主題

분산 시스템 기반의 보안정책 정보공유 기술

한국전자통신연구원 김기영, 장종수, 호남대학교 신 영 석

차 례

1. 서론

인터넷 서비스의 폭발적인 증가와 사용자의 부가 서비스 및 양질의 서비스 품질(QoS) 요구에 따라 통신망이 점차 복잡해지고 있다. 이와 같이 복잡한 통신망을 관리하기 위하여 네트워크 구성장치(Network Element: NE)를 통합하여 상호 간에 네트워크 관리와 운영에 필요한 정보를 공유하여 보다 효율적인 네트워크 관리에 대한 여러 연구가 진행되고 있다.

일반적으로 네트워크 정보를 공유하기 위해서 한 개의 서버를 설정하여 특정 영역으로 구분된 네트워크 환경에서 NE의 정보를 서버와 클라이언트 접속 방식에 의해 정보를 수집하는 관리체제로 구성된다. 이는 한정된 영역과 서버의 중앙집중식 관리로 점차 시스템 확장으로 인한 네트워크 트래픽 증가와 제공되는 정보의 일관성, 집중된 서버의 성능, 접속 프로토콜의 유연성 등의 문제점을 보여 왔다. 한편 이러한 문제점을 해결하기 위하여 OMG의 CORBA (Common Object Request Broker Architecture)를 비롯한 분산 미들웨어 기반의 분산 시스템 환경을 이용하여 네트워크 관리 서버와 구성장치를 접속하여 관리하는 방식으로 발전해왔다. 이는 결국 관리자들이 정해진 운영 정책을 네트워크 상태에 따라 손쉽게 관리할 뿐만 아니라, 신속하게 NE의 관리 정보를 취득함으로서 수집된 정보에 의해 새로운 네트워크 운영정책을 수립하여, 이를 신속하게 네트워크에 적용이 가능하도록 하였다.

네트워크 관리 기능인 FCAPS(Fault, Connection, Account, Performance, Security)에서 대용량에 따른 트래픽 증가로 인한 시스템 성능 저하와 통신망에서 해킹은 날로 증가되는 추세임에 따라 성능과 보안 기능이 종전의 네트워크 관리 기능과 통합된 보안관리(Enterprise Security Management: ESM)로 발전되고 있다. 특히 보안관리에서는 악의적 사용자에 의해 새로운 침입으로 통신망의 운영관리가 어려움에 따라 네트워크 보안과 성능 분석에 대한 시스템 개발에 많은 관심을 보이고

있다. 따라서 각 네트워크 구성장치 간에 보안 및 서비스 품질에 관련된 정보를 공유하여, 이를 토대로 네트워크의 효율적인 정책을 수립하여 네트워크를 관리하는 방향으로 연구개발이 진행되고 있다. 이를 위해서는 네트워크 구성장치에 대한 정보공유가 먼저 선행되어야 한다.

본 논문에서는 이러한 보안정책 관련 정보를 보다 손쉽게 공유하며, 이를 기반으로 효율적이고 편리한 보안관리를 위한 정보공유기술을 살펴보기로 한다. 제2장에서는 정책 기반의 정보보안 시스템에 대한 구조를 살펴보며, 제3장은 보안정책 정보를 공유하는 방향을 검토한다. 제4장에서는 검토된 보안정책 정보 공유 기술을 기반으로 한 보안정보 시스템의 구조를 제시한다. 마지막으로 제5장에서는 결론과 향후 연구 방향을 살펴본다.

2. 정책 기반의 정보보안 시스템

2.1 정책 기반 시스템

정책 기반의 통신 시스템 관리(Policy-Based Network Management: PBNM) 기능은 IETF 표준화 문서에 정립되어 있다[6]. 정책 기반의 통신망 관리는 통신망에서 제공하는 QoS, 정보보호 및 자원 제어를 위한 정보를 제공하고, 이를 효율적으로 관리하는 데 있다. 따라서 정책 기반의 관리를 위해서는 NE의 MIB 혹은 PIB(Policy Information Base) 등의 정보를 SNMP, COPS(Common Open Policy Service), CLI, LDAP(Light Directory Access Protocol) 등의 프로토콜을 사용하여, 통신망 구성장치를 모니터링하여 정책을 관리하는 시스템에 정보를 전달한다. 정책관리 시스템은 수집된 정보를 분석하여 운영자가 내리는 정책규칙에 따라 수행하도록 세부 명령을 내리면 된다.

