2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

보안정책모델을 적용한 네트워크보안제어서버 구조

방효찬*, 김기영*, 김건량*, 장종수*
*한국전자통신연구원 네트워크보안구조연구팀
e-mail : bangs@etri.re.kr

Architecture of Network Security Control Server for applying Security Policy Model

Hyo-Chan Bang, Ki-young Kim, Geon-Lyang Kim, Jong-Soo Jang
*Dept. of Network Security Architecture research Team,
Electronics and Telecommunications Research Institute

요 약

본 논문에서는 정책기반 네트워크보안 프레임워크의 전체적인 구조와 주요 아키텍처에 대해서 논하고 특히 보안정책 서버의 역할을 담당하는 네트워크보안제어서버의 구조와 메커니즘에 대해 구체적으로 기술한다.

1. 서론

현재의 네트워크 보안 기반구조는 개발사 별로 보안기능 및 인터페이스가 서로 상이한 장비 위주로 형성되어 있기 때문에 광역 네트워크 차원에서의 보안기능 통합 및 운용관리의 일원화가 매우 곤란한 실정이다. 이러한 문제를 해결하기 위한 방안으로 각각의 보안 시스템들을 구조적으로 통일하고 분산된 관리방법을 일원화 하기 위한 통합보안관리(ESM : Enterprise Security Management)가 연구되기 시작하였다[1]. 그러나 이러한 통합보안관리 솔루션들 역시 아직까지는 자사제품 간의 통합이나 중앙감시 수준에 머물고 있으며, 기존의 네트워크 관리 시스템(NMS : Network Management System)과의 유기적인 통합이라는 커다란 문제를 안고 있다[2]. 이처럼, 지금까지는 네트워크 운용관리와는 별도로 취급되어 왔던 네트워크보안관리 영역을 하나의 공통된 프레임워크로 통합시켜 일관된 네트워크 자원관리 및 보안관리를 제공할 수 있는 정책기반의 네트워크보안 기반구조가 제안되고 있다[3].

정책기반의 네트워크보안관리 프레임워크에서는 보안관리자가 규정한 보안정책에 따라 관리 영역 내의 보안 기능이 자동으로 운용된다. 즉 보안정책에 의해 동작이 규정되는 네트워크 보안 장비로 구성되어 운용되는 네트워크보안관리 구조라고 할 수 있다[4]. 본 논문에서는 개발 중인 정책기반 네트워크보안관리 프레임워크의 전체적인 구조와 주요 아키텍처에 대해서 논하고 특히 보안정책 서버의 역할을 담당하는 네트워크보안제어서버에 대해 구체적으로 기술한다.

2 정책기반 네트워크보안관리 프레임워크

정책기반 네트워크보안관리 프레임워크의 구성요소는 크게 보안정책을 생성하는 S-PMT, 보안규칙에 따라 보안행위를 결정하는 S-PDP, 보안결정에 따라 보안행위를 수행하는 S-PEP, 보안 규칙들을 저장하는 S-PR, S-PDP 와 S-PEP 간의 보안정책 송수신을 위한 통신 프로토콜로 구성된다[5,6]. 그림 1 은 프레임워크의 구성요소와 상호간의 관계를 나타내고 있으며 각각의 기능은 다음과 같다.

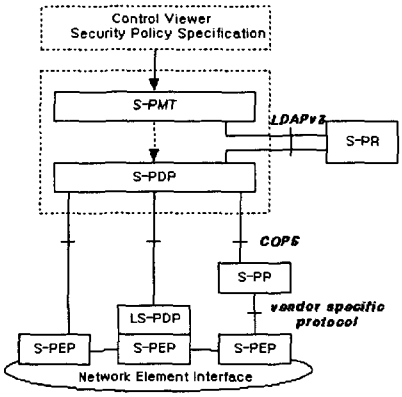
2.1 S-PMT(Security Policy Management Tool)

S-PMT 는 관리자가 수립한 정보보안 및 자원보호 목표에 따라 보안관리자가 생성한 네트워크 보안운용 규칙을 망 내의 모든 보안장치가 인식할 수 있는 일관된 형식으로 생성하고 관리하는 기능을 제공한다.

2.2 S-PDP(Security Policy Decision Point)

S-PDP 는 보안정책에 따라 보안장비가 수행해야 하는 보안행위를 결정하고 이를 S-PEP 에 통보하는 보

안정책 결정기능을 제공한다. 또한 S-PEP 가 단독으로 결정할 수 없는 보안 행위에 대한 의사결정을 수행하여 S-PEP 에 통보 한다. 또한, 관리 영역내의 모든 S-PEP 의 보안정책수행 상황을 모니터링하여 정책 적용 모순을 탐지하는 보안정책 감사기능이 있다.



