# 웹 기반의 방화벽 통합 보안 관리 시스템 개발

이 동 영[†]·김 동 수[†]·홍 승 선[†]·정 태 명[††]


## 요 약

정보통신과 컴퓨터기술의 발전으로 인하여 불법침입으로 인한 정보 피괴, 서비스거부공격 그리고 컴퓨터 바이러스 등에 의한 역기능이 날로 증가하고 있는 추세이다. 또한, 이러한 공격들로부터 네트워크를 보호하기 위해서 침입차단시스템(일명 방화벽), 침입탐지시스템, 접근제어시스템 등 많은 보안제품들이 개발 및 적용되고 있다. 그러나 이러한 보안 제품들에 대한 관리를 위해서는 많은 직업과 비용이 소요된다. 따라서 이들 보안제품들에 대한 효율적인 관리와 일관된 보안 정책을 적용할 수 있는 관리시스템이 필요하게 되었다. 본 논문에서는 대표적인 보안제품인 침입차단시스템에 대한 통합관리 및 보안 정책 수립을 수행하는 웹 기반의 통합보안관리시스템을 설계하고 구현하였다. 구현된 시스템은 웹 클라이언트, 통합엔진, 그리고 에이전트 등 크게 3개 부분으로 구성되어 있으며, 다른 보안 제품과의 확장성과 효율성 그리고 단순하고 개념적인 보안 서비스를 통해 보안 정책에 대해서 전문적인 지식이 부족한 관리자의 경우에도 쉽게 보안 관리를 할 수 있는 기능을 제공한다.


# A Development of Web-based Integrated Security Management System for Firewalls

Dong-Young Lee[†] · Dong-Soo Kim[†] · Seung-Sun Hong[†] · Tai-Myoung Chung[††]


## ABSTRACT

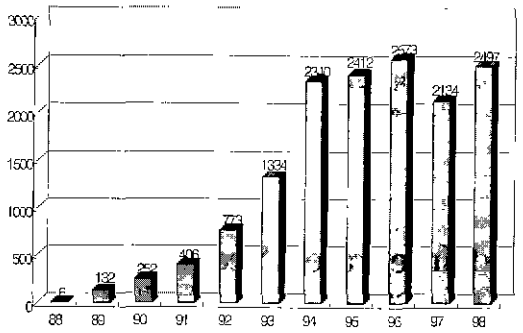
*With a remarkable growth and expansion of Internet, the security issues emerged from intrusions and attacks such as computer viruses, denial of services and hackings to destroy information have been considered as serious threats for Internet and the private networks. To protect networks from those attacks, many vendors have developed various security systems such as firewalls, intrusion detection systems, and access control systems. However, managing those systems individually requires too much work and high cost. Thus, integrated security management and establishment of consistent security policy for various security products has become more important. In this paper, we propose integrated security management system called WISMSF(Web based Integrated Security Management System for Firewalls) to monitor and control various kinds of firewalls. WISMSF consists of three components - clients, integrated engine, and agents. It supports the transparent management functions of security products, easy ways of defining security policies, and simple expansion of managed ranges*


## 1. 서 론

정보화 사회로 발전하면서 통신서비스 이용자들은 보다 신속하고 다양한 서비스를 요구하게 되고, 이에 부응하여 컴퓨터와 정보통신 기술의 발달은 전자 메일, 파일 전송 등과 같은 기본적인 서비스 뿐 만 아니라 분산 환경을 바탕으로 하는 멀티미디어, 전자 결제, 전자 상거래 등과 같이 복합적인 네트워크 서비스들로 확장되고 있다. 그리고 이와 같은 발전은 전송 속도의 고속화, 대용량의 데이터 전송 등으로 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화

† 준 회 원 : 성균관대학교 대학원 건기전자및컴퓨터공학부
†† 종신회원 : 성균관대학교 전기전자및컴퓨터공학부 교수
논문접수 : 1999년 12월 27일, 심사완료 : 2000년 10월 2일

시켜주는 긍정적인 효과를 거두고 있는 반면, 개방형 네트워크인 인터넷의 확산에 의한 외부자의 시스템 불법 침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 공격 등 부정적인 기능들도 날로 증대시킴으로서, 이로 인한 피해 규모는 심각한 수준에 이르고 있다. 단편적인 예로 미국 CERT/CC(Computer Emergency Response Team/Coordination Center)에서 집계한 해킹 대응 관련 통계 수치는 (그림 1)에서 보는 바와 같다.




자료: 정보보호센터

(그림 1) 미국 CERT/CC 집계 해킹 사고 변화

또한, 통신망의 고도화, 지능화 추세에 따라 통신망의 관리 방식과 개념의 변화가 요구된다. 즉, 복잡하고 다양한 방식의 보안관리 및 통신망 관리체계의 집중화, 자동화된 관리체계로의 전환, 그리고 이종간의 보안 시스템들에 대한 통합적인 관리가 요구되고 있다. 그러나, 효율적인 보안 관리를 위해서 관리자는 보안 제품들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야하며, 개방형 네트워크 환경의 경우 새로운 보안 제품이 추가되면 새로운 보안 정책과 기술을 적용해야 한다. 이로 인하여 전산망 운영기관의 보안 관리 비용을 가중시키며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오히려 보안 문제를 야기시키는 역기능을 초래할 수 있다. 그리고, 보안 제품의 개발과 공급이 다수의 공급자에 의해서 공급되므로 서로 상이한 특성을 갖는 보안 제품들로 구성된 보안 관리 구조의 효율적인 운용과 유지에 상당한 어려움이 있다. 이와 같이, 다수의 이질적인 방화벽을 사용하는 경우, 현재로서는 각 방화벽을 따로 관리할 수밖에 없으며, 앞서 언급한 정책 일관성 문제 등의 관리상의 어려움이 그대로 존재한다.

