네트워크 보안을 위한 정책 기반 망 관리에 대한 핵심 정책 정보 모델 적용

김숙연,[0] 김건량, 김명은, 방효찬, 김기영, 장종수
한국전자통신연구원
(sykim, glkim, mekim, bangs, kykim, jsjang)@etri.re.kr

Policy Core Information Model in Policy-Based Management for Network Security

Sook-Yeon Kim[0] Geon-Lyang Kim Myung-Eun Kim Hyo-Chan Bang Ki Young Kim Jong-Su Jang
Electronics and Telecommunications Research Institute

요 약

본 논문에서는 네트워크 기반의 침입 탐지 및 대응을 위한 정책 기반 망 관리 (NS-PBNM : Network Security Policy Based Network Management)에 핵심 정책 정보 모델 (PCIM :Policy Core Information Model) 을 적용하는 시스템 구현 방안을 제시한다. 이 시스템은 여러 장치를 유연성 있게 통합적으로 관리한다는 정책 기반 망 관리의 목적뿐만 아니라, 정책을 표현, 관리, 공유 및 재사용하는데 있어 호환성 및 확장성을 확보한다는 PCIM의 목적을 동시에 달성한다. 먼저 NS-PBNM의 구조를 제시하고 이 구조를 기반으로 PCIM을 적용하는 방안을 제시한다. PCIM은 네트워크 침입 탐지 및 대응이라는 기능을 수행하는데 있어 네트워크 보안 정책 정보 모델로 확장된 후, 정책 서버의 정책 관리 도구와 정책 저장소의 구조를 결정한다.

1. 서론

인터넷의 중요성이 각종 산업에 있어서 갈수록 더욱 증가함에 따라 인터넷 서비스도 다양하게 확대되고 있고 사용자도 폭발적으로 증가하고 있다. 그러나 TCP/IP의 구조적인 취약성으로 인한 보안 허점의 노출과 보안 사고의 발생도 기하급수적으로 늘어나고 있는 상황이다.

이에 따라 네트워크 보안에 대한 연구 개발이 활성화되었고, 침입 탐지 시스템 (IDS: Intrusion Detection System)이나 방화벽 같은 네트워크 기반의 보안 시스템들이 각자의 전문성을 자부하며 시장에 선보이게 되었다. 그러나 이러한 보안 시스템들은 서로 다른 동작 구조와 관리 방법을 가지므로 일반적으로 상호 동작하지 않는다. 이러한 비호환성은 여러 개의 보안 장비들을 포함하는 망을 통합적으로 관리해야 하는 관리자에게 큰 부담을 주게 되었으며 이들을 쉽게 통합 관리하는 문제는 뜨거운 논쟁의 대상이 되고 있다.

한편 보안에 국한되지 않는 일반적인 망 관리 정책을 제공하는데 있어 유연성과 확장성을 확보하는 방안으로서 PBNM (Policy Based Network Management)이 논의되고 있다. IETF (Internet Engineering Task Force)의 RAP(Resource Allocation Protocol) WG (Working Group)은 COPS-PR(Common Open Policy Service-policy provisioning)을 통하여 정책 제공을 용이하게 해주는 객체들을 정의하고 있다[1]. 한편 IETF의 Policy Framework WG에서는 정책을 표현, 관리, 공유, 재사용하는데 있어 호환성 및 확장성을 확보하기 위한 정책 정보 모델을 제시하고[2,3], 이 모델을 LDAP 스키마에 대응시키는 작업을 하고 있다[4].

Policy Framework WG의 핵심 정책 정보 모델 (PCIM: Policy Core Information Model) 은 RFC3060으로 표준화되었으며[2] 그것의 수정 보완판도 준비중이다[3]. 핵심 정책 정보 모델은 모든 응용 분야에 적용되는 것을 목적으로 정의되었으나 QoS (Quality of Service) 와 IPsec (IP SECurity protocol)을 위해서 확장되었을 뿐[5,6] 다른 응용 분야에 대한 적용 방안은 숙제로 남아 있다.

