主題

안전한 정보보호 인프라 제공을 위한 글로벌 네트워크 보안제어 프레임워크

장종수, 김기영, 류걸우

차 례

1. 서 론

인터넷은 가상생활환경의 제공과 정보공유 환경의 제공, 가상 업무환경의 제공 등과 같은 생활의 편의성을 제공하고 있지만 누구나 쉽게 접근할 수 있는 개방망 환경으로 인한 해킹, 바이러스 유포, 지적 재산권의 침해, 사이버 범죄에의 이용 등과 같은 정보화 역기능의 위협도 만만치 않은 것이 현실이다. 이러한 사이버공격은 더욱 분산반사서비스거부(DRDoS: Distributed Reflected Denial of Service)공격과 같이 지능화, 님다바이러스와 같이 웜바이러스내에 악성코드를 심는 통합화, 개별시스템에 대한 공격에서 네트워크 또는 서비스를 공격대상으로 하는 대규모화, 자동화된 공격도구를 이용한 자동화 및 대중화, 분산서비스거부(DdoS: Distributed Denial of Service)공격과 같은 분산화 및 트로이 목마와 같은 은닉화의 특성을 나타내고 있다.

정보통신환경 변화에 따라 개별 보안기능별 제품에서 방화벽+VPN(Virtual Private Network), IPS(Internet Protection System)와 같은 통합보안 형태의 제품으로 발전하고 있고, 네트워크 차원의 정보보호 서비스의 중요성이 증가하여 네트워크 침입탐지시스템 및 네트워크 바이러스 백신 등과 같은 제품들이 등장하고 있으며, 방화벽, IDS와 같은 방어적인 정보보호 제품에서 IPS와 같은 능동적인 정보보호 제품으로 발전하고 있다. 각 보안제품은 성능면에서도 수백 Mbps에서 기가급을 처리할 수 있도록 진화하고 있지만 개별 시스템 단위의 보안기능의 한계가 존재한다. 이러한 문제를 해결하기 위하여 네트워크 내에 산재해 있는 보안제품들을 효율적으로 통합 관리하여 관리비용 절감, 안정적 보안환경 유지, 운영의 편이성 제공 등을 얻기 위한 통합보안관리 솔루션인 ESM(Enterprise Security Management)이 보안시장에서 각광을 받았다.

그러나, 트래픽의 과도한 증가와 다양한 공격유형에 보다 효율적으로 침입대응하기 위해서는 현재의 지역적 보안환경을 광역망 또는 백본망 환경으로 확장 적용하기 위한 글로벌 네트워크 보안제어 프레임

워크 기술이 필요하다. 지역망의 경우는 자신의 입력 트래픽의 분석에 주력하지만 광역망의 경우는 각 지역망의 출력 트래픽들을 종합 분석하고 망의 구성정보, 상태정보, 주요 관리요소 정보 및 트래픽 통계정보 등과 연계한 다단계 분석을 통한 침입예측 및 환경에 적합한 대응정책의 결정, 인가가 가능하게 될 것이다. 이를 위해서는 고속의 센서, 분석엔진, 트래픽 측정엔진 등의 개발이 필요하며, 이들이 제공하는 정보를 축약하기 위한 기법의 개발과 이들을 전달하기 위한 프로토콜의 표준화, 인접 영역과의 보안제어를 위한 협력 메커니즘의 수립, 계층적인 침입분석 기법의 개발, 종합적인 침입대응 시나리오의 정의, 사용자의 요구에 따른 차별화된 보안서비스 품질을 제공하기 위한 차등보안서비스 개발, 효율적인 관리를 위한 공통정보모델링 등이 필요하다.

이를 효과적으로 관리하기 위해 보안관리 프레임워크 구조로는 IETF 차세대 인터넷의 서비스 품질 보장을 위해 정의하고 있는 정책 프레임워크를 따라 각 보안정책 도메인 관리를 위한 보안정책서버를 두고, 각 보안정책 도메인은 사이버공격 분석 및 이벤트정보 수집을 위한 멀티에이전트들을 분산 구성한다. 분산관리객체를 효율적으로 관리하기 위해 보안관리정책 공통정보 모델을 정의하여 관리자의 운용의 편이성과 체계적 관리가 가능하게 하며, 보안정책서버와 에이전트들간의 정보전달을 위한 보안정책정보 전달 프로토콜과 보안관리메커니즘을 정의한다. 역할기반의 침입분석과 대응 방법의 소개와 차세대인터넷 환경에 따른 사용자요구기반의 차별화된 네트워크 보안서비스 제공방안을 소개한다.

Ⅱ. 기존의 보안 서비스

현재 제공되고 있는 보안 서비스는 보안사고에 대한 예방과 탐지 및 보안관리를 대행하는 통합 서비스로 일반적으로 고객사의 컴퓨터와 네트워크 장비에 대한 침입 탐지 및 역추적을 중앙에서 감시 통제하는 서비스를 말한다. 일반적으로 기업의 보안 역량의 진단 및 대책 수립, 보안시스템 구축, 24시간 관리 및 보안사고에 대한 실시간 대응, 정보 재해복구 지원 및 보안교육과 모의 해킹, 컨설팅에 이르는 광범위한 서비스를 제공하는 것을 목표로 하고 있다.

