 기능 지원 - 감사기록(Log) 및 보안정책 데이터의 암호화 저장
네트웍 운용	NAT 게이트웨이 방식 브릿지 방식 Gigabit 지원
방화벽 관리	보안정책 설정 검증기 전용 S/W를 이용한 원격 관리 방화벽 시스템과 동일한 GUI 독립적인 실시간 경보관리 시스템 자체로그 Disk 보관 및 관리 SMS 기능 지원
유해정보 차단	E-mail Virus 차단 유해사이트 차단
Contents Filtering	Oracle SQL Net Proxy 지원 HTTP, FTP, Telnet, SMTP, DNS, Gopher, NNTP 외
접근 통제	강제적, 임의적 접근통제 10단계 이상 보안등급 설정 OTP 지원

표준)의 지침에 따라 보안 인증평가의 움직임이 일고 있다. 정보보안의 기반구조를 굳건히 하는 고무적인 상황이라 할 수 있다.

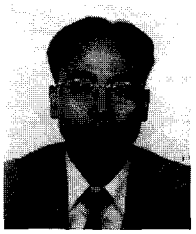
필자가 제안하는 UniSecure Firewall은 국내 최초로 Windows 기반의 K4E등급을 받은 제품으로 국가 정보원의 인증 요구사항을 충족시킴과 동시에 다음과 같은 부가적인 기능을 갖추고 있다.

마지막으로 보안제품을 선택할 때에는 반드시 국가기관에서 그 성능과 신뢰성을 인증한 제품을 선택하기를 권한다. 하지만 제품의 구입과 설치만으로 보안이 이루어 지는 것은 아니다. 보안은 제품(Product)이 아닌 과정(Process)라고 하는 말이 있다. 단지 보안장비의 설치로 끝나는 것이 아닌 보안에 관련된 온라인 오프라인 전반에 걸쳐 지속적인 교육과 관리가 더욱 중요함을 강조하는 바이다.

* 참고 사이트

한국정보보호진흥원, www.kisa.or.kr
국가정보원, www.nis.go.kr
한국정보침해사고대응팀, www.certt.or.kr
전자신문사, www.etnews.co.kr
한국정보보호산업협회, www.kisia.or.kr
디지털타임즈, www.digitaltimes.co.kr
㈜유니와이드테크놀러지, www.uniwide.co.kr

저자약력



김 재 헌

1988년 건국대학교 전자계산 졸업
금성사 정보기기연구소 주임연구원
(주)한아시스템 기술연구소 선임연구원
(주)유니와이드테크놀러지 수석연구원
관심분야 : 네트웍 프로토콜, 호스트/네트웍기반 정보보호

조 자 영

1981년 경북대학교 컴퓨터공학과 졸업
1992년-1993년 서강대 경영대학교 중퇴
1983년-1987년 금성사 컴퓨터 기술실
1988년-1993년 왕 컴퓨터 영업부
1993년-1997년 서영 BST 대표이사
1998년-현재 유니와이드 솔루션 사업본부장