본 논문에서는 대표적인 보안제품인 침입차단시스템에 대한 중앙 집중적으로 관리하기 위한 웹 기반의 통합 보안관리 시스템(WISMSF : Web-based Integrated Security Management System for Firewalls)에 대해서 설명한다. 2장에서는 통합보안관리시스템에 대한 관련 연구 동향을 살펴보고, 3장에서는 이종의 방화벽을 관리하는 통합보안관리시스템인 WISMSF의 상세 설계에 대해서 기술한다. 4장에서는 WISMSF의 구현 결과에 대해서 살펴보고 마지막으로 5장에서는 결론 및 향후 연구 과제에 대해서 언급하고자 한다.

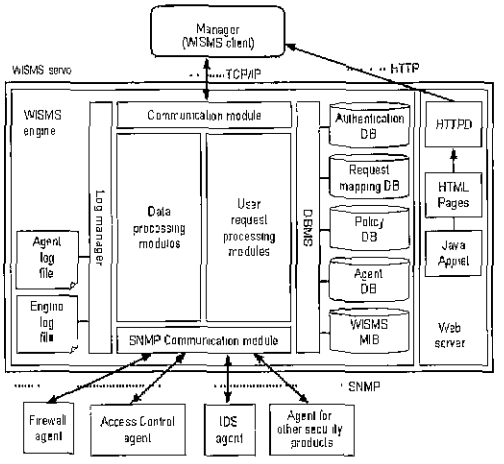
## 2. 관련 연구

통합보안관리시스템에 대한 연구 동향을 살펴보면 Checkpoint, Inc.의 OPSEC(Open Platform Security) [1-4]과 Network Associates, Inc.의 Active security [5-7]시스템의 개발이 가장 활발하게 연구되고 있다.

OPSEC은 각 보안 시스템들간의 상호협력을 통해서 궁극적으로 관리자의 개입 없이 자동적인 보안관리를 목적으로 한다. Checkpoint사의 Firewall-1/VPN-1 제품을 중심으로 이들이 갖추지 못한 보안 기능들을 Outsourcing 시켜 Business Network의 보안을 강화하기 위한 시스템이다. 전체적으로는 각 보안 시스템들이 동등한 위치에서 상호 협력한다는 면에서 분산 보안 시스템의 특징을 갖고 있다. 그러나 OPSEC은 Business Network의 입구가 되는 지점(Gateway)에 자사(Checkpoint Inc.)의 제품이 설치되어 있는 환경을 기반으로 정책 설정한다. 이에 각 보안 시스템들(OPSEC Framework Partners에 가입된 기업의 보안 시스템)이 VPN-1/Firwall-1과 연동을 하도록 한다는 기본 조건을 만족하여야 한다. 그리고 OPSEC환경에서 보안 시스템들간의 상호 연동은 OPSEC SDK(Software Development Kit) 프로토콜을 통해서만 구현이 가능하다. 따라서, OPSEC의 통합 보안 기능을 적용하기 위해서는 Checkpoint Inc 제품의 VPN-1/Firwall-1의 구입과 이들의 기능을 보완하기 위한 보안 시스템은 OPSEC Framework Partners에 소속된 회사의 것으로 한정된다는 단점을 갖고 있다.

Network Associates, Inc.의 Active security의 구조를 살펴보면, 개념적으로 보안과 관련되는 이벤트를 탐지하는 시스템인 센서(sensor), 보안에 대한 어떤 동

작을 수행하는 시스템인 행위자(actor), 그리고 이들의 행위를 중재하고 조율하는 중개인(arbiter)으로 구성되어 있다. OPSEC과는 달리 중개인(arbiter)이라는 존재(event orchestra)를 두어 정책과 각 보안 관련 사건의 수집 및 사건들에 대한 행위를 중앙에서 제어하는 기능을 갖는 중앙 집중적인 보안 시스템이다. 현재 이를 지원하는 제품군은 다양하지 않으며, OPSEC과 같이 Network Associates사의 보안 제품군들간의 상호 연동만을 지원하는 단점을 갖고 있다




(그림 2) WISMS의 전체 구조

이에 본 논문에서 제안하는 웹 기반의 통합 보안관리 시스템(WISMS : Web-based Integrated Security Management Systems)의 특징을 살펴보면 다음과 같다.

WISMS는 보안 관련 시스템을 중앙 관리를 목적으로 하며, 보안 관리자에게 네트워크 보안 상태의 전체적인 뷰(View)를 제공한다. 각 보안 시스템들에 설치된 SNMP(Simple Network Management Protocol) 에이전트(agent)를 통해 보안 시스템들에 대한 제어 및 사건 보고를 수행하며, 보안 시스템과 에이전트 사이의 명령어 수행은 SNMP를 이용함으로써 시스템 범용성과 확장성을 고려하였다. 또한, 보안 정책에 대해서 전문적인 지식이 부족한 사용자의 추상적인 정책 설정 요구에 대해서 통합 엔진(Integrated Engine)에서 이를 수행하며, 추가로 보안시스템에 대해서 통합 관리를 하고자 할 경우에는 기존의 보안 시스템들의 재 구현이나 수정이 필요 없이 그에 해당하는 에이전트를 추가함으로써 이들을 수용할 수 있는 확장성을 갖고 있다.

(그림 2)는 본 논문에서 제안하는 웹 기반의 통합보안관리시스템(WISMS)의 전체 구조를 나타낸 것이다.

