主題

Policy기반 QoS+Security 지원 메커니즘

한국외국어대학교 정보통신공학과 정 일 영, 백 승 호,
한국전자통신연구원 장 종 수

차 례

요 약

네트워크 환경이 복잡해지고 제공되는 서비스 및 사용자의 요구들이 다양해짐에 따라 안정적이고 효율적인 환경을 유지하기 위한 운용관리는 점점 더 어려워지고 있다. 이와 관련하여 각 서비스 정보의 보안에 대한 필요성 및 중요성이 크게 논의되고 있다. 그러나 현재의 인터넷 구조에서 네트워킹의 보안과 QoS를 동시에 만족할 수 있는 방안은 거의 불가능한 상황이다. 즉, 현재의 정보통신 환경에서 보안 기능과 함께 차별화된 서비스의 제공이 절대적으로 필요하지만 이의 효과적인 제공 방안은 현실적으로 없다는 점이 본 논문과 관련된 연구의 주된 동기가 된다. 즉, 특별히 보안성이 요구되는 정보들 중에는 상당히 많은 부분이 서비스 QoS도 역시 요구하고 있다는 점이 정보 서비스에서 보안과 QoS를 분리하여 단순히 처리하는 것이 부적절하다는 점이다. 따라서 본 논문은 보안 기능과 QoS를 이용자 및 서비스의 요구에 따라 효율적으로 제공할 수 있는 환경의 구축 및 요구되는 주요 메커니즘을 제안하고자 한다. 그리고 Policy 기반의 Security+QoS 기능을 제공하는 통합 메커니즘에 대한 연구 결과를 소개한다.

1. 서 론

지금까지 정보통신 분야의 네트워크 보안을 위하여 장치 자체에 대한 침입방지, 네트워킹 관련 정보의 유출 및 해킹으로부터 보호하기 위한 방안에 집중적으로 연구 개발이 이루어진 것이 그 원인이 되고 있으며, 또 다른 사항은 네트워킹 보안에 대한 인식의 부족으로 이를 필요로 하는 이용자들의 요구가 그리 많지 않은 점도 또 다른 이유인 것으로 분석된다. 또 다른 사항을 분석하면 인터넷의 라우팅 기능이 매우 고속화

되고, 다양화되어서 라우터 혹은 네트워크 장치에서 보안 기능을 위한 알고리즘이 수행되는 데 상대적으로 많은 처리 지연이 발생하게 되고, 이를 적용하는 시도를 적극적으로 하지 않는다는 점 또한 다른 이유가 될 수 있다. 즉, 모든 네트워크 제어 정보들이 일률적으로 보안 메커니즘을 수용하게 되면 전체적인 네트워크 성능이 현저히 저하되기 때문에 쉽사리 이를 수용하지 못하는 점도 상당히 크다고 여겨진다.

이러한 상황 인식을 바탕으로 네트워크 장비 및 링크 등에서 장비 자체가 지니고 있는 자체 보안 기능을 미리 모니터링 하여 분석할 수 있고, 이를 바탕으로 보안 등급에 따른 라우팅 및 경로 설정이 이루어진다면 네트워킹 상에서의 정보들의 보안성에 대한 불안이 해결될 수 있을 것이다. 나아가 네트워킹 QoS까지 고려하여 라우팅 및 경로 설정이 이루어진다면 안전한 경로를 통하여 정보가 전달되는 보안 경로가 만들어지고 이를 이용자들이 필요에 따라 선택하여 사용할 수 있게 할 수 있을 것이다. 네트워크 차원에서 보안 기능이 이용자의 선택에 의하여 제공되는 보안 네트워킹이 제공되거나 네트워크 관리자의 제어 기능에 의하여 제공된다면 보안 기능을 수행하기 위하여 겪는 이용자의 서비스 성능의 불편함을 덜게 할 수 있다는 장점도 있다. 이를 이용자로 하여금 선택하게 하고, 이용자 혹은 네트워크 관리자는 차별화 된 보안 네트워킹 기능을 이용할 수 있게 하는 것은 고도 정보화 사회 구현을 위하여 아마 필수적인 사항이 될 것이다.

QoS 및 보안 라우팅을 위한 전체적인 네트워킹을 위하여 도입되는 Policy 기반의 시스템 구조는 먼저, 액세스하는 쪽에서의 액세스하는 쪽에서의 네트워킹 구조를 제시하면 다음 그림 1과 같다. 이 그림에서 PE (Provider Edge) 시스템에 라우팅을 위한 테이블이 1개만 있는 것이 아니라 독자적인 특성을 가진 가상의 네트워킹을 필요로 하는 이용자 그룹만을 위한 라우팅 테이블이 만들어진다. 이러한 가상 라우팅 메커니즘을 추가로 도입되어 복수개의 가상 라우팅이 물리적으로 하나인 네트워크에서 여러 개로 나누어진다. 이를 VRF (Virtual Routing and Forwarding) 테이블이라 한다. 이 VRF 테이블은 원래 각 VPN들을 위해 도입된 라우팅 테이블 개념이며, 물리적으로 하나인 네트워크에 가상의 사설망을 여러 개 만들어 이용자들에게 실제로 존재하는 사설망과 같은 기능을 가지게 하는 것이다. 최근에는 많은 관심의 대상이 되고 있는 NGN (Next Generation Network)의 효율적인 구축을 위하여 일부 도입되어 가상의 네트워크를 구성하는 라우팅 메커니즘이기도 하다. 이에 대한 구체적인 방안에 대해서는 본 논문에서 기술된다.

