主題

고성능 네트워크 정보보호 시스템 개발

정보통신부 사무관 김 경 우

차 례

초 록

인터넷에 대한 의존성이 증가하면서 온라인상에서도 다양한 형태의 사이버 위협이 상존하고 있으며, 특히 시스템의 취약성을 공격하는 해킹 방식은 대규모의 트래픽을 발생하여 네트워크 자체에 대해 큰 위협이 되고 있다. 지난 1.25 인터넷 침해사고 이후 전역통신망 차원에서의 네트워크에 대한 침입을 능동적으로 탐지하고 대응할 수 있는 고성능 네트워크 정보보호시스템 개발이 절실히 요구되고 있는 실정이다. 본 고에서는 세계의 네트워크 기술과 보안 기술 발전 추세에 발맞추어 추진 중인 정책 기반의 실시간 침입 탐지, 대응 및 예측 기능이 복합적으로 융합된 종합 솔루션인 NGSS에 대해서 기술개발 추진의 타당성, 시스템의 주요 특징을 소개하고자 한다.

1. 서 론

현대인에 있어서 인터넷은 삶의 곳곳과 연결되는 불가분의 요소가 되었다. 이렇듯 인터넷에 대한 의존성이 증가하면서 오프라인과 마찬가지로 온라인상에서도 다양한 형태의 사이버 위협, 특히 시스템의 취약성을 공격하는 해킹 방식은 대규모의 트래픽을 발생하여 네트워크 자체에 대해 큰 위협이 되고 있다. 따라서 이러한 사이버 위협을 차단하고 예방하기 위해 다양한 네트워크 보안 제품들이 등장하고 있으나, 그 대응 범위가 지엽적이어서, 전역적인 DDOS 공격에 대해서는 적절히 대응하는데 한계가 있다. 따라서, 전역통신망 차원에서의 네트워크에 대한 침입을 능동적으로 탐지하고 대응할 수 있는 고성능 네트워크 정보보호시스템 개발이 절실히 요구되고 있는 실정이다.

세계시장을 살펴보면, IT 산업 전체 성장율은 6.7% 정도인데 반해, 2002년 현재 203억달러 규모인 정보보호 산업은 성장율이 21.5%, 99억달러 규모인 네트워크 보안사업은 23.3%의 높은 성장

율이 예측되고 있다. 네트워크 보안 분야의 높은 성장가능성을 보고, 그 기반이 되는 기술인 고성능 네트워크 정보보호시스템 (시스템명 : NGSS, Next Generation Security Systems) 개발을 ETRI를 중심으로 2002년부터 2006년까지를 개발기간으로 해서 추진 중에 있다.

본 고에서는 NGSS 시스템에 대해 개요 관점에서 소개하고자 한다. 먼저, 네트워크 보안 기술의 진화 방향 분석을 통해 NGSS 기술개발의 타당성을 살펴본다. 그 다음으로 NGSS를 구성하는 침입 탐지 및 이상 트래픽 감지 시스템, 이상징후 수집 및 분석 시스템, 침입 차단 및 대응 시스템을 소개하고자 한다.

2. 네트워크 정보보호 기술 진화 방향

네트워크 정보보호기술의 발전방향은 크게 3가지로 요약할 수 있다. 첫째, 네트워크의 성능을 저하시키지 않도록 성능보장형 보장장비가 나오고 있다. 즉, 소프트웨어 기반 보안 제품에서 하드웨어 기반 보안제품으로 변화하고 있다. 둘째, 통합 보장 장비의 출현이다. F/W (방화벽)과 VPN (가상사설망)이 통합된 제품, IDS와 F/W이 통합인 IPS (Intrusion Prevention System, 침입방지시스템) 등이 그 예가 되겠습니다. 네트워크 장비에 보안 모듈이 탑재된 보안라우터, 네트워크 장비에 'Plug-In'으로 놓이게 되는 standalone형 보안어플라이언스가 출현하고 있다. 셋째, 사이버상의 침해에 대해 국가적인 대응의 필요성이 제기 되고 있다. 미국의 경우 2001년 911 테러이후 미국방부 다음으로 규모가 큰 DHS (Department of Homeland Security, 국토안보부)를 설립하고, 도로, 항만, 댐 등의 물리적인 국가 기반시설 외에 인터넷 등의 사이버 기반시설에 대해서도 국가안보차원에서 대응책을 추진하고 있다. 우리나라 또한 2003년 1.25 인터넷 침해사고로 인하여 국가차원의 대응책을 마련하고 있다.