## 3. WISMSF의 설계 및 구현

본 논문에서 설계하고 구현한 웹 기반의 침입차단시스템 통합 보안 관리시스템(WISMSF)은 앞서 언급한 WISMS의 관리대상 보안 제품 중 침입차단시스템 제품에 대한 통합 관리시스템이다[8-9]

WISMSF의 관리 대상 보안 제품의 조사 및 분석은 침입차단시스템을 중심으로 수행하였으며, 각 보안 제품이 제공하는 기능의 설정을 위한 외부 인터페이스, 정책 설정 및 구성방법의 분석을 중점으로 연구하였다. 또한, WISMSF의 프로토타입을 설계 및 구현하기 위하여 공개 소프트웨어 침입차단시스템인 ipfwadm [10], TIS-FWTK[11], 그리고 상용 제품으로 국내 보안소프트 개발회사인 (주)시큐어소프트에서 개발한 침입차단시스템인 SecureShield[12]를 관리 대상 보안 제품으로 설정하였다. <표 1>은 WISMSF의 관리대상 보안제품들의 특징을 나타낸 것이다

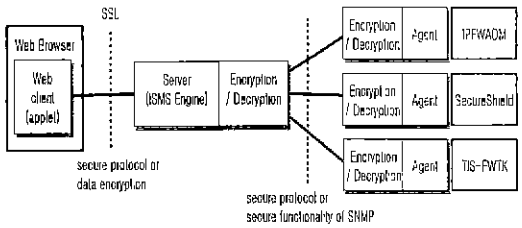
〈표 1〉 WISMSF의 관리대상 보안제품

| 보안제품 | 특 징 | 비 고 |
|---|---|---|
| SecureShield | 패킷필터링과 응용게이트웨이 프락시를 채용한 하이브리드방식 | 상용제품 |
| ipfwadm | Linux Kernel에서 제공하는 패킷 필터링기능을 제어하는 도구 | 공개s/w |
| TIS-FWTK | 응용게이트웨이 방식 | 공개s/w |

### 3.1 WISMSF의 통신 인터페이스

WISMSF의 통신 인터페이스는 크게 클라이언트-엔진간의 통신 인터페이스와 엔진-에이전트간 통신 인터페이스로 구분할 수 있으며 안전한 데이터 전송을 보장하여야 한다. 클라이언트-엔진 인터페이스의 경우, 클라이언트가 HTTP를 이용하여 웹 페이지 Java Applet을 전달하는데 이를 보호하기 위해서 SSL(Security Socket Layer)[13-14]를 사용하고, 이후에 Java Applet과 엔진과의 통신은 Java Crypto API를 이용한다. 엔진-에이전트 인터페이스는 SNMP[15-17]을 이용하며 SNMP 메시지 자체를 암호화하여 송신하고 수신측에서는 이를 복호화함으로써 안전한 메시지 전송을 보장한다. WISMSF는 사용자 ID와 IP를 이용한 인증은 구현하였으며, 메시지에 대한 암호화 부분은 현재 구현

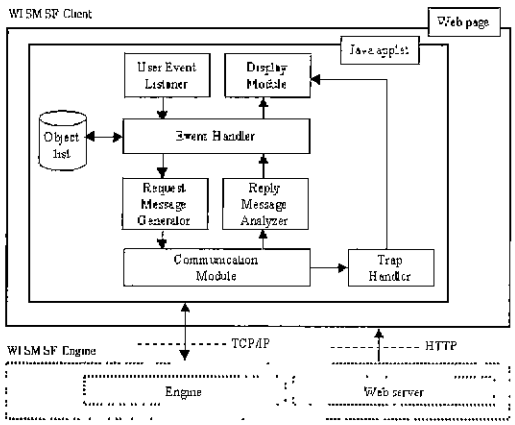
은 진행중이다. (그림 3)은 WISMSF의 인터페이스 구조를 나타낸 것이다.




(그림 3) WISMSF의 인터페이스 구조

3.2 WISMSF 클라이언트

웹 클라이언트는 호스트에 어떤 보안 제품이 설치가 되어있는지에 대한 정보가 없는 일반 사용자 관점에서 전체적인 통합 보안 관리시스템에 대한 제어 기능을 수행하며 사용자에게 명령, 보안 정책, 보안 시스템의 위치 등의 정보를 통합적으로 수용할 수 있는 GUI(Graphical User Interface)를 제공한다. (그림 4)는 WISMSF 클라이언트의 세부모듈을 나타낸 것이며 상세 내용은 다음과 같다.



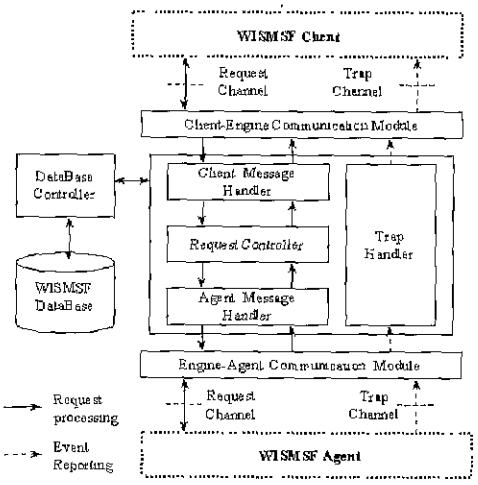

(그림 4) WISMSF 클라이언트의 세부 모듈

- User Event Listener
  사용자로부터 보안 서비스들의 이벤트를 수집한다
- Event Handler
  입력된 이벤트를 분석하고 엔진 또는 객체 리스트에게 이벤트를 요구하고 이벤트 메시지 전송 을 위한 필요한 필드들을 명령어 생성기(Request Message Generator)에게 전달한다. 그리고 수집된 정보를 사용자에게 제공하기 위해서 디스플레이 모듈(Display Module)에게 전송하고 객체 리스트(Object List)에 저장된 정보를 갱신하는 이벤트를 처리한다.
- Request Message Generator
  사용자 인증, 관리대상 호스트의 추가 및 삭제, 보안 정책의 설정 및 변경 등 보안 서비스의 요구 형태에 따라 메시지를 생성한다.
- Communication Module
  엔진과 통신 채널을 형성하여 보안 서비스 관리에 필요한 메시지를 송·수신한다.
- Reply Message Analyzer
  엔진으로부터의 응답 메시지를 분석한다.
- Trap Handler
  관리 대상 침입차단시스템에 대한 오류 발생과 같은 시스템 발생 이벤트와 사용자의 요구에 의해서 주기적으로 엔진이 에이전트에게 정보를 수집한다
- Display Module
  처리결과를 클라이언트 GUI상에 출력한다
- Object List
  엔진과 초기 통신 설정 후에 전송 받은 메시지 중에서 웹 클라이언트에서 저장하고 있는 객체들의 집합이다. 여기에는 내/외부 호스트 또는 그룹의 리스트, 정책 테이블 등이 있으며 이들 정보들에 대한 변경사항이 발생했을 경우 실시간으로 갱신된다.

