韓國 OA學會 論文誌
第7卷 第3號, 2002. 9.

2002-7-3-3-1

안전한 인터넷을 위한 보안관리 시스템 설계

정 연 서* 박 배 욱** 손 승 원* 오 창 석***

The Design of the Security Management System for Secure Internet

Youn-seo Jeong* Bae-wook Park** Sung-won Sohn* Chang-suk Oh***

요 약

본 논문에서는 인터넷의 네트워크 보안을 관리하기 위한 정책기반의 통합보안관리 시스템을 설계하였다. 기존의 망 관리와 현재 진행되고 있는 통합보안관리 시스템의 개발 동향을 살펴보고, 기존의 시스템들을 분석하여 시스템 설계시의 고려사항들을 도출하였다. 제안된 시스템은 효과적인 네트워크의 보안관리를 위해서 IETF의 정책기반의 망관리(Policy Based Network Management:PBNM) 기술을 적용하여 설계하였다.

Abstract

In this paper, we designed the Policy-based ESM(Enterprise Security Management) for network security in Internet. First, we consider the existed network management and present ESM. And then analyze existent systems and drew consideration items at system design. This paper applied to PBNM technology in order to improve security network management.

* 한국전자통신연구원
** 충북대학교 컴퓨터공학과 박사과정
*** 충북대학교 전기전자컴퓨터공학부

논문접수 : 2002. 6. 7
심사완료 : 2002. 9. 10

Ⅰ. 서론

인터넷의 발전과 네트워킹 문화의 확산으로 다양한 분야에서 인터넷을 업무에 접목시켜 생산성을 증대시키고 있다. 그러나, 개방을 근간으로 출발한 인터넷은 그 기반 구조의 취약으로 인하여 외부로의 공격에 많은 취약점을 드러내고 있다. 네트워크를 통한 외부의 불법적인 공격과 침입에 대응하고자 다양한 방안들이 연구되고 있다.

허나, 이러한 노력에도 불구하고 갈수록 지능화 되는 침입수법들과 새롭게 발견되는 시스템들의 버그로 인한 보안체계의 헛점들은 보안 관리를 어렵게 하고 있다. 이를 해결하기 위해서는 적절한 보안정책에 따른 상시적인 관심과 유지 관리가 필요하다.

보안분야에서는 인터넷의 전체적인 보호를 위해 보안정책(security policy)에 관한 연구가 진행되고 있다[1-2]. 이에 발맞추어 보안정책을 일관성 있게 유지 관리하고, 개별적인 보안제품들을 유기적으로 관리하기 위한 통합보안관리에 대한 관련 연구가 진행중이다.

본 논문에서는 IETF(Internet Engineering Task Force)에서 진행되고 있는 정책기반의 네트워크 관리 기술을 도입한 통합보안관리 시스템을 설계하고자한다. 2장에서는 정책기반의 네트워크 관리 기술과 통합보안관리 연구 동향에 대해서 살펴보고, 3장에서는 제안된 정책기반의 통합보안관리 시스템과 관리 모델에 대해서 기술한다. 끝으로 4장에서 결론을 맺는다.

Ⅱ. 관련 연구동향

1. 통합 관리

다수의 이기종 시스템들과 다양한 프로토콜로 구성된 복잡한 인터넷 환경하에서 수동적인 관리 체계로는 효율적으로 관리하기가 어렵다. 이의 해결을 위해 시스템 관리(System Management System:SMS)와 네트워크 관리(Network Management System:NMS) 등의 다양한 통합관리 솔루션들이 개발되었으며, 이를 위한 제반 연구로 망 관리 표준을 위한 SMI(Structure of Management Information), MIB (Management Information Base), SNMP(Simple Network Management Protocol)로 구성되는 망 관리 표준들이 제정되었다[3].