이러한 보안 서비스의 종류는 대체로 4가지로 분

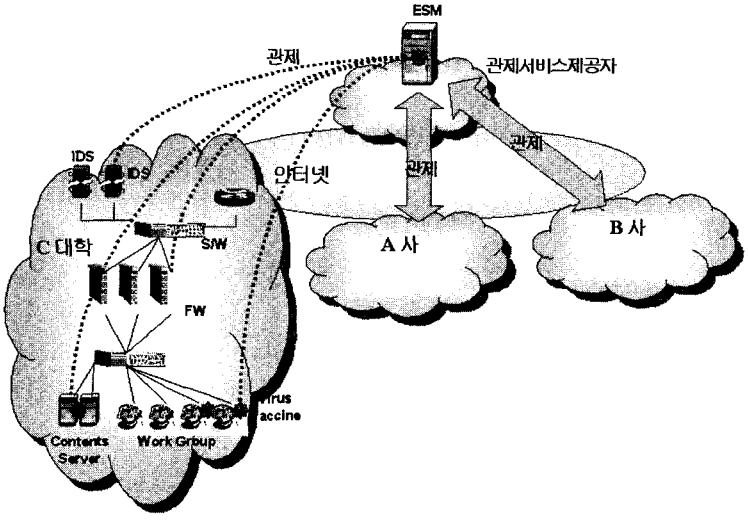


그림 1. 보안관제 서비스 개념도

류하여 정의할 수 있다.

1. 보안 호스팅 서비스 : 고객 시스템과 네트워크의 보안을 위해 서버의 보안상태를 점검하고 방화벽, 침입탐지시스템, 항바이러스 등의 각종 보안시스템을 설치하여 24시간 관리, 감시, 실시간 대응 및 보고서 제출 등을 제공하는 보안 토탈 서비스를 말한다. 이는 사용자 인증/인가 서비스, 접근제어 서비스, 암호/키 관리 서비스, 정책관리 서비스, 침입탐지 및 경보 서비스, 보안감사 서비스, 라우팅 서비스 등으로 구성된다.
2. 보안 클리닉 서비스 : 고객의 시스템에 적합한 보안점검 및 대책 수립을 위한 기본 컨설팅 패키지로서, 고가의 컨설팅 비용을 부담하지 않고 자사 서버에 대한 보안 점검을 통해 취약성을 찾아내고 이를 보완함으로써 서버의 안전상태를 확보하는 서비스를 말한다. 이는 시스템의 취약성 분석, 보완 및 보고서 제출, 각종 보안 도구 설치 및 구성, 보안 상담 및 교육, On-line 정보보안 서비스 등으로 구성된다.
3. 보안 컨설팅 서비스 : 정보 시스템 보안관련 원칙인 기밀성, 무결성, 가용성, 신뢰성의 기준을 바탕으로 위험요소, 위협요소, 자산요소 분석을 통해 효과적인 보안 및 대응책을 수립하는 서비스를 말한다. 이는 사용중인 보안서비스의 보안설정 점검, 위험분석 보고서 제출, 네트워크 보안구성 설계, 시스템 보안구성 설계, 보안 시스템 구축, 보안관리자 교육 등으로 구성된다.
4. 모의 해킹 서비스 : 고객과 협의 하에 고객 시스템에 의도적으로 해킹을 시도하여 고객 시스템 및 네트워크의 허점을 발견하고 이에 의해 발생할 수 있는 사고에 대한 보완책을 제시하는 서비스를 말한다. 이는 외부 크래커를 가장한 공격, 내부의 악의적 사용자를 가장한 공격 등으로 구성될 수 있다.

현재의 보안관제서비스 제공자들에 의해 한정적인 사용자들을 대상으로 제공되고 있는 보안서비스는 보안서비스 제공자가 관리하는 보안 구성요소들에 의해 제공되며, 기업망 또는 캠퍼스망을 대상으로 하고 있다. 항상 문제는 보안서비스를 제공받는 곳보다는 이를 제공받지 않는 망 또는 장비들로 인하여 네트워크 전체의 보안 취약성을 제공하게 되는 것이다. 이러한 문제를 해결하기 위하여서는 보안 호스팅 서비스를 광역망으로 확장 적용하는 것이 필요하며, 보안관리의 저변확대와 네트워크 자원의 효율적인 보호관리가 가능하게 되는 종합적인 네트워크 보안관리구조 정립이 필요하다.

Ⅲ. 글로벌 네트워크 보안관리 프레임워크

글로벌 네트워크 보안관리 기술이란 지역 망의 보안관리 방법을 보완하기 위해서 네트워크 수준의 보안관리를 통하여 망 인입점에서 유해 트래픽을 분석 및 차단하여 네트워크의 성능 저하를 미연에 방지하고 네트워크의 자원 및 주요 통신장비의 보호 기능을 수행하는 것을 목표로 한다. 이는 인접 도메인과의 보안관련 정보의 교환 및 상호 협력을 바탕으로 하여야 하며, 이를 통하여 사용자가 사용하는 전역망에서 동일한 보안 서비스 품질을 유지할 수 있을 것으로 본다.