본 논문에서는 네트워크 기반의 침입 탐지 및 대응을 위한 PBNM (NS-PBNM: Network Security PBNM)에 PCIM을 적용하는 시스템 구현 방안을 제시한다. 이 시스템은 여러 장치를 유연성 있게 통합적으로 관리한다는 PBNM의 목적뿐만 아니라, 정책을 표현, 관리, 공유 및 재사용하는데 있어 호환성 및 확장성을 확보한다는 PCIM의 목적을 동시에 달성한다. 먼저 NS-PBNM의 구조를 제시하고 이 구조를 기반으로 PCIM을 적용하는 방안을 제시한다.

2. NS-PBNM의 구조

이 절에서는 IETF의 PBNM의 구조를 간략히 살펴본 후, 이에 기반을 둔 NS-PBNM의 구조를 밝힌다.

IETF에서 표준화 되고 있는 PBNM은 다음 그림 1과 같이 PMT(Policy Management Tool), PR(Policy Repository), PDP(Policy Decision Point)와 PEP(Policy Enforcement Point)의 구성 요소를 가진다. PMT와 PDP는 정책 서버에 위치하며 PR은 정책 서버에 함께 위치할 수도 있지만 따로 분리되어도 무방하다. PEP는 정책 서버가 관리하는 네트워크 장치라 봐도 무방하다.

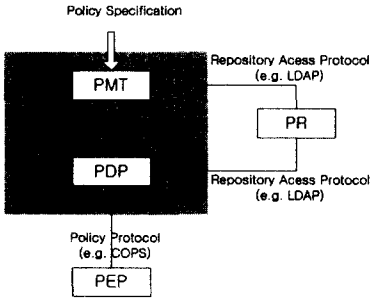

그림 1. PBNM의 구조

NS-PBNM의 구조는 기본적으로 IETF의 PBNM의 구조를 따른다. PMT, PDP, PR등은 CPCS (Cyber Patrol Control System)이라는 보안 정책 서버에 구현되고 PEP는 SGS (Secure Gateway System) 라는 보안 장치에 구현된다. PR을 CPCS와 분리된 DB에 구현하여도 무방하다. PR에 대한 접근 프로토콜은 LDAP이며 PDP와 PEP간의 프로토콜은 COPS-PR이나 SNMP이다. NS-PBNM의 간단한 구성 예를 개념적으로 표현해 보면 다음 그림 2와 같다.

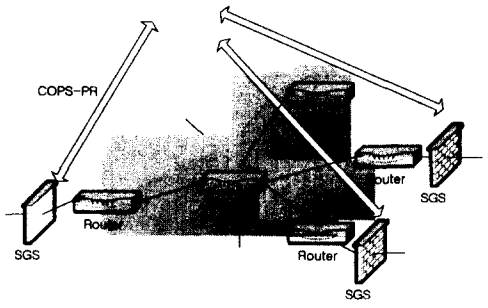

그림 2. NS-PBNM의 구성 예

SGS는 방화벽과 IDS를 포함하는 기능을 가진다. 즉 패킷 캡쳐 기능, 침입 탐지 기능, 실시간 보고 기능, 접근 통제 기능 등을 가진다. CPCS는 기본적으로 각 SGS의 정책을 편집과 저장 및 제공하는 PMT 과 PR 및 PDP 의 기능을 가진다. 이와 더불어 각 SGS로부터 얻은 침입 정보 및 세션 정보들로부터 복잡하고도 다양한 형태의 침입을 탐지하고 대응하는 기능을 가진다. 이러한 탐지에는 통계적 분석 및 데이터 마이닝 등의 기법이 사용될 수 있다.

3. PCIM을 적용하는 방안

이 절에서는 NS-PBNM에 PCIM을 적용하는 방안으로서 NSPIM (Network Security Policy Information Model)을 정의하고 이를 근거로 하여 PMT 구조를 설계하고 LDAP 스키마를 정의하고 PIB/MIB 구조를 확장하는 것에 대하여 기술한다.

