主題

안전한 라우터를 위한 능동형 보안 엔진 구현

한국전자통신연구원 선임연구원 팀장 김 정 녀
한국전자통신연구원 책임연구원 부장 손 승 원
충남대학교 컴퓨터공학과 부교수 이 철 훈

차 례

요 약

기존의 보안 시스템은 침입탐지, 침입차단, 그리고 VPN 등과 같은 기능을 각 개별 시스템에서 제공한다. 이로 인하여 관리하기가 불편하고 비용면에서도 효율적이지 못하다는 제한성이 있다. 이를 해결하기 위하여 침입탐지, 침입차단, 그리고 VPN 기능을 통합하여 제공하는 능동형 보안 엔진 개념이 부각되었다.

본 논문에서는 이러한 능동형 보안 엔진을 라우터나 스위치 등과 같은 네트워크 노드에 탑재하여 안전한 네트워킹이 가능하도록 하는 보안 프레임웍을 소개한다. 또한 침입탐지, 침입차단 기능을 통합하여 제공하는 라우터용 능동형 보안 엔진의 구조를 소개하고, 이를 위해 구현된 핵심 기능을 기술한다. 이러한 능동형 보안 엔진이 탑재된 안전한 라우터로 구성된 보안망 구조와 기존의 개별 시스템으로 구성된 보안 망 구조와의 비교를 통하여 능동형 보안 엔진의 효율성을 설명한다.

1. 서 론

기존의 인터넷 망에서는 방화벽[2][3][4], 침입탐지시스템[4], VPN 시스템[4], 서버 보안 시스템 등 여러 가지의 개별 보안 시스템들을 통하여 보안 해결책을 마련했다. 그러나 이러한 환경에서 네트워크 상의 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 가

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

본 고에서는 이러한 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, VPN, 그리고 침입감내 기능을 하나로 통합하여 시스템 및 네트워크 수준의 해킹을 감지 및 차단, 그리고 대응하는 보안 처리 엔진이다. 본 고에서는 통합 보안 엔진의 구조와 함께 통합 보안 엔진이 갖는 보안 기능 요소들을 소개한다.

본 고의 구성은 2장에서는 능동형 보안 엔진 제품 및 관련 연구에 대하여 소개한다. 3장에서 능동형 보안 엔진의 개념과 필요성을 살펴보고, 본 연구실에서 개발한 안전한 라우터용 능동형 보안 엔진의 구조, 기능 그리고 현재 구현 정도를 소개한다. 4장에서 그 중 핵심 기술인 침입탐지/차단 및 침입감내 기술의 설계 및 구현 내용을 기술한다. 5장에서 개별 보안 시스템으로 구성된 기존 망과 능동형 보안 엔진이 탑재된 라우터로 구성된 구성망을 소개하고 능동형 보안 엔진의 장점을 제시한다. 마지막으로 6장에서는 결론과 앞으로 더 해야 할 연구의 방향을 제시해 보고자 한다.

2. 관련 연구 동향

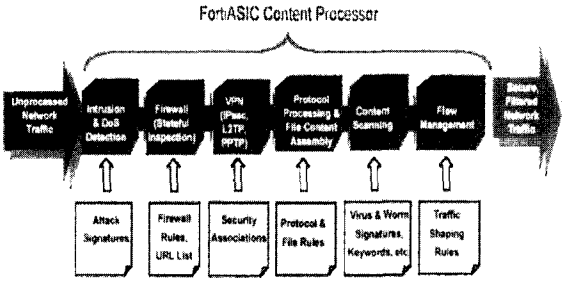
보안 제품들은 개별 시스템에서 통합 보안 장비 형태로, 시스템 보안에서 네트워크 전반에 걸친 보안의 형태로 변화되고 있다. 특히 요즈음 들어서는 관리되어야 하는 보안 관리 기능도 무시하지 못한다. 통합 보안 엔진이 탑재되는 제품은 다음과 같이 크게 두 가지로 통합 보안 장비(Appliance)와 통합 보안 네트워크 노드(라우터 또는 스위치)로 나누어 볼 수 있다.

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. 방화벽, 침입탐지, VPN 그리고 항 바이러스 기능까지 제공하는 제품은 크로스빔사의 X40S, Fortinet 사의 Fortigate, 그리고 시만텍사의 Security Gateway 등이 있다.