(그림 2)는 글로벌 보안관리 네트워크의 개념도를 나타낸 것으로, 코어망의 보안성을 강화하고 사용자의 서비스 트래픽을 안정적으로 제공하기 위한 오버레이망 구조이다. 광역 네트워크 차원의 보안관리를 수행하기 위해서 해결해야 하는 문제들은 서비스 규약 적용의 미흡, 네트워크 관리자의 보안의식 결여, 보안장비들의 통합 관리체제 미흡, 침입탐지에 대한 실시간 대응 능력의 부재, 보안기능으로 인한 네트워크 전반적인 성능저하로 인한 보안장비 운용의 기피, 전역망을 통한 보안서비스 제공이 불가능하다는 것을

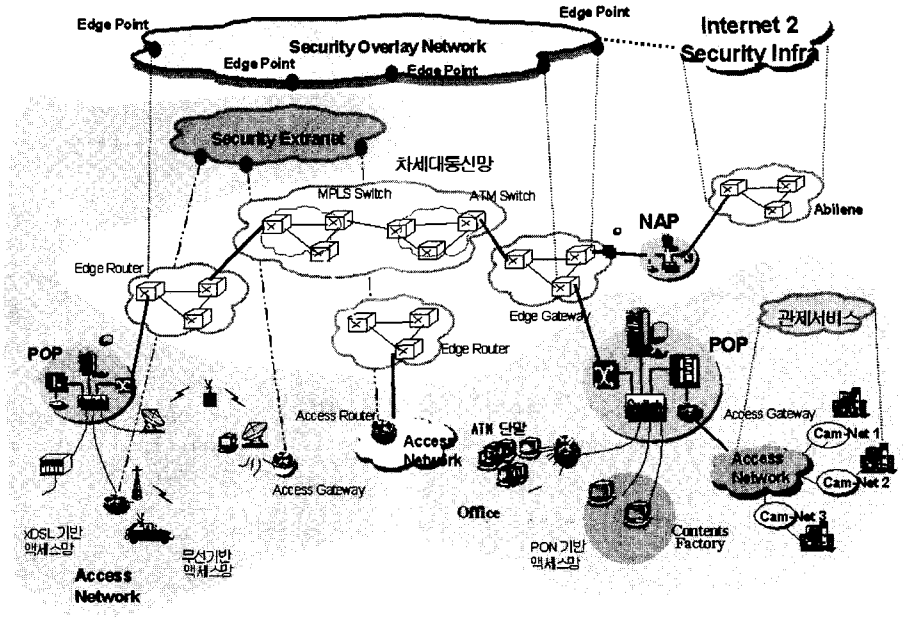


그림 2. 글로벌 보안관리 네트워크 개념도

들 수 있다.

본 절에서 이러한 광역 네트워크 차원의 보안관리를 수행하기 위해서는 해결해야 하는 문제들을 중심으로 네트워크 보안관리 프레임워크가 가져야 하는 구성요소를 검토하도록 한다.

1. 네트워크 관리자의 보안의식 결여 : 보안관리의 편의성 제공

보안사고의 대부분은 네트워크 관리자의 보안의식 결여에서 기인한 경우가 많다는 것이 보안사고 사례에서 나타나고 있다. 방화벽과 침입탐지 시스템 등의 보안장비의 구축에도 불구하고 보안침해가 일어나고 있는 것은 네트워크 관리자들의 관리 능력의 부족으로 인한 기본 구성설정의 변경을 하지 않아 보안장비의 성능을 제대로 발휘하지 못한 것이 원인인 경우가 많았다. 그리고 개별적인 관리 기준과 관리 방법의 다양화로 인해 체계적이고 효과적인 관리가 불가능한 것도 한 요인으로 생각할 수 있다. 이러한 문제를 해결하기 위하여서는 네트워크 관리자 또는 보안관리자가 사용하기에 편리하고 통합 관리가 가능한 네트워크 보안관리 프레임워크의 구축이 필요하다.

가. 보안관리 구조 : 정책기반 보안관리 구조

구조적으로는 체계적인 관리와 통합 관리를 제공할 수 있도록 IETF 정책프레임워크를 적용하는 것이 바람직 할 것으로 보인다. 따라서, 보안정책 기반의 보안관리 프레임워크는 보안정책서버와 보안정책서버의 관리를 받는 다수개의 정책대상시스템으로 구성된 중앙집중화된 관리구조를 갖는다. 여기서, 보안정책서버가 일관성있는 정책으로 관리하는 관리영역을 도메인이라고 부르고 이 도메인에서 발생하는 모든 보안관련 상황은 해당 도메인의 보안정책서버로 전달되어 체계적이고 종합적으로 관리되며 필요시 인접 도메인으로 전파할 수 있다.

