시스템별 기능 및 취약점을 분석하라

인터넷의 개방성으로 인하여 발생되는 전자상거래의 취약점을 최소화하기 위하여 우리는 보안 기술을 사용하게 된다. 그러나 보안 기술을 사용함으로 인하여 서비스 속도가 느려지거나 사용자에게 불편을 주지 않아야 한다. 현재 가장 이슈가 되고 있는 인터넷 쇼핑몰의 실례를 보면서 보안 적용 방안을 제시하고자 한다.

■ **이청희**/에스원 정보사업부

최근 들어 컴퓨터 통신의 확산과 함께 인터넷의 사용이 전 세계적으로 급증함에 따라 인터넷의 용도는 지금까지의 학술 및 연구를 대상으로 한 정보공유의 목적에서 인터넷을 마케팅의 대상으로 보고 이를 상업적으로 이용하려는 시도가 증가하고 있다.

즉 인터넷의 전세계를 하나로 엮는 개방성과 지역적 통합성으로 인해 인터넷을 이제 단순한 정보통신의 통로라기보다는 시간과 공간을 초월한 전자상거래를 가능하게 하는 새로운 시장으로 여겨지고 있는 것이다.

전자상거래는 컴퓨터와 디지털 네트워크를 근간으로 하고 있다. 그러므로 대부분의 거래는 인터넷을 이용하여 거래가 성립된다는 사실에 비추어 볼 때 이에 대한 보안 문제의 해결이 절실히 요구된다. 즉 인터넷을 통하여 물품 구입을 하기 위해서는 사용자의 카드번호 및 신상정보를 제시해야 하며 이것은 곧 안전하지 못한 통신망에 개인의 중요 정보를 노출하는 결과가 되고 만다.

특히 전자상거래가 인터넷을 많이 활용할 것으로 전망되기 때문에 인터넷에서 사용하는 TCP/IP 프로토콜의 안전성을 충분히 검토해야 한다. 현재의 TCP/IP 프로토콜은 자체의 보안 기능이 전혀 없기 때문에 누구나 네트워크의 자료를 모니터링 할 수 있다. 또한 쇼핑몰과 같은 가상 상점의 사용자 정보가 보관된 인터넷 데이터베이스의 안전한 보관이 필요하다. 이러한 보안의 필요성은 전자상거래가 가지고 있는 가장 큰 특징인 익명성에서 비롯된다. 일단 사용자들은 서로 만나지 않고 거래를 이루며 지역적으로도 전세계로 흩어져 있다. 이런 사람들이 서로 거래를 쉽게 이룰 수 있다는 것은 전자상거래의 장점이기도 하지만 반대로 상호 간의 신분에 대한 인증이 쉽지 않다.

1. 일반적인 쇼핑몰의 네트워크/시스템 구성 현황

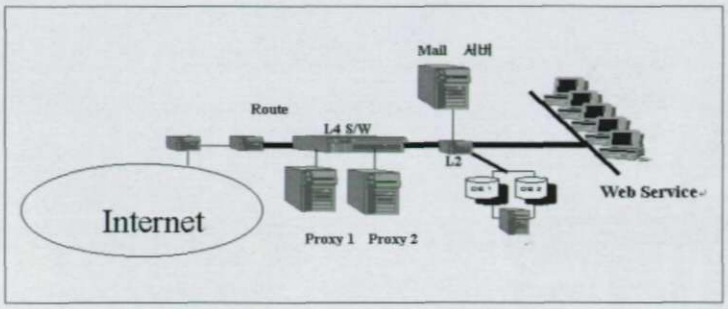
일반적으로 인터넷 쇼핑몰은 다음의 서버들로 구성된다.