세계 최대 기술 리서치 그룹인 Yankee Group에서는 보안 시장에 대해 2003년까지는 '할 수 있는 부분까지만 제공한다(Best-of-Breed)' 는 것에 초점을 맞춘 솔루션 기반의 제품 위주였던 것에 반해 2003년에서 2005년까지는 모든 critical 시스템에 보안이 확장되는 제품 방향으로 발전하여, 2005년 이후에는 보안의 규격화 및 제도화(institutionalization)가 이루어지는 단계로 나아갈 것이라고 전망하고 있다. 특히, 2005년 이후를 보안의 'Persistence Phase' 로 정의하고, 보안 및 보호를 요구하는 대상이 어플리케이션 및 네트워크 모든 부분으로 확대되어 사용자의 요구에 맞는 정책 기반의 보안이 필요하게 될 것이라고 예측하고 있다. 또한 2008년 이후엔 기존의 개별 제품에 한정되었던 보안 서비스가 네트워크 레벨로 확장되어 지원될 것이고, 보안뿐만 아니라 QoS 측면에서도 정책 기반의 시스템의 요구가 증대할 것으로 예측하고 있다. 따라서 정책에 기반한 네트워크 보안 시스템이 요구될 것이며, 이를 위해 네트워크 보안 제품들과 통신하며 정책을 생성 및 관리할 네트워크 보안 관리 시스템의 역할 및 이때 송수신되는 정보에 대한 보안이 중요하게 될 것이다.

가트너에서 2002년 11월 예측한 자료에 의하면, 2002년 현재 보안 제품들은 기능 단위의 Firewall(방화벽), Intrusion detection(침입탐지시스템), Vulnerability Assessment(취약성 평가 제품), Gateway antivirus(게이트웨이 백신 제품) 등이 단품으로 판매되고 있다. 2004년을 전후로 해서는 여러 보안기능들이 하나의 플랫폼에 통합될 것으로 예측된다. 통합방법은 개방형 플랫폼에 다양한 회사의 보안 모듈이 탑재되는 형태와 major 회사의 폐쇄된 플랫폼에 여러 보안 모듈이 내장되는 형태를 취할 것으로 예측된다. 즉, 기능 통합에 주안점을 두는 시기라고 할 수 있

다. 2006년 전후로 해서는, 보안제품들이 놓이게 되는 네트워크 상의 위치에 따라 특화된 제품이 나올 것으로 예상된다. 먼저, ISP 네트워크에 놓이게 되는 경우, 라인인터페이스가 1Gbps 이상의 고성능 네트워크 정보보호제품으로 트래픽월, 해킹월 기능이 침입에 대한 차단/대응에 초점을 맞추게 된다. 고객망(기업망, 캠퍼스망 등)에 놓이게 되는 제품은 파이어월, 바이러스월 등 성능보다는 다양한 기능들이 우선 시 되며, 다양한 기능들이 통합된 보안장비일수도 있고, 특정 기능만 수행하는 전용장비일 수도 있으나, 주로 침입을 예방하는데 초점을 맞추게 될 것이다.

3. NGSS 시스템 개요

3.1 시스템 개발 목표

현재 ETRI에서 개발 중인 NGSS는 전역통신망(Global network) 환경에서 네트워크에 대한 침입을 능동적으로 탐지하고 대응할 수 있는 고성능 네트워크 종합침해대응시스템이다. 통신사업자의 네트워크 정보보호체계 고도화 방향, 국내 기술의 국제 경쟁력 확보 등을 고려하여 연도별 개발 목표를 그림 3.1과 같이 설정하였다. 그림에서 보는바와 같이 2003년 말까지 10G급, 2004년말까지 20G급, 2005년말까지 40G급, 2006년말까지 100G급 네트워크 종합침해대응시스템 개발을 목표로 하고 있다.