3.1. NSPIM의 정의

NS-PBNM에 PCIM을 적용하려면 보안 정책을 나타내는 정보 모델링이 먼저 이루어져야 한다. 이러한 정보 모델 NSPIM의 기능요구사항은 다음과 같다. 첫째, 다양한 SGS의 기능을 제어할 수 있는 규칙들을 모두 표현할 수 있어야 한다. 둘째, 관리자가 쉽게 규칙들을 이해하고 조작할 수 있게 해야 한다. 셋째, 정책 규칙의 구현 대상과 방법이 바뀌더라도 NSPIM이 변경되지 않아야 한다. 넷째, 새로운 형태의 규칙을 수용하기 위하여 NSPIM을 수정할 필요가 있을 때에도 기존의 모델들에 대한 변경은 최소화되어야 한다.

이러한 요구 사항을 만족시키는 NSPIM의 주요 클래스들의 상속 관계는 다음 그림 3과 같다. 클래스들의 연결 관계를 표현하는 어소시에이션들의 상속 관계는 생략한다.

```
ManagedElement (abstract) [2,3]
|
+--Policy (abstract) [2,3]
|  +---PolicyCondition [2,3]
|  |   +---CompoundPolicyCondition [3]
|  |       +---PacketMonitoringPolicyCondition (abstract)
|  |           +---OnePacketPolicyCondition
|  |           +---LinearPacketPolicyCondition
|  |           +---RepeatedPacketPolicyCondition
|  +---PolicyAction [2,3]
|  |   +---CompoundPolicyAction[3]
|  |   |   +---PolicyIntrusionResponseAction (abstract)
|  |   |   |   +---PolicyAlertAction (abstract)
|  |   |   |   |   +---PolicyAggregatedAlertAction
|  |   |   |   |   +---PolicyMessageStoreAction
|  |   |   |   |   +---PolicyMessageShowAction
|  |   |   |   |   +---PolicyWindowPopUpAction
|  |   |   |   |   +---PolicyEmailAction
|  |   |   |   +---PolicyBlockAction (abstract)
|  |   |   |   |   +---PolicyPacketDropAction
|  |   |   |   |   +---PolicySessionDropAction
|  |   |   |   +---PolicySessionEventLogAction
|  |   |   |   +---PolicyTraceBackAction
|  |   |   |   +---PolicyICMPUnreachableMessageSendingAction
```

그림 3. 클래스의 상속 계층 구조

NSPIM으로 보안 정책 규칙을 표현하는 예를 한가지만 들어 보자. '소

스 주소가 134.250.17.0/24이고 목적지 포트 번호가 80인 패킷들을 차단하라'라는 규칙은 다음 그림 4와 같이 모델링 된다.

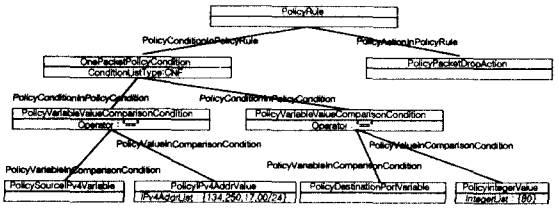

그림 4. NSPIM의 예제

3.2. NSPIM에 근거한 PMT의 구조 정의

PMT는 정책을 편집 및 표현하는 기능과 함께 규칙의 변환 및 충돌 검사를 하는 기능을 지닌다. PMT의 기능 모듈은 정책의 검색, 삽입, 삭제, 수정 등으로 구성되며 각 기능 모듈의 구조는 NSPIM에 근거하여 그 구조가 설계된다. 다음 그림 5는 PMT 기능 모듈의 구조를 개략적으로 나타낸다.