2. 정책기반 망 관리

사용자의 다양한 서비스 요구와 인터넷의 급속한 확산에 따라 데이터 네트워크가 급속도로 확대되고 네트워크 구성이 복잡해짐에 따라 정책 기반의 네트워크 관리(Policy-based Network Management: PBNM) 기술에 대한 관심이 고조되고 있다. IETF에서는 정책기반 관련 시스템 기능 정립 및 프로토콜에 대한 표준화를 위한 작업그룹을 구성하여 정책기반(Policy-based)의 프레임워크(Framework)를 근간으로 접속 프로토콜, 정책 정보모델(Common Information Model), 서비스 품질(Quality of Service) 제어를 위한 방식으로 구분하여 연구하고 있다[4,5]. 네트워크의 운용과 유지보수에 막대한 비용을 지불하고 있는 기간통신사업자 및 ISP (Internet Service Provider) 들은 보다 효율적인 네트워크 운용이 가능한 PBNM 도입의 필요성을 강하게 인식하고 있으며, 향후의 네트워크 진화에 따른 운용 환경에 대한 연구도 활발히 진행되고 있다.

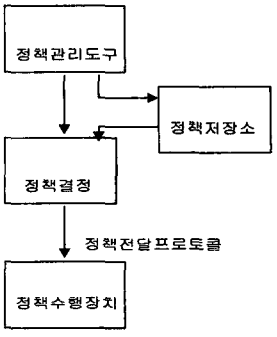

그림 1. IETF 정책기반 관리 구조
Fig 1. IETF Architecture of Policy-based Management

IETF에서는 정책기반의 인터넷 망 관리와 관련된 표준화 작업을 지속적으로 진행하고 있으며, 기존의 네트워크 관리 기술과의 접목도 본격적으로 추진되고 있다.

네트워크 차원의 보안정책을 수립하고 관리하기 위해서는 정책기반의 기술이 필요하며, IETF에서는 정책기반의 네트워크 관리 구조를 그림 1과 같이 제시하고 있다.

정책 기반의 네트워크 관리(PBNM : Policy-Based Network Management)기술은 기본적으로 자신의 네트워크에 있는 특정 트래픽에 영향을 미치도록 필요한 구성상의 변경을 이해 및 이행, 그리고 추적이 가능하여 네트워크의 QoS 및 보안 관리를 가능하게 하고 능동적 네트워크 모니터링, 네트워크 서비스 수준 협정 관리, 사용자 기반 정책들을 위한 다중 네트워크 운영시스템 통합 기능 등을 제공하고 있고, 하드웨어 액세스 및 제어, 사용자와 자원 및 정책에 대한 정보를 수집하게 된다.

3. 통합보안관리 시스템

통합보안관리는 방화벽, VPN, 바이러스 검사, 컨텐츠 필터링, URL 모니터링/필터링, 침입탐지 등의 많은 보안 제품들, 즉 별개의 보안 구성 요소를 일관적인 전체로 결합하여, 인증과 감시, 허가에서 네트워크 관리에 이르기까지 모든 것들을 망라하는 통합관리로 연구되고 있다[6].

3.1 통합보안관리 연구 동향

국내의 ESM에 관한 시장 형성과 연구개발은 2002년에 들어서서 본격적으로 활발하게 이루어지고 있으며, 개발의 기본 초기 모델에 따라 아래와 같이 분류해 볼 수 있다.

- 프레임워크 기반의 솔루션 개발
- 서비스 기반의 순수 ESM 개발
- 개별 솔루션 개발
- 콘소시움 구성 산업체 표준 제정

가장 먼저 연구 시작된 프레임워크 기반의 솔루션을 개발하고 있는 업체는 IBM, HP, CA(Computer Associate)등이 있다. 보안측면 보다는 시스템 관리 측면에 초점을 맞춘 제품들이다. 이에 반해 다양한 이기종의 보안 솔루션의 통합로그 관리에서 시작된 서비스 기반의 솔루션과 자사의 제품 통합관리를 위해 시작된 개별 솔루션 개발은 순수하게 보안솔루션을 위해 시작되었다. 최근 인터넷 시큐리티 시스템즈(ISS)·시만텍·e-시큐리티 등이 개발한 ESM 제품들은 네트워크 및 시스템의 취약점·위험요소를 분석하고 이에 대한 모니터링 정보들을 통합하는 기능들을 갖추고 있다. 이글루시큐리티·인젠·어울림정보기술 등 국내 업체들이 최근 발표한 제품들도 여기에 해당된다. 미국의 OPSEC이나 국내 어울림정보기술은 보안 제품들간의 프레임워크 제공을 위해서 API를 개발하여 배포하고 있으며, 마크로테크놀러지의 경우는 산업체 표준안 제정을 통한 통합화를 꾀하고 있다. 허나 대부분의 제품이 아직까지는 중앙관리모듈만을 제공하거나 자사 제품간의 통합 수준에 머물고 있다[7].

