BcN 인프라 보호를 위한 다중 도메인 보안 관리 프레임워크와 성능 평가

장 정 숙[†] · 전 용 희[††] · 장 종 수[†††]

요 약

증가된 QoS 제공과 보안 능력, IPv6를 가진 BcN이 다양한 네트워크 애플리케이션을 지원하기 위하여 개발되고 있다. BcN과 같은 고속망에서는 네트워크 자원들이 여러 가지의 침입 행위에 더욱 노출되기 쉽다. 침입의 전파 속도도 기존 인터넷에서보다 더욱 빨라질 것으로 보인다. 본 논문에서는 BcN의 다중 도메인에서 전역적인 침입탐지를 위하여 사용될 수 있는 다중 도메인 보안관리 프레임워크를 제안하고 특성을 기술한다. 성능평가를 위하여, 먼저 보안 노드에 대한 시험 결과를 제시하고 다른 제품과 성능을 비교한다. 다음에 제안된 프레임워크에 대한 OPNET 시뮬레이터를 설계 및 구현하고 시뮬레이션 결과를 제시한다. 시뮬레이션 모델에서는 보안 오버레이 네트워크에서 경보 정보의 성능에 초점을 맞춘다.

키워드 : 광대역통신망, 침입탐지시스템, 보안관리, 통신모델, 성능 평가, 시뮬레이션

Multi-Domain Security Management Framework and Its Performance Evaluation for Protecting BcN Infrastructure

Jang Jung-Sook[†] · Jeon Yong-Hee[††] · Jang Jong-Soo[†††]

ABSTRACT

BcN(Broadband convergence Network) is being developed in order to support a variety of network applications, with enhanced capabilities of QoS(Quality of Service) provisioning and security, and IPv6. In a high-speed network environment such as BcN, it is more likely for the network resources to be exposed to various intrusion activities. The propagation speed of intrusion is also expected to be much faster than in the existing Internet. In this paper, we present a multi-domain security management framework which may be used for a global intrusion detection at multiple domains of BcN and describe its characteristics. For the performance evaluation, we first present test results for the security node and compare with other products. Then we design and implement an OPNET simulator for the proposed framework, and present some simulation results. In the simulation model, we focus on the performance of alert information in the security overlay network.

Key Words : Broadband Convergence Networks, Intrusion Detection System, Security Management, Communication Model, Performance Evaluation, Simulation

1. 서 론

광대역 통합망(BcN : Broadband convergence Network)이란 통신·방송·인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊김 없이 안전하게 이용할 수 있는 차세대 통합네트워크를 말한다. 이를 위하여 BcN 전달망은 고도의 통신망 관리 기능과 보안(Security) 기능, 서비스 품질(QoS : Quality of Service) 보장, IPv6 주소체계의 수용을 통하여 다양한 서비스를 쉽게 창출할 수 있는 개방형 망구조(Open API)를 도입한 통신망으로 유선·무선·방송 등의 다양한 가입자망의 특성을 통합하여 수용해야 하며, 표준 인터페이스를 통해 다양한 응용서비스의 개발 및 이용 환경을 제공할 수 있어야 한다.

정보통신부가 추진하고 있는 IT839 프로젝트에서 3대 인프라로 BcN, IPv6, USN(Ubiquitous Sensor Network)가 있다. BcN과 같은 광대역 통합망 환경에서는 보안침해 사고가 발생하면 그 피해가 전체 네트워크로 광범위하게 확산되어 심각한 통신피해가 우려되고, 사이버 공격의 추세가 지능화, 악성화 되고, 다양한 경로를 통하여 통신망에 쉽게 접근이 가능하여 지기 때문에 네트워크 보안을 위한 대책이 절실히 필요

† 정 회 원 : 대구가톨릭대학교 IT교수
†† 종신회원 : 대구가톨릭대학교 컴퓨터정보통신공학부 교수
††† 정 회 원 : 한국전자통신연구원 정보보호연구단
논문접수 : 2005년 7월 20일, 심사완료 : 2005년 9월 23일

하다. 네트워크 혹은 서비스 제공자는 위협 분석과 위험 평가의 결과를 근거로, 어떤 보안 대책을 수립할 것인지를 결정해야 한다. 다른 형태의 전송 구조를 고려하여, BcN에서 발생할 수 있는 주요한 위협의 형태로는 다음과 같은 것이 있다[1].