가장 기본적으로는 월드 와이드 웹(World Wide Web) 환경을 위한 웹서버가 존재한다. 웹서버는 단순 데이터 뿐만이 아니라 음성, 화상, 영상 등의 멀티미디어 서비스가 제공되므로 다양한 분야에서의 웹의 이용이 증대되고 있다. 그 가운데 특히 웹에 대한 일반인들의 참여가 활발해지면서 전세계적으로 많은 회사들이 관심을 가지고 적극적으로 사업화에 나서고 있다.

두번째로 메일서버가 존재하는데, 사용자들의 인터넷 메일 계정이 등록 및 저장되어있으며, 등록된 사용자에게 인터넷 메일 서비스를 제공한다.

그리고 DB 서버가 웹서버와 연동되는데, 이는 쇼핑몰을 이용하는 사용자의 구체적인 정보들이 저장된다.

마지막으로 웹의 서비스 속도를 더욱 빠르게 하기 위하여 Proxy 서버를 사용하는데, 이는 실제 웹서버의 Data를 캐싱



〈그림 1〉 인터넷 쇼핑몰 구성도

(Cashing)하고 있다가 사용자의 요구에 따라서 빠르게 서비스를 제공한다. 제품에 따라서 더욱 빠른 속도의 서비스를 위하여 개별 O/S를 특별히 사용하기도 한다.

2. 쇼핑몰 보안을 위한 요구사항

2-1 취약점 분석

1) 각 시스템별 분석: 윈도우 NT, 유닉스, 리눅스 등

2) 각 기능별 분석: 웹 서버, 메일 서버, 프락스 서버, DB 서버 등

3) 네트워크 구성상의 문제점 분석: 라우터, 스위칭 허브, 구성 변경 고려 등

2-2 요구 기능 분석

1) Performance의 유지

보안툴을 적용시킬 경우, 일반적으로 서비스의 속도가 느려지게 된다. 이를 최대한 유지시킬 수 있는 보안 적용이 선행되어야 한다. 이를 위해서는 다음과 같은 기술의 사용이 필요하다.

■ Load-Balance: 네트워크 트래픽을 분산시켜주는 방법으로 전형적인 알고리즘은 Round-Robin 알고리즘과 자동 분산 스케쥴 기능을 제공하는 Least-Busy-Scheduling 알고리즘을 사용하여 시스템 서비스의 속도를 최대로 유지시킨다.

쇼핑몰에서는 웹 서비스를 Load-Balance를 시켜줌으로써 고객의 접속 속도를 보다 빠르게 할 수 있다. 이 부분은 쇼핑몰에서 생명이라고 할 수 있는데, 만약 고객이 접속을 위하여 항상 많을 시간을 기다려야 한다면 그 고객은 곧바로 다른 쇼핑몰로 접속하여 거래를 진행하게 될 것임이 틀림없기 때문이다.

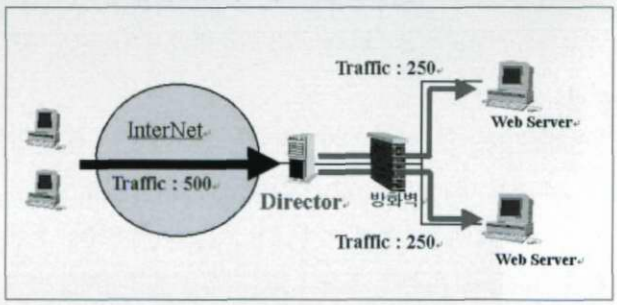
이러한 서비스는 웹서버들의 앞 단(Front-End)에 Load-balance 장비를 설치하여 디렉터(Director) 기능을 담당하도록 하거나 각 웹 서버마다 Load-balance 소프트웨어를 설치하고 트래픽을 분산시킬 수 있는 방법이 있다.

가장 간단한 방법은 DNS 서버에서 각각 웹서버들의 DNS를 공유(Sharing) 시키는 방법을 통해서도 어느 정보의 Load-Balance 효과를 얻을 수 있다.

■ Fault-Tolerance: 시스템의 장애로 인한 서비스 중단을 막기 위하여 다수의 같은 서비스 시스템들을 병렬로 구성하여 특정 시스템이 장애 시에 서비스 요구자에게 같은 서비스를 제공하는 다른 시스템에서 요구된 서비스를 제공할 수 있도록 하는 방법이다. Load-balance에서 명시한 방법과 유사하게 웹 서버 앞 단에 Fault-tolerance Director를 두거나 각 서비스 서버들에 S/W를 올릴 수 있다. 그러나 유감스럽게도 분산컴퓨팅환경(DCE)에서 제공하는 CELL환경에서만 S/W를 통한 Fault-Tolerance 기능 구현이 가능하다.

2) 침입차단시스템

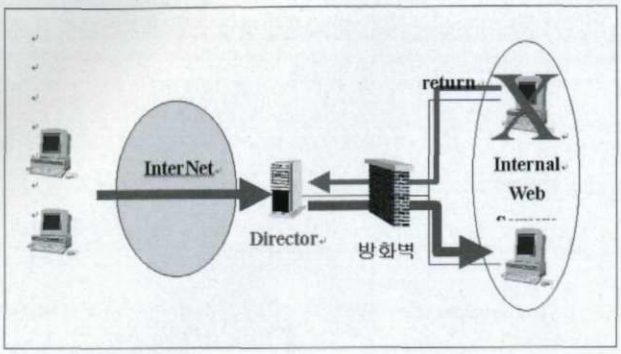
침입차단시스템이라는 것은 외부로부터 내부망을 보호하기 위한 네트워크 구성요소 중의 하나이며, 외부의 불법 사용자의 침입으로부터 내부의 정보와 자원을 보호하고 외부로 부터의 유해 정보 유입을 차단하기 위한 정책 및 이를 지원하는 H/W, S/W를 의미한다. 현재 국산 방화벽으로 K4 등급을 받은 제품들이 나와 있다. 그 구현 원리상 하이브리드 방식을 채택하고 있다.



〈그림 2〉 Load-balancing Director

그 기본원리와 기본 기능은 불법 침입자나 비인증자가 인트라넷이나 엔터프라이즈 네트워크로 접근하는 것을 막기 위하여 고안되었다. 그러므로 방화벽은 다음의 기본적 기능을 수행할 수 있다.

■ 인터넷에서 들어오고 내부망에서 나가는 여러 형태의 네트워크 트래픽(Telnet, Ftp 등)을 통제한다.



〈그림 3〉 Fault-Tolerance Director

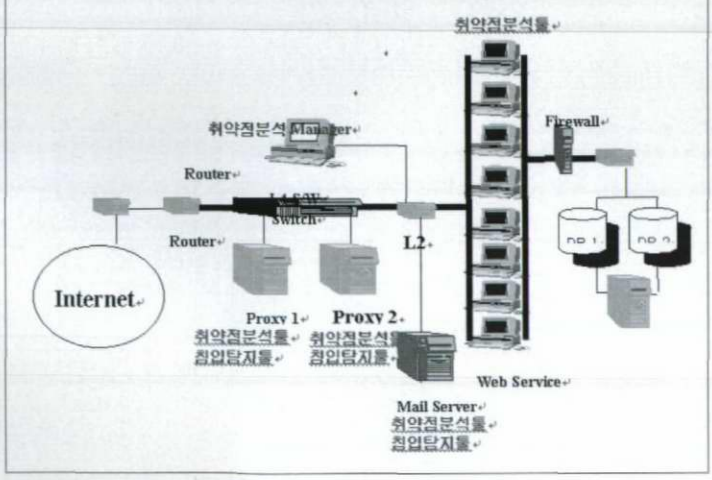
① 비인증자가 내부 네트워크의 자원과 정보에 접근을 차단하고, 이러한 불법적인 사용자에 대하여 외부에서 들어오지 못하도록 한다.

② 인트라넷에서 인터넷으로 접근하는 사용자를 통제, 관리하여 보안성을 높인다.

■ 네트워크 사용자에게 여러 가지 서비스를 제공하면서 서비스의 허용 또는 실패에 대한 정보를 기록한다.

그러나 쇼핑몰에서 있어서 침입차단시스템의 네트워크 상의 위치는 거의 엄청난 차이를 가져온다. 어쩌면 가장 민감한 보안 제품 중의 하나라고 말할 수도 있을 것이다. 왜냐면 침입차단시스템의 수행력(Performance)은 다른 보안 제품에 비하여 상당히 떨어진다.

물론 네트워크 보안의 첫 관문이기 때문에 어쩔 수 없는 것은 사실이다. 그러나 이를 설치함으로 인하여 생기는 역효과는 무시할 수 없다. 침입차단시스템을 설치할 때는 먼저 현 쇼핑몰에서 제공하는 서비스와 이를 사용하는 동시 접속 사용자의 수를 정확히 감안한 시스템 사양과 제품의 선정이 중요하다.



〈그림 4〉 XX쇼핑몰 보안 적용 사례

3) 웹 보안(쇼핑몰 웹 서버)

웹의 근간을 이루고 있는 인터넷은 정보에 대한 공유를 기본으로 하고 있어서 다른 대부분의 인터넷 응용과 마찬가지로 보안 문제를 고려하지 않고 설계했기 때문에 보안이 요구되는 민감한 분야에 사용하기는 적합하지 않은 것이 사실이다. 웹이 단순한 정보 검색 만이 아니라 신용카드 정보와 같은 타인에게 노출되어서는 안될 중요한 정보의 전송과 같이 용도가 다양해짐에 따라 정보 보호를 위한 서비스 제공이 절대적으로 필요하다.

■ 웹 보안을 위하여 요구되는 기능

① 정보의 이용과 접근에 대한 사용자별 접근 제어: 서버의 정보나 자원에 대하여 접근하는 사용자에 대하여 특정 사용자나 특정 그룹에 소속된 사용자들에게만 허용할 수 있는 부분에 대한 접근을 제어할 수 있어야 한다.

그러므로 민감한 정보에 대한 접근은 구성원별로 차등을 둘 수 있어야 한다. 즉 읽기만 가능한 정보와 읽기와 쓰기가 가능한 정보 형태의 접근 제어가 가능하게 할 수 있다.

이러한 접근 제어에 대하여 다음과 같은 용어를 사용하여 구분하기도 한다.

- **Fine-grained Security:** 서버의 객체 단위 접근 제어를 의미한다. 예를 들면, 파일, 디렉토리 등에 대한 정교한 접근 제어를 의미한다.
- **Coarse-grained Security:** 여러 서버로 구성된 네트워크에서 각 서버에 대하여 접근하는 사용자를 서버 단위로 제어할 수 있는 기능을 의미한다.

② 민감하고 중요한 정보가 네트워크 간에 교환/전송될 때 클라이언트와 서버는 상호 인증 서비스를 제공할 수 있어야 하고 교환되는 메시지나 문서 자체에 대한 인증도 요구된다.

③ 웹을 이용하여 상품, 재화 또는 비밀 정보 등을 상거래하기 위한 응용은 전자 지불, 판매자의 정당성 인증과 구매자의 안전한 지불 기능이 요구된다. 이때 판매자와 구매자를 위한 인증 서비스도 요구된다.

④ 웹 상에서 이루어지는 통신 내용의 비밀 보장 서비스를 통하여 교환 정보가 타인에게 노출되지 않아야 한다.

■ 웹보안을 위하여 사용되는 보안 기술

기존의 보안시스템을 웹과 접목하여 웹에 보안 기능을 제공하고자 하는 대표적인 시스템으로는 OSF DCE, Kerberos, PGP 등이 있다.

① PGP(Pretty Good Privacy): 웹의 전자우편에서 암호화 및 전자서명에 많이 사용되고 있는 PGP와 모자익 웹의 CCI(Common Client Interface) 기능을 이용한 방법은 〈그림 5〉와 같다.

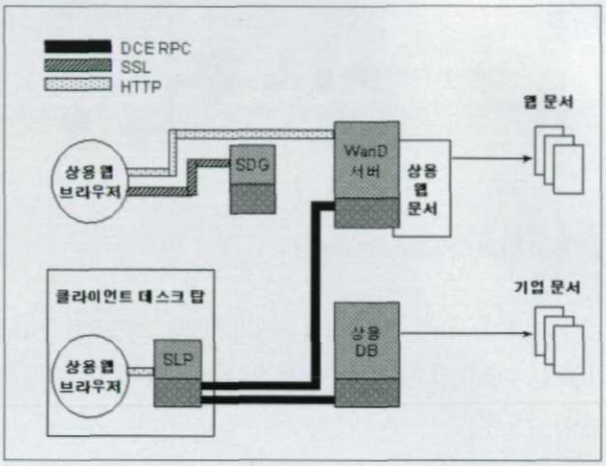
② DCE Web: DCE Web의 목적은 기업들이 웹 인터페이스를 통해 가용한 웹 문서, 서버 스크립트, 그리고 다른 서비스에 대한 안전한 접근을 제공할 수 있는 소프트웨어 요소를 제공하기 위한 소프트웨어를 유지하며, 모든 클라이언트/서버 통신은 웹에서 사용하는 TCP/IP보다는 DCE의 RPC(Remote Procedure Calls)를 사용한다.

기본적으로 DCE Web은 다음의 3요소로 이루어진다.

● **WanD 서버**: TCP 상의 RPC와 HTTP를 모두 사용할 수 있는 강력한 고성능의 웹서버로서 웹에 대한 안전한 접근과 표준적인 접근 모두를 지원하고 있으며 이미 설치된 웹서버와 손쉬운 통합을 위해서 WanD 서버를 프론트 엔드로 위치시킬 수 있다.

특별히 최근의 제품은 Public Key를 통합하여 SSL을 사용할 수 있다.

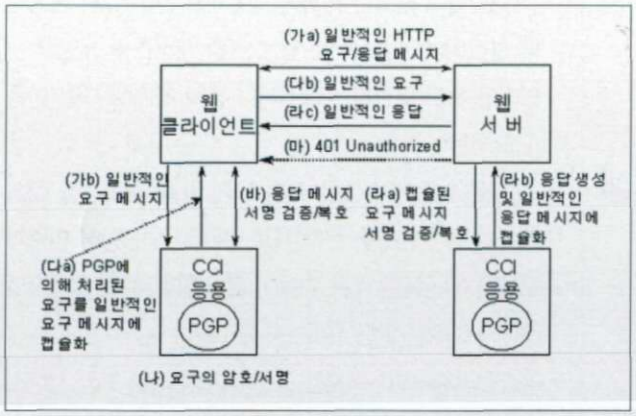
● **보안 로컬 프락시(Secure Local Proxy)**: 보안 로컬 프락시는 클라이언트 브라우저에게 DCE-Web에 안전하게 접근하는 근본적인 방법을 제공한다. 그러므로 상용 브라우저와 함께 클라이언트 컴퓨터에서 수행되는 작은 크기의 소프트웨어이다. 즉 보안 클라이언트 모듈이고 실제 HTTP를 RPC로 변환시킨다. 이를 이용하지 않을 경우, 특별한 접근이 불가능하며 표준적인 웹서버로의 접근이 허용된다.



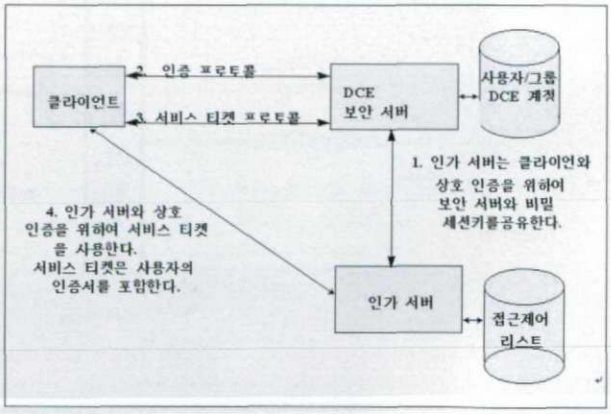
〈그림 6〉 DCE WanD 웹 서버 구조

● **보안 도메인 게이트웨이(Security Domain Gateway)**: 보안 로컬 프락시가 설치되지않은 클라이언트에게 SSL 공개키 인증을 가능하도록 지원하고 이를 게이트웨이로 하여 보안 로컬 프락시가 설치되지 않은 클라이언트에서의 DCE Web의 개인 식별자와 패스워드를 사용하여 WanD 서버에 로긴할 수 있다.

③ 커버로스 웹(Kerberizing the Web): 커버로스 시스템을 이용한 웹 문서 접근 제어를 하고자 하는데서 대두되었으며 가장 중요한 이유는 네트워크 상에서 암호화되지 않은 패스워드의 전송을 막고자 한다. 현재 주로 사용되는 기본 인증이나 다이제스트 인증방법과는 대조적으로 민감한 중요 정보가 있는 모든 웹 서버에게서 패스워드 및 그룹 파일을 설정해야하는 관리 상의 번거러움을 피할 수 있다는 장점과 기본 인증과 같이 네트워크 상에서 패스워드가 전송되는 것을 막을 수 있다.



〈그림 5〉 PGP Common Client Interface

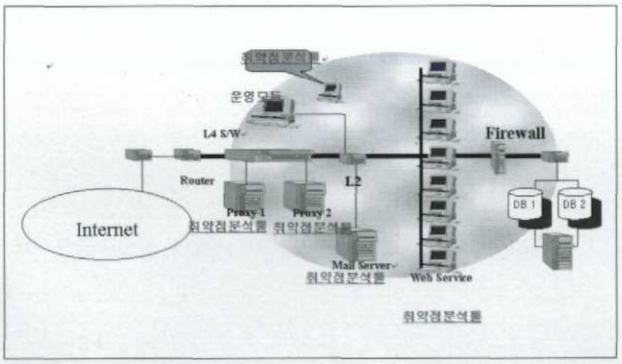


〈그림 7〉 커버로스를 사용한 DCE의 인증기법

4) 취약점 분석툴

취약점분석툴은 시스템 기반의 취약점 분석툴과 네트워크 기반의 취약점 분석툴로 구분되는데 가장 초기에 네트워크/시스템 구성의 정보와 취약점을 분석하기 위하여 사용되는 제품이 네트워크 기반의 취약점 분석툴이고 중요 시스템마다 취약점 분석 모듈을 실행하고 있는 제품이 시스템 기반의 취약점 분석툴이다. 쇼핑몰 운영자는 네트워크 취약점 분석툴을 통하여 원격 분석 및 시스템과 네트워크의 전반적인 분석이 가능하며, 중요 시스템의 취약점을 정밀하게 분석하고 대응하기 위하여 주기적으로 시스템 취약점 분석툴을 실행시킬 필요가 있다. 또한 시스템 취약점 분석툴을 통하여 O/S의 패치 여부, 계정 보안의 취약점, 최신 발견된 버그 등을 분석, 대응할 수 있게 된다.

그러나 네트워크 기반 취약점 분석툴과 달리 시스템 기반의 취약점 분석툴을 운영시킬 때에는 트래픽이 가장 적은 시간에, 그리고 너무 많은 항목의 취약점 분석을 해서는 안 된다. 경우에 따라서는 시스템 기반 취약점 분석툴을 운영시킴으로써 서비스에 결정적인 문제를 일으킬 수도 있다.



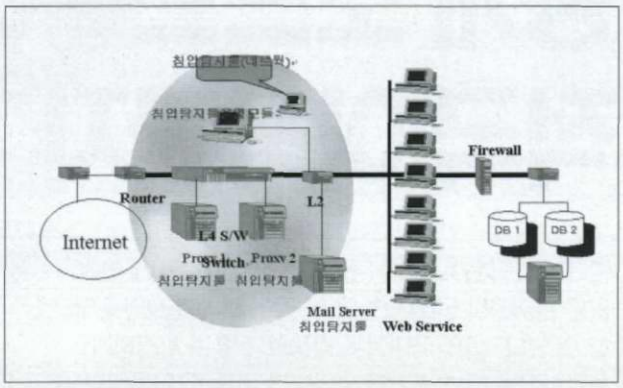
〈그림 8〉 취약점분석툴의 적용

5) 침입탐지툴

침입탐지툴은 네트워크 상이나 개별 시스템에서 불법적인 침입 시도를 발견한다.

역시 네트워크 기반의 침입탐지툴과 시스템 기반의 침입탐지툴로 나눌 수 있으며, 취약점 분석툴과 마찬가지로 시스템 기반의 침입탐지툴은 각 시스템에 침입탐지툴의 모듈을 각기 장착시킴으로써 개별 시스템에서 일어나는 침입시도를 모니터링하고 대응할 수 있다. 시스템 기반의 침입탐지툴은 자신에게 설정된 침입 및 불법접근 시도에 관하여 그 세션을 차단할 수 있으며 전화나 호출기 등을 통하여 이를 운영자에게 통보한다.

그러나 네트워크 기반의 침입탐지툴은 시스템과 네트워크 장비의 테이블까지 실시간 감시를 할 수 있으며, 침입 시도 시스템에 역공격을 가할 수 있는 기능이 연구, 검토 중이다.



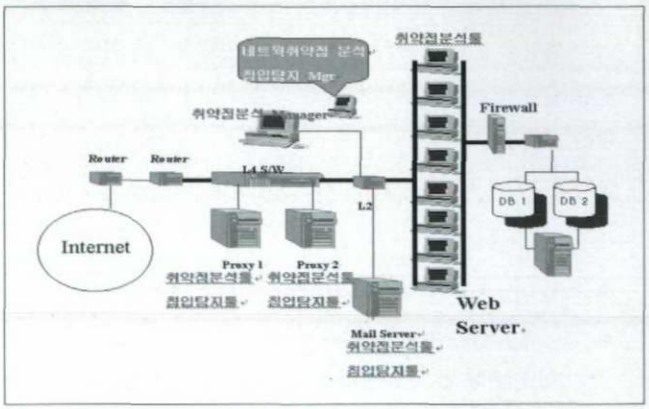
〈그림 9〉 침입탐지시스템 적용

6) 보안제품 간의 상호연동 구현

쇼핑몰 보안을 위하여는 많은 보안 솔루션과 네트워크의 재구성이 이루어져야 한다.

먼저 웹서버는 Dual-Home 구조를 가지며 데이터베이스 서버는 침입차단시스템에 의하여 분리된 다른 네트워크에 위치한다. 그리고 각기 침입탐지툴과 취약점분석툴, 침입차단시스템 간에는 동적인 연동이 이루어져야 한다. 새로운 유형의 침입시도를 발견시에는 보안툴 간의 유기적인 대응이 이루어질 수 있으며, 실시간으로 이러한 침입과 공격에 대한 툴 간의 상호 반영으로 보다 효과적인 보안을 유지할 수 있다.

또한 운영자는 이용자가 가장 적은 시간에 취약점 분석툴이 시스템을 분석하도록 설정함으로 주기적인 패치 및 취약점 보완을 실시하여야 하며, 개발 업체는 주기적인 제품 업그레이드 및 새로운 보안 규칙을 제공하여야 한다.



〈그림 10〉 보안 적용과 네트워크 재구성을 적용한 쇼핑몰의 예