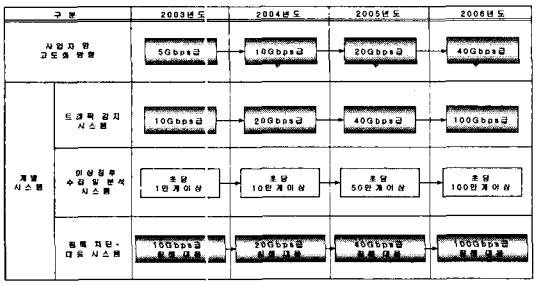


그림 3.1 연도별 개발목표 및 내용

NGSS는 사용자 혹은 사용자 시스템 보호가 목표가 아닌, 네트워크 자체 혹은 네트워크기반 서비스 제공의 보호를 목적으로 하는 보안 장비로서, 3가지 세부 기술로 구분할 수 있다. 첫째, 네트워크로 유입되는 침입에 대한 탐지와 이상 트래픽 감지를 수행하는 시스템이다. 둘째, 이상징후 정보를 전역통신망 차원에서 네트워크 장비들로부터 수집하고, 수집된 정보들간의 상관관계 분석을 통해 침입 여부를 판단하는 시스템이다. 셋째, 침입으로 판단되면 이에 대한 대응기술로서 침입자의 IP 주소나 TCP 포트 번호 등을 차단하거나, 이상트래픽의 플로우를 조절하는 시스템이다.

3.2 시스템 구성

NGSS는 이상징후 수집 및 분석 시스템 기능을 수행하는 보안관리시스템과 침입 탐지 및 이상 트래픽 감지 시스템, 침입 차단 및 대응 시스템 기능을 수행하는 보안노드시스템, 그리고 이들 사이의 상호작용을 제공해주는 인터페이스로 구성된다. 보안관리시스템은 정책기반망관리(PBNM)에 기반한 중앙 집중적인 관리 기법을 사용하므로 보안노드를 관리하기 위해 정책을 수립하고 각 보안노드에 적절한 정책을 배포하여 수립된 정책대로 보안노드가 수행되도록 함으로써 관리자가 다수의 보안노드를 손쉽게 중앙에서 관리할 수 있게 한다. 그림 3.2는 NGSS의 시스템 구성을 나타내는 논리 구조도이다.

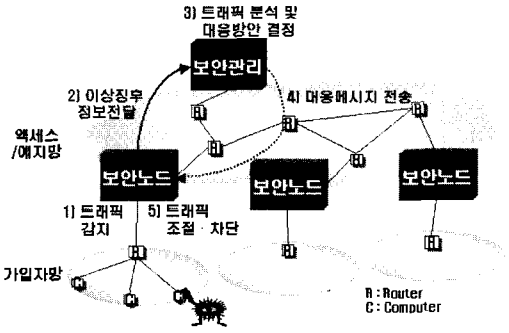


그림 3.2 NGSS 시스템 구성

아래의 절에서는 NGSS, 보안노드 및 보안관리시스템으로 구분하여 주요 특징을 살펴보고자 한다.

3.3 NGSS 주요 특징

본 절에서는 Secure Networking, High Performance, ISP 망 적용, 기술 발전, 시장경쟁력 측면에서 NGSS 시스템의 주요 특징을 소개한다.

1) Secure Networking 측면

첫째로, 대상 범위가 지역망에서 액세스망과 광역망으로 확대된다는 것이다. 현재 ESM의 대상 범위가 지역망이었던 것에 반해 NGSS는 그 대상 범위가 액세스망과 광역망으로 기존의 네트워크 보안 장비들에 비해 그 범위가 넓을 뿐만 아니라 전달망에서 집중적으로 보안 기능을 제공함으로써 고객망의 보안 위협을 감소시킬 수 있다.

