정보통신 시스템 인프라를 위한 침입 방지용 통합 보안 기술

한국전자통신연구원 김정녀, 장종수, 손승원

차 례

요 약

기존의 정보통신 보안 인프라 강화를 위하여 많은 개별 보안 시스템들이 활용된다. 침입차단, 침입탐지, 그리고 가상사설망 장비들을 설치하여 보안성을 향상 시켰는데, 이로 인하여 각 보안 시스템 간의 정책 충돌이 발생하기도 하여 보안상 효율성이 떨어지기도 하고, 여러 보안 시스템들을 관리하여야 하는 관리 상의 복잡성과 비용상의 문제점이 존재한다. 이를 해결하기 위하여 침입탐지, 침입차단, 그리고 가상사설망 기능을 통합하여 제공하는 통합 보안 엔진 개념이 부각되었으며, 이러한 통합 보안 엔진 기능을 라우터에 탑재하여 정보통신 인프라의 보안성을 강화시킨다.

본 논문에서는 통합 보안 엔진을 라우터나 스위치 등과 같은 네트워크 노드에 탑재하여 안전한 네트워킹이 가능하도록 하는 보안 프레임웍을 소개한다. 또한 침입탐지, 침입차단, 가상사설망 기능을 통합하여 제공하는 라우터용 통합 보안 엔진의 구조를 소개하고, 이를 위해 구현된 핵심 기능을 기술한다. 이러한 통합 보안 엔진이 탑재된 보안 라우터와 기존의 보안 기능이 있는 상용 라우터와의 비교를 통하여 통합 보안 엔진이 탑재된 보안 라우터 시스템의 효율성을 설명한다.

한글키워드 : 통합 보안 엔진, 방화벽, 침입탐지, 가상사설망, 노드 침입 감내

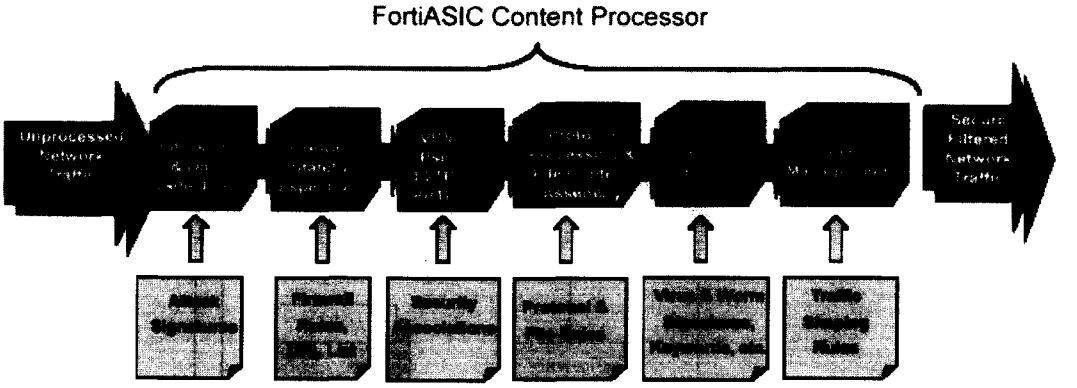
영문키워드 : Integrated Security Engine, Firewall, Intrusion Detection, Virtual Private Network, Node Intrusion Tolerance

1. 서 론

초고속통신망의 보급으로 인하여 우리나라는 어느 선진국보다도 정보통신 인프라 구축이 잘 되어 있어, 좋은 네트워크 환경과 폭 넓은 사용자를 확보하고 있다. 2004년 7월말 초고속 인터넷 가입자수는 1,167만 명에 달하고 있으며, 2003년 말 전자상거래 규모가 235조 원, 인터넷을 통한 전자상거래 비중은 전체의 16.5%에 이르고 있는 실정이다[1][2]. 이처럼 인터넷을 통한 전자상거래가 급증하고 네트워크 이용이 크게 증가하면서 외부 침입 및 내부자의 중요 기밀 문서 외부 유출이 중요한 사회적 문제로 떠오르고 있다[3]. 이렇듯 정보화가 발전될수록 인터넷의 해킹은 갈수록 늘어가고 있으며, 이러한 정보화 역기능에서 발생되는 문제점들을 해결하기 위해 더 많은 노력이 필요하다. 최근 들어 해킹, 바이러스 등 사이버 상의 위협은 점차 자동화, 지능화, 대중화, 분산화, 대규모화, 은닉화되어 가는 경향을 띠고 있으며 단순한 실력 과시용 위협에서 점차적으로 악성화, 경제 범죄화되고 있다[4]. 이렇듯 정보화가 발전될수록 인터넷의 해킹은 갈수록 늘어가고 있으며, 이러한 정보화 역기능에서 발생되는 문제점들을 해결하기 위해 더 많은 노력이 필요하다. 최근 들어 해킹, 바이러스 등 사이버 상의 위협은 점차 자동화, 지능화, 대중화, 분산화, 대규모화, 은닉화되어 가는 경향을 띠고 있으며 단순한 실력 과시용 위협에서 점차적으로 악성화, 경제 범죄화되고 있다[4]. 이와 같이 해킹 기법의 변화와 해킹의 목적이 바뀌어 감에 따라 이에 대응하기 위한 새로운 방어 수단들의 개발이 필요하며, 최근에는 시스템 위주의 독자적인 공격보다 네트워크를 통한 동시 다발적인 공격이 증가하고 있어 이러한 해킹 기법에 대응하기 위한 정보통신 인프라 보안의 필요성이 더욱 대두되고 있다[5].

이를 막기 위한 솔루션으로 방화벽, 침입 탐지 시스템, 그리고 가상 사설망 등의 개별 보안 시스템들이 있다. 그러나 이 개별 솔루션들은 각자 나름대로의 역할을 하기도 하지만 상호 연계하여 운용되었을 때에 더욱 효율적이다. 그러나 서로 다른 이 기종의 개별 보안 시스템을 상호 연계하여 사용할 때 상호 연동 문제가 발생하며, 상호 운용 시에는 관리의 복잡성과 어려움이 대두되었다. 이를 극복하기 위해 각 개별 보안 솔루션을 통합하고자 하는 통합 보안 솔루션의 개념이 등장하였다. 또한, 공격의 발전 형태를 보아도 초기에는 시스템 공격 위주로 한 해킹 기법들이 시도되다가 점차 네트워크와 서버를 마비시켜 서비스를 방해하는 형태로 발전되고 있어, 개별적인 보안 솔루션 보다 시스템과 네트워크 전반에 걸친 통합적인 보안 솔루션에 대한 필요성이 제기 되었다[6][7]

기존의 인터넷 망에서는 방화벽[9][10][11], 침입탐지시스템[11], 가상사설망 시스템[11], 서버 보안 시스템 등 여러 가지의 개별 보안 시스템들을 통하여 여러가지 보안 해결책을 마련하였다. 그러나 이러한 환경에서 네트워크 상에 다수의 방화벽 또는 다수의 침입탐지시스템 등 개별 보안 시스템이 설치 되어 있을 경우, 각각의 방화벽이나 침입탐지시스템에 대한 정책을 관리하는데 있어서 정책이 서로 충돌하거나 하나의 개별 보안 시스템에 설정된 정책이 다른 개별 보안 시스템에 영향을 줄 수 있다. 이에 따라 네트워크 방화벽의 존재가 무의미해지거나 네트워크의 정상적인 동작을 방해할 가능성도 존재한다. 또한 기존의 개별 보안 시스템의 경우에는 침입탐지와 차단이 별도로 이루어져 빠른 대응이 어려울 수 있으며, 네트워크 차원에서의 보안 문제를 근본적으로 해결할 수 없었다. 이러한 문제점을 해결하기 위하여 방화벽, 침입탐지시스템, VPN 시스