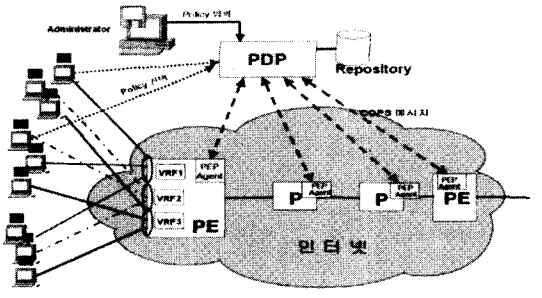

그림 1 Policy 기반의 가상 라우팅을 위한 네트워킹 구조

2. Policy 기반 가상네트워킹

2.1. Policy 기반 네트워킹의 프레임워크

IETF에서 Policy 프레임워크는 PEP(Policy Enforcement Point), PDP(Policy Decision Point), 관리 콘솔, 디렉토리로 구분하고 있다. PEP는 정책을 수행하는 장치로써 기본적으로 라우터, 스위치 등의 네트워크 요소를 나타내며,

PDP는 정책에 대한 결정을 하는 곳으로써 일반적으로 Policy Server(PS)로 사용한다. 이 네 가지 컴포넌트 들은 다음의 프로토콜과 언어를 사용하여 서로 연결된다. 그림 2는 IETF Policy Frame의 전체 구조를 나타낸다.

- COPS(Common Open Policy Protocol) 프로토콜: COPS 프로토콜은 PEP로부터 중앙 PS로 요청을 보내고, 그 후 보낸 요청에 대한 응답을 받을 때 사용된다. 또한 COPS는 정책 결정에 대해 동기화 기능을 제공하며, 확장기능과 TCP와 Keep-Alive 메시지를 사용하여 신뢰성을 제공한다.
- PDL(Policy Definition Language): PDL은 상태와 동작 룰에 따라 새로운 정책을 제작할 때 사용하는 언어이다. '정책을 생성할 때 어떤 언어를 사용할 것인가'에 관한 사항은 현재 표준화가 끝난 상태가 아니며, 기본적으로는 자체적인 policy 제작 언어를 사용해서 정책을 생성한다.
- LDAP(Lightweight Directory Access Protocol): X.500 Directory access protocol의 축소 기능을 가진 디렉토리 버전이며 디렉토리/Repository에서 사용자 정보 혹은 정책에 관한 정보를 검색하여 가져오는데 사용된다.

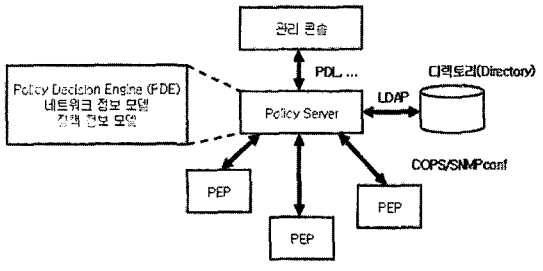

그림 2 Policy Server에서의 Framework

Policy Framework에서 중요한 이슈 중의 하나는 state transition이나 이벤트에 의해 어떤 방법을 통해 정책 룰이 실행되는지에 대한 사항이다. PDE(Policy Decision Engine)은 요청에 대한 사항을 처리한다. 예를 들어 RSVP에 COPS를 적용시키는 경우, PEP는 COPS 요청을 생성하여 PS에게 보내고 PS는 그에 대한 결과를 PEP로 리턴하여 그 정보를 기반으로 RSVP 패스 메시지를 거부하거나 받아들일 것이다. PDE는 요청을 받아들일 경우 그 요청에 해당하는 룰과 매칭되는 것이 있는지 찾기 위해 사용할 수 있는 정책 룰을 검색한다. RSVP path message와 RSVP reservation message가 RSVP 데몬에 도착하면 COPS 클라이언트 컴포넌트로 변환되어 COPS 요청을 PS에 있는 COPS server 모듈에게 보낸다. RSVP 관련 COPS 요청은 어플리케이션 룰에 따라 사용할 정책 룰을 결정하기 위해 PDE로 보내진다.

Policy Framework에서의 두 번째 중요한 이슈는 PS와 함께 다루어져야 할 것은 정책 정보를 표현하기 위해 사용되는 정보 모델이다. 정책 정보 모델은 IETF Policy working 그룹과 CIM Extension을 개발한 DMTF(Distributed Management Task Force)에서 공동으로 개발 중이다. IETF Policy Architecture에서 Policy Server에서는 정책 결정, 네트워크 정보 핸들링, 정책 정보 핸들링 등의 역할을 수행해야 한다. 이를 효과적으로 하기 위해 개념적 레벨에서의 구분이 필요하다.

2.2. Policy Core Information Model 구조

네트워크 정책을 기술하는 특정 언어를 정의하지 않고, 포괄적인 객체 지향 정보 모델을 정의하여 네트워크 정책의 특성을 표현하는 데, 여기에서 사용되는 PCIM(Policy Core Information Model)은CIM(Common Information Model)에서 확장된 형태이다.

PCIM 모델은 QoS를 제공하기 위한 방법을 제공하기 위해 접근 제어 정책, 관리 정책을 제

공한다. IETF의 PCIM모델은 비즈니스 정책을 하이 레벨 언어로 표현할 수 있게 하고 네트워크 토폴로지와 QoS 방법론을 접목시켜 새로운 형태의 정책 정보 모델을 정의하였다. 이는 서로 다른 네트워크 디바이스 설정을 매핑 시킬 수 있는 장점을 제공한다.