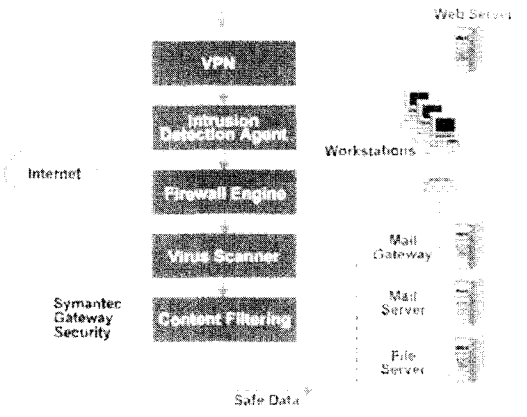
- o 크로스빔 사의 X40S : 오픈 보안 장비로, 기존 보안 소프트웨어 제품을 모듈로 탑재하여 다양한 기능을 구현한 멀티기가 비트 지원 제품이다. 방화벽, IDS, VPN, 항 바이러스, URL 필터링을 탑재한 통합 솔루션의 역할을 할 수 있고, 새로운 보안 제품을 구현하거나 쉽게 업그레이드 할 수 있다. 다양한 기능을 통합하면서 시스템을 단순하게 구현했고, 새로운 보안 제품을 적용하거나 업그레이드하는 것은 모듈만을 탑재하면 되기 때문에 수월하다는 것이 특징이다.
- o Fortinet사의Fortigate : FortiAsic content processor와 FortiOS content processing OS로 구성된 보안 장비로 방화벽 최대 2Gbps와 VPN 최대 7000Mbps 의 성능을 제공한다. 보안 기능으로는 Stateful-inspection Firewall, 고성능 IDS와 DoS/DDoS 예방, Virus와 Worm 스캐닝, 컨

텐츠 필터링 그리고 트래픽 세이핑 기능을 제공한다. Fortigate 시스템이 제공하는 보안 기능 구조는 <그림1>과 같다.



<그림 1> Fortigate 시스템 보안 기능 구조

o 시만텍사의 Security Gateway : 방화벽, IDS, VPN, content filtering 그리고 Anti-virus 기능이 통합된 다중 보안 기술이 구현된 보안 장비로 구조는 다음 <그림2>와 같다.



<그림 2> Symantec Gateway Security 구조

2.2 통합 보안 네트워크 노드

보안 기능을 갖는 특수 목적의 네트워크 노드들로 라우터나 스위치에 방화벽, 침입탐지, 그리고 VPN 기능 등과 같은 보안 기능이 추가되어 있다. 현재 방화벽과 VPN 기능을 제공하는 제품으로는 엔터라시스 네트웍스에 XSR-1800, 노텔 네트웍스에 Contivity 1700 등이있으며, 추가로 침입탐지 기능까지 제공하는 제품으로는 CISCO 1710 Security Access Router와 CISCO 6500 Series Switch 등이 있다.

o CISCO 1710 Security Access Router : 고성능의 VPN, 강화된QoS(Quality of Service)를 제공하며, 다중 기능이 통합된 All-in-one solution 이다. 기능은 VPN, Stateful inspection Firewall, Intrusion Detection System 기능을 포함하며, Full-featured CISCO IOS 소프트웨어에 의한 다중 프로토콜 라우팅 기능과 강화된 QoS feature 를 제공한다. 성능은 양방향 4.0Mbps 이상의 IPsec DES/3DES 암호화 속도에 최대 100개 터널을 동시에 지원한다.

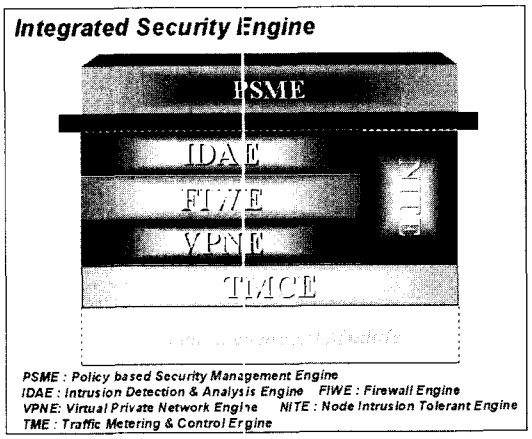
o 노텔네트웍스의 Contivity 1700 : 보안 기능으로는 PKI 지원에, VPN, Stateful Firewall, 그리고 DoS 예방 등의 기능을 제공하며, 성능으로는 양방향 25Mbps 이상의 IPsec 3DES 암호화 속도에 최대 500개 터널을 동시에 지원한다.