PBNM 시스템은 정책규칙을 제정하고, NE를 실시간으로 모니터링하여, 동적으로 변화되는 정보를

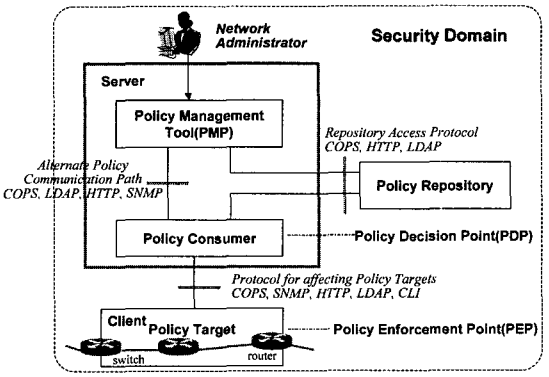

그림 1. 정책 기반의 통신 시스템 구성

신속하게 PBNM 서버에 전송해야 한다. 이를 위해서 PBNM 시스템은 기능적으로 정책관리 도구(Policy Management Tool: PMT), 정책 저장장치(Policy Repository: PR), 정책 결정장치(Policy Consumer), 정책수행 대상장치로 그림 1과 같이 구분한다. 또한 통신망 사업자 관점으로 볼 때, 운영자에 의하여 정책을 관리하고 통신망 동작을 모니터링하는 운영자 시스템, 정책규칙 및 각종 통신망 정보를 관리하는 PDP(Policy Decision Point) 혹은 정책서버와 라우터 등의 PEP(Policy Enforcement Point)로 구분한다.

PBNM 시스템은 그림 1과 같이 4개의 기능 컴포넌트로 구분되며, 이들 간에 그림 2와 같은 요소기술이 요구된다. 세부 요소기술로는 컴포넌트 간의 접속 프로토콜, PDP, PEP, PR에서 운영되는 네트워크 관리정보에 대한 정보모델링 기술, PR의 정책 객체를 액세스하는 공유정보 액세스 기술, 정책서버에 탑재되는 네트워크 관리기술, 이들 컴포넌트를 한데 묶는 정보공유 기술인 분산시스템 기술로 구분된다.

현재 PBNM 시스템의 접속 프로토콜로는 SNMPv3, CLI, COPS-PR, HTTP 등이 있으며, 정보공유 액세스를 위해서는 LDAP, COPS-PR, HTTP, SQL과 분산시스템으로는 CORBA, DCOM 등의 기술을 들 수 있다.

