실시간 인터넷 보안 서비스 제공을 위한 정책기반 통합 서버 설계 및 시뮬레이션

김 기 영[†] · 안 개 일[†] · 장 종 수[††] · 이 상 호[†††]

요 약

개방형 구조를 갖는 인터넷이 전 세계적으로 광범위하게 활용되면서 네트워크상의 보안 취약점에 대한 사이버테러 위험성이 급증하고 있는 추세이다. 지금까지 네트워크 상의 정보보호는 주로 보안 호스트 및 특정 보안 시스템에 대한 수동적인 정보보호였다. 그러나 이러한 소극적인 정보보호만으로는 전세계적으로 연결된 인터넷 시스템들의 침해에 대한 방어 능력이 취약하여, 사이버테러의 방어에 한계가 있다고 판단된다. 즉 보안 호스트에 국한되는 소극적인 보안이 아니라, 전체 네트워크 차원의 통합 보안관리기능이 제공되어야 한다. 본 논문에서는 보안 문제점들의 기술 제약요인 및 제반 환경요인의 해결방안에 접근하기 위하여 네트워크 차원의 능동적 정보보호 기능을 위한 정책(Policy) 기반의 정보보호 서비스 구조, 제공 기능에 대하여 살펴본다. 그리고 정보보호 서비스 제공을 위한 목표시스템의 설계와 향후 네트워크 차원의 전개 방안에 대하여도 네트워크 보안 시뮬레이션을 통하여 검토한다.

Design and Simulation of Policy Based Integrated Server System Capable to Provide Real-time Internet Security Service

Kiyoung Kim[†] · Gae il Ahn[†] · Jong Soo Jang[††] · Sang Ho Lee[†††]

ABSTRACT

Recently, due to the open architecture of the internet and wide spread of internet users, the cyber terror threatens to the network's weak point are tending grow. Until now, information security solutions are passive on security host and particular security system. This passive information security solution is weak from the attacks through the networks connected worldwide internet systems, and has limitation on the defense against cyber terror attacks. Therefore, network level integrated security function must be provided. In this paper, we consider technology limitations on the information security problems and its environment. Then we present the architecture and functions of policy-based information security services for network level active information security function. This paper also includes design of target system, which provide information security services. Finally, we discuss network level system deployment direction and discuss with Network Security Simulation.

키워드 : Security Service, 정책기반 보안서버(Policy-Based Security Server), PBNM, Network Security Simulation, 침입탐지 시스템(IDS), 침입차단 시스템(Firewall)

1. 서 론

정보화 사회의 활성화와 정보통신 인프라로서 인터넷의 중요성이 급속히 부각되고 있으며, 이를 통한 중요 정보의 유출 문제가 날로 심각해지고 있다. 더욱 현재의 정보통신 기반구조는 서로 밀접하게 연관된 단위구조 들로 연관되어 있어 네트워크 구조의 복잡도 증가로 인한 문제가 확산되고 있다. 특정 단위구조에 대한 사이버 테러 발생시 연결된 구조로의 피해 확산이 우려될 뿐 아니라, 실제 피해규모도 추산키 어렵고, 이에 따른 효율적인 차단 및 복구에도 어려움이 가중되고 있는 실정이다[9].

특히, 현재 제공 가능한 보안 정책이 분산 및 네트워크 차원의 침해에 대하여 개별 호스트 위주의 단편적인 대책에 머물고 있어 전체 네트워크 측면의 종합방지대책 수립이 절실히 요구된다.

네트워크 보안방편으로 침입차단 시스템을 통한 접근 제어는 네트워크의 보안 사고나 위협이 더 이상 내부 네트워크로 확대되지 않도록 막고 격리하는 기술이다. 내부 네트워크를 보호하기 위해서 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가받은 트래픽만 들어오도록 하는 방법이다.

한편, 최근 연구와 적용이 활발해지고 있는 침입탐지 시스템은 침입차단 시스템의 다음 차세대 보안 솔루션으로 부각되고 있으며, 방화벽이 뚫렸을 경우에 대한 피해를 최

† 정 회 원 : 한국전자통신연구원 선임연구원
†† 정 회 원 : 네트워크 보안 연구팀 팀장
††† 종신회원 : 충북대학교 컴퓨터과학과 교수
논문접수 : 2001년 7월 26일, 심사완료 : 2001년 8월 28일

소화할 수 있을 뿐만 아니라 네트워크 관리자 부재시에도 시스템 자체적으로 대응할 수 있는 보안 방법이다.

침입탐지 시스템은 단일 혹은 복수 호스트에 기반한 동작 방식을 갖거나 네트워크에 기반한 침입탐지 기능을 수행하며, 지식에 기반한 오용(misuse) 탐지 기능과 행태(behavior)에 기반한 이상(anomaly) 탐지 기능을 주로 제공한다. 즉 공격의 유형을 misuse와 anomaly로 구분하고 각각 지식과 행태에 대한 분석을 통하여 침입인지의 여부를 판단하게 된다. 이와 같은 분석을 위하여 전문가 시스템, signature 분석, Petri Net, 통계 기법 등의 개념이 복합적으로 활용된다[1].

현재 정보보호 기술은 기존의 기술을 활용한 서버차원의 시스템 보호기능과 접속점에 대한 네트워크 보호 기능을 연동한 통합 정보보호 프레임워크로 발전될 전망이다. 즉, 인터넷으로 연결된 네트워크 환경에서 다양한 침입에 대하여 효과적으로 대응하기 위해서는 탐지 및 차단 기술이 상호 유기적으로 접목될 필요가 있기 때문에 방화벽과 연동된 침입탐지 시스템의 필요성은 더욱 커질 것으로 보인다[6].