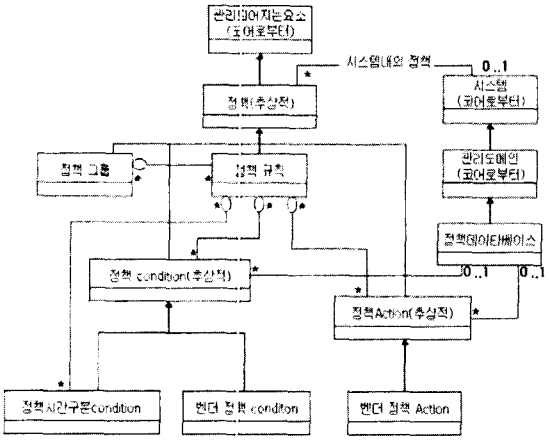

그림 3 Policy Core Information Model

그림 3은 PCIM에서 정의한 클래스와 그 각각에 관한 관계를 나타낸다. 정책 룰은 정책 그룹으로 그룹화 되어 정책을 정의하며 사용되는 어플리케이션에 따라 서로 관계가 형성된다. 여기서는 파라미터화 된 룰이나 정책 그룹에 대한 메커니즘은 나타나지 않고 개념적 레벨에서의 관계를 명시한다. 주지할 사항중의 하나는 action과 condition은 정책 데이터베이스(repository)에 서로 독립적으로 저장되고 많은 정책 룰에 의해 재사용된다는 점이다.

정책 룰은 우선순위를 두고 연관되어 룰의 충돌을 해소할 수 있다. 이러한 접근 방식은 규모가 큰 네트워크에서 서로 다른 관리자에 의해 서로 다른 여러 가지 룰이 지정되는 경우에 확장성을 제공하지 못한다. 정책 룰은 한 개 혹은 그 이상의 역할(role)에 의해 tag를 첨가할 수 있다. 여기서 역할이란 기능적 특성 혹은 리소스의 성능을 백본 인터페이스, 프레임 릴레이 인터페이스, BGP 가능 라우터, 웹서버, 파이어월 등에 적용할 수 있는 형태의 정책을 표현하는 의미로 사용된다.

IETF에서 제시한 정보 모델링 접근 방식의 장점은 이 모델을 쉽게 구조화된 명세와 매핑시킬 수 있다는 것이다. 즉 XML과 같은 언어를 사용하여 매핑을 시킬 경우 정책 분석과 정책에 대한 분배 등을 용이하게 할 수 있다는 것이 강점으로 작용한다. CIM모델과 XML 매핑은 현재 작업 중에 있으며 IETF는 PCIM과 LDAP을 사용한 디렉토리 내에서 구현될 수 있는 형태의 매핑을 정의하고 있다.

또 한가지 다른 접근 방식은 IETF의 rule 기반 접근방식을 사용하여 트래픽 제어를 지정하기 위해 특정 언어를 사용하는 것이다. 예를 들어 path-based policy language(PPL)을 들 수 있다.

2.3. COPS (Common Open Policy Service)

COPS(Common Open Policy Service)는 PDP(Policy Decision Point)와 클라이언트(PEP: Policy Enforcement Point) 사이에 정책 정보를 교환하기 위한 용도로 사용된다. PEP는 라우터혹은 그 밖의 IP를 핸들링 할 수 있는 디바이스가 되며 정책 기반 하에 데이터 플로우에 대한 입장(admission) 제어를 한다. PDP는 특정 데이터 플로우가 입장 가능한지 혹은 입장 가능하지 않은지를 결정하기 위해서 PEP를 포함하여 네트워크 도메인 내의 전부를 견지할 수 있어야 한다.

COPS 프로토콜은 클라이언트 서버 구조를 채택했으며 PDP가 서버로 동작하고 PEP가 클라이언트로 동작한다. 이 둘간에 데이터를 전송할 때는 TCP 연결을 사용하기 때문에 자체적으로 신뢰성을 제공하기 위한 기법이 필요하지 않다. 그리고 높은 레벨의 보안을 제공하기 위해서 HMAC 알고리즘을 이용하여 메시지에 보안 해

시 함수를 적용할 수 있다. 또 다른 방법으로는 COPS 정보를 전송할 때에 IP 패킷에 IPSEC을 적용하여 보호할 수 있다.

COPS는 매우 간단한 구조를 채택하고 있으며, 그 단순성으로 인해 쉽게 확장될 수 있고 여러 가지 폭넓은 환경에서 기능성을 제공한다. PEP는 요청의 형태로 메시지를 보내고, PDP에서 메시지를 받아서 처리한 후 그 결과가 다시 PEP로 전달되면 그에 따라 Update, 삭제 등의 기능을 수행한다. 이때 비 동기 방식으로 메시지가 전달되며 PEP로부터 온 요청 메시지에 대해 직접적으로 응답하지 않는다.

하나의 단일 PEP는 동일한 PDP에 대해 TCP 연결을 사용하여 동시에 여러 개의 COPS 세션을 활성화 시킬 수 있다. 이는 handles라는 고유 ID를 관련 메시지 속에 담아 보냄으로써 여러 개의 세션을 열더라도 서로 영향을 받지 않는다. 그리고 Handle은 각 PDP의 client-type에 대한 고유한 ID를 가진다. Client-type은 COPS 세션의 실제 사용을 지정하는데 사용되며, 새로운 client-type은 COPS 메시지를 핸들링하고 보내기 위한 방법을 지정하는데 사용된다. COPS에서는 정책을 전달하여 적용하기 위해 COPS-PR을 사용하며 이는 특정 client-type을 의미한다.]