이 정책프레임워크에서는 정책서버, 정책저장소 및 정책대상의 기능 구성요소를 가진다. 정책서버는 크게 정책관리도구 및 정책결정기능으로 구성되며 정

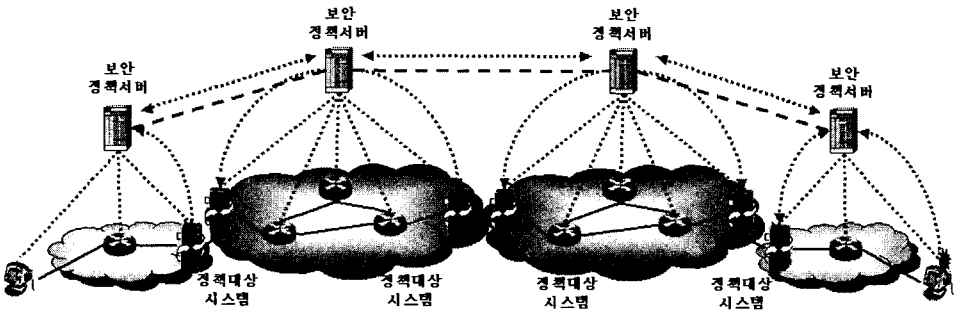


그림 3. 정책기반 보안관리 구조

책저장소는 정책서버와 독립적인 시스템으로 존재할 수도 있다. 또한 정책대상은 정책을 실행하는 네트워크 시스템으로 자원관리관점에서는 경계라우터가 이에 해당된다. 글로벌 네트워크 보안관리 구조에서 보안정책서버는 정책서버 구성요소로 보안정책 도메인의 보안관련 정보를 종합관리하며, 보안게이트웨이시스템은 정책대상 구성요소로 트래픽의 분석 및 대응 기능을 수행한다.

나. 체계적인 보안관리 방안

정책도메인내에서 프로토콜, 장치, 공급업체에 독립적인 관리가 가능하고 분산되어있는 관리객체의 효율적인 관리를 위해 자원관리관점에 표준화되고 있는 IETF의 PCIM (Policy Core Information Model) 정보 모델링 기법을 보안관리 관점으로 확장하여 적용한다.

정보모델은 구현 전에 이해할 수 있도록 지식을 추상화하는 것을 말하여, PCIM은 정책정보 모델을 표현하기 위해 제시하는 객체지향 정보모델이다. 이는 정책 핵심 정보모델로써 어플리케이션들과 연관된 어떤 정책이든지 표현할 수 있도록 일반적이고 핵심적인 클래스들을 정의하고 있고, 정책의 제어와 정책정보를 표현하는 구조 클래스와 구조 클래스의 상호연관성을 나타내는 연관 클래스를 정의하고 있다. 정책은 정책 규칙들의 집합을 사용하여 적용되고, 각 정책 규칙은 조건들의 집합과 동작들의 집합으로 구

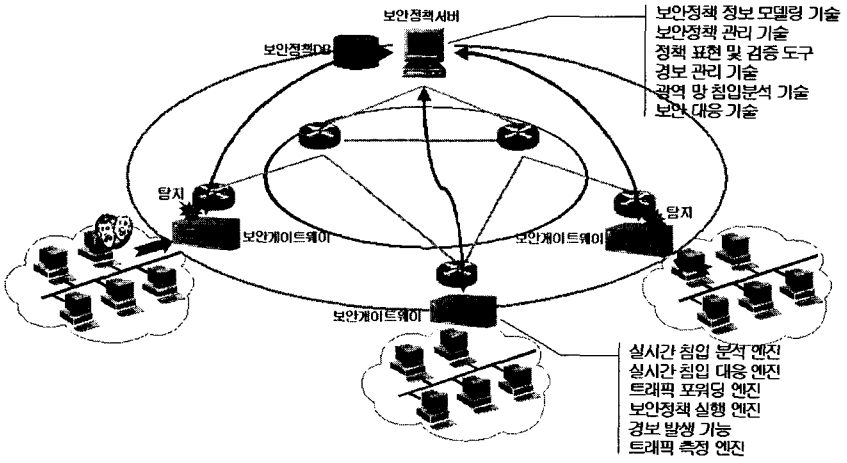


그림 4. 정책기반 보안관리 구조 동작 개념도

성된다. 여러 정책 규칙들은 정책 그룹들과 결합되고, 이러한 그룹들은 또 다른 그룹을 구성할 수 있다.

따라서, IETF의 PCIM 정보모델에서 침입분석 및 침입대응과 관련한 정책규칙 등을 추가하여 확장한 네트워크 보안 정책정보 모델을 NSPIM (Network Security Policy Information Model)이라 부르며, 침입을 탐지하고 대응하는 시그니처 정책들을 위한 모델로써 적용한다.

2. 보안장비들의 통합관리 체제가 미흡 : 종합적인 보안 상황 판단 수단 제공

보안장비들의 개별 관리와 이들간의 연동이 불가능 함으로 인하여 네트워크 관리자들은 통합 관리의 어려움을 겪고 있고 완벽한 보안 시스템의 운용에 한계를 보이게 된다. 개별 보안장비들은 단일 시스템 레벨에서의 단면적인 침입 분석을 수행함으로 인하여 네트워크 차원의 종합적인 침입 예측을 수행할 수 없는 문제점을 나타내게 된다. 따라서, 이러한 문제를 극복하기 위해서는 보안장비의 분석과 이의 이벤트 정보와 경보 정보를 기반으로 하여 네트워크 전반에 걸친 분석을 수행하도록 단순분석과 통계적분석으로 이루어진 계층적인 침입분석 기법을 적용한다. 이를 통하여 정책 도메인내에서 발생하는 모든 보안 이벤트 정보를 수집하고, 이를 체계적으로 관리하고 전체 정책도메인에 따른 보안 상황의 분석을 수행함으로써 종합적인 네트워크 보안관리 프레임워크를 구축할 수 있다.