본 논문은 네트워크 상에서 실시간 인터넷 보안 서비스 제공을 위한 IETF표준 정책기반 제어 기능을 제안 및 설계한다. 사용자들이 망과 접속하는 망의 액세스 포인트에서 유해 트래픽을 탐지하고, 이에 따른 경보의 전파 및 침입 유형에 따른 정책기반의 침입 방어 메커니즘을 선택 및 수행할 수 있도록 구성한다.

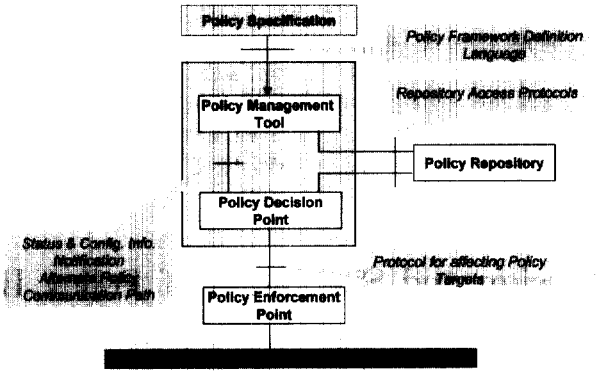
여기에서는 초기 보안 서비스 제공을 위한 구조 설정을 위하여, IETF(Internet Engineering Task Force) / DMTF (Distributed Management Task Force, Inc.) 표준에서 제시하는 목표 시스템의 침입탐지 문제를 CIM(Core Information Model) 접근 방법으로부터 접근한다[6, 16]. 그리고, 정책기반 침입탐지 관리 및 서버 측면에서 갖춰야 할 요구 사항과 조건들을 차례로 도출한다. 이러한 요구사항을 바탕으로 기존 IDS 및 Firewall 기술들을 통합한 네트워크 보안 제어시스템을 설계한다. 이의 안정성 검증을 위하여 UC Berkeley에서 제공하는 VINT 프로젝트의 네트워크 시뮬레이터(NS)를 통하여 목표시스템의 타당성을 미리 검토한다 [2, 13, 14].

본 논문의 구성은 제1장 서론에서 정책기반의 네트워크 침입탐지 서버 시스템의 개념을 기술하고, 제2장에서 정책기반 관리 표준화, 제품개발 동향 및 네트워크 기반 통합 보안제어구조에 대해 분석한다. 제3장에서 정책기반 통합서버 시스템을 제안하고, 적용 가능한 정책전달 프로토콜과 계층적인 시스템 구조를 설계한다. 그리고, 제4장에서 네트워크 시뮬레이터를 이용한 네트워크 보안시스템의 성능평가를 수행하고, 그 결과를 기반으로 향후 정책기반 보안서버 시스템의 기능을 확장하며, 단계별 보안 서비스 전개방안을 수립한다.

2. 실시간 보안 네트워크

2.1 정책기반 관리 표준화 및 제품 개발 동향

정책기반의 네트워크 관리구조는 IETF에서 (그림1)과 같이 정책 관리를 위한 Policy Management Tool(PMT), 정책 저장을 위한 정책저장소(Policy Repository : PR), 정책 결정을 위한 Policy Consumer(Policy Decision Point : PDP), 정책 적용을 위한 Policy Target(Policy Enforcement Point : PEP) 등의 기능적 구성요소로 표현 가능하다.



(그림 1) IETF 표준 정책기반 관리구조

정책 관리부는 망 운용자가 서비스의 목적 및 사업목표에 따라 결정된 망 운용 규칙을 네트워크 상의 모든 장치가 인식할 수 있는 일관된 형식으로 생성하고 변환하는 기능을 제공한다. 다양한 서비스 요구사항에 대한 복잡한 망 운용 정책을 망 내의 모든 네트워크 기기가 이해할 수 있는 일관성 있는 정책 데이터로 변환하기 위해서 PFDL(Policy Framework Definition Language)이 일반적으로 이용된다.

망 관리 정책은 정책저장소(Policy Repository : PR) 저장되며 망 내에 분산되어 있는 PDP에 의해 실시간으로 검색된다. 정책 저장소에 수용되는 데이터는 정책을 결정하기 위한 정책결정 조건과 결정된 정책에 따라 해당 네크워크 기기에서 적용되어야 하는 정책 동작으로 구성되며, 보다 효율적인 정책 데이터 검색과 유지 관리를 위하여 정책규칙(Policy Rule)과 그룹(Policy Group) 등의 데이터 스키마를 제공하고 있다. 저장된 정책을 조회하거나 신규 생성된 정책을 저장하기 위한 프로토콜로는 디렉토리 서비스에 널리 이용되고 있는 LDAP이 사용된다.

정책기반 네트워크관리구조에서 일반적으로 먼저 운용자는 새로운 정책을 생성하거나, 서버의 디렉토리 서버스로부터 정책규칙을 검색한다. 여기에서 정책규칙은 PMT에 의해서 GUI 형태로 제공 가능하며, "if (conditions), Then (actions)"의 형태로 주어진다. 즉, 입력된 정책규칙은 syntax 확인 등의 과정을 거쳐 서버 저장소의 내용 형식에 따라 변환되고, 운용자는 새로이 생성한 정책을 클라이언트의 policy target인 PEP에 적용하도록 명령한다.

이러한 명령 수행 후, PR에 해당 서비스를 위해서 새로운 정책규칙이 저장되며, policy consumer는 새로운 정책규칙을 적용할 policy target을 찾아서 수행 형태를 협상한다. 그리고, policy consumer는 PR에서 정책규칙을 가져오고, 정책규칙을 policy target에 적용 가능한 형태로 변환하여 target으로 전송한다. 그러면, policy target은 새로운 정책규칙을 수행하고, 이를 정책서버에 알린다. 이러한 과정을 feedback이라고 한다. policy target은 event 혹은 일정 시간마다 수행 상태를 정책서버에게 보고한다. 이러한 시나리오를 바탕으로 정책기반 보안 네트워크 구조가 제공된다.