[그림 1] Policy based Network Security Management Framework

2.3 S-PEP(Security Policy Enforcement Point)

S-PEP 는 S-PDP 에서 결정된 보안행위를 네트워크 레벨에서 실제로 적용시킨다. 즉 네트워크 내에 산재해 있는 다양한 보안장비가 S-PEP 에 해당된다. 그러나, 네트워크 상의 모든 보안장비가 PBNM 을 이해하는 S-PEP 의 구조로 구성되기는 어렵기 때문에 이러한 기존의 보안장비에 대해서는 S-PP(Security Policy Proxy)를 이용한다. 보안정책대행(S-PP)은 S-PDP 와 보안장비 간의 상이한 통신 인터페이스를 정합하고, 상호간의 제어 메시지를 번역하여 전달함으로써 관리자의 보안정책이 일관적으로 적용될 수 있도록 한다.

2.4 S-PR(Security Policy Repository)

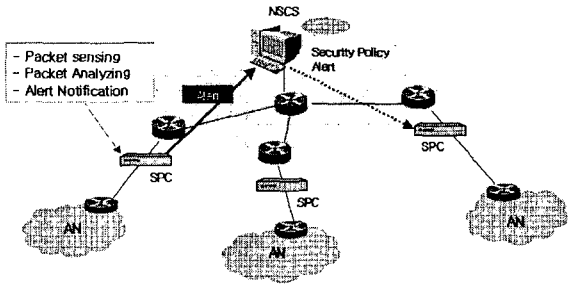
S-PMT 에서 생성된 모든 보안규칙(security rule)은 S-PR 에 저장되어 일원적으로 관리된다. S-PR 은 디렉토리 서버로 구성되며, S-PMT, S-PDP 와의 통신은 LDAPv3 을 통해 이루어진다. S-PR 은 물리적인 위치에 상관없이 독립적으로 구축될 수 있으며, 광역 네트워크에 분산되어 있는 S-PDP 에 의해 실시간으로 검색된다.

2.5 COPS(Common Open Policy Services) 프로토콜

S-PDP 와 S-PEP 가 통신하기 위해 제안된 프로토콜이며, 기존의 MIB 정보보다 복잡하고 데이터량이 큰 보안정책정보(SPIB)를 효율적으로 전달하기 위해 설계되었다. 기존의 망 관리 프로토콜인 SNMP 에 비해 안정성과 확장성이 크게 향상된 프로토콜이다[7].

3. 정책기반 침입탐지/대응 시스템

이 장에서는 정책기반 네트워크보안관리 프레임워크에 기반 한 침입탐지/대응 시스템[3,6]에 대해 기술하고 실제 네트워크 상에서 각 요소들이 기능하기 위한 메커니즘에 대해 논하고자 한다. 정책기반 침입탐지/대응 시스템의 전체적인 구조는 그림 2 와 같다.