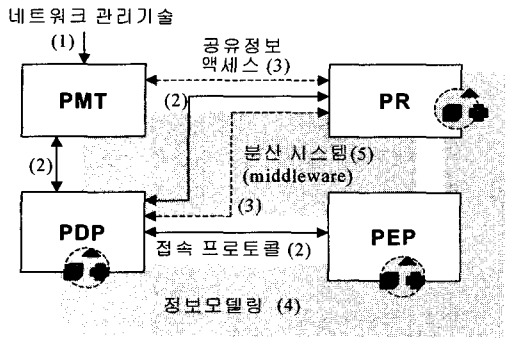

그림 2. PBNM 구축을 위한 요소기술

2.2 정책 정보모델링

정보모델은 종전의 SNMP 프로토콜을 적용한 경우 MIB를 이용함에 따라, ASN.1 혹은 GDMO (Guideline for the Definition of Managed Objects), GRM(General Relationship Model) 방식에 의한 모델을 사용하고 있다. 그러나 객체지향 설계 기술과 분산 시스템의 기술 발전으로 객체 기반의 정보모델이 OMG, TINA(Telecommunication Information Network Architecture), ITU-T, IETF, DMTF 등의 표준화 연구기관에서 정착되었다. 한편 인터넷의 보급으로 데스크 탑 PC에서 웹 브라우저를 이용하여 네트워크를 관리함에 따라, 웹 서버에 네트워크 관리정보가 HTML 형태로 제공되는 것이 보다 편리해지고 있다. 따라서 객체화된 네트워크 관리정보를 웹 브라우저로 표현을 위해 변환 프로토콜이 필요함에 따라 이를 보다 유통성 있게 표현하고자, XML(Extensible Markup Language)으로 모델링하는 연구가 DMTF에서 진행되고 있다. 현재 DMTF의 CIM(Common Information Model) 버전 2.6에서는 796개의 Class와 3,089 Properties를 개발 중에 있으며, 그림 3은 보안정책 정보모델을 보이고 있다.

3. 보안정책 정보공유

PBNM 시스템은 PEP에서 물리적으로 네트워크와 접속되어 네트워크에 관련된 패킷 모니터링과 운영에 따른 정보를 실시간으로 수집하여 이를 해당 정책서버로 전송한다. 정책서버는 운영자에 의해 정책규칙에 따라 이를 근간으로 네트워크 장비를 통합하여 관리하며, 특정 기능에 대하여 별도로 정책에 따른 명령을 PEP에 전송하여 관리한다. 본 장에서는 PBNM 시스템을 구성하는 장치들 간의 보안정책정

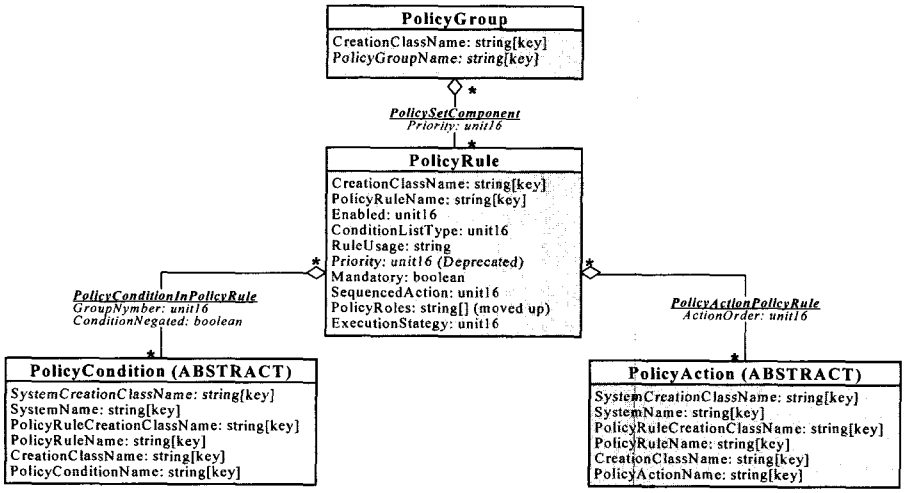

그림 3. DMTF CIM의 보안정책 정보모델링

보를 공유하여 운영하는 대표적인 3가지 방안에 대하여 살펴본다.