현재 사이버 공간에서의 경제활동 증가와 정보의 자산적 가치가 크게 증대됨에 따라 네트워크 정보보호 제품 및 서비스에 대한 관심과 수요가 지속적으로 증가하고 있으나 관련 제품들의 개발 수준은 국내외적으로 초기단계라고 할 수 있다. 결국 분산 네트워크 환경에서 보안관리를 가능하게 하고 자신의 네트워크에 있는 특정 트래픽이나 정보보안을 통합적으로 관리하는 정책 기반의 네트워크 관리기술 개발이 요구되고 있으며, 이러한 기술을 적용한 업체의 제품으로는 Cisco의 QoS Policy Manager(QPM)1.1, User Registration Tool(URT)1.2, Orchestream의 Enterprise Edition 2.0, Allot Communications의 NetPolicy, Extreme Networks의 Exetreme Ware Enterprise Manager(EEM)2.0, HP의 HP OpenView PolicyXpert1.0, IP Highway의 Open-Policy System, Lucent의 RealNet Rules, Notel Networks의 Optivity Policy Services 1.0, Spectrum Management의 PBNM Suite 등이 있다[10-12].

이들 제품들은 기본적으로 능동적 네트워크 모니터링, 네트워크 서비스 수준 협정 관리, 사용자 기반 정책들을 위한 다중 네트워크 운영시스템 통합 기능 등을 제공하고 있고, 하드웨어를 액세스 및 제어하거나 사용자와 자원 및 정책에 대한 정보를 수집하는 방법으로 CLI(Command Level Interface), SNMP, COPS 및 LDAP 등을 이용하거나 이용할 예정으로 있다[3-5, 7].

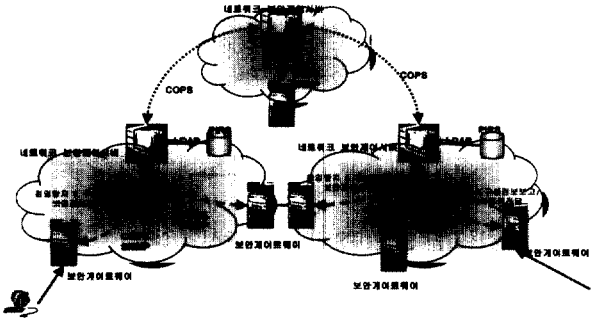
기존의 제품들은 CLI 명령어를 이용하여 정책을 준비하고 있으나 더 복잡해지는 정책변수들을 처리하는데 어려움이 있어서 현재는 다중 네트워크 운영 시스템 통합이 가능한 COPS와 LDAP을 이용하여 처리하고자 한다. 시스코는 COPS 프로토콜을 기반으로 한 COPS Agent를 이용하여 네트워크상의 다른 대부분의 제품들까지도 통합하고자 하며, 루슨트, 익스트림 네트웍스, 얼랏 등은 LDAP 프로토콜을 이용한 디렉토리지원 정책 관리 솔루션을 제시하고 있다. 특히, 얼랏의 넷폴리시는 정책관리자가 실시간으로 네트워크에 특정 정책을 배치하고 그 결과로 흐름과 흐름에 미친 정책의 효과를 추적할 수 있는 능동적인 피드백 메커니즘을 제공한다. 그러나, 시스코와 IP 하이웨이의 경우는 주어진 조건에 부합하는 모든 트래픽을 거부할 수 있는 능력을 제공하지 못한다. 따라서, 이들은 네트워크 보안적인 측면의 악의적인 트래픽의 침입에는 한계를 보이고 있으며, 또한 능동적인 네트워크 보안 정책의 적용은 아직 고려하고 있지 않은 상태이다.

2.2 네트워크 통합 보안 구조

정보통신 기반이 개방형 네트워크로 진화됨에 따라 사이버테러에 대한 위험성이 증대되고 있다. 특히, 인터넷의 경우 사이버테러의 발생시각, 발원지, 침입자 추적 등이 어려운 형편이다. 이러한 상황에서 네트워크 차원의 정보보호 기반기술의 취약성은 더욱더 심각해지고 있어서, 기존의 컴포넌트 위주의 시스템 보안에서 대규모 네트워크에서 보안정책기반의 보안관리를 위한 새로운 패러다임이 절실히 요구된다. 네트워크 차원의 보안관리를 위해 IETF등 국제 표준화단체에서는 보안정책언어 및 정책배포기술에 대한 표준화 작업을 진행하고 있고 Cisco, Lucent등 대형 네트워크 장비업체에서도 정책기술을 적용한 프로토타입 장비를 개발하고 있는 실정이다.

정책 기반 보안 네트워크는 현재의 망을 구성하고 있는 보안 라우터, 게이트웨이 및 서버 시스템 같은 망 구성장치들의 PBNM(Policy-based Network Management) 형태로 사용자들에게 제공된다. IETF/DMTF 접근에서 정책은 DEN(Directory Enabled Network), WBEN(Web-based Enterprise Network), Policy Framework, Policy Architecture, COPS와 LDAP, HTTP 등 같은 구현 가능한 프로토콜, 그리고 CIM과 같은 정책표준 등으로 나뉘어서 생각할 수 있다.