3.3 WISMSF 엔진

WISMSF 엔진의 주요 기능은 WISMSF 클라이언트의 인증 및 정보 관리 기능뿐만 아니라 웹을 통하여 WISMSF 엔진에 접속하고자 하는 사용자들에 대한 통신 채널의 관리와 접근 제어 기능을 포함하다. 그리고 클라이언트 관리 기능과 이기종의 침입차단시스템 관리를 위한 제어 기능과 보안 정책의 적용 현황 분석을 위한 정보 수집 및 보고 기능으로 정의 할 수 있다. 제어 기능은 크게 보안정책 제어와 관리대상 시스템들에 대한 형상관리 제어 기능으로 구성되며, 정보 수집 및 보고 기능은 로그정보 및 통계정보 수집 그리고 Trap을 이용한 보고 기능을 수행한다. (그림 5)는 WISMSF 엔진의 세부 모듈을 나타낸 것이며 상세 내용은 다음과 같다

- Client-Engine Communication Module
  클라이언트와 엔진간의 통신채널 설정을 위하여 정의된 모듈로써, 명령어 처리 통신 채널 관리자와 Trap 보고 통신 채널 관리자 그리고 WISMSF 클라이언트들의 세션 관리를 수행하는 세션관리자(SM : Session Manager) 등으로 구성되어 있다.
- Client Message Handler
  클라이언트로부터 전달된 명령어 메시지를 엔진에 정의된 명령어 처리단위 데이터 구조의 변환한다.

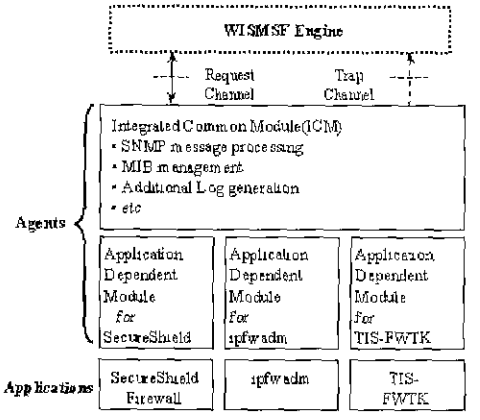



(그림 5) WISMSF 엔진의 세부 모듈

- Request Controller
  DataBase Controller와 WISMSF Database의 Mapping Table을 참조하여 Client Message Handler로부터 전달된 명령어를 처리한다.
- Agent Message Handler
  엔진과 에이전트간의 통신 채널을 설정하며, 이를 통해서 해당 에이전트에 전송할 명령어를 SNMP PDU형태로 변환한다.
- Engine-Agent Communication Module
  엔진과 에이전트간의 통신을 담당한다
- Trap Handler
  Trap 채널을 통해서 전달된 에이전트의 Trap 명령어를 처리하고 이를 통보하는 기능을 수행한다

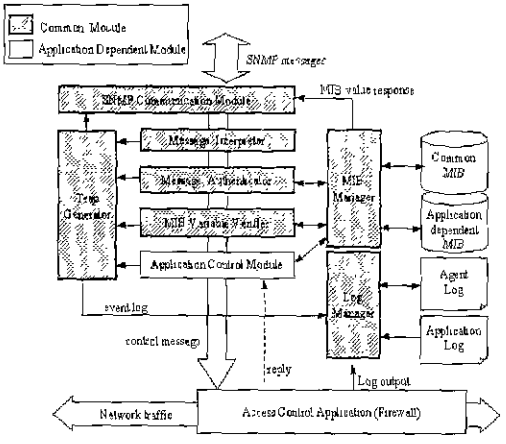
### 3.4 WISMSF 에이전트

WISMSF에이전트는 엔진으로부터 받은 SNMP명령을 받아 이를 해석하여 관리 대상 응용 프로그램에 이를 적용하고, SNMP 응답 메시지를 이용해서 엔진에게 결과를 전송하는 기능을 수행하는 WISMSF의 핵심적인 부분이다. (그림 6)은 WISMSF 에이전트의 개념적인 구성을 나타내고 있다.




(그림 6) WISMSF 에이전트의 개념적인 구성

에이전트는 확장성과 이식성을 높이기 위해서 크게 ICM(Integrated Common Module)과 ADM(Application Dependent Module)로 구성되어 있다. ICM은 각 에이전트가 관리하는 침입차단시스템의 종류에 상관없이 동일하게 공통적으로 실계 구현된 공통기능모듈이며, ADM은 에이전트의 관리대상이 되는 침입차단시스템을 직접적으로 제어하고 응용프로그램과 에이전트의 정보 교환을 수행하는 응용프로그램에 의존적인 모듈이다.