3.1 WBEM에서 정보공유

WBEM(Web-Based Enterprise Management)는 인터넷 상에서 웹을 기반 한 네트워크 관리에서 관리 프로토콜의 불일치를 극복과 테스크 탑 PC 기반으로 편리한 네트워크 운영을 위해 Microsoft, Cisco, Compaq, Intel 및 BMC 소프트웨어 등이 주축이 되어 '96년 7월 구성한 컨소시엄(DMTF)에서 연구되었다. 네트워크 관리자가 데스크 탑 PC 상에서 웹 브라우저를 이용해 호환성이 없는 시스템이나 네트워크 및 애플리케이션을 관리할 수 있도록 하는 표준규격 개발을 목표로 한다. WBEM의 표준은 SNMP, DMI(Desktop Management Interface) 및 CMI 프로토콜과 같은 기존의 네트워크 구성장치의 데이터 수집 에이전트와 웹 서버와 접속을 함으로서 네트워크 정보를 효과적으로 수집하여, 이를 웹 브라우저로 관리자가 관리할 수 있는 환경을 제공한다. 따라서 그림 4와 같이 웹 서버는 NE에 존재하는 네트워크 운영관리 정보(CIM)를 중앙집중식으로 수집하며, 관련 정보를 HTTP 프로토콜로 클라이언트에게 제공한다. 그러나 실제 네트워크 구성장치의 정보는 CIM 정보모델 형태에 따라 CIM 정보를 웹 상에서 쉽게 볼 수 있도록 변환하여 XML(xmlCIM) 형태로 제공한다.

WBEM 방식에 의한 정보공유는 중앙집중식으로 네트워크 구성장치의 에이전트와 웹 서버(정책서버) 간에 다양한 접속 프로토콜에 의해 수집된 보안정책 정보를 XML 형태로 변환하여 이를 공유하도록 한다. 따라서 CIM 클라이언트에 의해 요구된 메시지에 의해 해당 메시지를 서버는 정송하면 된다. 또한 그림 5와 같이 서버에는 CIMOM(CIM Object Manager)이 상주하여 해당 정보를 일관성 있게 관리해야 한다. 네트워크 구성장치에는 CIM Schema의 정보를 수시로 혹은 Event에 따라 서버에 전송해야 한다.

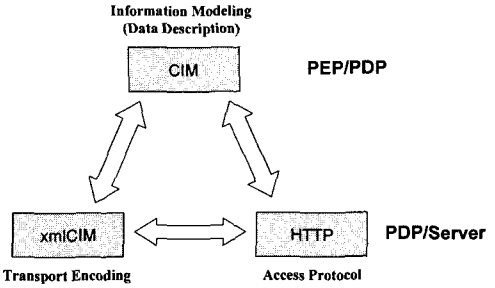

그림 4. WBEM 구성 기술 환경

WBEM 방식은 클라이언트 측면에서는 웹 브라우져를 이용하여 정보공유가 가능하며, 구현이 용이하지만, 중앙 집중식의 서버에 의존성 높으며, NE 간에 다양한 접속 프로토콜에 의해 접속됨으로서 NE 간의 일관성 있는 접속을 제시하지 못하고 있다. 또한 정책서버 간의 정보교환을 위한 별도의 관리 기능이 요구된다. 클라이언트와 서버 간의 접속은 특정 네트워크 정보인 경우에는 별도의 액세스 허가권이나 세션에 보안 기능을 두어 접속하는 방향으로 연구되고 있다.

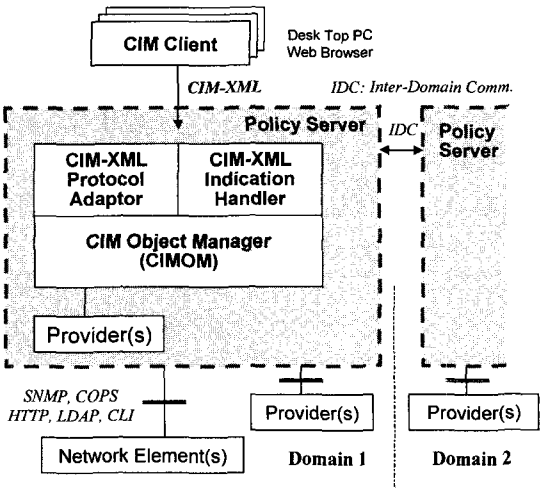

그림 5. WBEM 기능 구성

3.2 CORBA 기반의 정보공유

보안정책이나 관련 네트워크 정보를 공유하는 데 있어서 다양한 벤더의 NE와 정책서버 간의 연결, 국한된 관리영역, 다양한 접속 프로토콜을 야기시켰다. 이로서 PEP와 PDP에서 객체와 이들 정보 간에 접속 프로토콜이 상이하여 이를 위한 프로토콜 변환 모듈과 여러 인터페이스에 따른 다양한 NE를 접속하기에 한계성이 노출되었다.