(그림 5)는 계층적 침입분석 및 대응구조를 나타낸 것으로, 먼저 망의 인입점에 위치하는 보안게이트웨이 시스템은 시그니처기반의 침입탐지를 수행하는 비교분석과 트래픽의 변화 유형을 모니터하는 관측분석을 통한 하위계층 침입분석을 수행한다. 하위계층 침입분석의 결과를 기반으로 보안게이트웨이시스템에서 실시간 대응을 하거나 상위계층의 보안정책서버로 경보 정보를 전달함으로써 상위계층 침입예측을 가능하게 한다.

그리고, 네트워크 전체의 보안관련 정보를 수집하고 관리하는 보안정책서버는 통계적 데이터를 기반으로 유사성 분석, 잠재성 분석, 침입가능성 분석을 통한 상위계층 침입예측을 수행한다. 이를 근거로 네트워크내에 적용할 대응 정책을 생성 및 적용을 결정하거나 침입의 징후에 대한 정보를 인접 도메인과의 통신을 통해 전파함으로써 글로벌 네트워크 차원에서

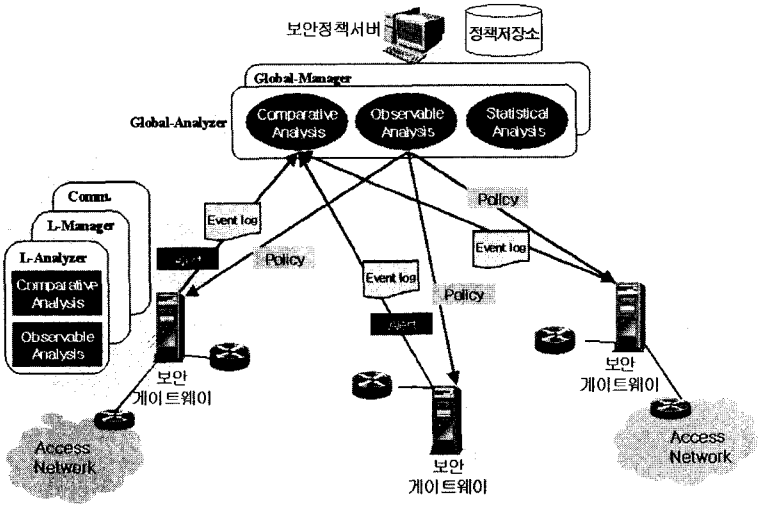


그림 5. 계층적 침입분석 및 대응구조

침입대응 협업 체계를 구축할 수 있다.

3. 침입탐지에 대한 실시간 대응 능력의 부재 : 실시간 대응 구조 및 정보전달 수단 제공

기존의 보안장비들의 통합 관리를 목적으로 하는 전사적 보안관리 시스템의 경우는 각 보안장비에서 발생하는 경보정보 및 로그 정보를 수집하여 모니터상에 표현하거나 다른 수단으로 전달하는 기능을 수행하여 보안관리자에 의한 수동적인 대응을 수행하고 있다. 그러나 잘 알려진 공격을 분석하기 위한 시그니처기반의 침입분석의 경우는 보안관리자의 개입 없이 침입탐지와 함께 실시간으로 대응할 수 있는 수단이 제공되어야 하고, 이를 위한 관리 정책의 실시간 갱신이 가능한 구조를 제공하여야 한다. 이를 위해서는 기존의 ESM에서 사용하는SNMP를 이용하여서는 실시간 정보 전달에 어려움이 있어, 경보 전달을 위해서는 IAP(Intrusion Alert Protocol) 또는 IDXP(Intrusion Detection Exchange Protocol)를 사용하도록 IETF IDWG(Intrusion Detection Working Group)에서 표준화하고 있고, 보안관리를 위한 보안정책의 질의 및 전달을 위한 정책전달 프로토콜로는 COPS(Common Open Policy Service)를 사용하도록 표준화하고 있다.

IAP는 침입탐지 구성 요소인 패킷 센서(Sensor) 또는 침입분석(Analyzer) 엔진과 관리자(Manager) 사이에 침입 경보 데이터를 교환하기 위한 응용 계층 프로토콜이며, 전달되는 경보는 IDMEF(Intrusion Detection Message Exchange Format)으로 표현한다. 수송계층 프로토콜로는 TCP를 사용하고 통신 모드는 요청과 응답의 쌍으로 수행하며 연결설정 단계와 데이터 전달 단계로 구분된다.

COPS프로토콜은 정책서버의 정책결정기능(PDP: Policy Decision Point)와 정책대상 시스템의 정책집행기능(PEP: Policy Enforcement Point) 사이의 TCP기반 정책 정보 전달 프로토콜로 클라이언트-서버 모델을 사용하고 있고 이벤트 기반 정보전달 구조를 제공한다.