3. 능동형 보안 엔진

3.1 능동형 보안 엔진 구조

능동형 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 능동형 보안 엔진은 개념적으로 <그림 3>과 같이 나타낸다. 이와 같이 방화벽, 침입탐지, 가상사설망,

트래픽 측정 및 제어, 그리고 노드 자체 침입 감내 기능과 함께 이를 관리하기 위한 정책기반의 보안 관리 엔진으로 구성된다. 기존 망에서의 정보보호가 시스템 또는 서버내의 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 능동형 보안 엔진이라고 할 수 있다. 능동형 보안 엔진을 구성하는 기능은 다음과 같다.



<그림 3> 능동형 보안 엔진 개념도

3.2 능동형 보안 엔진 기능

3.1.1 방화벽 엔진

방화벽 엔진은 네트워크 노드에 수신되는 패킷에 대하여 필터링 규칙에 의하여 허가된 패킷은 수신하고 허가되지 않은 패킷은 거부하는 기능을 수행한다.

3.1.2 침입탐지 및 분석 엔진

침입탐지 및 분석 엔진은 패킷과 시스템 로그 정보 분석을 통해 침입을 탐지하고 침입이 탐지되었을 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 가상적으로 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

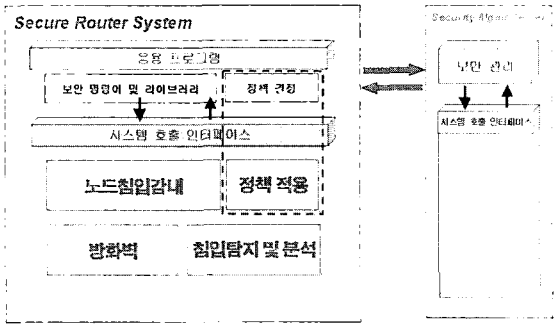
정책 기반의 보안 관리 엔진은 통합 보안 기능을 제공하는 네트워크 노드의 보안 관리를 위해 정책에 기반한 보안 관리 기능을 제공한다. 네트워크 노드를 관리하는 보안 관리 서버 시스템의 제어를 받으며, 정책을 수신하거나 패킷 모니터링 정보나 침입 패킷 정보 등을 보안 관리

서버 시스템에 보내어 안전한 네트워킹 기능을 제공한다.

4. 라우터용 능동형 보안엔진

4.1 안전한 라우터 시스템 구성도

본 장에서는 네트워크 노드인 라우터에 설계 및 구현된 능동형 보안 엔진을 소개한다. 본 고에서 소개하는 엔진은 위의 엔진 기능 중 방화벽, 침입탐지/분석, 노드침입 감내, 그리고 정책 기반 보안 관리 엔진 기능을 구현한 능동형 보안 엔진으로 라우터에 탑재되어 해당 라우터의 하위 망 내의 시스템의 보안과 안전한 네트워킹 기능을 제공한다. 기존의 라우터 기능을 방해하지 않고 보안 기능을 제공하는 능동형 보안 엔진이 탑재된 라우터 시스템의 구성도는 다음 <그림 4>와 같다.



<그림 4> 능동형 보안 엔진이 탑재된 보안 라우터 시스템 구성도

4.2 능동형 보안 엔진 구현

4.2.1. 방화벽 엔진

방화벽 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. 패킷 필터링 규칙은 Source IP, Destination IP, Protocol, Source Port, Destination Port 등으로 구성되어 각 필드에 따라 필터링을 한다. 그 이외에도 위의 규칙에 의한 필터링에 적용하기 어려운 필터링으로 TCP 필터링과 ICMP 필터링이 있다. TCP 필터링은 TCP 연결 시 설정되는 Code 비트를 이용하여 SYN Flooding 같은 공격에 대한 방어 기능을 제공한다. ICMP 필터링은 ICMP 헤더 정보 중에 Type 필드와 Code 필드 정보를 이용하여 패킷 필터링 기능을 제공한다.