한편 네트워크 정보는 객체 지향 기반으로 설계되었지만, 접속 프로토콜은 메시지 기반으로 운용됨에 따라 객체 지향 시스템의 성능을 발휘하지 못하였다. 그러나 TINA-C와 ITU-T TMN에서는 네트워크를 객체화로 모델링하고 있으며, 분산 시스템 환경에서 NE와 운용 관리 시스템 간의 분산 시스템 환경을 제공하여 네트워크 관리를 통합하고 있다. 이로서 NE와 관리 시스템 간의 분산 시스템 환경에서 객체화된 네트워크 정보를 공유하는 방향으로 관리되고 있다.

분산 시스템의 미들웨어에 해당하는 CORBA는 '98년 설립된 OMG(Object Management Group)에서 제정한 표준화 규격으로 서로 다른 운영체제나 프로그램 언어로 구현된 모듈 간에 상호 간의 운용이 가능하게 하는 일종의 소프트웨어 버스이다. '96년 CORBA 2.0 규격이 발표되면서 급속히 분산 컴퓨팅을 위한 응용 프로그램의 개발이 용이하여 하드웨어, 운영체제, 프로그램 언어와 무관하게 분산객체 간에 통신이 가능해졌다.

PBNM 시스템도 같은 맥락으로 볼 수 있다. 그림 5와 같이 Orchestram의 *Service Activator* 상용제품은 정책 서버, PMT, PDP, PEP에서 CORBA 환경을 기반으로 객체를 공유할 수 있도록 설계되었다. 특히 Orchestram은 CORBA 2.0 규격을 기반으로 *DPE2*(Distributed Policy Engine 2)라는 분산 시스템 환경을 자체 개발하여, 이를 정책서버와 PDP, PEP에 실장 하였다. 기존의 NE인 라우터, 방화벽, IDS, 스위치 등에 직접 실장을 하지 못하는 경우에는 별도의 디바이스 드라이버(프록시)를 두어 관장하도록 하였다. 또한 서비스 측면에서 제3의 서비스 사업자 혹은 응용 서비스 개발 위해서 CORBA-API를 정의하여 *DPE2* 환경에서 네트워크 정책 정보나 QoS 정보를 공유함으로서 신규 네트워크 서비스를 제공하도록 하였다.

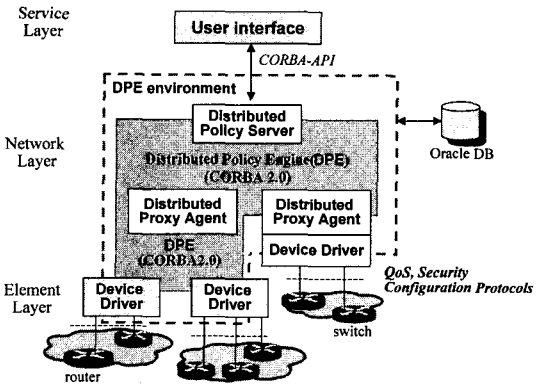

그림 6. CORBA 기반의 보안정책 관리 시스템

3.3 DEN(Directory Enable Network)

CORBA는 분산 시스템 환경에서 정보를 공유하는 기술인 반면에 DEN는 DMTF에서 디렉토리 안에 네트워크 요소 및 서비스를 표시하기 위한 표준 정보모델 개발을 목표로 한다. 따라서 DEN은 디렉토리와 네트워크가 통합되어, 네트워크 구성요소를 쉽게 디렉토리로 파악할 수 있다. 즉 사용자와 서버 혹은 프린터 등의 컴퓨팅 리소스 뿐 만이 아니라 네트워크 장치, 서비스 및 응용 프로그래밍을 비롯한 IP 주소, QoS, 보안 등의 정책에 관련된 정보를 저장 및 관리할 수 있게 한다. 이로서 디렉토리가 디렉토리 내의 모든 요소 간의 관계에 대한 정보를 수용한다는데 이점이 있다.