[그림 2] 정책기반 침입탐지/대응 시스템 구조

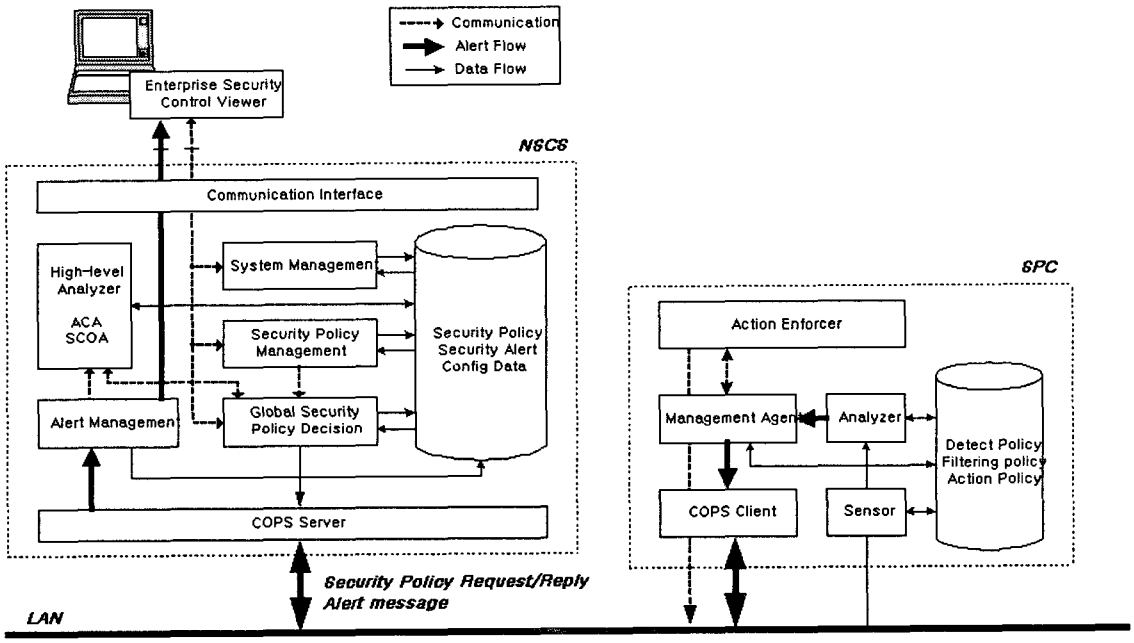
이 모델은 네트워크 접속점(ingress, egress point)에서 주어진 보안정책에 따라 네트워크 침입탐지/대응 기능을 수행하는 SPC(S-PEP)와 보안정책서버에 해당하는 NSCS(S-PMT, S-PDP, S-PR)로 구성된다. 그림 1 의 하단 중앙에 표시된 S-PEP 와 같이 SPC 는 침입탐지 및 차단에 대한 정책결정을 실시간으로 수행할 필요가 있기 때문에 NSCS 로부터 로컬보안정책 정보를 사전에 다운로드 받아 지역보안정책결정(LS-PDP : Local Security Policy Decision Point)을 수행하도록 설계되었다[8]. 네트워크보안제어서버(NSCS : Network Security Control Server)는 보안관리자가 규정한 보안규칙에 따라 관리영역 내의 모든 SPC(Security Policy Client)를 중앙 관리하고, SPC 단독으로 결정할 수 없는 광역 보안정책결정을 수행한다. (그림 3)은 NSCS 의 구조와 구성모듈 간의 상호관계를 나타낸 그림이다.

NSCS 는 시스템을 구성하는 각 기능 요소들의 수행상태를 감시하고 시스템 구성정보를 관리하는 시스템 관리 모듈, 다양한 보안규칙을 생성, 수정하고, 구조적으로 저장, 관리하는 보안정책관리 모듈, 보안정책을 해당 SPC 에 실시간으로 온라인 배포하는 보안정책배포 모듈, 네트워크 전반에 걸친 광범위한 통합 분석을 통하여 SPC 단독으로는 결정할 수 없는 복잡한 보안정책결정을 수행하는 광역보안정책 결정 모듈, 보안정책 및 시스템 상태정보 등을 SPC 와 주고 받기 위한 통신 모듈, SPC 로부터 송신되는 경보 데이터를 수집, 저장하는 경보관리 모듈, 통합관제 에이전트와 상호간의 통신을 위한 인터페이스 모듈 등으로 구성된다. 논문에서는 SPC 에 대한 구체적인 설명은 생략하고 네트워크보안제어서버(NSCS)의 구조와 기능에 대서 구체적으로 언급한다.

4.1 시스템 관리 모듈

시스템 관리 모듈은 NSCS 를 구성하는 모든 구성요소 들의 상태를 점검하고 관리한다. 시스템관리 모듈은 통합관제 클라이언트의 GUI 를 통해 보안관리자에 의해 직접 제어되며 관리 대상은 다음과 같다.

- 시스템 구성요소의 프로세스 상태
- 관리 영역 내의 SPCs 상태 정보
- SPC 초기화 정보 및 상태변경 정보
- 경보 및 보안정책 관리를 위한 DBMS 상태 정보
- 관리 영역 내의 네트워크 Topology 정보 등



(그림 3) Architecture for NSCS & SPC

4.2 보안정책

NSCS-SPC 시스템에서의 네트워크 보안정책이란 네트워크 전역에 적용되는 보안규칙의 집합을 의미한다. 보안정책은 SPC 에서 네트워크 레벨의 침입탐지/대응을 위해 필요한 로컬보안정책과 NSCS 에서 수행되는 통합분석 및 광역 정책결정에 필요한 글로벌보안정책이 있다. 로컬보안정책으로는 SPC 가 네트워크 패킷을 선택적으로 수집하도록 하는 " 패킷 필터링 규칙" 과 유해 패킷을 탐지하기 위한 " 유해 패킷 탐지 규칙" 및 탐지된 보안위반 사건에 대응하기 위한 " 자동 대응 규칙" 등이 있다. 글로벌보안정책으로는 통합분석을 위한 Traceback Policy, Boundry Blocking Policy, Alert Control Policy 등이 있다. 보안정책정보는 DMTF 에서 제안하고 있는 PCIM(Policy Core Information Model) 표준 모델을 확장하여 개념적으로 모델링 된다[9].