이러한 네트워크 보안 기능을 설계/구현하고 인터넷 백본에 적용하기 위하여는 (그림 2)와 같은 구조로 모든 사용자들이 네트워크 백본과 접속하는 망의 액세스 포인트에서 해커의 침입을 탐지하고 이에 따른 경보의 전파 및 침입 유형에 따른 정책기반의 침입 방어 메커니즘을 시행하는 것이 용이할 것으로 생각된다.



(그림 2) 정책기반 보안네트워크 개념 구성도

네트워크 보안 관점의 침입 탐지는 망의 액세스 포인트에 위치한 보안 게이트웨이 시스템 내의 보안 망 관리 에이전트 기능을 수행하며, 침입 방어는 보안 게이트웨이 시

스템에 탑재된 정책 기반 침입 방어 메커니즘들에 의해 수행 가능하다.

보안 게이트웨이 시스템에서 수행하는 침입 방어 메커니즘들은 해킹 유형에 따라 다른 대응 방법들을 제공하며 이는 망의 보안 정책에 따라 제어된다. 따라서 보안 게이트웨이 시스템과 정책기반 망 관리 시스템간의 긴밀한 통신 수단이 필수적이며, 이는 보안성을 가지는 연결을 통하여 보안 정보들이 실시간으로 전달이 가능하도록 COPS와 SNMP 같은 정책전달 프로토콜이 제공된다.

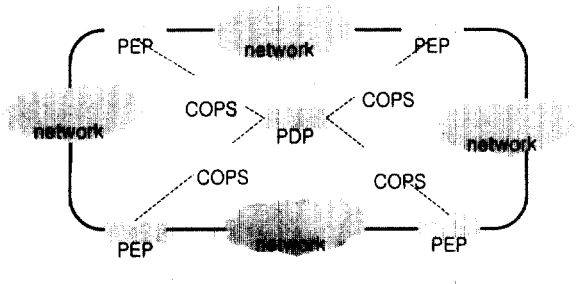
한편, 정책기반 망 관리 시스템은 보안 게이트웨이 시스템의 보안 망 관리 에이전트가 수집하여 정책전달 프로토콜을 이용한 전달한 정보를 기반으로 보안 정책을 결정하고, 보안 게이트웨이 시스템에서 해당 트래픽에 대한 대응 메커니즘을 선택 및 시행할 수 있는 정책 제어 정보를 전달한다. 이러한 메커니즘의 적용으로 보안정책을 제공할 영역의 경계가 정해지고, 호스트 기반 보안서버에서 해결할 수 없었던 네트워크 보안이 실시간으로 제공 가능하게 된다.

3. 정책기반 통합 보안관리 서버

3.1 정책전달 프로토콜

정책기반 관리는 네트워크 환경에서 동적으로 손쉽게 네트워크의 운영방침을 적용하여 효율적인 네트워크 운영에 그 목적이 있다. 이러한 정책기반 관리를 제공하기 위하여 정책전달을 위하여 기존의 망 관리 프로토콜인 SNMP와 실제 정책전달을 위하여 설계된 COPS를 고려한다.

COPS는 PDP와 PEP사이의 client/server model로request/response방식으로 동작하고, client /server간의 신뢰성을 위해TCP 연결을 이용한다. (그림 3)과 같은 개념 구성으로 인터넷 백본 망에 적용 가능하며, <표 1>과 같은 10개의 메시지로 구성되어 있다.

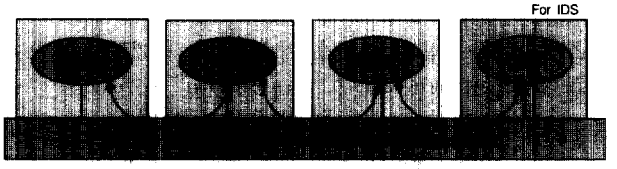


(그림 3) COPS 적용 망 구성의 예제

COPS는 자체 수정 없이 다양한 클라이언트 세부정보 지원할 수 있는 확장성을 지니고 있어 COPS-PR, COPS-MPLS, COPS-RSVP, COPS-TE 및 COPS-IDS로 (그림 4)처럼 정의하여 사용 가능하다. PDP와 PEP사이의 보안과 인증을 위해 IPSEC/HMAC-MD5를 이용하기도 한다. 한편, 클라이언트와 서버간 Request/Decision state를 공유하기도 하고, 서버 구성정보를 클라이언트에게 push/disposal이 가능하다[4, 5].

<표 1> COPS 메시지

OP코드	메 시 지	From	To	OP코드	메 시 지	From	To
1	Request	PEP	PDP	6	Client-Open	PEP	PDP
2	Decision	PDP	PEP	7	Client-Accept	PDP	PEP
3	Report State	PEP	PDP	8	Client-Close	Both	Both
4	Delete Request state	PEP	PDP	9	Keep-Alive	PEP	PDP
5	Syn state Request	PDP	PEP	10	Syn Complete	PEP	PDP