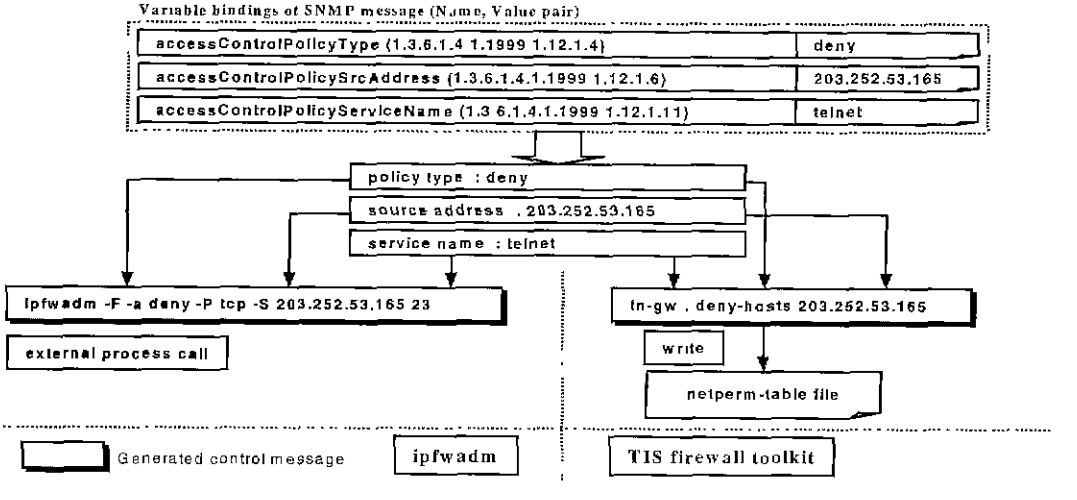



(그림 7) WISMSF 에이전트의 기능별 세부 모듈

또한, (그림 7)은 에이전트의 공통기능모듈(ICM : Integrated Common Module)과 응용프로그램에 의존적인 모듈(ADM : Application Control Module)의 기능별 세부 모듈을 나타낸 것이며 상세 내용은 다음과 같다.

- SNMP Communication Module
  엔진과의 통신을 담당하며, WISMSF 엔진의 요구를 처리한 결과를 전송하는 SNMP GetResponse 메시지 혹은 Trap 메시지를 엔진 측으로 전송한다.
- Message Interpreter
  SNMP Communication Module로부터 SNMP 메시지를 전달받아 이를 메시지의 각 필드로 구분하여 각 필드의 데이터형에 맞게 그리고, 내부적으로 사용하기 용이한 자료형으로 해석하며, 해석된 결과를 에이전트가 기능 수행을 위해 이용하는 구조체 형태의 자료구조에 저장한다.
- Message Authenticator
  각 필드로 구분된 SNMP 메시지에 대한 인증 기능을 수행한다.
- MIB Variable Verifier
  수신한 SNMP 메시지 내에 포함된 MIB(Management Information Bases)값들이 에이전트가 관리하는 MIB내에 존재하고 그 자료 형과 값의 범위가 허용되는 범위 내에 존재하는 지를 검사한다
- MIB Manager
  침입차단시스템에 대한 관리 및 제어 동작을 수행하기 위한 MIB을 관리한다.
- Log Manager
  에이전트의 동작 수행 도중에 발생하거나 침입차단시스템으로부터 감지한 사건들을 로그 파일을 기록한다.
- Trap Generator
  각 기능모듈에서 각자의 작업을 수행하는 도중에 발생한 오류를 수신하고 이에 해당하는 SNMP Trap 메시지를 발생시킨다.
- Application Control Module
  직접적으로 침입차단시스템과 상호 동작하는 부분으로써 침입차단시스템을 제어하는 방법에 따라 각 에이전트마다 다르게 구현한다

본 논문에서 제시한 WISMSF에서 관리자가 자바 인어를 이용해서 구현된 웹 인터페이스를 통해 개념적인 즉, "203.252.53.165에서 요청되는 telnet서비스를 거부한다"라는 보안 정책 설정 명령어를 관리 대상 보안 시스템에 대한 제어 명령어로 변환되어 수행되는 과정을 살펴보면 (그림 8)과 같다. 우선 ADM(Application Dependent Module)에 속하는 ACM(Application Control Module)에서 MIB 변수에 정의된 통해서 SNMP 메시지 내에 적용할 정책의 형태를 나타내는 accessControlPolicyType이라는 객체에는 "deny"라는 정책을 설정하



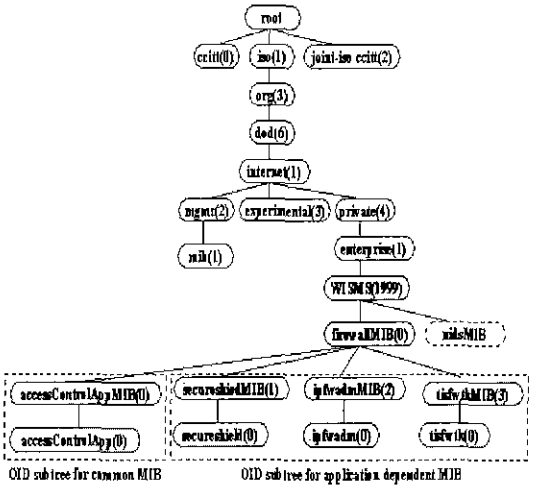

(그림 8) 개념적 보안서비스의 명령어를 제어 명령어로의 변환 과정

고, 근원지 주소를 나타내는 accessControlPolcySrcAddress라는 객체에는 "203.252.53.165"를 지정하며, 해당 보안 서비스를 나타내는 accessControlPolicyServiceName라는 객체에는 "telnet"이라는 서비스 명을 지정한다.

그리고 (그림 8)에서 보는 바와 같이 개념적인 보안 서비스 명령어를 관리 대상 보안시스템에 대한 제어 명령어로 변환되는 과정과 정책 설정에 콘솔(console) 명령어를 이용하는 ipfwadm의 경우와 정책 설정 파일을 이용하는 TIS firewall toolkit의 제어 메시지의 예를 나타내었다. 각각의 제어 메시지는 콘솔 명령어의 경우에는 외부 프로세스 호출의 방법을 사용하여 침입차단시스템에 적용하고, 정책 설정 파일의 경우에는 제어 메시지를 해당 파일에 기입하여 정책을 적용한다.