3.2 설계시 고려사항

본 절에서는 기존의 통합보안관리시스템을 비교 분석하여 설계시 고려사항들에 관하여 분석한다.

현재 대부분의 통합보안관리 관련 제품들은 앞에서도 언급했듯이 로그 통합 수준이다. 실제적인 통합보안관리가 이루어지려면 전체 관리 대상 네트워크의 다수의 보안장비들의 보안정책을 일관되게 관리할 수 있어야 하고, 수립된 정책의 배포, 집행, 관리 등을 처리할 수 있어야 한다. 타 관리 망과의 수평적 정보 전달도 필요하며, 이를 위한 표준화된 프로토콜의 제정이 필요하며, 관리 망들 전체가 연계되어 크게는 국가적, 전세계적으로 관리할 수 있는 광역차원의 대규모 관리를 고려하게 되면 계층적 관리 구조가 적합할 것으로 보인다. 그리고, 기존의 시스템 관리와 망 관리 기능들과 결합이 되어야 하는데, 통합보안관리 시스템이 이를 정보들을 수집하는 기능을 모두 포함하는 방안과 필요정보들을 기존의 관리 시스템들로부터 가져다가 사용할 수 있는 연계된 통합방안도 고려되어야 한다.

표 1. 설계시 고려사항
Table 1. Considerations in Design

	현재상태	설계시 고려사항
관리대상	· 자사제품 위주 · 연동되는 타사제품	· 표준화된 프로토콜과 API 설계 적용 · 이기종 다수 제품간적용 설계
보안기능	· 로그 통합 수준 · 제한적 세션 차단 기능	· 차단, 탐지, 바이러스, VPN 등의 연계된 종합보안 관리 · 연계된 차단, 추적 기능
적용범위	· 사설망 위주	· 광역망 적용
프로토콜	· 개발사 선택에 따른 다양한 프로토콜 적용	· 표준화된 프로토콜 (COPS, SNMP 등)
관리형태	· 클라이언트-서버	· 계층적 관리

Ⅲ. 정책기반 통합보안관리 시스템

1. 시스템 구성

제안된 정책기반의 통합보안관리 시스템은 그림 2와 같이 구성된다.

크게 기능으로 분류해 보게 되면 정책관리(policy management), 정책저장(policy repository), 정책결정(policy decision), 정책집행(policy enforcement)으로 나누어 볼 수 있다. 구성요소는 정책을 수집하여 분석하고 수립하게 되는 정책결정부(Policy Decision Point:PDP), 생성된 정책을 편집하고 배포, 일관성 유지를 위한 관리 등을 담당하는 정책관리부(Policy Management Tool:PMT), 정책을 보안 시스템들 즉, PEP로 정확하게 전달하고 보고되는 정보를 전달할 정책 전달 프로토콜이 필요하다.

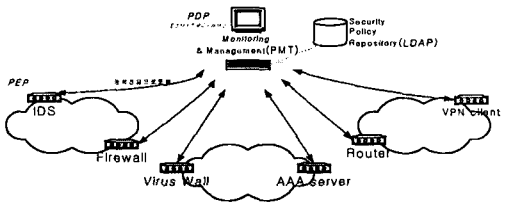

그림 2. 정책 기반 통합보안관리 시스템 구성도
Fig 2. System Configuration of Policy-based ESM

2. 구성 요소별 기능

본 절에서는 각 요소들에 대하여 상세하게 기술한다.

■ 정책 관리부 (Policy Management Tool)

정책관리부는 관리자가 관리 범주 내에 있는 장비들에게 배포할 정책을 작성하고 각 장비들의 설정 상태를 상시 확인할 수 있는 관리 기능을 제공하게 된다. 다양한 서비스 요구사항에 대한 복잡한 보안 정책을 망 내의 모든 네트워크/보안 장비들이 이해할 수 있는 일관성 있는 정책 데이터로 변환하기 위해서 PFDL(Policy Framework Definition Language)이 이용된다.