4. 보안기능으로 인한 성능 저하 : 분석엔진의 사용자 평면 처리 기능 분리

현재의 보안장비들은 소프트웨어기반의 침입분석 엔진을 적용하고 있다. 이는 망의 접속 대역폭이 증가함에 따라 이로 인한 네트워크 성능 저하를 초래하게 되고 침입분석 엔진의 패킷 손실률이 증가하게 되는 문제점을 가지게 된다. 또한 침입분석 엔진을 광역 망으로 적용 범위를 넓히게 되면 더욱 심각한 문제를 야기하게 될 것이다.

일단 패킷 손실률을 줄이기 위해서는 패킷을 수집하는 패킷 센서의 고속화, 침입을 분석하는 분석엔진의 고성능화가 필요하다. 현재 이를 위한 접근 방법은 크게 두가지로 해결하고 있는데, 하나는 하드웨어 전용 칩(ASIC) 구현을 통한 접근 방법이고 다른 하나는 기가급 네트워크 프로세서를 이용한 접근방법이다.

또한 침입분석 엔진으로 인한 네트워크 성능 저하의 문제를 극복하기 위해서는 침입분석을 위한 전용 프로세스를 통한 사용자 평면과 보안관리자 평면의 분리가 필수적이다. 이들은 공히 새로운 침입유형의 적용이 용이하여야 하고, 순차적 패킷 분석 및 비정상 행위 탐지와 같은 복잡한 침입분석 기술의 적용이 가능하여야 한다.

5. 서비스 규약 적용의 미흡 : 차별화된 보안서비스 제공

인터넷의 보편화와 사용량의 폭발적 증가는 인터넷 트래픽의 폭증을 야기하게 되었고, 인터넷의 수요를 공급이 따라주지 못하면서, 서비스 이용 폭주 시간대의 접속 성공률이 급격하게 떨어지는 등 질적인

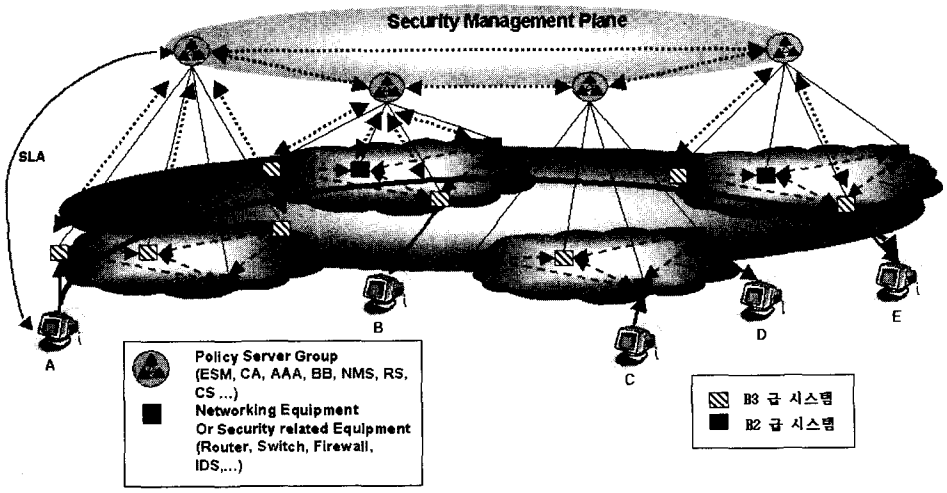


그림 6. 차별화된 네트워크 보안서비스 제공 예

문제가 대두되었다. 이에 따라 이용자들은 일정수준 이상의 서비스 제공을 요구하게 되었고 서비스 공급업체들은 서비스 품질에 대한 고객의 만족도 제고와 경재업체와의 차별화를 위해 서비스 규약인 SLA (Service Level Agreement)를 적용하게 되었다. SLA는 서비스 공급업체의 서비스를 대상으로 성능과 가용성 등에 있어서 일정한 서비스 수준을 보장하기 위해 맺는 서비스 공급업체와 고객간의 계약으로 고객에게는 비즈니스 가치를 높여주고, 서비스 공급업체에게는 서비스 차별화 등으로 인한 경쟁 우위 확보와 매출의 증가를 기대하게 하는 수단이 될 것으로 기대하고 있다.

이러한 경향은 대역폭의 보장을 요구하는 것부터 시작을 하였으나, 최근에 해킹과 관련한 일련의 사건들로 인하여 정보, 시스템 또는 네트워크의 생존성 보장에 대한 관심이 증가하게 되었다. 또한, 인터넷이 보편화되어 전자상거래, 사이버주식거래, 인터넷 뱅킹 등과 같은 새로운 서비스의 출현은 트래픽의 보안 품질 보장에 대한 관심을 유발하게 되었다.

위에서 언급한 두가지 네트워크 보안 서비스 요구 중에서 사용자 트래픽의 보안 품질 보장성에 대한 차별화된 서비스를 제공하는 방법의 한 예를 살펴본다.