둘째, 정책 기반의 통합보안관리 구현이다. NGSS를 구성하는 보안노드시스템와 보안관리시스템은 기존의 네트워크 보안 시스템의 한계였던 정책 기반과 보안 시스템간의 협력에 중점을 두고 개발되는 시스템이다. 특히, IETF 표준인 COPS를 이용한 정책 기반 네트워크 보안 관리로 새로운 침입 유형에 대한 업데이트 및 침입 대응 방식에 대한 추가 등이 용이하다.

셋째로, 침입 정보의 공유이다. NGSS는 기존의 ESM 제품들이 타 보안 시스템들과 침입 정보 교환을 위해 단지 인터페이스를 공유했던 것과 달리 개별 시스템들을 동시에 개발하면서 내부 핵심 기술의 공유와 정책 기반 관리를 통해 각 시스템의 자체 보안 기능을 한 차원 업그레이드 할 수 있고, 새로운 침입에 대해 효과적으로 대처할 수 있는 시너지 효과가 예측된다.

2) High Performance 측면

첫째로, 속도와 성능 측면에서 대표 제품들과 비교 분석해 본 결과 보안노드시스템의 목표치는 업계의 최고 제품들과 대등한 수준이며, 보안관리시스템의 목표치는 초당 침해 정보 처리 수준이 2~20배 이상 월등한 것으로 증명되었다.

둘째로, 기능 측면에서 NGSS는 글로벌 관점의 실시간 침입 대응이 가능하고, 새로운 침입 유형을 정책을 통해 빠르게 업데이트 가능하다는 점에서 유리하다. 또한, NGSS는 일관된 정책을 적용한 개별 시스템간의 협업을 통해 더 정확한 침입 탐지와 이에 따른 적절한 대응 방식을 실시간으로 제공할 수 있으므로 나날이 다양해지고 복잡해지는 사이버 위협에 대한 신속한 대처가 가능할 것으로 보인다.

셋째로, 타 제품과의 차별성 측면에서 보안노드들은 보안 기능을 가진 전역망 네트워크 장비로 세계 최고의 기술을 가진 네트워크 업체 장비들의 라우팅 기능을 따라가기엔 다소 미흡하다. 하지만 전역망에서의 정책 기반 네트워크 보안 관리 시스템에 대한 시도는 NGSS 시스템에서 세계 최초로 시도하는 것이다. 따라서 NGSS는 보안노드의 성능보다는 보안관리시스템과의 연계를 통한 전역망에서의 침입 탐지 및 대응에 초점을 두고 있다. 보안관리시스템의 정책 결정 및 판단 능력, 정책 적용을 통한 신속한 침입 탐지, 대응 및 예측 기능이 NGSS 시스템의 차별되고 핵심적인 부분이라 할 수 있다.

3) ISP 망 적용 측면

첫째로, 광역통신망에서 정책 기반 네트워크 보안 관리를 제공하는 시스템이라는 것이다. 둘째로, 기존의 네트워크 노드의 성능에 영향 없이 보안 기능 추가가 가능하다는 점이다. 셋째로, Scalability를 제공한다는 점인데, NGSS는 망 구조의 변화없이 기존 시스템에 적용 가능하다. 넷

째로, 네트워크 차원의 실시간 보안 탐지 및 대응이 가능하다는 점인데, 보안관리시스템과 보안노드와의 연동을 통해 새로운 보안 위협에 대해 글로벌 분석으로 탐지가 가능하고 전역적으로 실시간 대응이 가능하다.

4) 기술 발전 측면

첫째로, 2005년 이후에는 정보 보호를 요구하는 대상이 어플리케이션 및 네트워크의 모든 부분으로 확대되고, 보안 서비스가 QoS처럼 SLA의 항목으로 포함되어 ISP는 사용자가 원하는 정책에 따른 보안 서비스를 네트워크 레벨에서 제공할 것으로 예측된다. 둘째로, 정책 기반의 보안 서비스 제공을 위한 네트워크 보안 장비의 수요가 증대할 것으로 예측된다. 셋째로, 정책 기반 시스템인 NGSS의 개발 방향은 세계의 네트워크 기술과 보안 기술 추세에 부합하고 있는 것으로 사료된다.