■ 정책 저장소 (Policy Repository)

정책관리부에서 신규 생성된 관리 정책은 중앙의 정책 저장소 (Policy repository)와 경우에 따라서는 장비들에 의해 로컬 영역에 저장되며 일관된 자료 검색, 갱신, 수정을 제공하여야 하며 대규모 정책에 따른 실시간에 근접한 성능을 제공하여야 한다. 저장된 정책을 조회하거나 신규 생성된 정책을 저장하기 위한 프로토콜로는 디렉토리 서비스에 널리 이용되고 있는 LDAP[8] 프로토콜이 많이 적용되고 있다.

■ 정책결정부 (Policy Decision Point; PDP)

침입이나 분산공격에 의한 트래픽 폭주 등 네트워크 환경에 변화가 발생하거나 장애와 같은 특정 이벤트가 감지되면 해당 네트워크 기기는 즉각적으로 해당 정책 결정부 (Policy Decision Point)에게 정책 결정을 요구한다. 정책 결정 요구를 수신한 정책 결정부는 정책 결정 조건과 정책 동작을 검색하여 정책 결정을 수행하고 정책 동작을 시행해야 하는 모든 정책집행부에 해당 정책을 보낸다.

■ 정책집행부 (Policy Enforcement Point; PEP)

정책결정부로부터 수신된 정책을 실제로 적용할 수 있도록 변환하여 보안정책에 따라 사용자의 접속이나 패킷을 제어하는 기능을 수행하며 주로 장비에 독립적으로 존재한다.

■ 정책전달 프로토콜 (Policy Transfer Protocol)

정책결정부와 정책적용부 간의 정책 전달을 위해 COPS (Common Open Policy Service) [9] 프로토콜이나 SNMP(Simple Network Management Protocol) 프로토콜이 이용된다. 통합보안관리를 위해서는 네트워크에 설치되어 있는 서버들의 시스템 상태정보와 망의 정보가 필수적이므로 두 프로토콜을 연계할 수 있는 방안도 수립이 되어야 한다.

현재의 인터넷 망 구성 장치에는 정책 적용 기능이 구현되어 있지 않으며, 제품에 따라 그 특성이 매우 상이하기 때문에 모든 망 구성장치가 상위의 정책 적용부에 직접적으로 의존하여 동작하는 이상적인 정책 적용 기능은 구현하기가 불가능하다. 정책적용 대행서버를 놓고 이를 대신할 수 도 있다.

3. 보안관리 구조

그림 3은 본 논문에서 제시하는 정책기반 통합보안관리를 위한 계층적 관리 모델을 보여준다. 그림에서 알수 있듯이 각 로컬의 ESM은 각각 할당된 보안영역을 담당하게 되며, 해당 영역의 정책 관리 및 판제, 감시 센터의 역할을 수행한다. 정책은 로컬에서 작성하게 되는 로컬 정책과 전체적으로 적용되는 글로벌 정책 두 가지가 있다. 로컬 영역의 경우 관리자에 의해서 수립된 로컬 보안 정책에 의해서 일관되게 관리되며 각 로컬 영역들은 다시 상위에 이들을 관리하는 매니저 ESM을 두고 상위에서 관리하게 된다. 이곳에서는 새로 발견된 바이러스나 해킹 기법, 취약점들에 대한 정보나 패치, 대응 등에 대한 정책 정보를 로컬영역에 실시간으로 전달하게 된다.

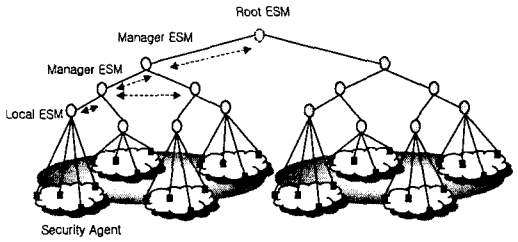

그림 4. 보안 관리 모델
Fig 3. Model for Security Management

매니저 ESM은 정책을 수립, 저장, 전달하는 Policy Server의 기능을 수행하게 된다. 매니저 ESM은 규모에 따라서 다단계로 존재할 수 있으며, 로컬에서 수집된 정보들을 분석하여 침입에 대한 추적이나 분산 공격 대응 등에 대한 광역 범주의 대응 방안을 수립하는 기능도 담당하게 된다. 가장 하단의 Security Agent는 실제 망에 설치되어 있는 보안장비들로 구성되며 정책 집행을 담당하게 된다. Agent는 자신이 관할하는 로컬 네트워크로의 침입 시도를 판별하여 이를 Manager에게 보고하는 기능을 수행한다.