'97년 Microsoft와 Cisco에 의해 주장된 DEN을 근간으로 적용한 프로토콜인 LDAP은 X.500 디렉토리 서버스가 너무 방대하며, 복잡하고 구현하기

어렵다는 점 때문에 일반 PC에 적용하기가 힘듬에 따라, 이의 해결책을 모색하기 위하여 간단한 프로토콜에 의한 디렉토리 서비스를 IETF에 제정하였다. 결국 DEN를 네트워크 자원의 여러 정보를 디렉토리 구조로서 LDAP을 이용하여 표현함에 따라 데스크탑 PC에서도 적용이 가능하여 보안정책정보를 공유할 수 있다. 그러나 WBEM에서와 같이 DEN을 위한 별도의 정보모델이 요구된다. 현재 DMTF에서는 DEN를 위한 보안정책 정보모델을 개발하고 있다. 따라서 DEN은 디렉토리 서비스를 위한 객체 Class와 관련 Attribute를 별도로 정의한다. 그림 7은 X.500, CIM과 DEN의 정보모델에서 10개의 기본 Class를 보였다.

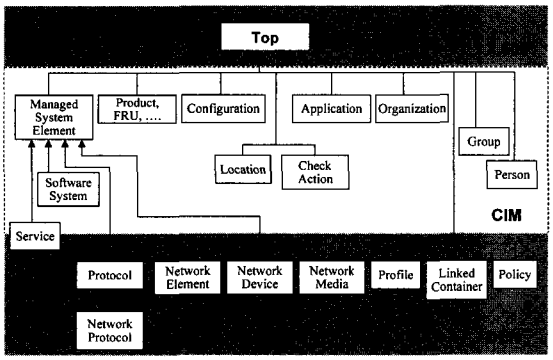

그림 7. DEN 시스템 구성도

4. 보안정책 관리 시스템

4.1 계층적 정보공유와 시스템 구조

정책 기반의 시스템에서 보안정책과 QoS 제공 정보를 공유하는 데 PEP와 PDP, 서로 다른 관리영역에서의 정책서버 간의 접속, 중앙집중식 정책서버 접속으로 구분된다. 또한 관리영역 측면에서는 동일 영역의 PEP와 PDP 레벨, 서로 다른 영역에서의 정책서버 레벨로 구분된다.

서비스 사업자나 통신사업자 측면에서 동일영역에서는 동일한 분산 시스템 환경이나 PDP 혹은 정책서버에 접속된 클라이언트 간에 정보공유가 가능하다. 그러나 다른 영역인 경우 사업자에 따른 보안정책 혹은 QoS 관련 정보를 공유하기 위해서는 기존의 분산처리 환경보다는 라우팅 프로토콜처럼 별도의 프로토콜(IDIP, AN-IDP 등)이나 분산 시스템 게이트웨이 등이 요구된다.

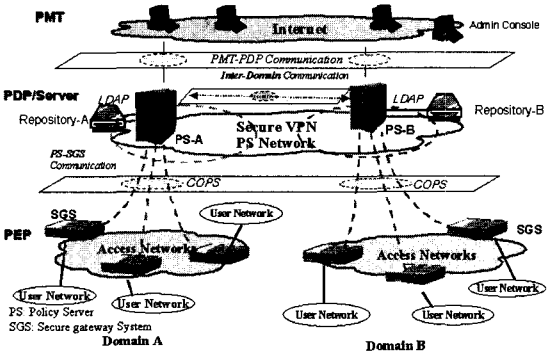

그림 8. 보안정책 관리 시스템 구성도

현재 사업자 혹은 상용 시스템 간의 상호 호환성 문제로 PDP와 PEP 간에 접속은 PBNM 소프트웨어 개발회사와 네트워크 구성장치 벤더들 간의 컨소시엄 형태로 해결하고 있으나, 앞으로 이들 간의 정보모델과 접속 프로토콜에 대한 표준화가 조속히 확정되어야 할 것으로 전망된다. 그러나 여러 NE를 적용하는 경우에는 그림 8과 같이 일정 영역에서 정책정보를 수집하여 이를 관장하는 정책서버와 다른 영역의 정책서버와 정보공유를 위한 간단한 메시지 기반의 프로토콜이 요구된다.