### 3.5 WISMSF MIB정의

WISMSF의 전체적인 동작을 위한 MIB값을 정의하기 위해서 침입차단시스템의 기능에 대한 직접적인 평가를 수행하였으며, 각 각의 침입차단시스템에 공통적으로 적용될 수 있는 제어항목과 필요한 정보를 정의한 공통MIB과 각 각의 침입탐지시스템의 독립적인 특성과 기능을 정의한 침입차단 응용프로그램에 의존적인 MIB으로 구성되어 있다. (그림 9)는WISMSF SNMP OID(Object Identification) Tree를 나타낸 것이다.




(그림 9) WISMSF SNMP OID Tree

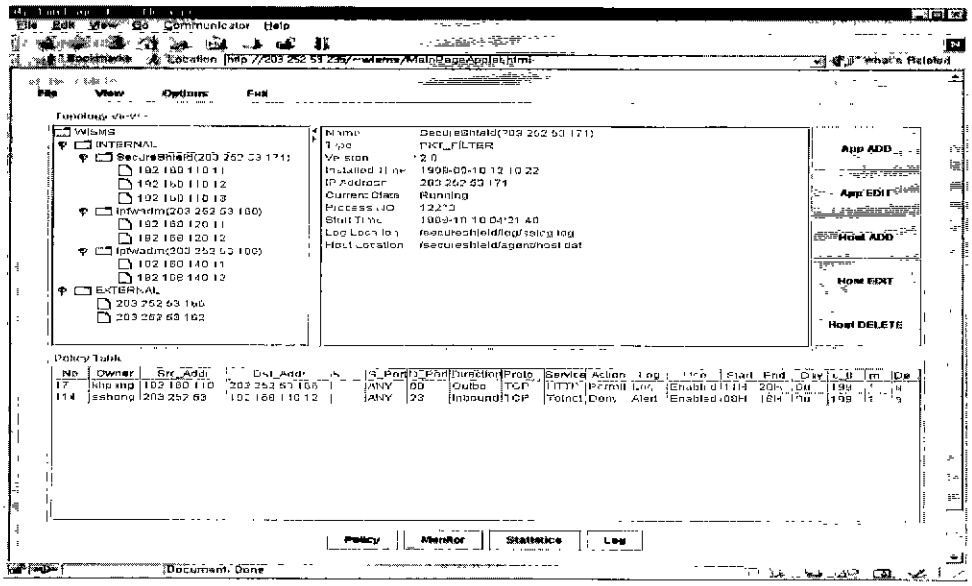
#### 3.5 1 WISMSF 공통MIB

WISMSF의 공통MIB은 크게 관리 대상 침입차단시스템의 자체 정보, 정책 설정을 위한 정보, 주기적인 정보, 침입차단시스템을 경유하여 진행되는 네트워크 서비스에 대한 세션 정보, 관리 대상이 되는 호스트들에 대한 목록 정보를 유지하는 객체들의 집합, 그리고 에이전트에서 발생할 수 있는 여러 가지 상황을 WISMS 엔진에게 알리기 위한 Trap 명령어에 대한 객체들의 집합 등 6개의 그룹으로 구성되어 있으며 각각의 MIB 그룹에 대한 기능을 살펴보면 다음과 같다.

- 침입차단 응용 프로그램 정보 MIB
  침입 차단 응용 프로그램에 관계된 정적, 동적인 값들을 저장하고 제어하는데 사용되는 MIB 객체들을 포함하는 그룹이다.
- 침입차단 응용 프로그램 정책 설정 MIB
  침입 차단 응용프로그램의 접근 정책에 관한 정보가 저장되는 MIB객체이다.
- 네트워크에 대한 현재의 세션 정보 MIB
  관리 대상 네트워크 상에서 침입 차단 응용 프로그램의 통제하에 있는 현재의 네트워크 세션에 관 한 정보를 저장하는 MIB객체이다
- 주기적인 정보의 수집을 위한 MIB
  WISMSF 엔진에서 필요에 의해 일정한 시간 간격으로 수집하고자 하는 객체를 지정하고 이 MIB 객체 테이블에 지정된 정보에 따라 에이전트는 주기적으로 해당 객체의 값을 WISMSF 엔진에게 전달하는 작업을 수행한다.
- 네트워크에 대한 호스트의 상태 정보 MIB
  침입차단시스템의 정책 설정과 관련되어 정책에 직접적으로 관련되어 있거나 차후에 정책을 적용할 목적으로 침입차단 시스템의 관리 대상이 되는 호스트들에 대한 목록 정보를 유지하는 MIB 객체들의 집합이다
- Trap 정보 MIB
  침입 차단 응용 프로그램에서 발생하는 상태 변화나 오류 메시지가 있을 경우, 이를 엔진에게 통보하기 위한 MIB 객체들이다.

#### 3.5.2 침입차단시스템에 의존적인MIB

응용프로그램에 의존적인 MIB은 각 침입차단시스템이 공통적으로 제공할 수 있는 항목 이외에 각 침입차




(그림 10) WISMSF 토폴로지 및 사용자 관리 화면

단시스템의 특성이나 기능에 따라 차별적으로 제공되는 정보와 제어 항목에 대한 MIB이다. 현재 관리 대상 침입탐지시스템에 설정된 정책에 관한 정보와 침입차단시스템에서 기록 정보 등의 그룹으로 구성할 수 있으며 상세 내용은 다음과 같다.