계층적 관리 모델을 적용하여 광역범주의 보안네트워크가 구성되었을 경우 각 로컬 ESM간 정보전달을 통해 침입에 대한 경로 추적과 위치를 파악할 수 있다.

4. 프로토타입 구현

현재 정책기반 보안관리를 위한 프로토타입을 구현하고 있다. 이기종 다수의 보안 에이전트(security agent) 기능을 위하여 리눅스 시스템에 C언어와 MySQL을 사용하여 침입탐지 모듈을 구현하여 설치하였으며, 보안정책 관리(PMT)를 위해 자바로 관리 콘솔을 작성하고, 보안 정책 자료의 저장과 검색에 오라클과 LDAP을 사용하여 기능 설계를 하고 있다. 그리고, 정책전달을 위한 프로토콜로는 COPS(Common Open Policy Service)를 이용하도록 설계하고 있다.

Ⅳ. 결론

앞에서 살펴본 바와 같이 복잡해지는 네트워크의 관리와 성능 향상을 위해서 기존의 단순 모니터링에서 실시간으로 망의 상태 정보를 모니터링하고 동적으로 장비들을 제어하여 효과적인 운용을 하려는 형태로 바뀌어 가고 있다. 보안의 특성상 망의 보안을 위해서는 더더욱 이러한 기술들이 적용되어야 할 것으로 보이며, 많은 종류의 보안 시스템들을 통합 관리하기 위한 통합보안관리 제품들이 연구 개발되고 있다. 최근에는 이기종 보안솔루션 통합은 물론 시스템자원관리(SMS), 네트워크자원관리(NMS)기능까지 추가하는 형태로 발전되어 가고 있다.

본 논문에서는 이들을 효과적으로 관리하기 위한 관리 프레임워크로 정책기반의 네트워크 관리 기술을 적용시킨 통합보안관리 시스템을 제안하였다. 이러한 통합보안관리 제품들이 본격적으로 상용화되면 기존 기업들이 개별적으로 이기종 보안솔루션을 설치하기 위해서 투자된 중복이나 IT자원 낭비를 최소화할 수 있고, 전문관리인력이 없어도 일관된 보안정책을 수립 및 유지 보수할 수 있어 그 채택과 적용이 활발해 질 것이다.

참고문헌

[1] http://www.ietf.org/html.charters/idwg-charter.html.

[2] R. Yavatkar, D. Pendarakis, R. Guerin, "A Framework for Policy-based Admission Control", RFC2753, Jan. 2000.
[3] J. Case, M. Feder, M. Schoffstall, J. Davin, " A Simple Network Management Protocol(SNMP)", MIT Lab. for Computer Science, RFC 1157, May 1990
[4] Introduction to Policy Based Networking & QoS, White paper, http://www.iphighway.com
[5] R. Yavatkar, D. Pendarakis, R. Guerin, A Framework for Policy-based Admission Control, RFC2753, Jan. 2000.
[6] ESM 동향 및 추세, http://www.kisa.or.kr/K_trend/KisaNews/200011/esm.html
[7] 정연서, 류걸우, 장종수, "네트워크보안을 위한 ESM 기술동향", 주간기술동향, 2001. 12
[8] RFC 2251, Lightweight Directory Access Protocol(v3) , Dec, 1997.
[9] D. Durham Ed., J. Boyle, R. Cohen, S. Herzog, and et. al., The COPS (Common Open Policy Service) Protocol, internet draft, July 2000.

저 자 소 개

정 연 서

1996년 : 충북대학교 컴퓨터공학과(공학석사)
2001년 : 충북대학교 컴퓨터공학과 박사
2000년 ~ 현재 : 한국전자통신연구원

박 배 욱

2000년 : 충북대학교 컴퓨터공학과(공학석사)
2001년 ~ 현재: 충북대학교 컴퓨터공학과 박사과정

손 승 원

현재 한국전자통신연구원 네트워크보안연구부 부장
관심분야 : 정보 보안, 암호기술, 생체인식

오 창 석

현재 충북대학교 전기전자컴퓨터공학부 교수
관심분야 : 인터넷 보안, 초고속망