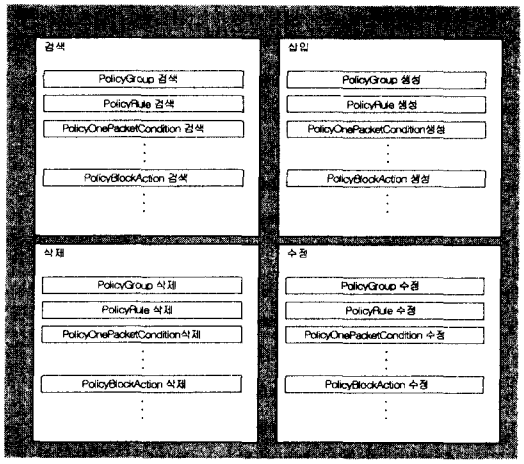

그림 5. PMT 기능 모듈의 구조

3.3. NSPIM에 근거한 LDAP 스키마의 정의

PR은 정책의 저장소로서 정책 검색의 기능을 제공한다. PR로 LDAP을 사용할 경우 NSPIM을 LDAP 스키마에 대응시키는 대응 규칙이 필요하다. NSPIM을 LDAP 스키마에 대응시킬 때 클래스들은 거의 그대로 LDAP 클래스로 대응되나 어소시에이션들은 디렉토리 구조에 적합한 형태로 변형된다. 또한 대량의 정보를 효율적으로 검색하도록 LDAP을 구성하기 위하여 NSPIM에 없으나 LDAP 스키마에 추가되는 클래스들도 있다. PCIM의 LDAP 스키마에 대한 대응은 IETF Policy Framework WG에서 표준화되고 있으므로[4], NSPIM 중 PCIM에서 온 클래스들의 대응은 표준을 따른다.

3.4. NSPIM에 근거한 PIB과 MIB의 정의

CPCS의 PDP가 SGS에 정책을 제공함에 있어 사용할 수 있는 프로토콜로는 COPS-PR과 SNMP등이 있다. 어느 쪽을 사용하든지 CPCS의 PDP와 SGS가 공유하는 가상의 정책 정보의 DB가 필요하다. COPS-PR의 경우 이 DB가 PIB(Policy Information Base)라 불리며 SNMP의 경우 MIB(Management Information Base)이라 불린다. PIB나 MIB의 구조는 표준화된 객체로서 제공되고 있다.

그러나 네트워크 기반의 침입 탐지 및 대응을 위한 객체의 정의는 아직까지 표준화된 것이 없다. 따라서 이러한 객체들을 추가적으로 정의하는데 있어 NSPIM의 역할이 중요하다. 왜냐하면 NSPIM의 클래스들을 기반으로 PIB이나 MIB의 구조를 정의할 수 있기 때문이다. 이때 망 규모의 정책 제공을 위해 표준화된 COPS-PR의 PIB이 디바이스 구성 및 모니터링을 위한 SNMP의 MIB보다 확장성 측면에서 더 우수하다.

4. 결론

본 논문에서는 NS-PBNM에 PCIM을 적용하는 시스템의 구현 방안을 제시한다. NS-PBNM는 기본적으로 IEFT의 PBNM의 구조를 따르되, PEP가 IDS와 방화벽의 기능을 하는 SGS에 위치하고, PMT 와 PDP는 SGS들을 총괄하는 CPCS에 위치한다. NS-PBNM에 PCIM을 적용하기 위해서 우선 NSPIM을 정의하였으며 이를 PMT 구조의 설계와 LDAP 스키마의 정의와 PIB/MIB의 확장 정의에 활용하였다. 현재 각 SGS에 적용되는 규칙 외에 CPCS에만 적용 가능한 규칙, 즉 복합적 정보에 근거하여 침입 탐지 및 대응을 하는 규칙에 대한 NSPIM을 정의하는 일은 향후 연구 과제로 남아 있다.

5. 참고문헌

[1] K. Chan, et al., "COPS Usage for Policy Provisioning (COPS-PR)", RFC 3084, March 2001.

[2] J. Strassner, E. Ellesson, B. Moore, and A. Westerinen, "Policy Core Information Model – Version 1 Specification", RFC 3060, February 2001.

[3] B. Moore, L. Raberg, Y. Snir, J. strassner, A. Westerinen, R. Chdha, M. Brunner, and R. Cohen, "Policy Core Information Model Extensions", work in progress, <draft-ietf-policy-pcim-ext-01>, April 2001.

[4] J. Strassner, et al., "Policy Core LDAP Schema", work in progress, <draft-ietf-policy-core-schema-11.txt>, May 2001.

[5] Y. Snir, Y. Ramberg, J. Strassner, and R. Cohen, "Policy Framework QoS Information Model", work in progress, <draft-ietf-policy-qos-info-model-03.txt>, April 2001.

[6] J. Jason, L. Rafalow , and E. Vyncke, "IPsec Configuration Policy Model", work in progress, <draft-ietf-ipsp-config-policy-model-02.txt >, March 2001.