〈그림 1〉 Fortigate 시스템 보안 기능 구조

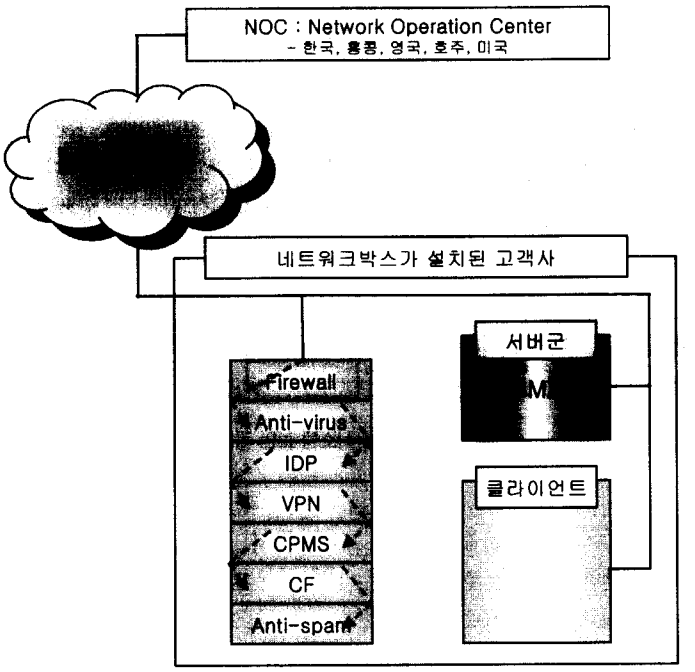
템, 그리고 서버 보안 시스템의 기능을 하나의 통합된 보안 엔진으로 구현하여 보안 관리가 용이하고 비용 측면에서도 저렴하며, 신속한 대응도 할 수 있도록 하였다.

이러한 통합 보안 엔진의 개념을 그 장점을 극대화하기 위하여 통합 보안 엔진 기능을 탑재하여 통합 보안 장비로 개발한다거나 라우터나 스위치 등과 같은 네트워크 장비에 여러가지 보안 기능을 통합하여 탑재하는 방식으로 개발이 이루어지고 있다. 전통적인 라우터는 패킷의 포워딩을 목적으로 개발된 제품으로, 내부 네트워크와 외부 네트워크를 연결하여 주는 중요한 장비이다. 본 고에서는 개별 보안 시스템의 문제를 해결하고, 보안 관리가 용이한 네트워크 노드(라우터 및 스위치)용 통합 보안 엔진 개념을 소개하고자 한다. 통합 보안 엔진은 기존의 개별 보안 시스템의 기능인 방화벽, 침입탐지, 가상사설망, 그리고 침입감내 기능을 하나로 통합하여 시스템 및 네트워크 수준의 해킹을 감지 및 차단, 그리고 대응하는 보안 처리 엔진이다. 또한 통합 보안 엔진의 구조와 함께 통합 보안 엔진이 갖는 보안 기능 요소들을 기술하고 이를 탑재하여 내부망 내의 해킹, 바이러스, 웜 등과 같은 네트워크 위협 및 공격으로부터 보호 할 수 있는 안전한 라우터 시스템을 소개한다.

본 고의 구성은 2장에서는 통합 보안 엔진이 탑재된 제품 및 관련 연구에 대하여 소개한다. 3장에서 통합 보안 엔진의 개념과 필요성을 살펴보고, 본 연구실에서 개발한 보안 라우터용 통합 보안 엔진의 구조, 기능 그리고 현재 구현 정도를 소개한다. 4장에서 그 중 핵심 기술인 침입탐지/차단 및 가상사설망, 그리고 침입감내 기술의 설계 및 구현 내용을 기술한다. 5장에서 통합 보안 엔진이 탑재된 라우터와 기존의 보안 기능이 있는 상용 라우터를 비교하고 통합 보안 엔진이 탑재된 라우터의 장점을 제시한다. 그리고 마지막으로 결론과 앞으로 더 해야 할 연구의 방향을 제시해 보고자 한다.

2. 관련 연구 동향

보안 제품들은 개별 시스템에서 통합 보안 장비 형태로, 시스템 보안에서 네트워크 전반에 걸친 보안의 형태로 변화되고 있다. 특히 요즈음 들어서는 관리되어야 하는 보안 관리 기능도 무시하지 못한다. 최근 들어 통합은 거스를 수 없는 대세이다. 보다 능동적이고 지능화된 보안 솔



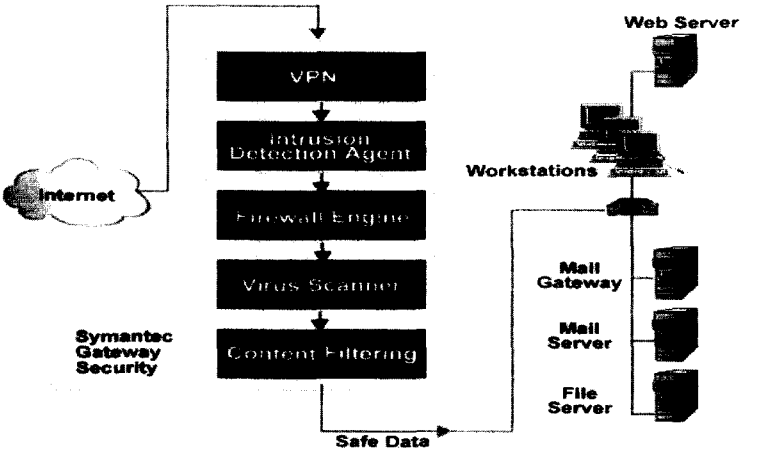
〈그림 2〉 Network-Box 시스템 보안 기능 구조

루션에 대한 요구가 금융권, 대기업, 통신사업자와 같은 대형 기업들의 필요에 의해 등장했다면, 지난 해부터 본격화되기 시작한 통합 보안 솔루션은 중소기업의 요구사항이 적용된 모델이다. 통합 보안 기능이 탑재되는 제품은 다음과 같이 크게 두 가지로 통합 보안 장비(Appliance)와 통합 보안 네트워크 노드(라우터 또는 스위치)로 나누어 볼 수 있다.

2.1 통합 보안 장비

최소 두가지 이상의 개별 보안 솔루션을 통합하여 제공하는 "통합 하드웨어 전용 제품"들로 개별적으로 보안 솔루션을 제공하는 것 보다 비용이 저렴하고, 관리가 용이하여 보안 시장의 주류가 되고 있다. 현재 국내에 소개된 제품은 대략 10 여개 정도로 요약되는데, 그 중 선두권으로 구분할 수 있는 업체는 시큐어소프트, 포티넷, 네트워크박스 등 3사이다. 이들 3사는 통합 보안 솔루션에 대한 업계의 부정적인 시각에도 불과하고 다수의 기업 고객들을 확보함으로써 통합이 대세 임을 입증해 보이고 있다. 방화벽, 침입탐지, VPN 그리고 항 바이러스 기능까지 제공하는 제품은 시큐어소프트 사의 수호신 Absolute 제품, 포티넷 사의 포티게이트, 네트워크박스사의 네트워크-박스 그리고 시만텍사의 Security Gate way 등이 있다.