4.2.2. 침입탐지 및 분석 엔진

침입탐지 분석 엔진[11]은 내부 또는 외부의 침입으로부터 시스템 및 네트워크를 보호하기 위하여 침입을 탐지하고 분석한다. 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, Scanning, ICMP attack 등과 같이 잘 알려진 공격을 대상으로 한다. 패키 헤더 및 페이로드 검사는 TCP flag check, TCP ack check, packet payload pattern matching 등을 대상으로 한다. 전처리 검사 및 탐지는 Back Orifice, http decode, Unicode와 같이 패킷의 헤더와 페이로드 정보를 통해서 탐지 할 수 없으므로 전처리를 통해 탐지하는 공격 기법 들을 대상으로 한다.

본 엔진에서는 보안 정책에 따른 네트워크 및 호스트 기반의 침입탐지/대응 역할을 수행한다. 침입탐지 시에는 패킷을 이용하여 서비스 거부 공격, 바이러스 및 인터넷 웜, 그 이외의 네트워크 공격에 대하여 시그니쳐 기반의 침입탐지 과정을 수행한다.

침입탐지 및 분석 엔진은 엔진 관리와 침입 핸들러 기능을 제공한다. 엔진 관리는침입탐지

관련 초기화와 모니터링 모드, 탐지 규칙 변경 요청 등의 처리를 수행하며, 침입탐지/분석 실행 중에도 동적으로 규칙을 변경할 수 있어서 능동적인 탐지가 가능하다. 침입 핸들러는 정의된 침입탐지 규칙과 방화벽 엔진에서 전달된 정보를 이용하여 침입을 판단하고 핸들링 한다. 침입탐지 수행순서는 전처리 검사, 패킷헤더 검사, 패킷 페이로드 검사의 순서로 진행되며 각 단계에서 침입이 탐지되면 대응함수 수행의 과정을 수행한다. 전처리 검사에서는 http decode, Unicode 공격과 같이 패킷의 헤더와 내용정보에 대한 검사를 통해서 발견할 수 없는 공격에 대한 검사를 말하며, 패킷 헤더나 페이로드 검사 이전에 수행한다. 패킷 헤더 검사는 패킷 헤더의 각 부분에 대한 탐지규칙에 정의된 내용이 존재하는지 검사하는 과정이다. 패킷 페이로드 검사는 패킷의 페이로드에 탐지규칙에 정의된 특정 문자열이 존재하는지를 검사하는 과정이다. 침입이 탐지된 후 이 침입에 대한 대응을 위한 대응 함수는 Notify와 Drop의 두가지 타입을 지원한다. Notify 타입은 Alert와 E-mail to target system으로 구분하여 처리한다. Alert의 경우에는 정책적용부를 통하여 보안관리 서버 시스템에 Alert을 보내는 것이고, E-mail to target system은 탐지 결과를 target 시스템으로 E-mail을 통해 전송한다. 특히 Alert을 보내는 경우 중 잘 알려진 공격의 경우에는 사용자 선택에 의해 바로 방화벽 엔진으로 차단을 요청하여 능동적으로 대응이 가능하도록 한다.

4.2.3. 노드 침입 감내 엔진

노드 침입 감내 엔진은 노드 자체의 보안 기능을 제공하는 엔진으로 크게 사용자 인증, 접근제어, 감사추적[8] 기능으로 나누어서 제공된다.

o 사용자 인증

- 안전한 노드 기능을 제공하기 위하여 사용자 인증시에 보안성을 제공한다. 사용자 인증은 접근제어와 연계하여 사용자 ID/Passwd 이외 접근제어를 위하여 필요한 사용자 역할에 기반한 다중 수준 인증 기능을 제공한다. 라우터에서 기본적으로 제공되는 역할은 보안관리자와 네트워크 관리자이며 추가로 6가지 역할을 사용자가 정의하여 사용이 가능하다.

o 접근제어(Role Based Access Control, 이하 RBAC)

- 라우터내의 자원을 접근하는 사용자는 제한이 되어 있으나, 시스템 관리자 권한만 획득하면 라우터내의 모든 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[6][7][8][13]. 직무 기반의 접근제어 정책인 RBAC은 상업적인 환경에서 가장 좋은 접근제어 정책으로 이는 Rabi Sandu 교수가 제안한 RBAC96 모델을 기반으로 커널 수준에서 구현하였다. 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.