COPS 프로토콜은 outsourcing과 provisioning인 서로 다른 두 개의 구조적 모델을 가지고 있다. Provisioning 모델에서는 PDP는 이벤트를 받아들이고, 요구되지 않은 결정(unsolicited decision)을 PEP에게 전달한다. Provisioning 모델에서는 PEP이벤트와 PDP 결정 간에서로 상관관계가 존재하지 않는다. PDP는 하나 혹은 그 이상의 PEP의 설정의 결과에 따른 이벤트에 대한 반응하며, 이벤트는 사용자, PEP 이벤트, 혹은 이 둘간의 조합에 의해 요구된 네트워크 리소스 예약 등이 될 수 있다. COPS가 policy provisioning을 제공하기 위해 COPS-PR을 사용하며 이는 정책 타입에 영향을 받지 않는 독립적인 특성을 지니고 있으며, QoS, VPN, 보안에 관계된 데이터를 전달한다. Outsourcing 모델은 네트워크로부터 데이터 플로우의 입장이나 묵시적인 방법을 통해서 이벤트가 생겨나면 해당 이벤트를 PDP로 보내어PDP에서 정책 결정을 하고 그 결과를 PEP로 전송하는 방식이다.

3. Policy 기반 QoS 라우팅 모델

3.1. Policy Server와 QoS Policy Manager 와의 연동

그림 4는 개념적 모델에서 QoS Policy 데이터베이스를 핸들링 하기 위해 세 가지 기능을 제공하는 QoS Policy Manager를 도입하여 QoS 정책 데이터베이스를 각 Edge SW에 전달하는 것을 보인다. 각 Policy 데이터베이스에 저장/로드시킬 때에Policy Server가 명령을 전달한다. 그림 4는 VPN형태로 연결되는 경우에서 가용한 네트워크 리소스가 VPN 서비스 관리 시스템에 전달되어 되고, 각 도메인에서 QoS 정책 데이터베이스에 있는 정보를 이용하여 필요한 조처를 처리하게 되는 예를 나타내고 있다. 즉, VPN 리소스 관리, 연결 제어 등을 지원할 수 있는 네트워킹 관리 모형을 모델링한 것이다.

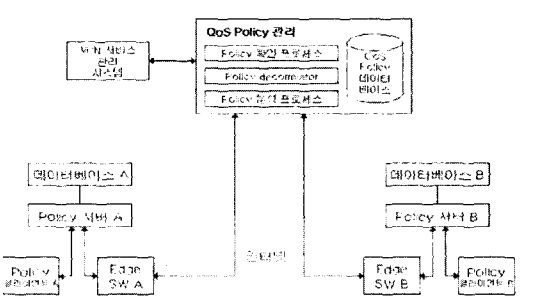

그림 4 Policy 서버를 이용한 QoS Policy 관리의 연동 구조의 예

3.2. Policy based Network의 정보 모델과 정책 추상화 방안

IP 네트워크에서 QoS를 제공하기 위한 정책 기반 네트워크 도입 방법에 추가적으로 정책 기반 네트워크에서 사용될 정책에 대한 정의가 필요하다. '정책'을 활성화된 개체로 보거나, 분산 소프트웨어의 실행 형태를 취한다고 할 때 복잡성을 제어하기 위해 정책 이라는 것을 두 가지 관점에서 살펴볼 필요성이 있다.

첫번째 접근 방법은 추상적 계층 구조를 사용하는 것이다. 정책은 추상의 정도에 따라 규정되며, 이런 방식을 통해 몇몇의 추상적 정책으로부터 구체적인 정책이 생성된다. 이때 추상화 정책을 파라미터화하여 사용하고 두 번째는 룰 기반 해석을 통해 구체화된 정책을 이끌어내는 방식이다. '정책'을 디자인 할 때 실제로 적용할 수 있는 실제적인 룰로 일반화 시키고, 추상화 시키는 방안이다. 추상화 된 개체들의 대표작인 기능은 다음과 같다.

- Requester: 사용자 혹은 어플리케이션
- Resource: 네트워크 리소스
- Identity of policy source
- Enabling conditions.
- QoS Specification
- Priority specification

정책 추상화는 정보에 대한 분류를 시작으로 처리 기능이 시작되며, 전 과정을 경유하게 되면 최종적으로 필요한 룰이 생성된다. 추상화에서부터 나온 세부적인 정책은 정보에 대한 애매모호함이 없어야 된다. 이같이 추상화된 정책 모델에서 다시 세부적인 정책을 생성시킬 때에 일반적으로 계층적 구조를 가지게 된다.

3.3. PDP와 ER간의 자원 예약을 위한 협상 모델

PDP는 네트워크 자원을 위하여 ER1 과 ER2 간의 RSP 프로토콜이 적용되는 과정에 관여하여 보다 효율적인 자원 예약을 하도록 한다. 그림 5의 (가)에서 보듯이 ER2에 의해 RESV 메시지가 도착하면, ER1은 PDP/BB에 COPS 프로토콜을 이용하여 COPS REQ 메시지를 보내어 자원 예약 요청에 대한 문의를 하여 네트워크 장치간의 자원에 대한 Decision 정보를 요청한다. 이에 대하여 PDP/BB는 요청한 자원이 가용하면 이에 대한 가능 여부에 대한 회신을 하여 준다. 이를 바탕으로 ER1은 RSVP의 프로토콜에 의해 정상적인 자원예약 절차를 거쳐서 요청한 자원을 예약하게 된다.