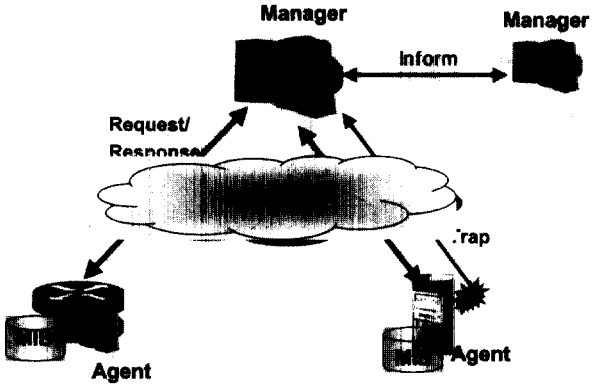


(그림 4) COPS확장 개념구조

정책전달을 위한 프로토콜로 COPS외에 SNMP도 고려되고 있다. SNMP는 본래 망 구성장치 관리로 많이 사용되는 프로토콜로써 가장 일반적인 네트워크 관리 툴로 알려져 있다. 현재 이를 수용하거나 확장하여 침입 탐지 시스템의 관리나 보안 시스템들의 통합에 사용하려는 연구가 많이 진행되고 있다. 분산 배치된 네트워크 자원을 집중관리 할 뿐 아니라 간단한 구조만으로도 이기종 간의 상호 접속성을 제공하여 최소한의 자원으로 동작할 수 있다. SNMP는 3가지 버전이 개발되어 사용되고 있으며 V1의 경우 manager to manager는 지원하지 않는 기능상의 결함과 보안상의 결함을 가지고 있다. 이를 보완하여 V2에서는 기능을 향상하여 지원하도록 하였으나 보안 기능은 삭제되었으며, 메시지 자체가 신뢰성이 없는 UDP로 동작되므로 TRAP 메시지의 전달을 확신할 수는 없다. 이러한 보안기능을 강화해서 SNMPv3는 네트워크보안 뿐 아니라 Access Control이 가능하며 SNMPv1과 SNMPv2의 기능을 통합하여 제공한다.

SNMP는 (그림 5)와 같이 Manager와 Agent사이에 Request/Response/Trap 메시지로 송수신한다. SNMP Agent의 경우 자신의 local환경에 대한 정보를 수집/유지하고, 관리국으로부터의 request에 대하여 응답하고, trap으로 통보하며 MIB를 유지한다. Manager의 경우, UI를 제공하고 성능감시, 구성제어, 계정관리, 장애 격리, 수정기능에 정책관리 기능까지 제공한다[3].

특히, SNMP는 전달 메시지의 크기가 1,500byte로 제한되어 있어 큰 메시지의 전달 시 패킷 들을 작게 나누어 대량으로 전달하게 되어 대역폭을 많이 낭비할 뿐 아니라, 폴링 수 또한 제한되어 있기 때문에 많은 수의 시스템을 관리해야 되는 대규모 망에서는 적용이 어렵다. 정책기반의네트워크에서는SNMP와 달리 TCP기반으로 상위레벨의 정



(그림 5) SNMP 프로토콜 기본 동작

책제공 및 통제 목적을 갖는 COPS가 오히려 정책을 전달하기 위하여 일반적인 망관리 프로토콜인 SNMP보다는 통합 보안관리의 정책전달에 적합한 프로토콜이라고 할 수 있다. 본 논문에서는 보안제어서버와 보안게이트웨이의 정책 전달 프로토콜로 메시지 크기가 64,000byte인 COPS를 채택한다.

지금까지 실시간 인터넷 보안 서비스 제공을 위하여 정책기반 보안 서버 및 게이트웨이 시스템으로 이루어진 통합 관리구조를 고려하였고, 이러한 보안 정책이 COPS정책 전달 프로토콜을 통하여 전달되도록 설계한다. 제공된 COPS는 Lulea에서 기본적으로 제공하는 COPS Basic 기능에 G-IDS (Global IDS)를 위해여 필요한 메시지 및 정책, 기능을 확장한 COPS-GIDS 를 고려한다.

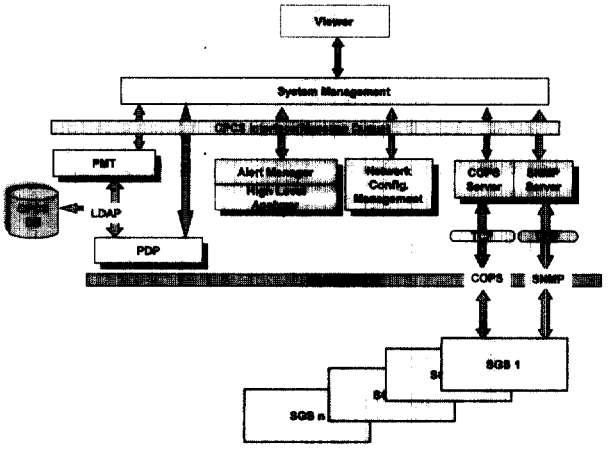
3.2 보안 서버 구성 기능 및 환경

네트워크 보안제어 시스템은 계층적인 구성을 가지며 적어도 2개의 계층으로 구성이 된다. 하나는 관리계층에 해당하는 리눅스 기반의 보안제어 관리서버(CPCS)와 다른 하나는 실행계층에 해당하는 접속 점에서의 해킹 트래픽 감지 및 대응을 위한 IDS기반의 보안 게이트웨이 시스템(SGS) 이다. 여기에서 보안제어 관리서버와 보안 게이트웨이 시스템은 (그림 6)에서와 같은 구성으로 이루어져 있다.

여기에서 보안제어 서버와 보안 게이트웨이 시스템간의 정책전달 COPS를 이용하여, 정책저장소와 정책관리 툴과의 정보전달은 LDAP을, 보안 게이트웨이 시스템 들간의 구성관리는 SNMP를 이용하여 구성한다.

보안제어 서버의 기능은 크게 보안 프로토콜 정합 기능, 정책 결정 기능, 사이버순찰 서버 기능, 정책 관리 기능, 정책 데이터베이스 기능 등으로 세분화 할 수 있으며, 이를 통합하여 관리하기 위하여 시스템의 운용 상태를 네트워크 차원에서 모니터링할 수 있는 통합GUI 즉, 관제기능이 있다. 각 기능 블록에서 제공해야 할 기능을 요약하면 <표 2>와 같다.