5) 시장 경쟁력 측면

첫째로, 정책 기반의 네트워크 보안 시스템인 NGSS는 Turnkey-based Solution으로 새로운 보안 기능, 침입 유형 및 대응 방식에 대해 신속하고 용이하게 업데이트를 제공하여 국제 시장에서 경쟁력을 가질 것으로 보인다. 둘째로, 보안노드는 하드웨어 방식으로 고성능을 제공하면서, 기존 시스템의 변경 없이 보안 기능 추가가 가능하도록 라우터/스위치에 Plug-in 형태로 장착되므로 시장 진입에 유리하다. 셋째로, 보안관리시스템은 표준화된 인터페이스를 이용해 타 네트워킹 또는 네트워크 보안 제품과 연동을 통해 정책 기반의 글로벌 보안 서비스 제공 가능 단독 시스템으로 경쟁력 있다고 판단된다.

3.4 보안노드 특징

대규모 네트워크 환경에서 침입 탐지 및 대응을 위한 보안노드는 보안관리시스템으로부터 전달된 보안 정책을 이용하여, 트래픽 폭주 또는 유해 패킷을 통한 네트워크 침해를 실시간으로 탐지 및 대응하고, 이러한 침해에 대한 정보를 보안관리시스템에 전달하여 광역차원의 네트워크 보안을 제공하는 시스템이다.

보안노드는 액세스망 또는 백본망의 엣지에 위치하며 라우팅 기능 없이 라우터나 스위치 뒷단에 Plug-in 형태로 장착할 수 있는 전용 보안 시스템으로 구현이 가능한데, 이 경우 망 구조의 변경 없이 추가 설치 가능한 장점이 있다. 또다른 구현 방법으로는 라우터나 스위치에 보안모듈 형태로 탑재될 수도 있다. 보안노드는 실시간 침입 탐지 및 침입 유형 분석 기능, 과다 트래픽 감지 기능, 그리고 침입 대응 기능의 특성을 가지고 있으며, IPSec을 이용한 신뢰채널을 통해 보안관리시스템과 안전한 통신 기능을 제공하며, 보안관리시스템으로부터 얻은 침입 정보 및 대응 방안을 일괄된 정책 기반의 보안 관리하에서 침입 탐지 및 대응에 활용할 수 있다는 장점을 가지고 있다. 또한, 보안노드는 IPSec의 암호화 알고리즘으로 국내 표준인 SEED를 추가로 제공함으로써 타 국외 VPN 제품들과 차별화하고, 하드웨어 ASIC 방식으로 성능 저하 및 패킷 손실 없이 100Gbps의 트래픽에 대한 침입 탐지 및 과다 트래픽 감지가 가능하다. 단, 보안노드시스템은 보안관리시스템과 연동을 위해 신뢰채널로써 IPSec 등의 보안 프로토콜을 지원하며, VPN Gateway 기능을 지원한다.

3.5 보안관리시스템 특징

보안관리시스템은 NGSS 시스템의 관리 대상 네트워크에 대한 보안 서비스의 제공과 효율적인 보안 관리의 제공을 위한 제반 기능을 지원하는 시스템이다.

보안관리시스템은 비교 대상의 ESM들이 지역

네트워크(LAN)에서의 보안 관리 서비스를 제공하는데 반해 광역 네트워크(예: ISP)에 위치하여 보안 관리 서비스를 제공한다는 것이 큰 차이점이다. 보안관리시스템은 IETF에서 표준으로 결정된 COPS를 기반으로 한 정책 기반의 네트워크 보안 관리 기능을 가지고 있다. 보안관리시스템은 실시간으로 침입 탐지 및 이상 트래픽 폭주를 분석하고 이를 통한 침입 대응 기능을 제공할 뿐만 아니라 비실시간으로는 트래픽 흐름의 통계를 통한 공격 예측 기능과 취약성 분석 및 보안 패치 기능을 가지고 있다. 보안관리시스템은 침입을 탐지했을 때 동적으로 정책을 결정하여 신뢰채널을 통해 보안노드시스템에게 적용시킴으로써 빠른 침입 대응 및 복구가 가능하게 한다. 또한, 공중망에 위치하는 시스템이므로 사용자 인증과 권한 부여를 통해 강력한 접근 제어를 보장한다. 보안관리시스템은 2006년 완료 시점에서 초당 100만개의 침해 정보 처리가 가능하다. 단, 현재 보안관리시스템이 목표로 하는 침해 정보 처리 수준은 기존 ESM 제품들에 비해 2~20배 이상으로 훨씬 월등한 것으로 생각된다.