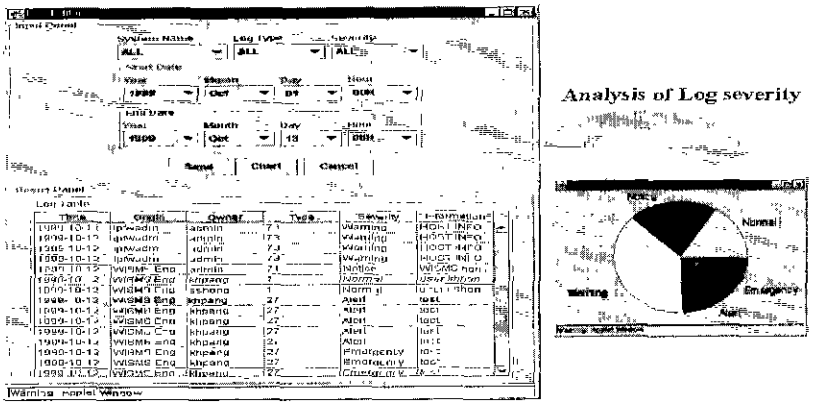
- 정책 적용 상태에 관한 정보 MIB
  이 객체들은 현재 침입차단시스템에 설정된 정책에 의해 영향을 받는 서비스 요구들에 대 한 기록을 시간적으로 가까운 순서로 저장하고 있는 객체들의 집합이다. 이 객체 그룹은 크게 허용된 서비스에 대한 정보와 거부된 서비스에 대한 정보로 나눌 수 있으며, 이들 집합을 통해서 정책적용 상태를 파악할 수 있다
- 침입차단시스템의 기록 정보 MIB
  침입차단시스템에서 기록을 유지할 수 있는 정보들에 관계된 객체들의 집합이다 보통 누적 정보들을 유지하고 있으며, 예로는 패킷의 양이나 서비스 연결 개수 등이 있다 이 객체 집합도 크게 허용된 서비스에 관련된 수치 정보와 거부된 서비스에 관련된 수치 정보로 구성된다 그러나, 이 정보는 관리 대상 침입차단 시스템에 따라 제공될 수도 있으며 지원되지 않을 수도 있다.

3.6 WISMSF의 구현

본 논문에서는 설계한 WISMSF의 구현환경을 살펴보면, 클라이언트는 Sun UltraSparc20시스템에 Solaris 2.6을 기반으로 개발 Toolkit은 JDK-1.2.1-A을 적용하였다. 엔진은 Sun UltraSpac20 시스템과 운영체제는 Solaris 2.6을 사용하였으며, 데이터베이스는 MySQL 3.23.2통해서 구현하였다 그리고 에이전트의 경우는 Sun UltraSpacrc20과 AlphaServer(PC164)를 사용해서 구현하였다.

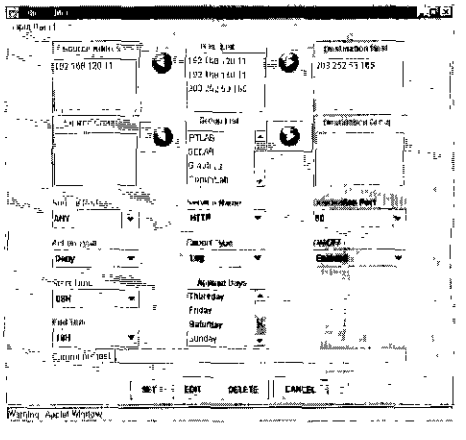
또한, WISMSF는 관리대상 보안제품에 대한 효율적이고 통합적인 정보를 제공하며 주요 기능을 살펴보면 다음과 같은 기능을 수행한다 (그림 10)은 WISMSF 토폴로지 및 사용자 관리 정보를 나타내는 화면이다.

- 사용자 관리
  사용자는 웹 브라우저를 사용하여 WISMSF엔진이 탑재되어 있는 웹 서버에 접근하며, 이때 접근을 하려는 사용자에 대한 관리가 이루어진다. 사용자 관리 기능은 웹 서버로 접속하는 client에 대한 인증 기능과 보안 관리의 이해와 정책 설정의 능력에 따라 일반 관리자(GM : General Manager), 서비스관리자(SA : Service Administrator), 그리고 보안전문가(SE : Security Expert) 등으로 사용자의 등급을 분류한다




(그림 12) 로그 정보 분석

- 보안 정책 설정 및 관리 대상 네트워크 구성 관리
  보안 정책을 적용하기 위해서 침입차단시스템들이 관리하는 네트워크 구성에 대한 정보 즉, 침 입차단시스템이 관리하는 내부 또는 외부 네트워 크에 위치하는 호스트정보와 다중 호스트에 대해 서 동일한 정책을 적용하는 그룹 정보에 대한 추가, 삭제 및 변경의 기능을 수행한다 또한 관리 대상 보안 제품들에 대해서 보안 정책 설정 그리고 설정된 정책에 대한 주기적인 정책 상태 감시 기능과 정책이 설정된 침입차단시스템을 통과하는 패킷을 통해서 현재의 연결 상태 감시 기능을 수행한다 (그림 11)은 관리 대상 네트워크 근원지 주소 192.168.120.11에서 목적지 호스트 203.252.53.165의 HTTP서비스에 대해서 거부정 책을 설정한 화면이다.



(그림 11) 보안 정책 설정 및 구성관리

- 통계 정보 수집 기능
  보안 정책이 적용된 관리 대상 보안 제품들로부터 수집된 통계적 데이터를 기반으로 기간별 패킷 통계, 서비스별 패킷 통계, 사용자 접속 통계, 그리고 관리 대상 침입차단시스템 상의 에러 메시지 발생 빈도 등의 정보를 제공한다.
- 로그 정보 수집 기능
  WISMSF 엔진과 에이전트에서 생성되는 로그 정보와 침입차단시스템 자체 내에서 생성되는 로그 정보를 수집하는 기능을 가지며, 사용자가 로그정보 분석을 수행할 때 편이성을 제공하기 위하여 로그정보 발생원, 로그정보 항목, 로그정보의 심각성을 분석하는 기능을 수행한다 (그림 12)는 로그 분석 화면을 나타낸 것이다.