- 서비스 거부(Denial of Service : DoS) : 다른 사용자에게 네트워크 자원이 이용가능하지 못하도록 데이터로 네트워크를 범람시킨다.
- 도청 : 송신자와 수신자 사이의 정보를 가로채어 비밀성을 위협한다.
- 해킹 혹은 침입 공격 : 침입자가 어떤 지역이나 자원의 집합에 불법적인 접근을 획득한다.
- 바이러스 및 웜 : 네트워크상에 확산되어 정보를 파괴하고 변조하며 전파된다.
- 위장 공격 : 신원을 위장하여 자원에 대한 접근을 획득한다.
- 재생 공격 : 패킷이나, 패킷 스트림을 시간이 지난 후에 재전송한다.
- 비인가 접근 : 비인가 접근으로 DoS, 도청 혹은 위장 공격이 발생할 수 있고, 위에서 언급한 위협의 결과로서 발생할 수도 있다.
- 정보 변조 : 패킷 변조나, 데이터 조작, 데이터베이스 파괴 등의 공격을 말한다.
- 송수신 부인(repudiation) : 통신에 포함된 사용자가 다른 사용자와의 통신을 일부 혹은 전부를 부정할 수 있다.

BcN의 효율적인 구축을 위하여 국내에서도 대책을 수립하여 추진하고 있다. BcN 구축 기본계획에서, 보안이란 정보통신망 기능의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 제반 위협과 부작용 등의 정보화 역기능에 대한 대응을 의미한다[2]. BcN 보안 대책을 위한 정보보호 기술의 고도화 및 정보보호 체계의 통합화를 통하여 안전하고 신뢰성 있는 건전한 사이버 네트워크 환경 구축을 추진하고 있다.

본 논문에서는 관련 연구로써 BcN 구현을 위하여 고려되어야 할 보안 고려사항들을 살펴보고, BcN 인프라 보호를 위한 대응 기술에 대하여 소개한다. 3장에서는 보안 오버레이 네트워크(SON : Security Overlay Networks)를 이용한 다중 도메인 보안관리 프레임워크를 제안하고, 4장에서는 BcN 인프라 보호를 위하여 하드웨어 기반으로 구현된 고성능 보안 노드의 성능 시험 결과를 제시하고, 침입탐지정보의 전달을 위한 성능평가를 위하여 시뮬레이터를 구축하고 성능평가 결과를 제시하고자 한다.

2. 관련 연구

2.1 보안 요구사항과 대응책

2.1.1 보안 요구사항

어떤 도메인에 대하여 이를 기초로 운용자가 정의하는 보안 서비스의 집합, 메커니즘의 강도를 '보안 정책'이라 한다. 보안 대책은 상황에 의존하여 취해져야 한다. 형식적인 정확한 방법으로 잘 정의된 보안 요구사항을 확립하는 과정은 다소 추상적이다. Alcatel NGN에서는 TIPHON[3]의 위협 분석이 지침서로 사용되었다. 일반적인 보안 요구사항은 다음과 같다 :

- 계정성(accountability) : 한 개체의 행동이 해당 개체에 대하여 유일하게 추적될 수 있도록 보증하는 성질
- 권한 검증 : 접속 권한을 기반으로 접속을 부여하는 권한 부여 기능
- 인증 : 수신된 데이터의 소스를 확인하는 기능

BcN 인프라 정보보호를 위하여, 네트워크의 인입점에서 네트워크 위협을 능동적으로 탐지하고 대응할 수 있는 보안 관리 기술, 네트워크의 발전 속도를 고려한 고성능 네트워크 위협 대응 기술, 알려진(known) 침입 공격에 대한 탐지 기술과 알려지지 않은(unknown) 침입에 의한 과다 트래픽(excessive traffic) 탐지 기술, 유해 트래픽(malicious traffic)에 대한 차단 및 대역폭 제어 기술 등이 요구된다[4].