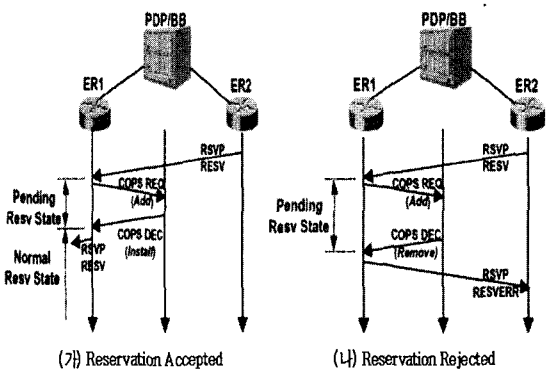

그림 5 ER1과 ER2의 PDP에 의한 자원예약 협상 절차

그리고 (나)에서 보는 바와 같이 자원 요청 메시지가 도착 하여서 이에 대한 문의를 PDP/BB에 문의한 결과 요구하는 네트워크 자원이 충분치 않을 경우에 PDP/BB는 Remove 메시지를 보내어 거부의 의미를 전달한다. 이를 받은ER1은 ER2에게 RESVERR 메시지를 보내어 요청한 자원에 대한 예약 요청이 이루어지지 못함을 알리게 되며, ER2는 필요에 따라 다른RESV 값을 이용하여 재협상을 시도하게 된다.

4. Security 제어 모델

4.1. Security특성 정보의 파라미터화 및 적용 모델

정책 기반 네트워크는 특정 룰과 정책에 따라서 네트워크가 동작하게 된다. 이때에 네트워크가 지정된 룰과 정책에 따라 적절하게 수행되게 하려면 보안측면에 대한 사항들도 매우 중요하게 유지 되어야 한다. 어떤 개인이나 단체가 악의로 네트워크의 자원, 특히 네트워크의 동작에 있어서 두뇌 역할을 하는 정책(policy)에 대한 것들이 공격하여 기존의 룰을 깨고 네트워크에 마비를 초래하면 정책 기반 네트워크를 도입했을 때의 장점보다 더욱 심각한 손해를 입게 될 것이다. 이러한 이유로 네트워크에서의 보안은 무척 중요하다고 할 수 있다.

따라서 정책 기반 네트워크에서는 현재의 네트워크 개념에서 좀더 향상하여 여러 가지 요구사항들에 부합하기 위해 네트워크의 동작 형태가 단편적이지 않고, 룰에 따라서 적용되도록 하여야 할 것이다. 이러한 관점에서 견지할 때 end-to-end 형태의 보안이 아닌 네트워크 디바이스 각자에 대한 보안 레벨을 알 수 있다면 정책 기반 네트워크에서 정책 결정 시에 보안 레벨이 높은 디바이스와 보안 레벨이 낮은 디바이스를 적절히 혼합하여 룰을 적용시킬 수 있을 것이다. 물론 보안 레벨이 높은 디바이스라 하더라도 경우에 따라서 보안 레벨을 낮추고 동작 시킬 수 있을 것이다. 즉 기존에는 네트워크 디바이스 각각의 보안 레벨이 고정되어 있었다면, 정책 기반 네트워크에서는 네트워크 디바이스 각각에 대한 보안 레벨이 고정되지 않고 디바이스 각자가 가진 보안 능력에 따라 적절하게 동작할 수 있다.

다시 말하면, 정책 기반 네트워크에서 정책을 결정할 때에 정책을 네트워크 장비에까지 영향을 미칠 수 있게 된다는 것이다. 이렇게 하기 위해서 네트워크 디바이스에 대한 보안 등급 정보를 취득해야 한다. 취득한 정보를 토대로 네트워크의 정책을 설정할 수 있기 때문이다. 네트워크 보안 레벨에 대한 이상적인 방법은 품질 표시 개념과 동일하게 네트워크 디바이스 자체에 대한 보안 레벨 등급을 표시해서 디바이스가 출시되는 것이다. 그러나 현재는 이같이 되어있지 않기 때문에 좀 우회적으로 네트워크 디바이스에 대한 보안 등급 정보를 수집할 필요가 있다.

4.2. Security 및 QoS 정보의 Decision Tree 구성 모델

Security 정보 수집을 위하여 사용되는 방법은 여러 가지가 있다. 보안성을 구분하기 위하여 필요한 정보를 추출하며, 수집된 정보는 앞서 기술한 분류 방법 및 체계를 적용하여 트리 구조를 만든다. 먼저 네트워크 장비 및 라우터의 보안 관련 정보를 수비하기 위하여 외부에 별도의 서버를 두어 이 서버로 하여금 보안 관련 정보를 주기적으로 수집하도록 하는 방안이 있고, 장치 내부에서 지니고 있는 특성을 보고하는 방식을 택하기도 한다. 그리고 해당 네트워크 장치의 특성을 off-line으로 검증하여 보안을 위한 장치 기능을 사전에 검증하여 보안 기능 등급을 분류하기도 한다. 이 중에서 정보 수집에 어려움이 있는 데이터는 네트워크 환경 및 사용되는 주변 환경에 따라 네트워크 보안에 관련된 변수가 바뀌는 경우이다. 이 경우는 주기적으로 네트워크에서 모니터링하여 이를 반영하여야 하는 데, 이것이 네트워크 보안의 전체적인 특성에 중요한 변수가 되기도 하므로 보안 등급을 결정할 때 신중히 고려되어야 할 사항이다.

인터넷 네트워크 보안성의 정도를 분석하기

위하여 네트워크상에 존재하는 시스템 및 서비스들의 다음 사항에 대하여 세부 정보를 수집한다.

- 보안 취약성 평가: 취약점들에 대한 정밀 조사 및 확인을 통해 보안상의 허점들을 가려낸다.
- 위험 관리: 혁신적인 데이터 브라우징 기술을 통해 취약성 데이터의 효율적인 관리를 가능케 한다.
- 의사결정 지원: 포괄적인 보고 및 챠트들을 통해 결과를 전달하며, 조직의 보안 상태 개선을 위허 효과적인 의사결정을 내린다.
- 보안 정책 검증: 보안 장치의 설치와 인증시에 이용될 수 있는 유효한 보안 정책들을 정의하고 시행한다.