A라는 사용자가 E라는 사용자에게 중요한 문서의 전송을 필요로 하는 경우를 가정하고, 이때 지연되어 전달되는 것은 좋으나 데이터의 손실이나 유출, 손상 등의 일은 절대 발생하지 않기를 바란다고 가정한다. 먼저 A라는 사용자는 자신이 속해 있는 정책도메인을 담당하는 정책서버와 해당 세션에 대한 서비스 규약을 협상하는데, 이때 자신의 트래픽이 전달되는 동안 기밀성과 무결성과 관련한 보안 조건에 대한 요구를 하고 이와 관련한 과금 원칙에 합의를 하게 된다. 기밀성을 제공하기 위해서는 정책서버는 해당 세션에 대해서 특정 암호원칙을 적용하거나 터널링 기법과 같은 안전한 연결성 제공 방안을 적용할 수 있을 것이고, 무결성 관점에서는 트래픽 엔지니어링 관점에서 패킷 손실이 발생하지 않도록 각 노드에 QoS 정책을 하달한다. 그러나 이것만으로 완전한 무결성을 제공할 수 없는데 이는 각 노드가 보안 취약성을 가지고 있다면 해당 노드에서는 해당 트래픽의 스니핑 및 세션의 스푸핑이 발생할 수 있기 때문이다. 이러한 부분을 막기 위해서는 해당 세션의 경로를 선정하는 과정에서 QoS관점으로 선정된 경로 후보들 중에서, 포함하고 있는 네트워크 노드들의 보안등급에 대한 검증 작업을 거쳐서 원하는 무결성 요구사항을 만

족하는 수준이상의 노드만을 거치는 경로를 선정한다. 위의 예에서는 일반적인 사용자들은 주로 미국방성 보안 등급 B2급의 네트워크 노드를 거치는 경로를 사용하지만, A 사용자가 E사용자와 연결하는 세션에 대한 경로는 B3급의 인정을 받은 네트워크 노드만을 거치도록 선정하여 더 안전한 네트워크 서비스를 제공할 수 있도록 하였다.

사용자 네트워크 생존성에 대한 차별화된 서비스를 제공하는 방법은 기존의 관제 서비스 제공자들에 의해 제공되고 있는 호스팅 서비스를 광역망으로 확장 적용한 것으로 생각을 하면 될 것이다.

6. 전역망을 통한 보안서비스 제공이 불가능 : 글로벌 보안 네트워킹

보안관제 서비스 제공자는 담당 네트워크 또는 시스템에 대한 감시와 정보수집 및 침입에 대한 보고 및 수동적인 대응을 수행한다. 해당 네트워크 또는 시스템과 인접한 네트워크 환경에 대한 분석이나 고려는 능동적으로 하기 어려운 것이 현실이다. 현재의 인터넷 보안은 단일 시스템 또는 특정 네트워크에 대한 보안으로는 사이버 공격을 방어하기에 한계를 느끼고 있어서, 네트워크 수준의 상호 협업을 통한 통합 보안 관리에 대한 연구를 수행하고 있다. 이러한 요구에 따라 글로벌 네트워크를 관리하기 위해서 계층적인 보안관리 및 대응 체계를 수립하고 상위 계층에 해당하는 관리평면에서는 인접 도메인의 보안정책 서버와의 유기적인 협력을 위한 글로벌 보안 네트워킹을 통하여 사이버공격에 대한 예측 방어 및 블랙리스트 또는 침입탐지 규칙 등과 같은 보안정책의 적용을 수행할 수 있도록 한다. 단, 현재의 인터넷 서비스 제공자 또는 네트워크 서비스 제공자들의 상호 정보교환에 대한 폐쇄적인 인식은 사이버공격자에 대해 효율적으로 대처하는데 상당한 문제점을 야기하게 될 것이므로 개방적인 인식으로의 전환이 무엇보다 선행되어야 할 것이다.

Ⅳ. 결론

사이버 공격 유형이 분산화, 지능화, 통합화, 대규모화, 자동화, 은닉화의 경향으로 발전하고, 인터넷이 사회생활 전영역에서 필수적인 요소로 자리를 잡