즉, 정책기반 정보보호 네트워크 통합관리는 Policy Management Application Layer, Policy Decision Layer, Device Adaptation Layer, Policy Target Layer로 구분되어



(그림 6) 보안 제어 서버와 게이트웨이 기능구성

〈표 2〉 보안제어 서버 시스템 제공기능

기 능 구 분	세 부 기 능
관제 기능 (Viewer)	⇨관리자 보안 등급별 접근 제어 가능 ⇨시스템 상태 및 실시간 경보 정보 제공 ⇨PMT와 GUI혹은 CLI로 인터페이스 제공
시스템 관리 기능 (System Management)	⇨정책서버 기능 블록간의 메시지 분배 및 자원 할당
서버 메시지 큐 관리 기능(Message Queue)	⇨서버의 각 블록간 통신시 메시지 큐 제공
보안 정책 관리 기능 (PMT)	⇨보안 정책의 신규 생성, 수정, 삭제 기능 제공 ⇨사용자로 입력된 정책을 LDAP 형태로 변환 ⇨정책 저장소(CPCS DB)와의 무결성 및 일관성 제공
보안 정책 결정 기능 (PDP)	⇨PMT로부터의 정책을 각 보안 구성장치들에게 분배 ⇨각 보안 구성장치로부터 요구사항/정책적용 문제점등을 수렴하여 정책정보에 반영
경보 관리 기능(AM)	⇨보안 게이트웨이로부터 경보 처리 기능 ⇨처리된 경보 DB에 저장 및 관제기능에 보고 기능 ⇨경보 DB의 통계처리 및 High-level 분석 기능에 제공
정책 저장소 기능(PR)	⇨네트워크보안 서버내의 보안 정책 데이터를 일괄적으로 관리하는 기능
High-level 분석기능	⇨기존의 경보관리에서 제공할 수 없는 고수준의 경보분석기능 ⇨active response 기능 제공
네트워크 구성정보 관리기능(Network Configuration Management)	⇨정책기반 보안 서버에서 현재 네트워크 상태를 감지하여 정책 적용 시스템을 관리하는 기능
COPS Server/SNMP Server 기능	⇨정책기반 보안 제어관리를 위하여 접속된 보안 게이트웨이 시스템들과의 정책정보 및 구성관리 정보 제공을 위하여 COPS와 SNMP 프로토콜을 제공

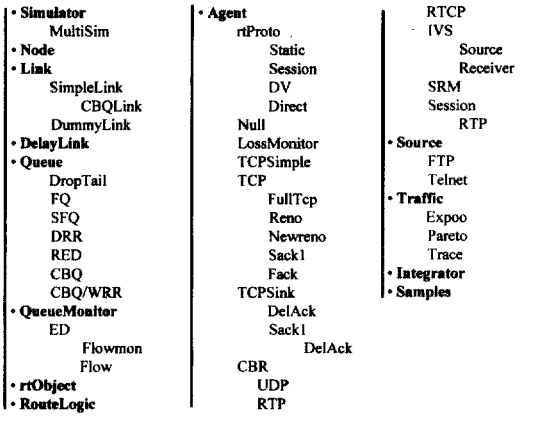
운영하도록 각각의 도메인을 구성하고, 여러 도메인간의 통신은 일단 Policy Decision Layer에서 Server-to-Server Protocol을 이용하여 가능하도록 구성한다. 정책 관리 응용 시스템과 정책서버 간의 정보보호는 IPsec VPN 혹은 IPsec을 적용하도록 하며, 이때 정책서버의 보안과 성능도 고려한다. 보

안 게이트웨이 서버는 서버에서 직접 제어 가능하도록 하고 도메인이 다른 경우, 서버-서버 인터페이스 프로토콜 같은 서버간 별도의 프로토콜을 제공하도록 한다. 그리고, 정보보호의 대항에 따라 End-to-End, Link-to-Link, Node 및 호스트 등의 차별화에 따른 대상 서비스의 범위 또한 결정한다.

4. 정책 기반 보안 시뮬레이션

본 보안관리제어 서버를 수십, 수백개의 노드로 구성된 코아 망에서 실험하는 것은 거의 불가능하다고 생각된다. 즉, 코아 망에서 IDS 시스템의 기술/성능 분석을 위한 네트워크 보안 시뮬레이션의 필요성이 시급하다.

여기에서 사용되는 네트워크 시뮬레이터는 UC Berkeley에서 제공되는 VINT 프로젝트의 결과이며, event scheduler와 IP기반 네트워크 컴포넌트들로 구성되어 있고 C++과 OTcl로 프로그램 할 수 있다[13, 14]. 다음 (그림 7)은 NS에서의 객체들에 대한 계층구조를 나타내고 있다.

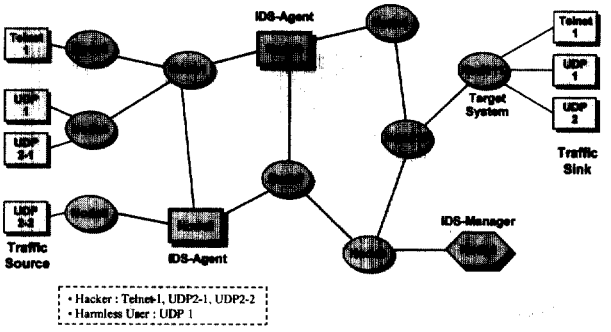


(그림 7) 객체들에 대한 계층구조

본 시뮬레이션에서는 통합 보안서버를 코아망에서 동작하는IDS Manager로 보안 게이트웨이 시스템을 edge망에서 주로 동작하는IDS Agent로 제공하며, 결과는 NAM(Network Animator)로 그래픽하게 제공한다[15]. 코아 망에서의 IDS 시스템은 현재 분산 Dos공격 탐지 및 침입 대응이 edge 망에서의 IDS 시스템으로는 어렵기 때문에 제안된 것으로 Anomaly Detection같은 새로운 침입탐지기술, Edge 망에서의 IDS 시스템에 비해 다양한 침입대응기술, 정책에 의한 각 Edge 망의 IDS들간의 실시간 차별성이 가능하도록 설계한다.