그리고 각 라우터에서 보안에 관련된 정보를 취득하여 분석 한 후에 해당 라우터가 제공할 수 있는 수준의 보안 레벨을 표시하기 위해 각 라우터에 대해 보안 등급을 지정해야 한다. 이때 라우터의 보안에 관련된 사항들은 단지 네트워크 혹은 네트워크장치가 지니고 있는 환경 및 관련 파라미터를 이용하여 Security Level이 분별 될 것이다. 이를 위하여 보안 정보에 관한 구조체 타입으로 Security Information Base(SIB)를 정의하여 보안 항목의 지정과 보안 레벨을 명시할 수 있다. 보안 정보에 대한 구조를 정의하기 위해 간략하게 세 가지 항목으로 구분할 수 있다. Exploit range, Vulnerability Type, Exposed component type 등으로 분류되며 Vulnerability Type의 하부 항목으로 Vulnerability consequence가 존재한다. 위 사항들을 고려하여 라우터의 Security 등급 평가를 위하여 Security Information Base (SIB)를 구축하여야 하는데, 이를 본 논문에서는 검토 분석하여 기본 구조를 다음 그림 6과 같이 모델을 구성한다.

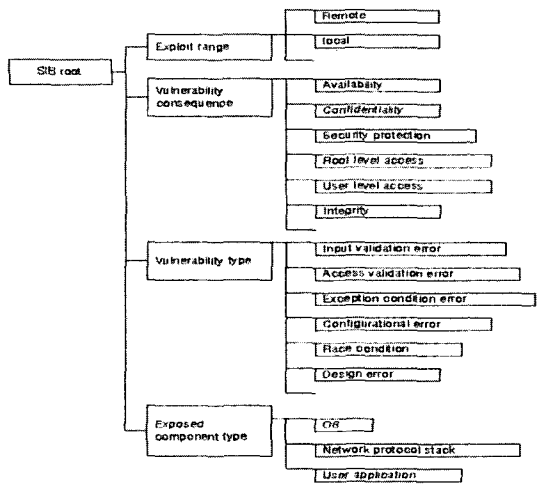

그림 6 라우터의 Security 등급 평가를 위한 Security Information Base Tree 구조

그리고 Security 등급에 대한 구분에서 단순히 라우터 및 네트워크 장비들의 내재요소 및 특성 그리고 주변환경 등을 이용하는 것 만으로는 부족하다. 왜냐하면 이용 및Administrator의 요구사항 및 판단에 의해서 변경되고, 그 중요도가 상황에 따라 변할 수 있기 때문이다. 따라서 이용자 및 Administrator의 policy가 방영되는 SIB가 필요하다. 이를 위하여 본 연구에서는 policy 반영을 위한 Security Policy 적용 체계도를 다음 그림 7과 같은 체계를 가진 모델을 개발하였다.

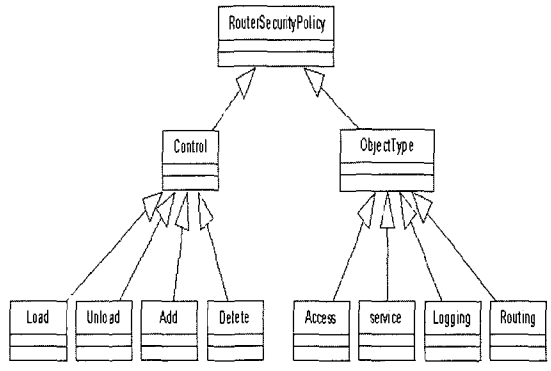

그림 7 Security Policy 적용 흐름 및 체계도 모델

5. Differentiated Securit+QoS를 위한 라우팅 알고리즘

5.1. Secure Routing 등급을 위한 VRF 기능

VPN의 기능 구조에서 PE는 CE 라우터들에 연결된 인터페이스를 가진 VRF와 Global 라우팅 테이블로 구성된다. VPN 라우팅은 BGP mesh에 연결된 PE 라우터들 간에 설정되고 MP-BGP는 VPNv4 prefixes와 VPN 레이블, next_hop 주소 그리고 PE 라우터들 사이의 route target(tag)를 전달한다. PE 라우터는 적절한 VRF에 대한 import/exports VPNv4 prefixes에 대한 필터를 사용한다. 이 때 적용되는 라우팅 및 Forwarding에 대한 개념은 다음 그림과 같다.