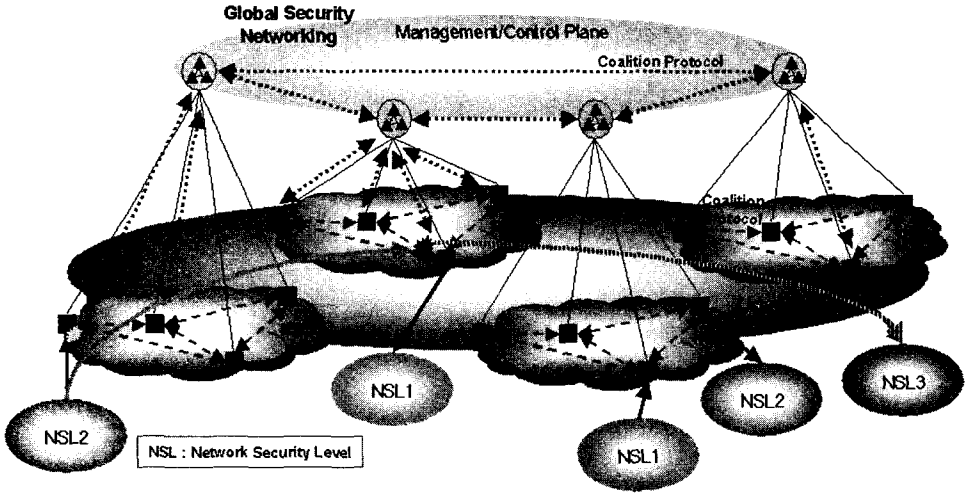


그림 7. 글로벌 보안 네트워킹 개념도

음에 따라 보다 안전하고 신뢰할 수 있는 정보통신 인프라의 구축이 절실하게 요구되고 있다. 이를 위해서는 네트워크 측면에서 개별 트래픽에 대한 기밀성, 무결성, 가용성을 보장할 수 있는 수단을 제공하여야 하며, 일관성 있는 감시, 관리 및 제어 정책의 집행이 가능하여야 한다. 그리고, 인접 서비스 제공자와의 보안관련 정보의 공유를 통한 상호협력을 수행하여 글로벌 네트워크 차원에서 보안성 강화방안이 수립되어야 한다.

이러한 글로벌 네트워크 보안관리 프레임워크는 아래와 같은 요구사항을 만족시킬 때 효과적인 사이버 공격 방어 수단을 제공할 것이며, 각 사용자들에게는 고품위의 응용서비스 지원기능을 제공할 수 있을 것으로 본다.

- 효율적인 보안정보 수집과 체계적이고 일관성있는 관리 정책의 적용이 가능한 구조를 가져야 하며,
- 분산 관리객체를 효율적으로 관리하기 위한 보안정보의 추상화 방법론을 적용할 수 있어야 한다.
- 그리고, 네트워크 범위의 종합적인 침입분석, 침입예측 및 침입대응을 위한 계층적인 분석 기법과 같은 종합적인 보안상황 판단 수단을 제공하여야 하며,
- 보안기능의 적용에도 네트워크 전달 성능에 영향을 주지 않는 독립적 운용이 가능한 전용 프로세서를 이용한 보안 분석엔진, 트래픽 측정 엔진 적용이 가능하여야 한다.
- 사용자의 네트워크 또는 트래픽 중요도와 과금의 의사에 따라 차별화된 보안규약을 선택할 수 있는 방안의 도입과 이를 제공할 수 있는 네트워크 서비스 제공 메커니즘의 개발이 이루어져야 하며,
- 사이버공격에 효과적이고 종합적인 대응이 가능하고 종단간의 차별화된 서비스의 보장을 위하여 서비스 제공자간의 보안관련 정보에 대한 상호 공유와 협상을 위한 글로벌 보안 네트워킹이 가능하여야 한다.

참고문헌

[1] DMTF Specification, White Paper : CIM(Core Information Model) for CIM Schema Release 2.4, 2000.5 (http://www.dmtf.org)

[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] 안개일, "정책기반 네트워크 관리구조에서 PCIM 정책전달 방안", NCS2001

[5] RFC 2753, "A Framework for Policy-based Admission Control", Jan. 2000.

[6] RFC 2401, "Security Architecture for the Internet Protoco", Nov. 1998.

[7] Introduction to Policy Based Networking & QoS, White paper, http://www.iphighway.com

[8] Young-Jun Heo, et al., "Architecture of Security Policy Agent for applying Security Policy Model", COMSW2001, pp, 193-197, 2001.

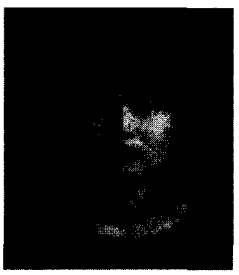
[9] RFC 2748, "The COPS(Common Open Policy Service) protocol", Jan, 2000

[10] K. Chan, et al., "COPS Usage for

Policy Provisioning (COPS-PR)", RFC 3084, March 2001.
[11] 윤승용, "보안정책 정보 전달을 위한 COPS-Security 프로토콜", 추계정보과학회 학술대회, 2001.10
[12] S. Northcutt, M. Cooper, M. Fearnow, and K. Frederick, "Intrusion Signature and Analysis," new riders, 2000.
[13] Byoung Koo Kim, D.S. Kim, and Tai M. Chung, "A Design of Integrated Intrusion Detection Systems in a Large Scale Network Environment", APNOMS 2000, pp. 187-197, Nara, Japan, Oct., 2000.

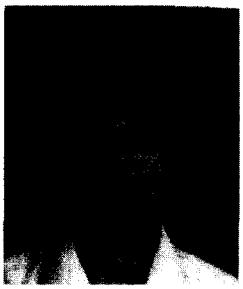
장 종 수

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



김 기 영

1988년 전남대학교 전산통계학과 이학사, 1993년 전남대학교 전산통계학과 석사, 2001년 충북대학교 컴퓨터공학과 박사, 1988년 2월~현재 한국전자통신연구원 선임연구원, 정보보호연구본부 보안게이트웨이연구팀



류 걸 우

\1990년 5월 MS. Computer Science, Unv. of Massachusetts, MA, USA, 1993년 5월 ScD. Computer Science, Unv. of Massachusetts, MA, USA, 1994년 7월~현재 한국전자통신연구원 책임연구원, 정보보호연구본부 보안게이트웨이연구팀