2.2.2 대응책

대응책은 일반적으로 예방적(preventive)과 탐지적(detective)으로 분류할 수 있다. 상기 위협에 대처할 수 있는 일반적인 대응책은 다음과 같다[1] :

- 인증 : 수신된 데이터의 소스를 확인하는 기능
- 디지털 서명 : 인증 메커니즘을 통하여 메시지 생성자가 서명 코드를 붙임으로써, 메시지 출처와 무결성을 보증한다.
- 접근 제어 : 접근의 허가를 가진 주체만이 객체들에게 접근할 수 있도록 하는 통제 행위
- 가상사설망(VPN) : 인터넷을 통하여 전송되는 데이터를 보호하기 위하여 암호화 기법을 사용한다. 단지 권한이 부여된 사용자만이 VPN을 통하여 연결가능하다.
- 암호화 : 평문 데이터의 암호화 알고리즘에 의한 난해한 형태로의 변환
- 침입탐지 및 방지 : 잠재적인 오용이나 정책 위반을 감시하기 위하여 네트워크 트래픽에 대한 감시를 하며, 공격 시그너처를 조사하여 침입탐지를 수행한다. 침입방지는 침입탐지와 결합하여 가능한 빨리 침입 공격이 성공하지 못하도록 하기 위한 것이다.
- 감사(auditing) 및 기록(logging) : 시스템 상태 정보에 대한 보고수단을 제공하기 위한 것이다.
- 부인방지 대책 : 송수신 부인(repudiation) 방지를 위한 대책을 말한다.

다음 절에서는 위에 기술된 대응책들 중에서 본 논문과 가장 관련이 있는 침입탐지 및 방지에 대하여 기술한다.

2.2 대응 기술

2.2.1 침입탐지

침입탐지시스템(IDS : Intrusion Detection System)은 권한이 부여되지 않거나 승인되지 않은 네트워크 행위를 식별하고, 평가하고, 보고하는 것을 도와주는 도구, 방법, 자원으로 정의될 수 있다[5]. 침입탐지시스템은 전체적인 보안 시스템 구성

의 일부에 지나지 않는다. 방화벽, IDS, IPS(Intrusion Prevention System) 모두가 네트워크로의 침입을 경보하고 방지하기 위하여 함께 사용된다. 다만 이들은 다른 기술을 사용할 뿐이다.

상업용 네트워크 기반 IDS(NIDS : Network-based IDS)는 1990년 중반부터 사용되고 있다[6]. 1세대 상업용 NIDS는 순수한 시그니처-기반(Signature-based) 모델이다. 순수 시그니처 기반 시스템의 문제점을 해결하기 위하여, 2세대 NIDS는 시그니처 대신에 룰(rule)을 사용한다. 여기서는 익스플로잇 시그니처 대신에 패킷 시그니처를 규칙의 집합에 대하여 비교한다. 패킷 시그니처 탐지에서, 트래픽을 정확하게 처리하기 위하여, 데이터의 오번역을 제거하기 위한 기술이 사용되어야 한다[7]. 2세대 NIDS의 성능과 정확성 결핍 문제를 극복하기 위하여, 제 3세대 NIDS는 공격을 탐지하기 위하여 프로토콜 이례(anomaly)를 사용한다. 프로토콜 이례 NIDS는 네트워크상에서 허용되는 프로토콜들의 적절하지 않은 사용을 관찰함으로써 공격을 식별할 수 있다. 프로토콜 이례 탐지(protocol anomaly detection)의 장점은 다음과 같다[7] :

- 공격이 프로토콜 표준으로부터 벗어난다는 사실에 기초하여, 알려지지 않은 새로운 공격을 탐지할 수 있다.
- 다른 탐지 방법을 구현한 시스템을 우회하는 공격을 탐지한다.
- 시그니처-기반 시스템을 회피하기 위하여, 공격의 강도에 영향을 주지 않고, 알려진 공격 패턴의 형식을 변경한 약간 수정된 공격을 탐지한다.

이에 대한 예로써 FTP bounce 공격 탐지와 서류화 되지 않은 버퍼 오버플로 공격 탐지가 있다.