정책전달을 위한 프로토콜로 SNMP와 COPS 둘 다 가능하지만 일단 COPS만 고려한다. (그림 8)은 지금까지 기술한 네트워크 보안 시뮬레이션을 위한 실험환경을 보여주고 있다.

네트워크 노드는 11개를 고려하였으며, 각 노드는 COPS 프로토콜로 접속되어있다. 각 보안 게이트웨이 즉, IDS-Agent에서 패킷을 분석한 다음 Anomaly packet detection이 발생되면 통합 보안서버 IDS-Manager(node 9로 가정)



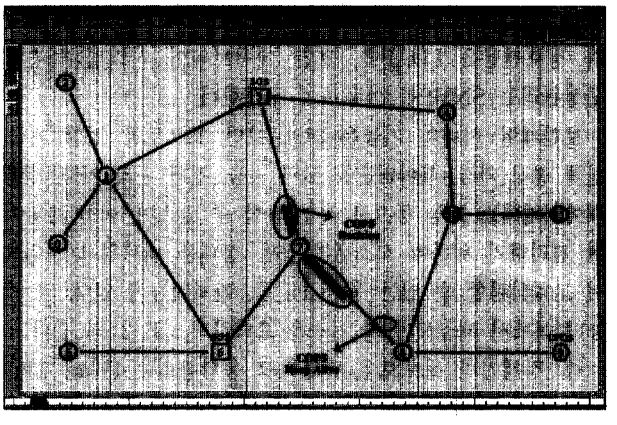
(그림 8) 네트워크 보안 시뮬레이션 실험환경

로 정책결정 요구 메시지를 보낸다. IDS-Manager는 요구 메시지 정보를 통합 분석한 다음 IDS-Agent(node3, node6으로 가정)로 정책 결정 메시지를 전달한다.

본 시뮬레이션에서는 트래픽 소스를 Telnet-1, UDP2-1, UDP2-2, UDP1 이라고 가정하고 목표시스템을 node11로 가정하며, 유해 트래픽의 정의나 유행은 초기화 값으로 설정한다. 여기에서 유해 트래픽은 사용자들이 hacking ID를 명세함으로 정의되도록 한다. 유해 트래픽의 경우 additive type으로 처음 접속한 이후에 받은 패킷의 양이 threshold를 넘으로 침입으로 간주한다든지 scalar type으로 일정 시간동안 받은 패킷 양이 threshold를 넘으면 침입으로 정의한다. 이러한 유형을 파악한 다음 실제 정상적인 패킷인지 유해한 패킷인지의 판단을 위하여 기준한time-interval이나 threshold 값에 의하여 판단하도록 한다. 즉, 연속된 telnet에 대하여도 이상 트래픽으로 감지하여 서버에게 통보하도록 가정한다.

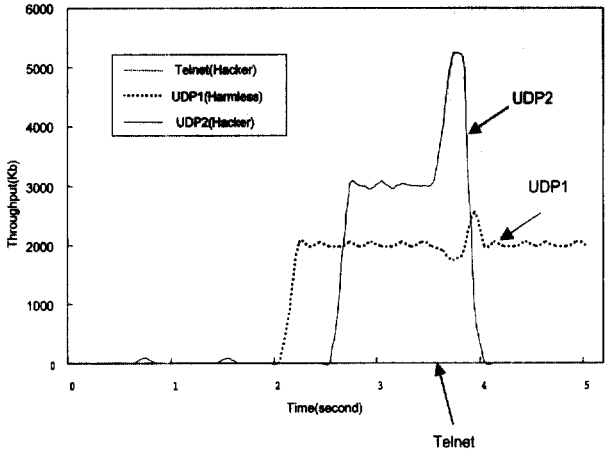
(그림 9)는 이러한 시나리오를 제공하기 위한 COPS 프로토콜을 통한 정책 분배과정을 나타내고, (그림 10)은 이러한 정책전달 프로토콜을 통한 정책 전달 후 IDS-Manager로부터 전달된 정책이 IDS-Agent로 전달된 유해 트래픽이 탐지되고, blocking된 결과를 나타낸다.

다음 (그림 11)에서는 지금까지 기술한 IDS-Manager와 Agent사이의 정책전달 및 정책전달 후 유해 트래픽 감지, 판정, 대응에 대한 각 트래픽 별 throughput 시뮬레이션 결과이다.



(그림 9) COPS 프로토콜을 통한 정책 분배과정

(그림 10) 유해트래픽 차단결과



(그림 11) 각 트래픽 별 throughput 시험결과

(그림 11)에서 알 수 있듯이, IDS-Manager로부터 정책이 전달되고 IDS-Agent에서 유해한 트래픽이라고 판정되면, 그 다음부터 해당 트래픽은 목표 시스템으로 전달되지 않고 blocking되고 있음을 알 수 있다. 본 시뮬레이션 결과를 통하여 제안된 정책기반 네트워크 보안 기능들이 실제 목표 망의 구성장치에 탑재되어 운영될 때, 목표 망이 인터넷 백본 이라면, 인터넷 보안 네트워크 서비스 제공은 보안관리제어 서버를 통하여 제공 가능하게 될 것이다.

5. 결 론

지금까지 현재 제공되고 있는 인터넷의 보안제어에 대하여 통합보안관리 측면에서 살펴보았다. 현 인터넷의 문제점으로는 적용 네트워크 장비들의 보안취약성 및 보안구조 부재로 인하여 인터넷 보안서비스 제공이 실시간으로 이루어지지 않는다는 것이다.