4.3 보안정책 관리 모듈

S-PMT 에 해당하며, NSCS 및 SPC 에서 사용되는 모든 보안정책규칙을 생성, 수정, 삭제하는 보안정책 편집 기능과 정책저장소에 저장된 보안정책규칙을 정책 버전 및 적용범위 등에 따라 관리하는 보안정책관리 기능을 수행한다. 보안관리자가 표준적인 모델링 기법을 통해 정의한 추상적이고 명세적인 보안정책은 보안정책 편집 모듈을 통해 일반적이고 구체적인 보안정책정보(Security Policy Information Base)로 변환된다. 즉, 모델링한 보안정책을 정책 저장소인 Directory Server 에 구조적으로 저장하기 위해서 PCIM Schema 를 Directory Schema 로 맵핑하기 위한 LDIF 포맷 변환이 내부적으로 수행된다. 보안정책 편집 모듈은 보안관리자가 이러한 내부적인 기능을 의식하지 않고 GUI 를 통해 간단히 새로운 보안정책을 생성하거나 수정할 수 있도록 한다. 또한, 보안정책 배포 시에 필요한 인코딩 규칙에 따라 보안정책정보(SPIB : Security Policy Information Base)를 적절한 전송 타입(BER, XML)으로 변환하여 주는 정책정보변환 기능도 수행한다.

4.4 광역보안정책 결정 모듈

S-PDP 에 해당하며 보안정책배포 기능과 광역보안정책결정 기능 및 감시 기능 등을 제공한다. 보안정책배포 기능은 SPC 에서 지역보안정책결정에 필요한 보안정책을 SPC 초기화 시에 COPS 프로토콜을 이용해 온라인으로 전송한다. 보안정책 배포는 SPC 가 네트워크에 최초로 적용되어 초기화되는 경우와 운용 중에 보안정책의 변경이 발생한 경우에 수행되며, 정책적용 대상(SPCs)은 정책 토폴로지 맵에 의해 관리한다. 광역보안정책결정 기능은 SPC 가 단독으로 결정할 수 없는 복잡한 결정, 예를 들면 네트워크 전체의 상태를 분석하여 대응 조치를 취해야 하는 경우 등에 수행된다. 광역보안정책결정 기능은 네트워크 차원의 계층적 통합분석 결과에 따라 운용자의 개입 없이 자동적으로 적절한 대응 방안을 수립하고 이를 실제 망에 적용한다. 현재 개발 중인 통합분석 기능에는 네트워크 전체에서 수집되는 경보데이터를 통합 분석하고 상호 연관성을 검출하여 침입의 확실성(certainty)과 심각성(severity)을 결정하는 ACA(Alert Comparative Analysis Function) 기능과 경보데이터의 발생량과 네트워크의 실제 트래픽을 감시하여 네트워크 전반에 걸친 보안상태를 정량적으로 결정하는 SCOA(Security Condition

Observable Analysis) 기능이 있다. 보안정책감시 기능은 정책적용 모순을 감시(audit)하고, 적용된 보안정책 상호간의 관계 및 영향을 조사하여 NSCS 관리영역 내의 모든 SPCs 에 적용되는 보안정책이 일관성을 유지할 수 있도록 한다.

4.5 경보관리 모듈

SPC 가 COPS 를 통해 송신하는 보안위반 경보를 실시간으로 수집하여, 통합관제 에이전트로 통보하고 데이터베이스에 구조적으로 저장한다. 또한 경보데이터의 근원지 IP 를 분석하여 불량 사용자를 관리하고, 과거 경보에 대한 실시간 검색, 통계, 백업 등의 부가기능도 제공한다.

4.6 보안정책전달 모듈

NSCS 와 SPC 간의 정책전달 및 통신을 담당하며 통신 프로토콜로는 COPS(Common Open Policy Services)를 이용한다. COPS 는 TCP 기반의 안정된 통신기반에서 양방향 정보전송을 지원하고, 대량의 정책정보를 효율적으로 전송할 수 있는 표준 프로토콜이다. 또한 SPC 초기화 시의 SPC 구성정보 전달 및 SPC 운용 중의 상태 정보도 전달한다.