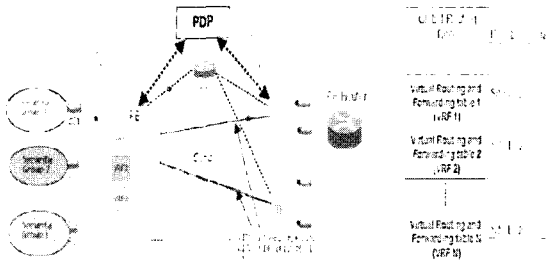

그림 8 PE에서 VRF 적용에 의한 차별화 된 라우팅 기능 모델

BGP VPN 구조에서의 주요 특징은 VRF(VPN Routing and Forwarding table)라 불리는 요소이다. VRF는 PE 라우터에서 routing 및 forwarding table을 해당되는 특정 VPN에만 한정된 라우팅 테이블을 만들고, 이를 통하여 forwarding 하는 데 사용하는 라우팅 테이블이다. 따라서 VRF는 개인적이거나, 같은 종류의 VPN 혹은 같은 서비스를 위한 VPN을 특성에 맞도록 효과적으로 라우팅하는 데 이용된다는 점으로부터 현재 많이 활용하려는 움직임이 다양한 형태로 나타나고 있다. PE 라우터에 작성된 VRF 라우팅 테이블은 사전에 협의에 의하여 상호 연계 되어 있는 다른 VPN들과 라우팅이 이루어져 상호 연결된다. 따라서 특정 VPN에 속해 있는 이용자 혹은 서비스들의 모든 라우팅 정보는 해당 VRF에 등록되어 있으며, 이것도 주기적으로 라우팅 기능에 의하여 update 된다. 해당 VPN 사이트를 통해 전달되는 모든 패킷들은 같은 VRF에서 라우팅 정보를 찾아서 라우팅 되고 전달된다. 일반적인 경우를 살펴보면, PE-CE 접속회선은 해당되는 하나의 VRF에 정해진 정보에 의하여 연결되어 있다. IP 패킷이 특별 접속회선으로 수신 되면, 목적지 IP주소는 연결된 VRF에서 찾게 된다. 그 lookup의 결과는 패킷의 라우팅 방법 결정에 사용되며, VRF는 "ingress VRF" 라고 알려진 특정 패킷의 라우팅을 위해서 패킷의 Ingress PE에서 사용된다. 만약 IP 패킷이 다른 어느 VRF와도 연결되지 않은 접속회선상에 도착된다면, 그 패킷의 목적지 주소는 디폴트 포워딩 테이블에서 찾게 되고, 그 패킷은 기존의 라우팅 메커니즘에 따라서 라우팅 된다. 디폴트 포워딩 테이블에 의해서 전달된 패킷들은 이웃 P 또는 PE 뿐만 아니라 VRF와 연결되지 않았던 일반 이용자 접속회선에 의해 패킷이 전달된다. 좀더 구체적으로 기술하면, "일반 경로들"이 적용되는 것은 디폴트 포워딩 테이블에 의해서 경로가 search 되며, "사설 경로들"에 의해 연결이 이루어지도록 라우팅 테이블을 관리하고 제어하는 메커니즘을 VRF 메커니즘이다.

5.2. Differentiated Security+QoS를 위한 Virtual 라우팅 모델

VRF에 의하여Virtual Routing 기능에 의한 VR (Virtual Router)가 구성되는 네트워킹 시나

리오를 그림 9에서 기술하고 있다.

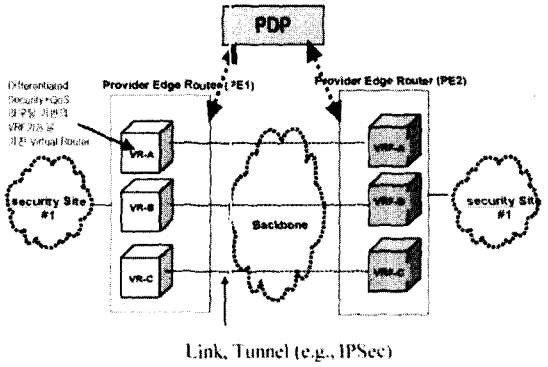

그림 9 Seciurity 레벨 와 PE-백본망-PE 에 의해 VPN 혹은VR 구성

그림 9는 양단에 PE 라우터가 있고 그 사이에 백본망이 있어서 Security 사이트 여러개가 단일의 PE에 여러 개의 복수개의 등급을 가진 Security site 사이트들이 연결되어 가상의 Security 등그에 따른 망이 존재하게 되는 경우이다. 위의 두가지 접근 방안은 네트워크의 사용용도에 따라 선택적으로 사용될 수 있으며, DSQ 라우팅 서비스의 망 구조 및 특성이 다양하게 달라질 수 있다.

5.3. Differentiated Security+QoS 라우팅 체계 도입

DSQ 라우팅은 앞서 기술된 바와 같이 Security 등급에 따라 구분된 VRF (Virtual Routing and Forwarding) 메커니즘에 따라 라우팅 테이블 그룹을 만들고, 만들어진 VRF 테이블 그룹 내에서 라우팅 알고리즘이 적용된다. Diferentiated Secure+QoS 라우팅은 PDP, SIB 및 PEP Agent와의 정보공유, 정보 교환, Security 라우팅 정보 배급에 대한 사항이 이루어지는 과정에 대한 알고리즘이다. 이를 위하여 PDP 에서는 다음과 같은 절차를 통하여 각 PEP agent로부터 Security 정보를 수집하고 분석한다.

- PDP는 COPS 프로토콜 메시지에 의거하여 SSA (Security State Advertisement) 메시지를 생성, 각 PEP agent에 전달. 생성된 SSA 메시지는 PEP Agent에 의하여 수신된다.
- 초기 단계에 만들어진SIB (Security Information Base)는 주기적으로 PEP Agent로부터 수집되는 Security 정보를 통해 cost table을 작성, 이는 PDP에 의하여 작성되어 PEP Agent에 전달된다.
- SSA 메시지를 테이블에 의거하여 PEP Agent는 패킷 전달 경로 테이블 (FIB: Forwarding Information Table) 을 만들어 주기적인 update를 수행한다. 이전에 PDP는 SSA의 내용을 Update 하게 되는 데, 추가 혹은 변경된 사항만 전파하는 summary-SSA를 전파 하고 있다. 이는 OSPF에서와 같이 전체 SIB 내용을 메시지를 전파하는 것이 아니라 summary-SSA를 전파하여 교환되는 메시지 트래픽을 최소화 한다.