o 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 정보

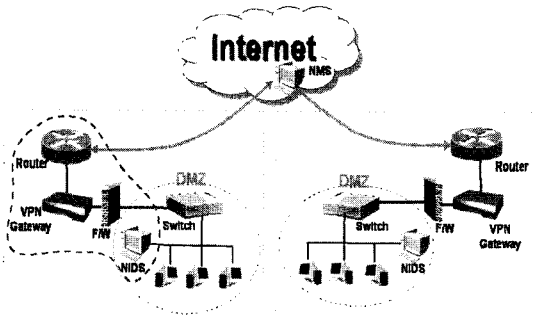
와 감사기록의 축약된 정보를 정책적용부로 보내어 모니터링이 가능하도록 한다.

4.2.4. 정책기반 보안 관리 엔진

정책기반 보안 관리 엔진[12]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 결정 기능으로 라우터에서 해당되는 정책을 보안관리 서버 시스템으로부터 받아 처리할 정책을 결정하는 것으로 보안관리 서버 시스템과의 통신, 정책 결정, 정책 DB로 구성된다. 마지막으로 정책 적용 기능은 보안관리 서버 시스템으로부터 받은 정책을 라우터에 적용시키는 것으로 패킷 모니터링 정보나 침입 패킷 정보 등을 정책결정부에 보내거나, 정책 결정부로부터 받은 정책을 적용하고 수행한다. 이는 방화벽 규칙을 변경하고, 침입탐지 규칙들을 설정하며, 접근제어 정책을 적용한다. 보안 관리 서버 시스템과 보안 라우터 사이의 통신은 소켓을 이용하였다.

5. 기존망과 능동형 보안 엔진이 탑재된 라우터 구성망

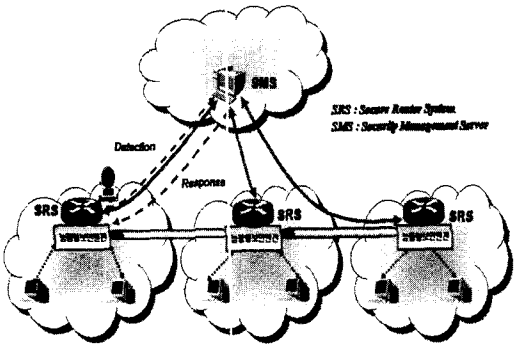
방화벽, 침입탐지 시스템, VPN 게이트웨이 등 개별 보안 시스템으로 구성된 기존망은다음 <그림5>와 같다. 기존의 망에서는 라우터와 VPN 게이트웨이, 방화벽, 그리고 네트워크 기반 침입탐지 시스템을 함께 연동하여 운영한다. 아래 그림에서 처럼 라우터를 통해서 들어온 패킷이 VPN 게이트웨이를 통해 방화벽을 지나고, 내부망 내의 DMZ 지역에 들어오면 내부망 내에 있는 네트워크 기반 침입탐지 시스템이 관여를 한다. 이처럼 패킷이 내부망내에 있는 서버에 오기까지 여러 개별 시스템을 거치므로 운영상의 관리도 만만치 않고, 각 장비의 설치를 위한 비용도 만만치 않다. 이러한 각 개별 시스템간의 정책들 간의 충돌도 있을 수 있으며, 다른 벤더 제품간의 상호 연동도 어려워서 실시간 대응이 어렵다는 단점이 있다.



<그림 5> 기존망 구성도

능동형 보안 엔진이 탑재된 안전한 라우터 시스템으로 구성된 망구조는 <그림 6>과 같다. 능동형 보안 엔진이 탑재된 안전한 라우터 시스템의 경우에는 위의 그림에 있는 방화벽, VPN, 침입탐지시스템의 기능이 하나로 구현되어 있어서 관리가 용이하며 비용 면에서도 훨씬 저렴하다. 또한 정책을 기반한 보안 관리 기능이 구현되어 있어서 보안 관리 서버 시스템으로부터의 정책을 받아 동적으로 정책 추가/삭제/변경이 가능하여서 능동적인 대응이 가능하다. 다음 그림에서처럼 안전한 라우터 시스템이 네트워크 또는 시스템 차원의 침입을 탐지하면 보안 관리 서버 시스템에게 탐지 정보를 보내고, 이를 감지한 보안 관리 서버 시스템은 안전한 라우터 시스템에게

해당 정책을 내려 능동적으로 대응을 할 수 있도록 한다.