본 논문에서는 이러한 문제점 해결을 위하여 실시간 인터넷 서비스 제공을 위한 정책기반 보안제어 서버 클라이언트 구조 및 기능, 보안제어 시스템의 설계에 대하여 IETF 표준화 중심의 정책전달 프로토콜 중심으로 살펴보았다. 그리고 이러한 기능을 바탕으로 실제 인터넷 백본 망에서 실현 가능한 보안 서비스를 정책 기반 시나리오를 작성한 다음 네트워크 시뮬레이션을 통하여 검토해 보았다. 제안한 정책기반 통합 보안제어 구조는 현재 인터넷에서 제공하기 어려운 네트워크 차원의 실시간 인터넷 보안 서비스를 능동적으로 제공하도록 한다. 즉, 보안 호스트 및 특정 보안 장비에 대한 수동적이고 소극적인 정보보호 정책이 아닌 전체 네트워크의 차원의 통합보안관리가 능동적으로 이루어진다고 할 수 있다.

추후 이러한 정책기반 보안제어 연구개발 내용들을 IETF 같은 세계적인 표준화 기구에서 인터넷 보안 관련 회의에 기고하도록 하며, 주요 요소기술에 대한 개발동향 파악 및 표준화 작업에 적극 반영 하도록 하여 국제 호환성을 추구하여야 할 것이다. 또한 이러한 기능들을 개선 및 확장하여 정책기반 보안제어 목표 제품들의 보안 관리기능에 탑재한 후, 실제 인터넷 백본 망에서 안전한 실시간 인터넷 보안 네트워킹 서비스 제공을 위하여 제공 가능하리라고 생각한다.

참 고 문 헌

[1] 서동일, 김기영, 이상호, 온/오프라인 기술 통합을 활용한 PC 기반의 침입탐지 시스템 설계, JCCI 2001, 2001.

[2] 김기영, 서동일, 이상호, 정책기반의 차세대 인터넷 보안 서비스 제공방안 NCS 2000, 2000.

[3] IETF, RFC 1157, A Simple Network Management Protocol (SNMP), 1990.

[4] IETF, RFC 2748, The COPS (Common Open Policy Service) Protocol, 2000.

[5] IETF, RFC 3084, COPS Usage for Policy Provisioning (COPS-PR), 2001.

[6] IETF, RFC 3060, Policy Core Information Model-Version 1 Specification, 2001.

[7] IETF, RFC 2251, Lightweight Directory Access Protocol (v3), 1997.

[8] 포항공대 유닉스 보안연구회, Security PLUS for UNIX, Youngjin.com, 2000.

[9] 한국정보통신진흥원, http : //www.certcc.or.kr.

[10] CISCO Systems, Benefits and Limitations of Context-Based Access Control(Using Cisco Secure Integrated Software), 2001.

[11] CISCO Systems, Security Technical Tips : Internetworking, 2001.

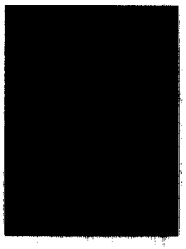
[12] CISCO Systems, white paper Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks, 2000.

[13] "ns Notes and Documentation," URL : http : //www-mash.cs.berkeley.edu/ns, 2001.

[14] "ns manual," URL : http : //www-mash.cs.berkeley.edu/ns/ns-man.html., 2001.

[15] "nam manual," URL : http : //www.isi.edu/nsnam/nam/, 2001.

[16] DMTF Specification, white paper CIM Core Policy Model for CIM schema release 2.4, 2000. http : //www.dmtf.org.



김 기 영

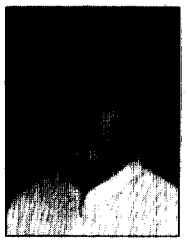
e-mail : kykim@etri.re.kr

1988년 전남대학교 전산통계학과 (이학사)

1993년 전남대학교 전산통계학과 석사 (이학석사)

1988년~현재 한국전자통신연구원 선임연구원

관심분야 : QoS-based and Policy-based Routing, Internetworking and Integrated Naming Service, Network Security



안 개 일

e-mail : fogone@etri.re.kr

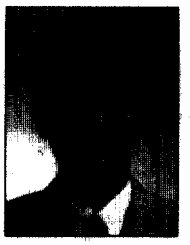
1993년 충남대학교 공과대학 컴퓨터공학과 (공학사)

1995년 충남대학교 공과대학 컴퓨터공학과 (공학석사)

2001년 충남대학교 공과대학 컴퓨터공학과 (공학박사)

2001년~현재 한국전자통신연구원 선임연구원

관심분야 : Traffic Engineering, MPLS(Multi-Protocol Label Switching), Network Security



장 종 수

e-mail : jsjang@winky.etri.re.kr

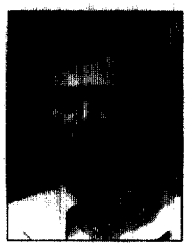
1984년 경북대학교 전자공학과(공학사)

1986년 경북대학교 전자공학과(공학석사)

2000년 충북대학교 공과대학 컴퓨터공학과 (공학박사)

1989년~현재 네트워크 보안 연구팀 팀장

관심분야 : Traffic Management & Control, IP-ATM Service-level Interworking, Inter-/Intra-domain Resource Management & Control, Network Security



이 상 호

e-mail : shlee@cbucc.chungbuk.ac.kr

1976년 숭실대학교 전자계산학과(공학사)

1971년 숭실대학교 전자계산학과(공학석사)

1989년 숭실대학교 전자계산학과(공학박사)

1979년~1979년 한국전력전자계산소

1981년~현재 충북대학교 컴퓨터과학과, 교수

관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture