차세대 네트워크 보안기술 기반의 침입방지시스템(IPS)

윈스테크넷 조현정

1. 네트워크 보안기술 동향

네트워크, 시스템에 대한 악의적인 접근과 정보위협이 증가하고, 그 피해 또한 기업에서 개인사용자까지 확대되고 있다. 그러나 네트워크는 몇 가지 취약성을 갖고 있다.

외부 네트워크와 내부 네트워크를 연결하는 라우터와 스위치는 Session기반의 해킹시도에 대한 방어나 단순 패턴 매칭에서의 오탐율(False Positive) 최소화 분야에 단점이 있는 것은 누구나 다 아는 이야기다.

네트워크 보안의 가장 기초적인 1세대 솔루션인 방화벽(Firewall)은 서비스 기준으로 방어정책을 설정함으로써 내부자용 서비스를 이용한 우회 공격에 대한 취약성을 갖고 있고, Web, SMTP, DNS 등 허용된 룰에 대해서는 무방비한 상태며, ID/FW 방식의 사용자 인증에 대한 취약성을 갖고 있어 백도어 등의 설치 시 암호 노출의 가능성이 크다는 이야기도 또한 보안관계자는 다 아는 이야기임에 틀림없다.

반면 침입탐지시스템(IDS)은 일반적으로 방화벽 다음에 구축되어 방화벽을 우회한 공격에 대해 분석, 탐지 기능을 제공한다. 그러나 단순한 CCTV의 역할을 수행해 분석과 감시는 가능하지만 발견과 동시에 차단 등의 대처능력에는 한계가 있다. 특히 Packet Passive 방식으로 작동해 패킷을 캡쳐해 분석하기 때문에 한번의 공격으로 이미 내부 시스템까지 감염되는 One-way Attack에 대해서는 사후 근거제시 외 방어는 어렵다.

이들 네트워크 보안시스템은 유기적으로 연동해 네트워크 위협을 최소화하고 공격을 완화하는데 중요한 역할을 하고 있지만, 각각의 취약성으로 인한 또 다른 위협을 야기하기도 한다.

이로 인해 요구되고 있는 기술은 △발생가능한 위협을 사전에 방지함으로서 자율적인 보호가 가능한 방지기술 △침입이 발생한 후에라도 역추적을 통해 근본 원인을 제거하거나 근본적인 취약성으로부터 시스템을 복원하는 능동적인 대응기술 △침입이 발생하더라도 신뢰할 수 있는 서비스를 제공하는 감내기술 등이다.

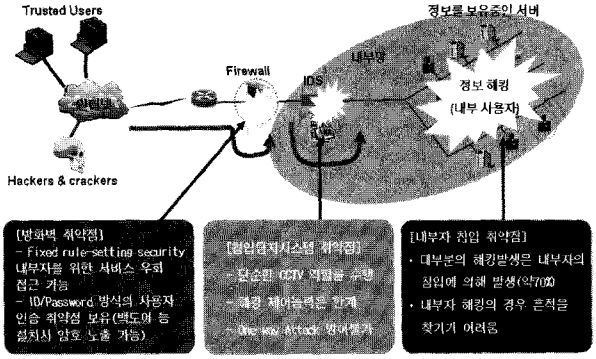

그림 1 네트워크 취약성

즉, 네트워크의 위협을 사전에 탐지하여 적절한 대처를 통해 침해사고를 방지하거나 그 피해를 최소화하는 것이 가장 완벽한 네트워크 보안이라 할 수 있다.

1.1 Protection 기술

일반적으로 라우터의 ACL(Access Control List)나 Stateless(비상태정보분석) 형태의 방화벽 또는 IPChain 기술 등이 가지고 있는 방어기법인 Packet Level Protection은 Two-way Communication에 절대적으로 약점을 갖고 있다. 일반적으로 단방향으로 방어를 구현하기 때문에 내부에서 외부로 쿼리된 트래픽(정상적인 트래픽)을 판단하지 못하는 단점이 있다. Packet Level 장비들은 일반적으로 다양한 프로토콜을 지원하지 못한다. 이는 서버와 클라이언트간에 데이터 전송을 위한 Random Port를 교환하는 일에 대하여 Traffic Flow를 판단하지 못하는 단점에서 기인한다.

Session Level Protection은 Network Flow를 통제할 수 있으며, 여러 시스템들의 Session 상태정보 추적과 드롭된 패킷의 정보를 파악할 수 있다. 일반적으로 Stateful Inspection Engine을 가진 방화벽들이 이러한 Connection-based 공격을 방어하는 기능을 가진다. Session Level 장비들은 일반적으로 개별적인 TCP Session안에 대량의 접속정보를 포함하고 있으며

다양한 프로토콜을 제공하여 인식된 포트를 통해 송수신되는 명령어 그룹을 판단하는 기능을 가진다.

Application Level Protection은 정밀하게 Network Flow를 파악하여 각종 공격과 침입을 탐지 및 방어할 수 있으며 특정한 어플리케이션을 이용한 공격 방법들을 차단할 수 있다. Protocol Attack, Buffer Overflow, Null Operation Code 등과 같이 어플리케이션을 공격하는 패턴들을 방어할 수 있다. Application Level 장비들은 일반적으로 Protocol Analysis, Traffic stream을 Reassemble함으로서 웜이나 바이러스 또는 컨텐츠의 헤더부분까지 분석이 가능하나 근래의 컨텐츠 위주의(첨부파일웜) File Level Protection은 불가능하다는 게 업계 전문가들의 의견이다.

File Level Protection은 네트워크 트래픽에서 파일을 추출하여 메일이나 네트워크를 통해 전파되는 웜, 바이러스, 트로이목마 등의 Malware의 본체를 정밀하게 검사하여 방어할 수 있다. 해킹이나 바이러스, 웜 등이 가지는 시그네처를 분석하여 HTTP Traffic(BBS Hack), E-mail Traffic(attached file)에 포함된 파일들의 해킹 진위와 감염여부를 파악할 수 있다. File Level 장비들은 일반적으로 IPS 또는 Gateway anti-virus 시스템 등이 해당되며 Packet Reassemble, File inspection(MIME, uucode, Base64)함으로서 웜이나 바이러스 또는 컨텐츠의 완벽한 검증 및 방어가 가능하다.

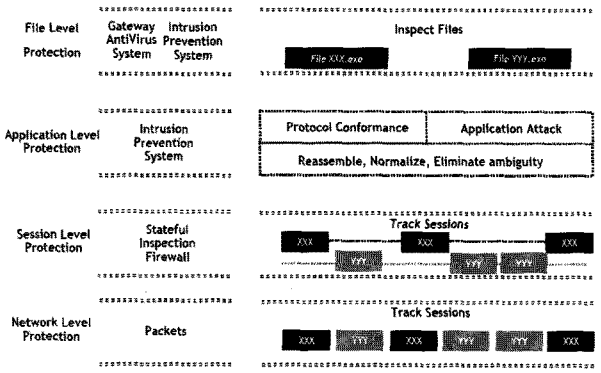

그림 2 계층별 방어장비

1.2 패킷검사기술(Inspection)

Stateful Inspection에서 패킷은 방화벽 패킷 필터링 위치에서 인터셉트되며 Inspection 엔진이 다음 임무를 수행한다. Inspection 엔진은 모든 어플리케이션으로부터 보안정책 결정을 위해 상태 관련 정보를 추출해낸다. 추출된 정보는 이어지는 연결시도를 감시할 수 있도록 동적 상태정보테이블(Dynamic Hashing Table)에서 유지 관리된다. Inspection 모듈은 TCP/IP Stack 중 가장 낮은 계층(MAC Layer)에서 작동하여 일반적인 어플리케이션 방화벽보다 빠른 처리속도를 구현하며, 보안관리에 있어서는 그 위의 모든 계층에 해당하는 관련 데이터들을 동시에 모두 추출하여 보안 규칙을 적용함으로써(어플리케이션별 상태정보 적용) 편리성을 제공한다.

Stateful Inspection에서 탐지 또는 방어하지 못하는 데이터 영역까지 추출해 낼 수 있는 DPI(Deep Packet Inspection)는 Protocol, Port, IP address 등의 헤더 정보와 Payload를 분석하여 탐지 패턴과의 해킹 진위여부를 분석할 수 있다. DPI는 DoS 공격, BoF 공격, NOP 공격, 컨텐츠 필터링에 대한 방어기능을 제공해 유해트래픽이 대상 네트워크나 시스템에 접근하기 전에 패킷을 차단시키는 능동적인 차단기능을 제공한다. Single Packet에서는 웜 방어기능이 가능하나 최근의 파일 단위의 웜은 방어가 불가능하다. 또한 고속으로 패킷을 처리하는데 적합하나 해킹이나 웜 코드가 단편화되어 전송되는 것은 탐지 및 방어가 불가능하다. Packet Reassemble 기능을 갖고 있지 않아 특정한 Evasion 공격에 대한 탐지 및 방어가 불가능하다.

Deep Packet Inspection에서 탐지 또는 방어하지 못하는 데이터 영역을 추출해낼 수 있는 고밀도 탐지엔진 ALSI(Application Level Stateful Inspection)는 Packet Reassemble, Normalization 기능을 갖고 있어 특정한 Evasion 공격에 대해서도 탐지 및 방어가 가능하다. 또한 DoS 공격, BoF 공격, NOP 공격, 컨텐츠 필터링에 대한 방어기능을 제공해 유해트래픽이 대상 네트워크나 시스템에 접근하기 전에 패킷을 차단한다. File, Documents, Program 등과 같은 Application Level 객체 안의 Payload를 Reassemble 하여 정확한 탐지 및 방어기능을 제공하며 컨텐츠 기반의 공격을 방어할 수 있다. 웜, 바이러스, 트로이목마, 부적절한 웹 컨텐츠(XSS, Infection), 이메일 스팸 등 단편화되어진 정보를 정확하게 탐지 및 방어한다.

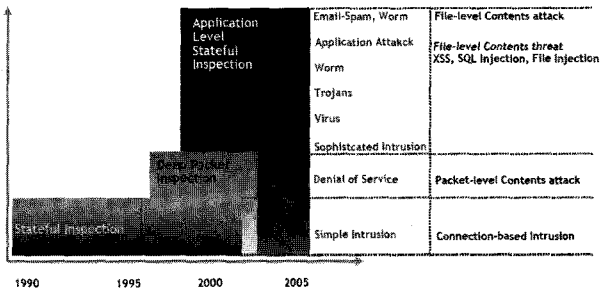

그림 3 Inspection의 범위

이같이 어떠한 방식을 기반으로 하느냐에 따라 보안 시스템의 보안성과 성능도 판가름난다고 할 수 있다.

실제로 일반적으로 열어놓는 서비스 포트에 대해서는 정상 트래픽으로 간주해 무조건 통과시키는 단순한 포트 기반의 방어방법인 방화벽은 Stateful Inspection기능으로 업그래이드 되었다. 그러나 실제 해킹의 진위는 판단할 수 없다.

IDS는 Packet Passive방식으로 방화벽을 통과해 시도되는 해킹 공격들을 정밀하게 탐지하지만 방어할 수는 없어 방화벽과의 연동으로 해킹 탐지 후 방화벽에 차단명령을 전달하는 방식으로 사용되어 왔다. 그러나 이 역시 One Way 공격(BOF, NOP)은 이미 패킷이 통과해 내부 감염이 끝난 상태가 되기 때문에 근본적인 방어는 어렵다.

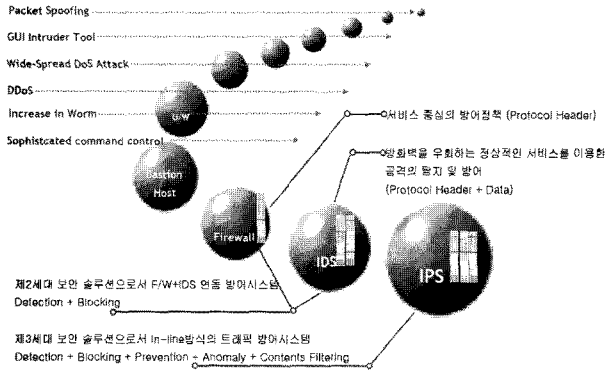

그림 4 네트워크 보안 시스템의 진화

2. 차세대 능동형 침입방지시스템(IPS)

이러한 네트워크 보안 기술의 진화로 보다 능동적인 대응이 가능한 침입방지시스템(IPS)이 나오게 되었다.

IPS는 방화벽, IDS 등을 기반으로 하지만 각각의 시스템이 갖는 취약성을 해결하기 위해 다양한 방식으로 개발되었고, 다양한 기능을 수행하고 있다.

IPS는 침입차단, 침입탐지, 바이러스 웜 및 유해 사이트 차단 등의 기능을 유기적으로 제공하면서 최상의 성능으로 공격의 탐지 및 방어를 수행하되, 기본적으로 네트워크 지연을 최소화하고 서비스의 중단이 없도록 별도의 대응기능을 포함한 시스템이다.

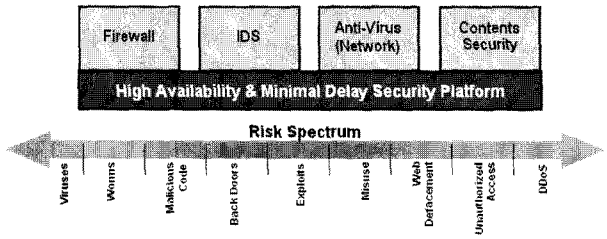

그림 5 IPS의 개념도

Deep Packet Inspection, Normalizarion, Reassemble, Pattern Matching, Packet Drop, Blocking list Registration의 기술로 마이둠, 베이글 등 이메일 웜과 One Way 공격을 차단하며, Application Level Stateful Inspection 기술로 HTTP Script Infection, Two-way 공격도 차단한다.

2.1 IPS의 핵심역할

2004년은 보다 다양하고 위협적인 웜이 출현하여 전 세계적으로 기업과 기관, 개인 사용자까지 큰 피해를 입힌 해였다. 대표적인 악성코드는 마이둠(MyDoom), 베이글(Bagle), 넷스카이(Netsky), 새써(Sasser) 등이다. 이들 대형 웜은 다량의 변종을 낳으면서 그 피해도 확대시켰다.

올해 1월말 첫 발생한 마이둠 웜은 이메일과 P2P 공유 프로그램을 통해 급속도로 전파되면서 27시간 만에 168개국 150만 건의 피해를 입혔다. 베이글 웜 역시 1월에 처음 발견되어 다양한 변종들을 발생시켰고, 비슷한 시기에 출현한 넷스카이 웜이 베이글 웜을 제거하는 등 경쟁적 웜 제작으로 이어져 사용자의 피해를 급증시켰다. 새써 웜은 4월 말 발견되었으며 넷스카이나 베이글 등과 달리 많은 변종을 만들어 내지는 않았으나 매우 빠른 속도로 확산하여 전세계 1,500만대 이상의 컴퓨터 피해를 유발하였다.

이렇듯 현재 국내·외 네트워크의 가장 큰 위협은 웜 등에 의한 유해트래픽이라 할 수 있다. 지난 1.25 인터넷 대란의 원인인 슬래머(Slammer) 웜이 그랬고, 국내 인터넷서비스제공업체(ISP)의 대형 백본(Backbone) 망에서 송·수신되는 평상시 트래픽 중 약 10%가 정상적인 서비스와 무관한 트래픽이라는 점을 봐도 그렇다.

따라서 IPS는 유해트래픽 차단을 통해 네트워크 자원의 효율성을 높일 수 있어야 하며 기본적으로 다음과 같은 조건을 만족시켜야 한다.

① IPS가 작동하든 안하든 네트워크 트래픽은 항상 동일하게 동작해야 하며, IPS가 정상적인 패킷 흐름을 방해해서는 안된다.

② 해당 네트워크의 최대 사용 속도 이상의 처리 성능을 보장하는 In-Line 네트워크 디바이스로 작동해, 패킷(Data)의 흐름 안에서 패킷과 세션을 분석하고 탐지(식별)한 후 어떤 것들이 악의적인지 판단해 실시간으로 차단(Drop)해야 한다.