4.2 공유객체 접속을 위한 시스템 기능구조

PEP에서 보안 네트워크 관리를 위해서 DMTF 혹은 IETF에서 정의된 정책 정보모델을 구현한 경우, PEP 에이전트는 해당 보안정보를 정책서버로 전송한다. 현재 보안정책 정보모델을 표준화기관에서 연구를 수행하고 있지만, 보안정보모델과 관련 접속 프로토콜은 벤더들의 정책기반 관리 시스템을 비공개

로 벤더들 간의 공유한 정보모델과 접속 프로토콜을 사용하고 있다. PEP에 해당되는 라우터, 스위치, 방화벽, IDS 등의 NE들도 일부 PBNM 개발회사와 컨소시엄 혹은 협력지원 그룹으로서 몇 개의 제품만 기능이 수용되도록 개발하여 상용모델을 출시하고 있다.

앞장에서 언급한 바와 같이 현재 보안정책 정보공유를 위한 모델로 WBEM과 DEN 구조는 손쉽게 기존의 NE를 중심으로 수용이 가능하여 활발한 연구와 제품 개발이 이루어지고 있다. 그러나 통신 사업자의 마인드에 따라 분산 시스템 기술의 확산과 객체지향 설계에 따른 NE의 원활한 관리를 위해서는 CORBA와 같은 미들웨어로 정보를 공유하는 것이 최종 목표가 될 수 있다. 그러나 당분간 상호 시스템이 혼용되어 사용도록 그림 9와 같은 시스템으로 PEP와 PDP 간은 기존 접속 프로토콜을 제공하는 구조를 보인다. 그러나 Cisco의 Post Office, DARPA의 SLSS(Survivability of Large Scale Systems) 프로젝트인 IDIP(Intruder Detection and Isolation Protocol), FTN (Fault Tolerant Network)의 AN-IDR (Active Network-Intrusion Detection & Response)과 접속도 가능하도록 정책서버의 기능 확장성과 별도의 디바이스 접속을 위해서는 디바이스 프록시 구조 등이 검토되어야 한다.

정책서버와 관리자용 클라이언트 간에는 웹 기반 혹은 GUI 기반의 응용 소프트웨어로 분산 시스템 환경이나 인터넷을 통하여 접속된다. 그러나 이러한 연결접속에서 네트워크 관리정보 수집 및 관리를 위해서는 별도의 연결과 세션에 대한 IPSec, SSL 등의 보안이 요구된다.

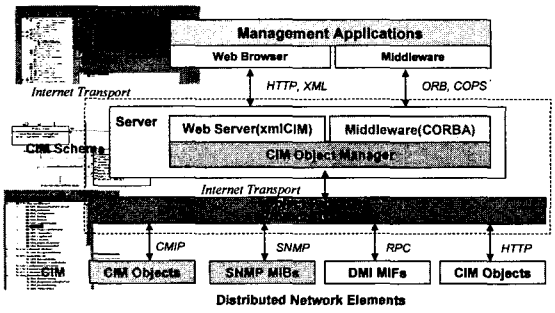

그림 9. 정보공유를 위한 시스템 접속 기능구조

V. 결론

정책 기반 시스템은 NE의 에이전트에서 수집된 정보를 정책규칙에 의거하여 원활하게 네트워크가 운용될 수 있도록 해야 한다. 이를 위해서는 실시간으로 PEP와 PDP 간의 정보 수집과 수집된 정보를 공유하여 정책서버에 원활한 관리가 요구된다.