- 시큐어소프트 사의 수호신 Absolute 제품 : 수호신 Absolute 제품은 기존의 방화벽, 침입탐지시스템 , 가상사설망 기능을 하나로 통합한 하드웨어 일체형(Appliance) 통합보안시스템으로 네트워킹 커널과 보안 소프트웨어가 통합된 핵심 모듈을 전용OS와 On-board로? 최적화하여 제공하는 솔루션이다. 수호신 Absolute 제품은 "전용서버 구비, OS 설치, 보안

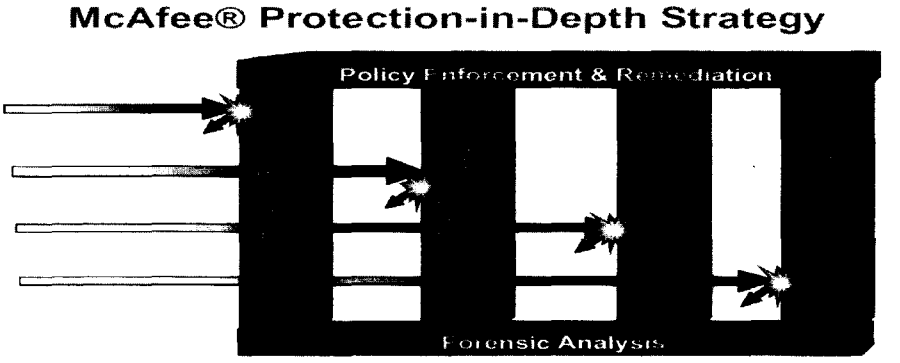


〈그림 3〉 시만텍사 Gateway Security 구조

소프트웨어 설치" 등 기존 보안 솔루션에서 필요했던 사전 준비 작업 없이, 원하는 곳에 배치(Deploy) 함으로써 최상의 보안 기능을 탑재한 보안시스템으로서의 완벽한 역할을 수행해 낸다.

o 포티넷사의 포티게이트[21]: FortiAsic 컨텐트 프로세서와 FortiOS 컨텐트 프로세싱 OS로 구성된 보안 장비로 방화벽 최대 2Gbps와 가상사설망 최대 7000Mbps 의 성능을 제공한다. 보안 기능으로는 Stateful-inspection Firewall, 고성능 침입탐지 기능과 DoS/DDoS 예방, 바이러스와 웜 스캐닝, 컨텐츠 필터링 그리고 트래픽 세이핑 기능을 제공한다. Fortigate 시스템이 제공하는 보안 기능 구조는 <그림1>과 같다.

o 네트워크박스 사의 All-in-one Solution 네트워크-박스 : 하나의 박스에 완벽한 보안 테크놀로지를 통합하여 보안 위협에 대하여 매우 효과적인 솔루션을 제공한다. 악의적 해커, 산업 스파이, 바이러스, 스팸 이메일 및 내부 직원으로부터 네트워크를 보호하고, 방화벽, 침입탐지시스템, 이메일 바이러스, 스팸 이메일, 가상사설망, 정책 관리 등의 기능을 제공하며 신종 바이러스 시그너



〈그림 4〉 네트워크 어소시에이트사 인투루쉴드 구조

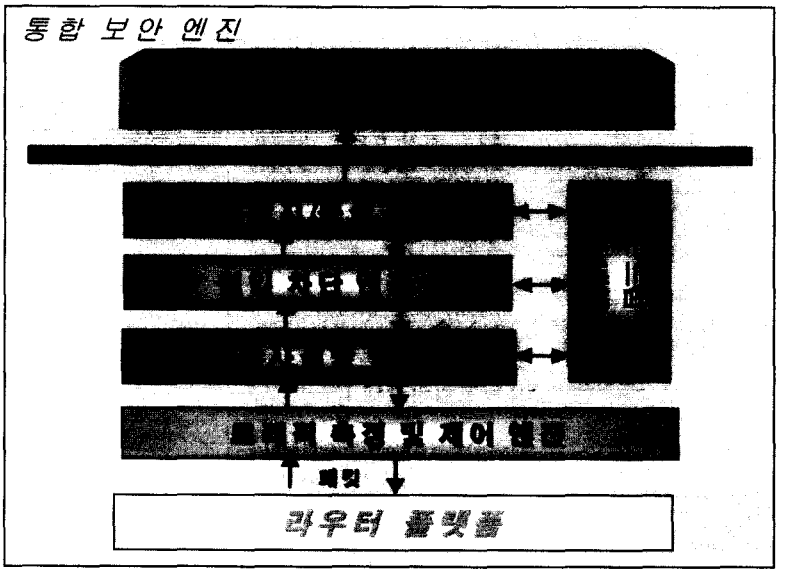
쳐 및 보안 패치 등의 자동적인 설치 등을 제공한다. 네트워크박스사의 ITP(Internet Threat Prevention) SME300, RM300, GB1000은 안티바이러스, 안티스팸, IDS, IPS, 콘텐츠 필터링, 방화벽, 가상사설망 기능을 통합 제공하는 장비와 더불어 글로벌 관제 센터인 NOC를 이용해 제품에 전문관리서비스까지 포함시킨 것이 특징이다. 제공하는 기능의 구조는 다음 <그림 2>와 같다.

- 시만텍사의 Security Gateway[22] : 방화벽, 침입탐지, 가상사설망, 컨텐츠 필터링 그리고 항-바이러스 기능이 통합된 다중 보안 기술이 구현된 보안 장비로 구조는 다음 <그림3>과 같다. 소프트웨어적으로 통합된 일체형 시스템으로 최대 성능은 90Mbps 정도이다.
- 네트워크 어소시에트사의 McAfee 인투루쉴드 : ASIC 기반의 하드웨어 일체형 장비로 통합 보안 기능 중 주로 IPS 위주로 구현된 제품이다. 인라인 모드로 제공되며, 동시 처리 세션수가 1,000,000 이고 성능 2G 정도이다. 제공되는 시그너쳐 개수는 2,700개 이상이고 기능은 Stateful Inspection, Deep Packet Inspection, 시그너쳐 기반의 탐지, 비정상 탐지(프로토콜, 응용, 통계치), URL 필터, 스팸 필터 등이 제공된다. 이러한 인트루쉴드의 보안 구조는 다음 <그림 4>와 같다.

2.2 통합 보안 네트워크 노드

보안 기능을 갖는 특수 목적의 네트워크 노드들로 라우터나 스위치에 방화벽, 침입탐지, 그리고 가상사설망 기능 등과 같은 보안 기능이 추가되어 있다. 현재 방화벽과 가상사설망 기능을 제공하는 제품으로는 엔터라시스 네트웍스의 XSR-3000, 노텔네트웍스의 Shasta 5000 BSN(Broadband Service Node) 등이 있으며, 추가로 침입탐지 기능까지 제공하는 제품으로는 CISCO 1710 보안 엑세스 라우터와 CISCO 6500 시리즈 스위치 등이 있다.