③ IPS는 알려진 공격에 대한 시그네처 분석을 넘어 네트워크 과부하를 일으킬 가능성이 있다고 정의된 프로토콜/패킷에 대한 탐지, 알려진 트래픽 패턴에서 벗어나 급격하게 변화하는 이상 트래픽을 경고하는 행동기반의 통계(Behavior Based Statistics)

분석 등 여러 방법론을 조합해 오탐지(False Positive)를 최소화하면서 침입 시도를 최대한 잡아내야 한다.

④ IPS는 복잡한 절차의 공격 시도는 물론, 슬래머 웜과 같이 패킷 단위로 이루어 지는 공격에 대해서도 탐지 및 차단 기능을 제공해야 한다.

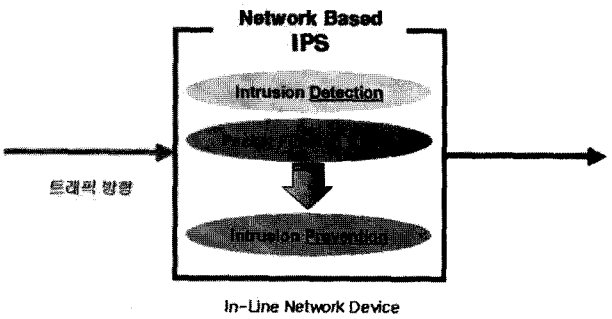

그림 6 In-Line 방식의 네트워크 IPS

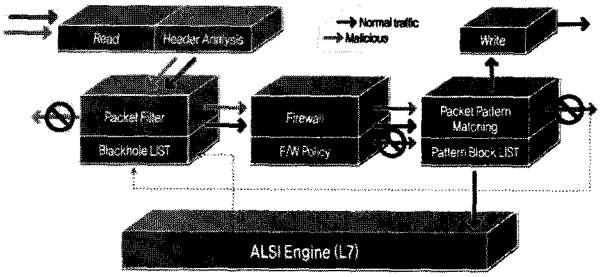

그림 7 IPS의 Engine Flow

2.2 IPS의 기능

IPS는 실시간 네트워크 트래픽 분석과 데이터 감시를 통해 정교한 해킹에서 웜, One-Way 공격형태 등 비정상으로 판단된 네트워크 트래픽을 안정적으로 차단한다.

2.3 IPS의 종류 및 발전방향

IPS는 IDS에서의 접근, 방화벽에서의 접근, 네트워크 장비에서의 접근 등 다양하게 접근해 다양한 형태로 개발, 출시되고 있으며 비정상 트래픽과 해킹의 사전 차단이라는 공통 목표로 발전하고 있다.

L7 스위치 기반의 IPS는 어플리케이션 컨텐츠(HTTP, DNS, SMTP)의 로드밸런싱, 라우팅, 스위칭을 위해서 개발된 장비로서, DoS/DDoS 공격과 시그네처 기반의 공격에 대한 대응이 가능하다. 인라인 방식의 침입탐지시스템과 유사하게 동작하나 시그네처 DB기술이 없는게 일반적이다. 특히 Session 기반의 탐지, 차단, 세밀한 차단정책 설정의 기능을 제공할 수 없으며, DPI기법을 응용한 Reassemble 및 Normalization이 불가능하다.

Stateful Inspection 기반에 DPI가 추가된 방화벽의 기술로 개발된 IPS는 DPI 방식의 탐지기법에서 문제가 되는 단편화된 웜을 정밀하게 탐지하거나 방어할 수 없으며, Session기반의 탐지, 차단, 세밀한 차단정책의 요소가 없다.

IDS 기반의 IPS는 각종 어플리케이션 컨텐츠의 정밀한 탐지 및 방어기능을 제공한다. ALSI와 DPI의 Dual Engine을 채택해 단편화된 멀티 패킷의 탐지 및 방어기능을 제공하기 때문이다.

Gateway Antivirus 기반의 IPS는 바이러스와 웜을

표 1 IPS의 주요기능

네트워크 트래픽 분석 (Traffic Breakout)	실시간 네트워크 트래픽 현황
	Protocol/Service별 네트워크 트래픽 트랜드 분석
	Packet Size/Protocol/Service/IP별 트래픽 분류 통계분석(Anomaly)
실시간 Network Data 감시	실시간 Network Data의 흐름 모니터링 및 로깅
	내부/외부 네트워크를 구분하여 세분화된 모니터링
	10/100 및 Giga 트래픽에서 네트워크 속도 저하 없이 안정적인 정상 동작 및 유해트래픽 차단
비정상 네트워크 트래픽 차단	방화벽 기능(Stateful Inspection 기능)
	정교한 해킹의 탐지, 추적, 차단
	침입 유형별 세부 탐지 및 차단
	Worm 탐지 및 차단
	In-Line Mode로 운영되는 Transparent 보장
	One-Way Attack 차단(Buffer overflow, No operation Code)
	침입탐지 내역 및 차단 현황에 대한 관리자 알림 기능(Alert, E-mail 등)
	Application-Level Stateful inspection Engine으로 오탐율 최소화
	해커 경로 및 근원지 추적
	탐지된 공격에 대한 추이 분석, 통계 분석 및 보고서 제공

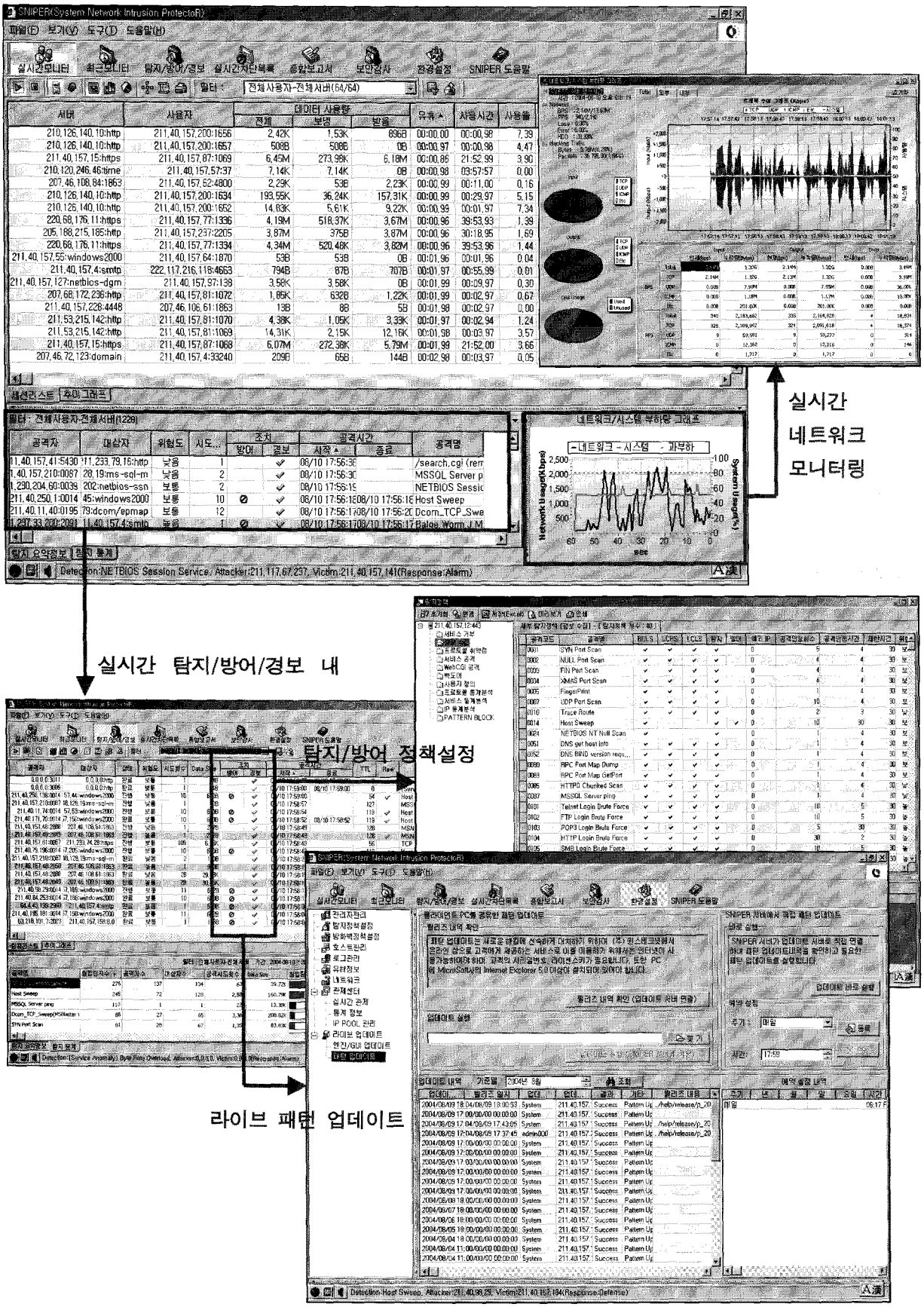

그림 8 IPS의 주요 운영화면

방어하기 위해 개발된 장비로서 해킹 탐지와 관련된 노하우가 부족하다. 즉 해킹에 대한 DB부족과 프록시 방식의 엔진구성으로 인한 과도한 네트워크 처리의 과부하를 어떻게 줄이느냐가 가장 큰 과제이다. 그러나 File Level의 탐지 및 방어기능을 제공하고 가장 상위의 Layer를 열어볼 수 있다는 장점을 보유한다.

결국 침입방지기술의 발전방향은 어플리케이션 레벨의 정밀한 데이터검사 기술과 기가비트 네트워크 환경에서의 과부하 극복이라는 두 마리 토끼를 동시에 잡는 방향으로 발전하고 있다.

방화벽과 IDS가 가지고 있는 근본적인 한계를 극복하고자 등장한 IPS는 네트워크 레벨에서 파일 레벨까지의 광범위한 계층에 분포되어 있는 악성트래픽을 효과적으로 탐지할 수 있는 검사기술와 이에 대해 효과적으로 대응할 수 유연한 정책관리 기능이 필수적이다.

아울러 이를 기가비트 네트워크 환경에서 뒷받침할 수 있는 고속 전용칩 하드웨어 형태의 제품으로 개발해 고속 데이터 처리성능을 보장하는 것이 중요하다.

2.4 IPS 시장전망

IPS 시장은 현재 인터넷서비스제공사(ISP)를 포함하여 전 분야에서 신규 도입을 고려하고 있을 만큼 성장하고 있다. 2003년 시·군·구 지방차지단체와 대학에서 먼저 도입하기 시작했고 최근 금융권에서 검토하기 시작해 현재 전 분야로 확대되고 있다.

초기 IPS 시장은 기술적인 개념에 대한 논란으로 시작해 고객의 혼란이 있었으나, 현재 시장이 어느정도 정착되어 외산 제품들도 국내시장에 승부수를 던지고 있다.

IPS는 현재까지 20여 개 이상이 출시되었고, 이 중 4-5개 국내 제품과 5-6개 외산 제품이 국내 네트워크 보안시장의 주류를 형성하고 있다.

이에 따라 국내 공공시장에서 필수로 요구되는 국가정보원의 CC(국제공통평가기준)인증에 관심이 집중되고 있다. 현재 IPS에 대한 CC인증은 기반기술의 보호프로파일(PP)을 기준으로 IPS 평가 가이드를 적용해 침입방지기능에 대해 인증해주는 형태로 진행되고 있다. 윈스테크넷, 시큐아이닷컴, 어울림정보기술 등 5개 국내 제품의 평가가 진행중이며, 몇 개 업체가 평가를 위한 자문을 진행하고 있다.

정부 및 공공기관에서는 내년 상반기까지 인증을 받는 제품 3-4개의 경쟁이 가시화될 것으로 보이며, 금융권 일부와 일반기업의 경우 외산과 토종업체 간의 경쟁이 이어질 것으로 전망한다.

조 현 정

관심분야 : 컴퓨터, 정보보호, 마케팅, 기획
E-mail : ajanee@wins21.com