Differentiated Security+QoS 라우팅 알고리즘을 적용하는 네트워크가 확대되어 여러 개의 PDP가 존재하는 네트워크로 발전하였을 경우에 복수개의 PDP로부터 SSA 정보를 받아서 처리하는 과정이 필요하다. 이러한 구조에서 복수개의 PDP로부터 받은 Inter-AS간의 SSA 메시지를 이용하여 PEP Agent는 경로 테이블을 작성한다.

Differentiated Security+QoS 라우팅 알고리즘에 대한 세부적인 내용에 대해서는 본 논문에서 기술하지 않고, 다음 단계의 논문에서 구체적인 세부 사항이 기술될 것이다.

5.4. Security Group에 대한 Addressing 방법

Security Group (SG) 주소는 VPN 메커니즘을

그대로 사용하기 때문에 12 byte로 구성되며, 8 byte 'Route Distinguisher(RD)"와 4 byte의 IPv4 주소로 구성 된다. 만일 두 개의 VPN이 같은IPv4 prefix를 사용한다면, PE는 서로 다른 RD를 사용하여 고유의 VPN-IPv4 prefix로 이들을 구별하게 된다. 즉, 같은 주소가 두개의 다른 VPN들에서 사용 될 경우, 각 VPN을 위해 각기 다른 경로로의 인스톨을 가능하게 해주게 된다.

PE 라우터들 상에서 Routing Differentiater (RD)를 설정하여 Security Group을 만들고, 같은 SG (Security Group: 예, VPN) 안의 모든 경로들의 동일한 RD의 사용은 요구 되지 않는다. 하나의 SG 에서의 각각의 VRF는 고유의 RD를 사용할 수 있다. 어쨌든, 서비스 프로바이더는 각 RD가 전체적으로 유일하다는 것을 보장해야 한다. 때문에 RD를 세팅할 때, 사설 자치 시스템 번호나 사설 IP 주소의 사용은 피해져야 한다. 그리고 글로벌의 고유 RD는 각각의 서비스 프로바이더가 자신의 주소 영역을 관리하고, 다른 서비스 프로바이더에 의해 만들어진 RD의 할당에 충돌이 없는 고유의 글로벌한 SG-IPv4 주소를 만들 수 있는 메커니즘을 제공한다.

6. 결 론

현재 인터넷에서 서비스되고 있는 정보의 종류는 매우 다양하고, 각 서비스 정보의 보안에 대한 필요성 및 중요성도 여러 가지로 구분될 수 있다. 그리고 인터넷에서 사용되고 있는 장비들도 각 장비가 지니고 있는 특성 및 기능에 따라 제공되는 보안 기능도 각양각색이다. 또한 보안성 유지를 위해 중점적으로 제공되는 장치의 자체 기능 혹은 네트워킹 기능에서 제공되는 보안 기능도 각기 다른 특성을 지니고 있다. 그리고 네트워킹에서 보안을 고려할 때 가장 중요하게 여기고 있는 것은 보안 기능의 추가로 말미암아 네트워킹 성능 혹은 기능이 저하될지도 모른다는 우려가 네트워크 장치들에 적극적인 보안 기능의 추가에 상당한 제동이 걸리고 있다고 보인다. 그러나 특별한 보안성이 요구되는 정보들에 대해서는 보안 기능이 잘 갖춰진 시스템 및 장치들을 경유하게 함으로써 Secure Networking 기능을 지니도록 하며, 이를 통하여 보안성이 유지된 네트워크를 구축하도록 하는 것이 본 논문의 주요 핵심 사항이다.

이를 위하여 본 논문에서는 Differentiated Security+QoS 라우팅 알고리즘을 연구 개발하였다. 그러나 본 논문에서는 Architectural Model을 중점으로 제시하였다. 본 논문에서 얻은 주요 결과는 정보의 중요도에 따라 정보가 전달되는 루트를 차별화하고, 이에 적용되는 보안 레벨은 이용자로 하여금 선택할 수 있도록 하여 다양한 인터넷 네트워크 서비스 기능을 이용할 수 있도록 할 것이다. 나아가, 고도의 "Security+QoS"가 보장되는 네트워크 기능을 가진 네트워크로 발전하게 될 것이다.

본 논문에서 기술한 라우팅 메커니즘을 통하여 인터넷에서 Security+ QoS를 동시에 얻을 수 있는 라우팅 알고리즘으로 확대 발전할 수 있을 것으로 사료되는 만큼 구체적인 연구 개발이 요구된다.

참고문헌

[1] Jie Yang and Symeon Papavassiliou, Improving Network Security by Multipath Traffic Dispersion, IEEE ICC 2001

[2] A. Campbell, K. Hahrstedt, "Building QoS into Distributed Systems",

Chapman and Hall, 1997
[3] S. Kent, R. Atkinson "Security Architecture for the Internet Protocol" RFC2401, November 1998
[4] S. Herzog Ed. J. Boyle, R. Cohen, D. Durham, R. Rajan, A. Sastry "COPS usage for RSVP" RFC2749, January 2000
[5] B.Moore et. Al, "Policy Core Information Model specification", IETF RFC3060, Feb. 2001.
[6] D. Durham, Ed, J.Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry "COPS Usage for Policy Provisioning (COPS-PR)" RFC3084, March 2001
[7] "Policy-based Network Management", Network computer Magazine, Dec. 1999.
[8] Steven L. Shaffer, Alan R. Simon "Network Security" AP Professional
[9] Simth, B.R, Murphy, S., and Garcia-Luna-aceves, J.J., "Securing Distance Vector Routing Protocols", Symposium on Network and Distributed System Security, Feb 1997.
[10] Tsung-Li Wu, S. Flix Wu and Feng-Min Gong, "Securring QoS: Threat to RSVP Message and their Countermeasure" Technical Report of NCSU, December 1999