- 엔터라시스 네트웍스에 XSR-3000[25] : 고성능의 사용하기 쉬운 방화벽, 가상사설망 기능이 내장된 보안 라우터이다. 보통은 라우터, 가상사설망 게이트웨이, 그리고 방화벽과 같이 세가지 역할을 지원한다. XSR 라우터는 다중의 WAN을 지원하고 라우팅과 QoS 호스팅을 지원한다. 가상사설망 성능으로는 3DES 를 사용하여 300Mbps 성능으로 동시 3,000 터널까지 지원하며, IPSec, IKE, PKI, EZ-IPSec, PPTP, L2TP over IPSec, RADIUS, EAP, MS-CHAP v2 and v1 등을 제공한다. 상태 기반의 침입차단(Stateful Inspection Firewall) 기능도 제공하며, 상태 감시 엔진은 FTP, SMTP와 HTTP, 내부 호스트들을 위한 DoS 보호, 로깅, 인증과 NAT 기능 등을 지원한다.
- 노텔네트웍스의 Shasta 5000 BSN[24] : Shasta BSN 시스템은 IPsec, NAT, 방화벽, 암호화/인증 등의 기능과 함께 계층 2-3의 터널링 기능을 지원한다. 보안 기능으로는 자체 기술과 다른 보안 제품과 함께 통합하여 완벽한 보안 솔루션을 제공한다. 가상사설망 기능은 동시에 수천개의 가상사설망 터널 기능을 제공하고, ICSA에서 인증을 획득한 상태 기반 침입차단(Stateful Firewall), 방화벽과 IP 가상사설망 게이트웨이로 사용하는 등 고성능의 방화벽 기능을 지원한다. 고가용성 측면에서도 클라이언트 측의 지원이 필요없는 안전한 원격 응용 환경을 제공하는 SSL 외부망 기능을 지원하는 등 완벽한 통합 보안 기능을 제공한다. 그



〈그림 5〉 통합 보안 엔진 개념도

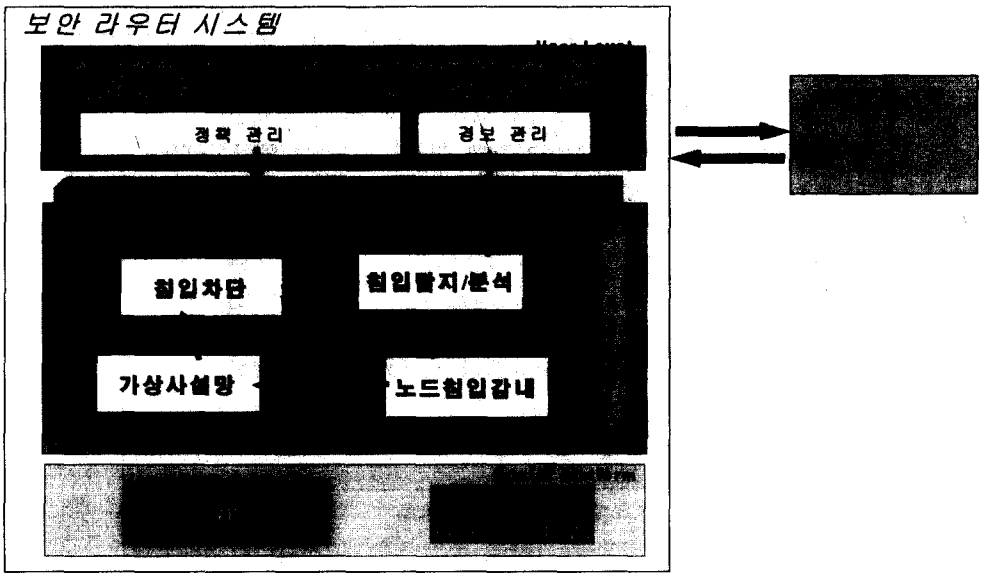
이외에도, 그리고 DoS 예방 등의 기능을 제공하며, 성능으로는 양방향 25Mbps 이상의 IPsec 3DES 암호화 속도에 최대 500개 터널을 동시에 지원한다.

- CISCO 1710 보안 엑세스 라우터[23] : 고성능의 가상사설망, 강화된 QoS(Quality of Service)를 제공하며, 다중 기능이 통합된 All-in-one solution 이다. 기능은 가상사설망, 상태 기반의 침입차단(Stateful Inspection Firewall), 침입탐지 시스템 기능을 포함하며, CISCO IOS 소프트웨어에 의한 다중 프로토콜 라우팅 기능과 강화된 QoS 기능을 제공한다. 성능은 양방향 4.0Mbps 이상의 IPsec DES/3DES 암호화 속도에 최대 100개 터널을 동시에 지원한다.
- CISCO 카탈리스트 6500[23] : 카탈리스트 6500 시리즈는 스위치로 방화벽, IPsec 기반 가상사설망, SSL, 네트워크 패킷 분석 등의 기능을 제공하며, 기존의 카탈리스트 6500 시리즈에 4개의 보안 모듈을 장착 할 수 있다. 방화벽 모듈은 5G의 처리 속도로 초당 100,000 접속을 지원하며, IPsec 가상사설망 모듈은 3DES로 1.9G의 성능에 8,000개의 동시 터널을 제공한다. SSL 모듈은 300M의 처리 속도에 초당 2500 접속을 지원하고, 네트워크 분석 모듈은 VoIP QoS 등의 통합 트래픽 전송 기능을 제공하며 1G 이상의 성능을 보장한다.

3. 통합 보안 엔진

3.1 통합 보안 엔진 구조

통합 보안 엔진이란 기존의 개별 보안 솔루션을 하나로 통합하여 보안 기능을 제공함으로써 시스템 및 네트워크의 해킹을 방지 및 차단 할 수 있는 보안 처리 엔진을 말한다. 네트워크 노드인 보안 라우터 또는 스위치에 탑재되는 통합 보안 엔진은 개념적으로 <그림 5>와 같이 나타낸다. 이와 같이 침입차단, 침입탐지/분석, 가상



〈그림 6〉 통합 보안 엔진이 탑재된 보안 라우터 시스템 구성도

사설망, 트래픽 측정 및 제어, 그리고 노드 자체 침입 감내 기능과 함께 이를 관리하기 위한 정책 기반의 보안 관리 엔진으로 구성된다. 기존 망에서의 정보보호가 시스템 또는 서버 내의 자원을 보호하기 위한 소극적인 보안이었다면, 새로운 차세대 정보보호의 개념은 네트워크 차원의 적극적인 보안이라고 할 수 있다. 이러한 네트워크 차원의 적극적인 보안을 위한 필수요소 중에 하나가 통합 보안 엔진이라고 할 수 있다. 특히 개별 보안 기능들이 다중 계층으로 구성되어 상호 연계에 의한 일관된 보안 정책을 제공하고, 침입 탐지에 의한 차단 또는 트래픽 측정에 의한 제어 또는 차단 등에 의해 실시간으로 신속하게 대응할 수 있다는 장점이 있다. 또한 상호 보완적인 연동에 의한 잇점을 최대화하기 위해 공유할 수 있는 데이터를 최대화하고 엔진을 최적화 한다면 가용성과 유연성 측면에서 그 효과가 극대화 될 것이다. 통합 보안 엔진을 구성하는 기능은 다음과 같다.

3.2 통합 보안 엔진 기능

3.1.1 침입차단 엔진

침입차단 엔진은 네트워크 노드에 수신되는 패킷에 대하여 필터링 규칙에 의하여 허가된 패킷은 수신하고 허가되지 않은 패킷은 거부하는 기능을 수행한다. 상태를 갖지 않고 단순히 접근 제어 리스트에 의한 필터링 기능과 상태 기반의 필터링(Stateful Inspection Firewall) 기능이 있다.

3.1.2 침입탐지/분석 엔진

침입탐지/분석 엔진은 패킷과 시스템 로그 정보 분석을 통해 침입을 탐지하고 침입이 탐지 되었을 경우, 침입에 대한 로그 기록을 수행하거나, 탐지된 침입 패킷 정보나 패킷 모니터링 정보 등을 알려주어 대응 조치를 취하도록 한다.

3.1.3 가상사설망 엔진

가상사설망 엔진은 전용선을 대체하여 가상적

으로 안전한 사설망을 구성하여 네트워킹에 대한 기밀성과 무결성을 제공하는 기능으로 IPsec을 이용하여 네트워크상의 데이터를 암호화 해서 보내고, 데이터를 복호화하여 처리하는 엔진이다.

3.1.4 트래픽 측정 및 제어 엔진

트래픽 측정 및 제어 엔진은 네트워크 트래픽을 측정함으로써 트래픽의 과부하를 포함한 분산 서비스 거부 공격을 감지하며 이에 따라 네트워크의 트래픽을 조절하는 엔진이다. 1.25 대란과 같은 트래픽 과부하에 따른 네트워크 마비를 막을 수 있는 트래픽 감지 시스템에 필수적인 기능이다.

3.1.5 노드 침입 감내 엔진

네트워크 수준의 많은 해킹을 방지하거나 차단 할 수 있으나 네트워크 노드 자체의 해킹을 막지 못하면 아무런 의미가 없다. 본 엔진은 네트워크 노드내의 접근을 제어하기 위한 노드 침입 감내 기능을 한다. 노드 침입 감내 기술로는 로그인 하는 사용자에 대한 다중 수준 보안 정책의 인증 기능, 사용자 직무에 기반한 접근 제어 기능, 노드 모니터링이 가능한 감사 추적 기능이 있다

3.1.6 정책 기반의 보안 관리 엔진

정책 기반의 보안 관리 엔진은 통합 보안 기능을 제공하는 네트워크 노드의 보안 관리를 위해 정책에 기반한 보안 관리 기능을 제공한다. 네트워크 노드를 관리하는 보안 관리 서버 시스템의 제어를 받으며, 정책을 수신하거나 패킷 모니터링 정보나 침입 패킷 정보 등을 보안 관리 서버 시스템에 보내어 안전한 네트워킹 기능을 제공한다.

4. 보안 라우터 시스템

4.1 보안 라우터 시스템 구성도

본 장에서는 네트워크 노드인 라우터에 실시간 침입 방지를 위하여 설계 및 구현된 통합 보안 엔진을 소개한다. 본 고에서 소개하는 엔진은 위의 엔진 기능 중 침입차단, 침입탐지/분석, 가상사설망, 노드침입 감내, 그리고 정책 기반 보안 관리 엔진 기능을 구현한 통합 보안 엔진으로 라우터에 탑재되어 해당 라우터의 하위 망 내의 시스템의 보안과 안전한 네트워킹 기능을 제공한다. 또한 라우터의 네트워킹 및 암호 처리 속도를 높이기 위하여 네트워크 프로세서와 암호 프로세서가 장착된 라우터 플랫폼을 설계 및 구현하였다. 기존의 라우터 기능을 방해하지 않고 보안 기능을 제공하는 통합 보안 엔진이 탑재된 라우터 시스템의 구성도는 다음 <그림 6>과 같다. 아래 그림에서 처럼 보안 관리 서버로부터 정책 기반의 보안 관리 및 제어를 받거나 라우터만으로 동작할 때는 GUI 를 통하여 정책 기반의 보안 관리 제어가 가능하도록 하였다.

4.2 통합 보안 엔진 구현

4.2.1. 침입차단 엔진

침입차단 엔진은 패킷의 전송 및 수신, 라우팅 과정에서 정해진 패킷 필터링 규칙에 의거해서 패킷을 허가 및 거부 하며, 침입 탐지 및 분석 엔진에 패킷 검사를 요청하는 역할을 수행한다. 주요 기능으로는 5-tuple 기반의 패킷 필터링, ICMP 헤더 정보를 이용한 패킷 필터링, IP Fragment 공격에 대한 대응, 그리고 TCP 연결에 상태 감시 기능 등이 있다.

5-tuple 기반의 패킷 필터링 기능은 기존 상용

방화벽에서 가장 보편적으로 사용하는 필터링 방식으로 IP 주소, 프로토콜, 그리고 포트 번호를 이용한 방식이다. 패킷 필터링 규칙은 근원지 IP, 목적지 IP, 프로토콜, 근원지 포트, 목적지 포트 등으로 구성되어 각 필드에 따라 필터링을 한다. 여기에서 IP 주소와 포트 번호는 각각 근원지 주소(source address)와 목적지 주소(destination address)의 쌍으로 존재하기 때문에 총 5개의 인자로 표시된다. ICMP 필터링 기능은 ICMP 헤더 정보 중에 Type 필드와 Code 필드 정보를 이용하여 패킷 필터링 기능을 제공한다. IP Fragment 공격 대응 기능은 네트워크에 의해 전송되는 모든 패킷은 각 전송 매체에 따라 패킷의 크기가 제한된다. 특히 큰 크기를 갖는 매체에서 보다 작은 크기의 패킷으로만 전달되는 매체로 전이되는 경우 기존 IP 패킷이 새로운 매체에 적합한 크기로 분할되는 과정을 Fragmentation 이라 하고 이렇게 분할된 패킷은 IP Fragment 패킷이라 부른다. 이러한 IP Fragment 패킷을 이용하여 기존 방화벽의 허점을 이용하여 공격하는 방법으로 Tiny Fragment Attack과 Overlapping Fragment Attack 이 있다. RFC1858[26]에 제안하고 있는 대응 알고리즘을 적용하여 이러한 공격들로부터 시스템을 보호한다. 마지막으로 상태기반 프로토콜인 TCP 연결 패킷을 관리하기 위해서 상태 감시(Stateful Inspection, 이하 상태 감시) 기능을 수행한다. TCP 프로토콜은 상태에 기반한 연결을 유지하며 통신하기 때문에 이러한 TCP연결에 대한 관리 및 제어는 보다 능동적인 보안 작업을 수행할 수 있게 한다. 이러한 TCP 연결 상태를 감시하면서 보다 능동적이고 효과적인 방화벽 기능을 제공하기 위해서 모든 TCP 패킷에 대한 감시 기능인 상태 감시 기능을 수행한다.

4.2.2. 침입탐지/분석 엔진

침입탐지/분석 엔진[18]은 내부 또는 외부의 침입으로부터 시스템 및 네트워크를 보호하기 위하여 침입을 탐지하고 분석한다. 본 보안 엔진은 보안 정책에 따라 네트워크 및 호스트 기반의 침입 탐지 기능을 수행한다. 이 엔진은 커널 내에서 동작하며 침입 탐지 시에는 패킷을 이용하여 서비스 거부 공격, 바이러스 및 인터넷 웜, 그 외의 네트워크 공격에 대하여 시그니쳐 기반의 침입탐지 과정을 수행한다. 또한, 패킷 및 TCP 상태정보에 기반한 비정상 침입탐지 기능을 수행한다.

침입탐지 및 분석 엔진의 가장 큰 특징은 동적으로 모드를 변경할 수 있다는 것이다. 시스템 상태에 따라, 공격의 탐지 정도에 따라 선택적으로 모드를 변경할 수 있다. 탐지 모드는 네가지로 공통 탐지 모드, 확장 탐지 모드, 상태 기반 탐지 모드, 확장 탐지 모드가 있다. 공통 탐지 모드는 각 탐지 대상에 대한 최소한의 정보를 이용하여 공격 가능성에 대한 탐지를 수행하는 모드이고, 확장 탐지 모드는 공통 모드를 통해 가능성이 높다고 생각되는 공격에 대하여 추가적으로 더 자세한 탐지를 수행하는 모드이다. 라우터의 상태 및 네트워크 부하 등을 고려하여 공통 탐지 모드와 확장 탐지 모드로 나누어 수행하며, 라우터에 최소한의 부하만으로 침입탐지를 수행할 수 있도록 한다는 데에 그 목적이 있다. 상태 기반 탐지 모드는 TCP 프로토콜의 상태 정보만 관리한다. TCP SYN, SYN/ACK, ACK에 대한 관리를 수행하고 세션이 연결되지 않는 곳에 대한 SYN 이외의 패킷은 모두 잘못된 패킷으로 처리 또는 허용 할 수도 있다. 비정상 탐지 모드는 두 가지 기능을 제공한다. 먼저 프로토콜 비정상 탐지로 세션에 해당하지 않는 패킷이 전송되면 드롭 처리를 하거나 확장 탐지를 한 후에 처리 하도록 한다. 다른 하나는 휴리스틱 탐지로 과도한 패킷이 전송되는 경우 이를 탐지하여 차단하는

것으로 예를 들면 1초내에 TCP SYN가 100개 이상 들어올 경우 무시하는 것 등과 같은 처리를 들 수 있다. 무엇보다도 각 모드를 라우터 실행 도중 동적으로 on/off 할 수 있어서 상황에 맞게 구성할 수 있다.

침입탐지 검사 및 대상범위는 잘 알려진 공격 기법 탐지, 패킷 헤더 및 페이로드 검사, 전처리 검사 및 탐지로 규정한다. 잘 알려진 공격 기법 탐지는 바이러스, 백도어, DoS, 스캐닝, ICMP 공격 등과 같이 잘 알려진 공격을 대상으로 한다. 패킷 헤더 및 페이로드 검사는 TCP 플래그 체크, TCP ACK 체크, 패킷 페이로드 패턴 매칭 등을 대상으로 한다. 전처리 검사 및 탐지는 백오리피스, http decode, Unicode 등과 같이 패킷의 헤더와 페이로드 정보를 통해서 탐지 할 수 없으므로 전처리를 통해 탐지하는 공격 기법 들을 대상으로 한다.

침입이 탐지된 후 이 침입에 대한 대응을 위한 동작 처리는 경보(Alert)와 무시(Drop), 그리고 종료(Terminate) 등 세가지 타입을 지원한다. 경보 타입은 보안 관리 GUI 또는 보안 관리 서버에게 경보 메시지를 보내는 것으로 처리한다. 특히 경보를 보내는 경우에는 잘 알려진 공격의 경우이면 사용자 선택에 의해 바로 침입차단 엔진으로 차단을 요청하여 능동적으로 대응이 가능하도록 한다. 두번째 무시의 경우에는 아무런 동작을 취하지 않는 것이고, 종료의 경우에는 세션을 종료시키는 처리를 한다.

4.2.3. 가상사설망 엔진

가상사설망 엔진은 보안 라우터 시스템의 네트워크 계층에서 IPsec 프로토콜을 이용하여 보안관리 시스템 및 보안라우터 시스템 사이에 전달되는 데이터에 대해 기밀성 및 무결성 등의 보안 기능을 제공한다. 보안 협상을 통해 형성된 인증 및 암호 알고리즘을 이용하여 패킷 전송 시 인증 및 암호화를 수행하는 기능을 제공하고, 보안 노드로부터 암호화된 패킷을 수신할 경우에도 보안 협상을 통해 형성된 동일한 알고리즘을 이용하여 암호화된 패킷의 인증 및 복호화를 수행한다. IPsec 처리를 위해 현재 사용 중인 보안 협상 내용에 대한 목록을 유지 및 관리하는 기능도 제공한다. 또한 패킷 인증 및 암/복호화의 고속 처리를 위하여 전용 가속보드 개념의 하드웨어를 사용한다.

본 엔진의 주요 기능으로는 키관리 기능, SA 협상 및 관리 기능, 패킷 무결성 제공 기능, 패킷 기밀성 제공 기능, 로그 기능 등이 있다. 먼저 키관리 기능은 보안 라우터 시스템 간에 보안 터널을 생성할 때 SA를 협상하기 전 상대 호스트를 인증하기 위해 사용되는 키를 관리하는 기능이다. SA 협상 및 관리 기능은 보안 라우터 시스템 간의 보안 터널을 형성하기 위해 보안 라우터 시스템 간에 SA 및 키 재료 등을 협상하는 기능이다. 각 노드에서 상대 노드를 인증하고, 패킷에 적용할 보안 프로토콜, 패킷 변환 방법, 패킷에 적용할 암호키 및 인증 키에 사용된 키 재료등을 협상하게 된다. 즉 보안 터널에 대한 속성을 정의하며, 이 기능은 RFC2408, RFC2409를 기반으로 한다. 패킷 무결성 제공 기능은 AH 프로토콜을 말하며 협상된 SA를 기반으로 보안 라우터 시스팀 간에 전달되는 패킷에 대해 무결성을 제공하는 기능이다. 즉 협상된 SA를 기반으로 약속된 키 재료 및 인증 알고리즘 등을 이용하여 패킷에 무결성을 제공하며, RFC2402를 기반으로 한다. 패킷 기밀성 제공 기능은 ESP 프로토콜을 말하며, 협상된 SA를 기반으로 보안 라우터 시스템 간에 전달되는 패킷에 대하 기밀성 및 무결성을 제공하는 기능이다. 즉 협상된 SA를 기반으로 약속된 키재료, 암호화 및 인증 알고리즘 등을 이용하여 패킷에 기밀성 및 무결성을 제공하며, RFC 2406을 기반으로 한다. 마지막으로

로그 기능은 본 엔진에서 일어나는 여러 가지 이벤트의 처리 내역 도는 오류 등을 로그에 남기는 기능을 한다. 즉 SA 협상 내역, SA 협상 갱신 내역, 패킷 처리 내역 및 오류 등이 로그에 남기는 내용이다.

4.2.4. 노드 침입 감내 엔진

노드 침입 감내 엔진은 노드 자체의 보안 기능을 제공하는 엔진으로 크게 인증인가, 접근제어, 감사추적[15] 기능으로 나누어서 제공된다.

- 인증인가 : 보안 라우터 시스템에 접근하는 사용자에 대한 인증인가 기능을 수행한다. 복수의 사용자를 지원하며 각각의 사용자에 따라 사용자 역할(Role)을 구분하여 부여한다. 사용자 인증은 접근제어와 연계하여 사용자 ID/Passwd 이외 접근제어를 위하여 필요한 사용자 역할에 기반한 다중 수준의 인증 기능을 제공한다. 라우터에서 기본적으로 제공되는 역할은 보안관리자와 네트워크 관리자, 네트워크 성능 관리자이며 추가로 역할을 사용자가 정의하여 사용이 가능하다.
- 접근제어(Role Based Access Control, 이하 RBAC) : 라우터 내의 자원을 접근하는 사용자는 제한이 되어 있으나, 시스템 관리자 권한만 획득하면 라우터 내의 모든 구성(Configuration) 을 바꿀 수 있으므로 접근제어 기능이 필요하다. 노드 침입 감내 엔진에서는 라우터 사용자의 접근통제를 위하여 DAC과 MAC 혼합 형태의 접근 제어 정책인 직무 기반의 접근제어 방식(Role Based Access Control)을 제공한다[13][14][15][20]. RBAC 메커니즘의 경우는 위의 DAC과 MAC의 혼합된 형태로 상업적인 환경에 가장 적합한 접근제어 방식으로 해당 주체의 권한을 최소화한 최소 권한(Minimum Privilege) 분리 원칙으로 사용자의 역할이나 직무에 최소화된 권한을 부여하고 그 역할이나 직무에 따라 접근을 통제하는 방식을 말한다.
- 감사추적 : 방화벽 엔진으로부터 전달되는 필터링 결과, 침입탐지 및 분석 엔진에서 발생된 침입탐지 결과, 그리고 노드 침입 감내 엔진에서 발생되는 접근제어 정보를 감사추적 DB에 기록한다. 또한 방화벽, 침입탐지 통계 정보와 감사기록의 축약된 정보를 정책적용부로 보내어 모니터링이 가능하도록 한다.

4.2.5. 정책기반 보안 관리 엔진

정책기반 보안 관리 엔진[19]은 네트워크 노드의 보안 정책을 기반으로 하여 보안 관리하는 엔진으로 크게 세가지 기능으로 나누어 제공된다. 첫째는 보안 관리 기능으로 라우터를 관리하는 보안 관리 서버 시스템에 구현된 정책 기반의 보안 관리 프레임웍으로 네트워크의 통합적인 보안 관리를 위해 보안 정책을 정의하고 정책 기반 관리를 수행한다. 보안관리 서버 시스템에 구현되어 네트워크 관리, 정책 DB 관리, 라우터와의 통신 기능을 한다. 둘째는 정책 관리 기능으로 라우터에서 해당되는 정책을 보안관리 서버 시스템으로부터 받아 처리할 정책을 결정하여 보안 라우터 시스템내의 각 보안 엔진으로 정책을 관리하고 적용하는 기능을 한다. 이는 침입차단/침입탐지 규칙을 설정하고, 가상사설망 규칙들을 설정하며, 접근제어 정책을 적용한다. 마지막으로 경보 관리 기능은 침입탐지/분석 엔진으로부터 오는 경보를 보안 관리 서버 시스템으로 보내고 경보를 축약하는 등의 기능을 한다. 보안 관리 서버 시스템과 보안 라우터 사이의 통신은 소켓을 이용하였다.

4.3 라우터 플랫폼 구현

4.3.1. 보안 라우터 메인 보드

보안 라우터 메인 보드는 보안 라우터 하드웨어 플랫폼의 메인 보드로서, 네트웍 프로세서를 이용하여 이더넷 카드의 SPI4.2 인터페이스로부터 들어오는 데이터의 라우팅 기능 및 침입탐지 기능 등을 수행한다. 하나의 NPU를 이용하여 ingress와 egress기능을 수행한다. 네트웍 프로세서로는 인텔사의 IXP28XX를 사용하며, 프로세서의 S/W처리를 위한 QDR SRAM, RDRAM, 그리고 TCAM을 장착한다. 그리고 이더넷 라인보드인 보안 라우터 네트워크 보드 또는 보안 라우터 암호 보드와의 연결을 위한 SPI-4.2 및 PCI 인터페이스를 가진다. 암호화 가속 기능 또는 성능 상의 요구에 따라 네트워크 보드와 암호 보드를 선택하여 사용할 수 있다. 또한 네트워크 프로세서 내의 마이크로 엔진에 침입탐지, 침입차단, 가상사설망 기능 등을 구현하여 보안 처리 성능을 높인다.

4.3.2. 보안 라우터 네트워크 보드

보안 라우터 네트워크 보드는 보안 라우터 하드웨어 플랫폼에서 MAC과 PHY를 담당하는 보드로서 네트워크 인터페이스를 제공하는 보드이다. 보안 라우터 메인 보드와 연결되어 외부망과 내부망 사이의 네트워킹 기능을 제공한다. 메인 보드와의 연결을 위해 SPI-4.2 및 PCI 인터페이스를 가지며, 네트워크 인터페이스로 SFP 및 RJ-45 포트를 가진다. 고속의 암호(IPsec 포함) 처리가 필요하지 않는 일반적인 라우터 시스템의 경우에 가격 경쟁력을 갖을 수 있다.

4.3.3. 보안 라우터 암호 보드

보안 라우터 암호 보드는 보안 라우터 하드웨어 플랫폼에서 네트워크 인터페이스가 가지는 기능을 수용하면서 추가적으로 IPsec 보안 메커니즘에서 적용되는 암/복호 알고리즘과 키 교환 모듈과의 유기적인 인터페이스, 데이터베이스 처리 기능 및 네트워크 처리 기능을 하드웨어적으로 지원하기 위한 보드이다. IPsec 보안을 하드웨어로 지원하기 위해 Cavium사의 칩을 사용하였으며, IPsec 처리 성능을 최대 10G까지 제공하므로 고속의 암호(IPsec 포함) 처리 기능이 필요한 라우터 시스템으로 활용될 수 있어서 성능 경쟁력을 갖는다. 보안 라우터 메인 보드와의 연결을 위한 SPI-4.2 및 PCI 인터페이스를 가지며 네트워크 인터페이스로 SFP 및 RJ-45 포트를 가진다.

5. 결 론

통합 보안 엔진이 탑재된 보안 라우터 시스템은 보안 기능이 있는 기존의 상용 라우터와는 다르게 동적인 구성이 가능하며 국제공통평가표준인 CC(Common Criteria)에 정의되어 있는 라우터/스위치용 보호 프로파일(Protection Profile)을 준수하여 EAL3급 정도의 기능 요구사항을 만족한다. IPsec 처리 또한 다른 상용 라우터와는 다르게 IPsec 코아와 암호 처리를 하드웨어로 제공하므로 최대 1G 정도의 높은 성능을 제공한다. 또한 침입탐지와 차단이 연동되어 실시간으로 탐지하며 능동적인 대응이 가능하다는 장점이 있다. 무엇보다도 시스코를 제외한 노텔이나 엔터라시스, 그리고 주니퍼사에서 제공하는 라우터는 방화벽과 가상사설망 기능만을 제공하나, 보안 라우터 시스템은 방화벽, 침입탐지, 가상사설망 기능과 노드 침입 감내 기능까지 제공한다.

본 고에서는 통합 보안 엔진의 개념과 통합 보안 엔진의 필요성을 기술하고 Linux 2.4.18 커

널을 기반으로 한 통합 보안 엔진의 설계 및 구현 내용을 소개하였다. 또한 구현된 통합 보안 엔진을 기반으로 한 보안 라우터를 소개하였다. 이는 커널 수준의 침입차단, 침입탐지, 가상사설망, 그리고 노드 자체의 침입 감내 기술 구현으로 성능이 우수할 뿐만 아니라, 통합된 보안 기능에 대한 정책기반의 보안 관리 기능으로 관리하기 용이하다는 장점이 있다. 이러한 통합된 하나의 보안 엔진 구현을 통해 비용면에서도 절감되어 경제적이며 동적인 규칙 변경이 가능하여 신속하고 능동적인 대응이 가능하다. 또한 침입차단, 침입탐지, 그리고 가상사설망 엔진 등과 같이 네트워크 계층에서 처리가 되는 보안 엔진의 경우에는 네트워크 프로세서를 이용한 구현으로 보안 처리 성능을 높혔으나, 좀더 효율적이면서 성능을 향상시킬 수 있는 코드 최적화 연구를 계속 진행하여야 할 것이다.

최근 들어서는 하나의 시스템을 목표로 하는 공격이 아닌, DNS나 네트워크 노드인 라우터를 공격하여 네트워크 전체가 마비되는 공격이 늘어나고 있다. 이에 대한 대응책으로 네트워크 트래픽을 측정하고 조절할 수 있는 트래픽 측정 및 제어 엔진 기술을 연구하여야 할 것이다. 단 소프트웨어 만으로는 트래픽 측정의 오버헤드가 크므로 본 시스템 구조에 알맞은 트래픽 측정 엔진의 하드웨어 연구도 필요하다. 또한 요즈음 들어서 더욱 시장의 요구가 많아진 네트워크 노드 차원의 감사 추적 기능 이나 시스템 모니터링 기능으로 시스템 및 네트워크 공격을 탐지하고 차단할 수 있도록 연구하여야 할 것이다.

References

[1] http://isis.nic.or.kr/sub05/sub05_index.html

[2] http://www.ecommerce.go.kr/tong1.asp

[3] Dorothy E, Denning, 'Information Warfare and Security', Addison-wesley, April 1999.

[4] 정연서, 류걸우, 남택용, 손승원, "사이버 위협에 대한 보안 솔루션 기술 동향," ETRI 주간 기술 동향, 2002 October.

[5] 조대일, 송규철, 노병구, 네트워크 침입탐지와 해킹 분석 핸드북, 인포북, 2001.

[6] Ulrich Ultes-Nitsche and InSeon Yoo, "An integrated Network Security Approach-Pairing Detecting Malicious Patterns with Anomaly Detection, " Proc. of Conference on Korean Science and Engineering Association in UK(KSEAUK2002), July 2002.

[7] InSeon Yoo and Ulrich Ultes-Nitsche , "An Intelligent Firewall to Detect Novel Attacks ? An Integrated Approach based on Anomaly Detection Against Virus Attacks," November 2002.

[8] An Introduction to Computer Security : The NIST Handbook, NIST Special Publication 800-12, January 1.

[9] William R. Cheswick, Steven M. Bellovin Firewalls and Internet Security: Repelling the Willy hacker, Addison Wesley, 1994.

[10] D. Brent Chapman, Elizabeth D. Zwicky, Building Internet Firewalls, O Reilly & Associations, Inc. January 1996.

[11] Chris Hare, Karanjit Siyan, Internet Firewalls and Network Security ? 2nd ed., New Readers, 1996.

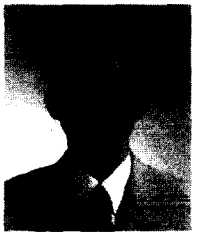
[12] Peter A. Loscocco, Wtephen D. Dmalley, Patric A. Muckelbauer, Ruth C. Taylor, S.Jeff Truner, John F. Farrel, 'The Inevitability of Failure: The Flawed Assumption of Security in Modern

Computing Environments', National Security Agency, 1997.
[13] David F. Ferraiolo, Ravi Sandu, & Serban Gavrila, "A Proposed Standard for Role-Based Access Control," ACM transaction on Information and System Security, VOL.4, NO.3, pp.224-274, Aug. 2001
[14] DoD 5200.28-STD. 'Department of Defense Trusted Computer System Evaluation Criteria', December 1985
[15] D.Ferraolo and R, Kuhn, "Role-Based Access Control", Proceeding of the 15th National Computer Security Conference, 1992
[16] Dorothy E, Denning, 'Information Warfare and Security', Addison-wesley, April 1999.
[17] Linux 2.4.18 Kernel-RELEASE Source Code
[18] B. H. Jung, J. N. Kim, "Design of Dynamic Intrusion Detection Rule Modification Technique for Kernel Level Intrusion Detection," 한국정보처리학회 추계 학술대회 논문집, Vol. 9, No. 2, Nov. 2002.
[19] S.H. Jo, J. N. Kim, & S. W. Sohn, "Design of Web-based Security Management for Intrusion Detection", Proc. of ICEB, ICEB '2002, 2002
[20] J. G. Ko, J. N. Kim, & K. I. Jeong, "Access Control for Secure FreeBSD Operating System," Proc. of WISA2001, The Second International Workshop on Information Security Applications, 2001.
[21] http://www.fortinet.co.kr/
[22] http://www.symantec.com/
[23] http://www.cisco.com/
[24] http://www.nortelnetworks.com/
[25] http://www.enterasys.com/
[26] RFC 1858, Security Considerations for IP Fragment Filtering

김 정 녀

1987년 : 전남대학교 전산통계학과 졸업
1995년 ~ 1996년 : Open Software Foundation Research Institute 공동 연구 파견(미국)
2000년 : 충남대학교 컴퓨터공학과 석사
2004년 : 충남대학교 컴퓨터공학과 박사
1988년 ~ 현재 : 한국전자통신연구원 선임연구원, 보안운영체제연구팀장

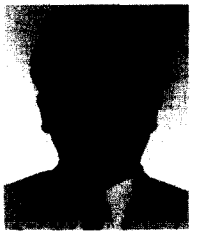
<관심 분야> 인터넷 정보보호, Secure OS, 네트워크 보안



장 종 수

1984년 : 경북대학교 전자공학과 졸업
1986년 : 경북대학교 전자공학과 석사
2000년 : 충북대학교 컴퓨터공학과 박사
1989년 ~ 현재 : 한국전자통신연구원 책임연구원, 네트워크보안그룹장

<관심분야> 네트워크보안, 정책기반보안관리기술, 비정상트래픽 탐지기술, 유해정보차단기술



손 승 원

1984년 : 경북대학교 전자공학과 졸업

1994년 : 연세대학교 컴퓨터공학과 석사

1999년 : 충북대학교 컴퓨터공학과 박사

1991년 ~ 현재 : 한국전자통신연구원 책임연구원, 정보보호연구단장

<관심분야> 이동인터넷 보안, 정보보호, 네트워크 보안