## 4. 결론 및 향후 계획

컴퓨터와 정보통신 기술의 발달은 전송 속도의 고속화, 대용량의 데이터 전송 등으로 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화 시켜주는 긍정적인 효과를 거두고 있는 반면, 개방 네트워크 구조인 인터넷의 확산으로 인한 컴퓨터 바이러스 및 정보 자원에 대한 침입 가능성은 날로 증대되고 있다. 따라서 다양한 보안제품을 적용한 보안 시스템의 필요성이 대두됨에 따라 본 논문에서는 서로 상이한 침입차단시스템에 대해서 통합적으로 관리하기 위한 다중보안기술을 수용하는 웹 기반의 통합 보안 관리 시스템(WISMSF)을 제안하고 구현하였다.

본 논문에서 구현한 WISMSF는 보안관리의 유연성

을 제공하기 위한 웹 인터페이스의 적용과 보안 정책에 대한 전문적인 지식이 부족한 일반 사용자도 쉽게 보안 관리를 수행 할 수 있는 개념적인 보안 서비스를 제공하며, 클라이언트, 엔진, 그리고 에이전트 등의 모듈화된 구성으로 확장성을 극대화하였다. 또한, 본 연구를 통해서 대규모 전산망 보안에 대해서 이종의 침입차단시스템들에 대한 효율적이고 통합적인 보안 관리 기술의 개발, 표준 프로토콜인 SNMP를 이용함으로써 기존의 관리시스템과의 연동 할 수 있는 시스템을 개발, 그리고 이기종의 보안 제품을 제어하고 관리하기 위한 SNMP MIB을 정의하였다

그리고 향후 과제로써는 WISMSF의 통신 채널 즉, 클라이언트-엔진간의 통신채널과 엔진-에이전트간의 통신채널에 대해서 안전한 정보 전송을 보장하는 기능이 강화되어야 하며, WISMSF의 결함(failure)에 따른 각 각의 관리 대상 네트워크에 대한 대응책에 관한 연구와 실제 네트워크 환경에서의 성능에 대한 검정 및 보완 작업 그리고 타 보안시스템과의 연동 및 확장을 위한 연구도 병행되어야겠다.

## 참 고 문 헌


[1] Open Platform for Security(OPSEC) Technical Note, Check Point Software Technology, Inc., 2000.

[2] Check Point OPSEC SDK Version 4.1 Release Notes, Check Point Software Technology, Inc , Nov 2, 1999.

[3] Check Point VPN-1/Firewall-1 OPSEC API Specification Version 4.1, Check Point Software Technology, Inc., Nov 4, 1999.

[4] Check Point Firewall-1 OPSEC Open Specification Version 1.01, Check Point Software Technology, Inc., Nov 8. 1998.

[5] The Active Firewall White Paper - A Dynamic New Model for Integrated Active Response Firewall Security, Network Associates, Inc , 1999.

[6] Automating Security Management while Reducing Total Cost of Ownership, Network Associates, Inc., 1999.

[7] Active Security Getting Started Guide Version 5.0, Network Associates, Inc., 1999.

[8] D. Y. Lee, D. S. Kim, K. H. Pang, H. S. Kim, T. M. Chung, "A Design of Scalable SNMP Agent for Managing Heterogeneous Security Systems," NOMS (Network Operations and Management Symposium)2000, pp.293-294. April 2000.

[9] 이동영, 김동수, 방기홍, 김홍선, 정태명, "SNMP를 이용한 웹 기반의 통합 보안관리 시스템," KNOM (Korea Network and Operations Management) Review Vol.2, No.1, pp.1167-1171. April 1999.

[10] Jos Vos, Willy Konijnenberg, "Linux firewall facilities for kernel-level packet screening," X/OS Experts in Open Systems BV, November 1996.

[11] "TIS Firewall Toolkit Overview," Trusted Information Systems Inc., June 1994.

[12] SecureShield Administrator s Guide Version 1.0, SecureSoft Inc.

[13] V Ahuja, "Network & Internet Security," Academic Press, 1996.

[14] Simson Garfinkel, Gene Spafford, "Practical UNIX and Internet Security - 2nd Edition," O' Reilly & Associates, Inc , April 1996, p637-646.

[15] William Stallings, SNMP, SNMP v2, SNMP v3, and RMON 1 and 2 - 3rd ed., Addison Wesley, 1999.

[16] David Perkins, Even McGinnis, Understanding SNMP MIBs, Prentice Hall PTR, 1997.

[17] W. Stalling, "Cryptography and Network Security - Principles and Practice Second Edition," Prentice-Hall, 1999.



**이 동 영**

e-mail : dylee@rtlab.skku.ac.kr

1993년 동아대학교 전자공학 (학사)

1998년 성균관대학교 정보공학 (석사)

1993년~1997년 기아자동차 중앙기술연구소 연구원

현재 성균관대학교 전기·전자 및 컴퓨터공학부 박사과정 수료

관심분야 : 네트워크 보안, 시스템보안, 네트워크 관리



**김 동 수**

e-mail : dskim@rtlab.skku.ac.kr

1998년 성균관대학교 정보공학 (학사)

2000년 성균관대학교 정보공학 (석사)

현재 성균관대학교 전기·전자 및 컴퓨터공학부 박사과정

관심분야 : 네트워크 관리, 네트워크 보안, 시스템 보안

## 홍 승 선

e-mail : sshong@rtlab.skku.ac.kr
1998년 성균관대학교 정보공학 (학사)
2000년 성균관대학교 정보공학 (석사)
현재 성균관대학교 전기·전자 및 컴퓨터공학부 박사과정
관심분야 : 네트워크관리, ATM 네트워크, Mobile Agents

## 정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학 (학사)
1984년 University of Illinois Chicago, 전자계산학과 학사
1987년 University of Illinois Chicago, 컴퓨터공학과 석사
1995년 Purdue University, 컴퓨터공학 박사
1985년~1987년 Waldner and Co, System Engineer
1987년~1990년 Bolt Bernek and Newman Labs., Staff Scientist
현재 성균관대학교 전기 전자 및 컴퓨터공학부 부교수
관심분야 : 실시간시스템, 네트워크관리, 네트워크 보안, 시스템보안, 전자상거래.