4. 맺음말

대표적인 리서치 기관인 Yankee Group와 Gartner의 자료에 의하면 향후 네트워크 보안은 정책 기반 관리 방식을 중심으로 통합 제품으로 발전할 것이라 전망하고 있다. 따라서, 앞으로는 여러 보안 기능을 포함하고 있는 통합 보안 장비 또는 복합 보안 장비들, 네트워크 보안 전용 장비 및 일반 네트워크 노드들이 기존의 NMS 기능에 보안 관리 기능을 함께 가지고 있는 관리 시스템과 정책 기반으로 정보를 공유하여 날로 다양해지고 복잡해져 가는 사이버 위협에 대처할 것으로 예측된다.

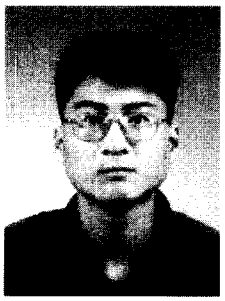
본 고에서는 세계의 네트워크 기술과 보안 기술 발전 추세에 발 맞추어 추진 중인 정책 기반의 실시간 침입 탐지, 대응 및 예측 기능이 복합적으로 융합된 종합 솔루션인 NGSS에 대해서 간략하게 소개하였다. 먼저, 네트워크 보안 기술의 진화 방향 분석을 통해 NGSS 기술개발의 타당성을 살펴보고, NGSS 시스템을 구성하는 보안노드 및 보안관리시스템의 주요 특징을 살펴보았다.

세계적 수준의 NGSS 시스템을 조기 확보함으로써 효율적인 네트워크 정보보호체계 구축 및 관련 산업의 발전 기반을 구축할 수 있다. NGSS의 침입 분석·차단기술을 방화벽, IDS, VPN, ESM 등 기존 보안장비의 기능 및 성능 제고에 활용함으로써 정보보호산업 전반의 기술 경쟁력 향상을 도모할 수 있으며, '04년부터 향후 5년간 세계 정보보호시장에서 국내업체들이 약 17,234억원의 매출증대효과 기대된다. 또한, 확보된 기술을 특화된 시장(중국, 중동 등)에 수출할 수 있을 것이다. 그 이유는 이들 국가들은 미국의 기술을 사용하는데 주저할 것이기 때문이다. 한편, NGSS는 향후 유무선 방송 통합 네트워크인 BcN에 적용 측면 및 확장성 측면에서도 현재의 보안 제품들보다 경쟁 우위를 점할 것으로 예측된다.

참고문헌

[1] 정보통신부, 차세대 능동형 네트워크 정보보호시스템 개발 계획 수정안, 2003. 4.
[2] ETRI, NGSS 기능분석서, 2003. 7.
[3] ETRI, NGSS 시스템 요구사항서 V1.0, 2003. 5.
[4] ETRI, NGSS 시스템 설계서 V1.0, 2003. 6.

[5] ETRI, 차세대 네트워크 보안 구조서, 2002. 11.
[6] Market Trends and Forecast for Firewall and IP Virtual Private Network Equipment: Worldwide, 2001-2006 , Market Trend, Gartner, Oct. 2002.



김 경 우
1998년 : 서울대학교 컴퓨터공학과 졸업
2001년 : 서울대학교 전기컴퓨터공학부 석사
2001년~현재 : 정보통신부 정보화기획실 사무관

<관심분야> 정보통신 정책