4.7 통합관제 에이전트 및 인터페이스 모듈

통합관제 에이전트(Enterprise Security Management Agent)는 모든 경보데이터를 중앙에서 일원적으로 실시간 모니터링 할 수 있는 경보감시 기능과 보안정책 편집 및 관리를 시각적으로 지원하는 GUI 기능, NSCS 및 SPC 를 제어하기 위한 GUI 기능 등을 제공한다. 즉 NSCS, SPC 의 모든 자원 및 기능을 하나의 Client Viewer 에서 제어할 수 있는 통합관제 기능을 제공한다. 인터페이스 모듈은 통합관제 에이전트와 NSCS 간의 통신 세션 관리 및 상호간의 메시지 송수신을 위한 기능을 제공한다.

5. 프로토타입 구현

NSCS 의 프로토타입은 SUN W/S 의 Solaris8 에서 개발되고 있으며, 개발언어는 C++와 Java 를 사용하였다. 정책결정모듈과 같이 실시간 처리를 요구하는 모듈은 C++을 이용하고 있으며 PMT 및 인터페이스 모듈과 같이 GUI 와 연관성이 있는 모듈은 Java 로 구현하고 있다. 시스템 내의 각 모듈간의 통신은 내부 메시지 큐(message queue)를 사용하며 향후 CORBA M/W 로 통합할 예정이다. 네트워크 환경은 현재는 10/100 Ethernet 을 사용하고 있으나 향후 ATM, Gigabit 네트워크 환경으로 확장할 예정이다. 경보데이터베이스는 오라클 RDBMS8.1.6 을 보안정책 데이터베이스는 Open LDAP 을 이용하고 있다. 보안정책 데이터는 소량이지만 복잡한 계층 구조를 가지기 때문에 Directory Server 를 이용하는 것이 효과적이다. 이 밖에도 네트워크 전역에서의 일원화된 관리와 접근 통제, 빠른 검색속도 등의 장점을 가지고 있다. 데이터베이스를 이원화 한 이유는 경보데이터와 같이 반복적이고 대량의 데이터를 관리하기 위해서는 안정적이고 고속의 상용 RDBMS 가 효과적이라는 점과 향후 계획 중인 데이터웨어 하우징과 마이닝을 통한 통계 분석 기능의 확장을 고려했기 때문이다.

6. 결론

계층구조를 갖는 정책기반의 침입탐지/대응 시스템은 네트워크의 보안상태를 실시간으로 통합 분석하고 상호 연동된 정책실행을 통해 광역네트워크 전역에 걸친 조기 대응을 가능하게 한다. 또한, 네트워크 전체의 보안상태를 보다 정량적으로 감지할 있는 상위 레벨의 통합분석기능을 제공하는 등 기존의 단일적인 보안장비로는 해결할 수 없었던 새로운 형태의 침입탐지/대응 메커니즘을 제공한다. 본 논문에서는 광역네트워크에서 체계적이고 통합된 보안 관리 기능을 제공하는 정책기반 네트워크보안관리 프레임워크와 보안시스템 간의 상호 연동 및 계층화된 통합분석 아키텍처를 제공하는 네트워크보안제어서버의 구체적인 아키텍처를 제안하였다. 향후 침입탐지/대응 규칙의 표준화와 범용적인 분석 알고리즘 및 광역네트워크에서의 통합보안상태 분석 기능 등에 대한 지속적인 연구가 필요하다.

7. 참고문헌

[1]ESM 동향 및 추세, http://www.kisa.or.kr/K_trend/kisaNews/200011/Esm.html

[2]정연서, 장종수, 김명은, " 정책기반의 통합보안관리" , COMSW2001

[3]방효찬,김명은,장종수," PBNM 최신동향 분석을 통한 정책기반의 네트워크보안제어 기술 제안" ,NCS2000

[4]방효찬,김명은,장종수," 정책기반 네트워크보안관리 프레임워크에서의 계층적 트래픽 분석을 통한 네트워크 침입탐지/대응 메커니즘" , 한국정보과학회 추계학술대회 논문지,2001.10

[5]" introduction to Policy based Network & QoS" , white paper, http://www.iphighway.com

[6]김기영,서동일,장종수,이상호," 광역망에서 보안서비스 제공을 위한 정책기반 통합보안 제어 구조" , COMSW2001

[7]RFC2748," The COPS(Common Open Policy Service) protocol"

[8]허영준외," 보안정책모델을 적용한 Security Policy Agent 구조" , COMSW2001

[9]J.Strassner, E. Ellesson, B. Moore, and A.Westerinen, " Policy Core Information Model □ version 1 Specification" , RFC3060, 2001.02