<그림 6> 능동형 보안엔진이 탑재된 라우터 구성망

6. 결론

본 고에서는 능동형 보안 엔진의 개념과 능동형 보안 엔진의 필요성을 기술하고 Linux를 기반으로 한 능동형 보안 엔진의 설계 및 구현 내용을 소개하였다. 구현된 능동형 보안 엔진을 기반으로 한 안전한 라우터를 소개하였다. 이는 커널 수준의 방화벽, 침입탐지, 그리고 노드 자체의 침입 감내 기술 구현으로 성능이 우수할 뿐만 아니라, 통합된 보안 기능에 대한 정책기반의 보안 관리 기능으로 관리하기 용이하다는 장점이 있다. 또한 이러한 통합된 하나의 보안 엔진 구현을 통해 비용면에서도 절감되어 경제적이며 동적인 규칙 변경이 가능하여 능동적인 대응이 가능하다. 그러나 아직까지는 성능적인 면에서 부족하므로 하드웨어 등 성능을 고려하여 좀더 효율적이면서 성능을 향상시킬 수 있는 연구를 하여야 할 것이다.

최근 들어서는 1.25 대란처럼 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. 또한 요즈음 들어서 더욱 시장의 요구가 많아진 가상사설망 엔진의 개발과 함께 노드 차원의 감사 추적 기능 이나 시스템 모니터링 기능으로 시스템 및 네트워크 공격을 탐지하고 차단할 수 있도록 연구하여야 할 것이다.

REFERENCES

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

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

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

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

[5] 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.

[6] 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

[7] DoD 5200.28-STD. 'Department of Defense Trusted Computer System Evaluation Criteria', December 1985

[8] D.Ferraolo and R, Kuhn, "Role-Based Access Control", Proceeding of the 15th National Computer Security Conference, 1992

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

[10] Linux 2.4.18 Kernel-RELEASE Source Code

[11] B. H. Jung, J. N. Kim, "Design of Dynamic Intrusion Detection Rule Modification Technique for Kernel Level Intrusion Detection," 한국정보처리학회 추계학술대회 논문집, Vol. 9, No. 2, Nov. 2002.

[12] S.H. Jo, J. N. Kim, & S. W. Sohn, "Design of Web-based Security Management for Intrusion Detection", Proc. of ICEB, ICEB '2002, 2002

[13] 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.

김 정 녀

1987년 : 전남대학교 전산통계학과 졸업

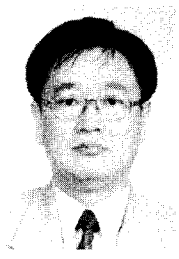
1995년 ~ 1996년: Open Software Foundation Research Institute 공동 연구 파견(미국)

1998년 ~ 2000년 : 충남대학교 컴퓨터공학과 석사

2000년 ~ 현재 : 충남대학교 컴퓨터공학과 박사

1988년 ~ 현재 한국전자통신연구원 선임연구원(팀장)

<관심 분야> 인터넷 정보보호, Secure OS, 네트워크 보안



손 승 원

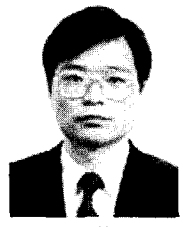
1984년 : 경북대학교 전자공학과 졸업

1994년 : 연세대학교 컴퓨터공학과 석사

1999년 : 충북대학교 컴퓨터공학과 박사

1991년~현재 : 한국전자통신연구원 책임연구원(부장)

<관심분야> 이동인터넷 보안, 정보보호, 네트워크 보안



이 철 훈

1983년 서울대학교 전자공학과 졸업

1983년 - 1986년 삼성전자 컴퓨터 개발실 연구원

1988년 한국과학기술원 전기 및 전자공학과 석사

1992년 한국과학기술원 전기 및 전자공학과 박사

1992년 - 1994년 삼성전자 컴퓨터사업부 선임연구원

1994년 - 1995년 Univ. of Michigan 객원연구원

1995년 - 현재 충남대학교 컴퓨터공학과 부교수

<관심분야> 운영체제, 병렬처리, 결함허용 실시간 시스템 등