본 논문에서는 PEP와 PDP 간의 보안정책정보를 효과적으로 공유하는 방안을 살펴보았고, 이를 위한 보안정책 정보공유 기능 구조를 시스템에 적용해 보았다.

앞으로 연구사항으로는 PEP와 PDP, 정책서버간의 정보공유를 위한 VPN 연결에 대한 보안, 정책서버 간의 정보공유를 위한 인터페이스, NE와 정책서버에 적용될 정책 기반의 보안 정보모델에 관한 연구가 필요하다.

참고문헌

[1] Dinesh C. Verna, "*Policy-Based Networking: Architecture and Algorithm*", New Rider, 2001.

[2] Stephen F Bush, et al, "*Active Networks and Active Network Management: A Proactive Management Framework*", Plenum, 2001.

[3] Curt Harler, "*Web-Based Network Management: Beyond the Browser*", Addition-Wiley, 1999.

[4] John Strassner, "*Directory Enabled Networks*", Macmillan Technical

Publishing, 1999.
[5] Chris Metz, "*IP QoS: Traveling in First Class on the Internet*", IEEE Internet Computing, March 1999.
[6] M. Stevens, "*Policy Framework*", Internet Draft, draft-ietf-policy-framework-05.txt, Sep 1999.
[7] B. Moore, et al., "*Policy Core Information Model-Version 1 Specification*", IETF RFC 3060, Feb 2000.
[8] B. Moore, et al., "*Policy Core Information Model Extensions*", Internet Draft, draft-ietf-policy-pcim-ext-02.txt, IETF, July 2001.
[9] DMTF Document, "*CIM Core Policy Model*", Version 2.6, DMTF, May 2001.
[10] IETF Policy Framework WG, *http://www.ietf.org/html.charters/policy-charter.html*, 2001.3.
[11] Orchestream, *http://www.orchstream.com*, 2001.
[12] DMTF, *http://www.dmtf.org*, 2002.
[13] IETF, *http://www.ietf.org/html_characters/policy-charter.html*, 2001.7.
[14] Check Point, *http://www.checkpoint.com*, 2001.
[15] Atsushi Tamamura, et al., "*Personalized Policy Management Architecture in Distributed Network*", IEICE Trans. Comm. Vol. E83-B, 2001.
[16] Alvin Tan and Alex Galis, "*Toward Policy-Based Management of Active Network*", DSOM-01, 2001.
[17] Oscar Diaz Alcantara, et al., "*QoS Policy Specification-A mapping from Ponder in the IETF*", DSOM-01, 2001.
[18] 손승원, "Active Security 기술발전 방향", Sigcom Review, Vol 1, No 1, 2000. 12.
[19] 장종수, 손승원, 신영석, "보안정책 기반의 보안 네트워크 기술동향", 인터넷정보학회지, 제1권 제2호, 한국인터넷학회, 2000. 12.

김 기 영

1988년 전남대학교 전산통계학과 이학사, 1993년 전남대학교 전산통계학과 석사, 2001년 충북대학교 대학원 컴퓨터공학과 박사, 1988년 2월~현재 한국전자통신연구원 선임연구원, 정보보호연구본부 보안게이트웨이연구팀, 관심분야 Protocol Engineering, Policy-Based Secure Routing, Network Security Architecture

장 종 수

1984년 경북대학교 공과대학 전자공학과 공학사, 1986년 경북대학교 대학원 전자공학과 석사, 2000년 충북대학교 대학원 컴퓨터공학과 박사, 1989년 7월~현재 한국전자통신연구원 책임연구원, 정보보호연구본부 보안게이트웨이연구팀 팀장

신 영 석

1982년 전북대학교 공과대학 전자공학과 공학사, 1984년 전북대학교 대학원 전자공학과 석사, 1993년 전북대학교 대학원 전자공학과 박사, 1984년~1998년 2월 한국전자통신연구원 선임연구원, 1993년~1994년 일본 NTT 통신망연구소 객원연구원, 1998년 3월~현재 호남대학교 정보통신공학부 조교수