2.2.2 침입방지

침입방지시스템(IPS : Intrusion Prevention System)도 IDS와 마찬가지로 호스트 기반과 네트워크 기반 시스템으로 분류된다[8-10]. 호스트 기반 IPS(HIPS : Host-based IPS)는 가트너의 정의에 의하면, 우선 소프트웨어 제품이어야 하고, 방화벽 규칙 집합과 같은 정책이나 정상/비정상 접근에 대한 학습을 통해 취약한 응용 프로그램을 보호할 수 있어야 하며, 커널과 독립적으로 작동하는 방식과 함께 동작하는 방식으로 구분된다. 전자는 시그니처와 행위 기반 분석 알고리즘을 이용 특정 규칙에 위배되는 이벤트를 필터링하는 제품들로 분류할 수 있다. 후자는 대부분 접근제어 기능을 가진 트러스트(trust) 운영체제 제품들로 분류할 수 있다.

역시 가트너의 정의에 의하면, 네트워크 기반 IPS(NIPS)는 침입방지 능력과 빠른 대응 속도를 위하여 네트워크 라인 상에 위치한 제품이어야 하며, 세션 인식 감시(session aware inspection)를 지원할 수 있는 시스템이다. 그리고 다양한 종류의 방지 방법 및 방식 즉 시그니처, 프로토콜의 비정상 행위 탐지를 통하여 악의적인 세션을 차단하는 것도 필수적이다.

2.3 IDS의 요구사항 및 성능 파라미터

본 절에서는 침입 탐지 시스템의 통신 프레임워크에서 요구사항과 성능 결정 요인들에 대하여 기술한다[11]. 이를 기반으로 제안된 통신 프레임워크의 성능분석을 위한 파라미터를 결정하고자 한다.

분산 침입 탐지 시스템을 구별하는 몇 가지 특징은 다음과 같다 :

- E(event)-박스의 수와 위치
- A(analyzer)-박스의 수와 위치
- 컴포넌트 사이의 조정(coordination)
- 통신 프레임워크

여기서 E-박스는 데이터 수집 장치, A-박스는 데이터 분석 장치에 각각 해당한다. 프레임워크는 실제 통신 메커니즘과 통신 모델로 구성되어 있다. 현재 통신 메커니즘 접근으로는 TCP, UDP, SSH(Secure Shell), SNMP(Simple Network Management Protocol) 등이 사용되고 있다.

IDS를 위한 통신 기법에서 바람직한 몇 가지 특징은 다음과 같다 : 신뢰성(reliability), 보안(security), 인증(authentication), 무결성(integrity), 비밀성(confidentiality), 부인 봉쇄(non-repudiation), 비-복제(non-duplication), 서비스 거부(DOS) 공격에 대한 저항, 확장성(scalability), 속도(speed).

분산 침입 탐지 시스템 기능의 중요한 한 부분은 다른 컴포넌트 사이의 통신이다. 메시지를 교환함으로써 컴포넌트들은 시스템의 전체적인 상태를 알 수 있다. 통신의 붕괴는 시스템의 오동작을 일으키고 실패를 초래할 수 있다. 다음의 요인들은 서로 배타적이지 않으며, 상호 의존적이다[12] : 컴포넌트의 수와 위치, 고려되는 데이터의 형태, 데이터 양, 데이터 생성빈도, 데이터 표현 방법, 데이터의 민감성.

3. 제안된 보안관리 프레임워크

3.1 개요

제안된 시스템은 정책 기반 시스템으로써, 보안 정책 시스템(SPS : Security Policy System)은 중요한 정보와 자원들이 특정한 시스템에서 관리되어 분산되는 방법을 규제하는 법 혹은 규칙을 설정한다. 보안 정책 시스템은 보안 정책 데이터베이스(SPD : Security Policy Database), 보안 정책 서버(SPS : Security Policy Server) 그리고 정책 클라이언트(PC : Policy Client)로 구성되며 보안 정책 프로토콜(SPP : Security Policy Protocol)을 사용하여 정보를 교환한다. 정책의 한 예로, 규칙-기반 정책은 IP 주소, 시간, 프로토콜, 그리고 차단, 로그인, 경고 혹은 통과 허용 같은 조치를 명시하기 위한 지시와 같은 qualifier를 사용하여 보안 정책을 자동으로 시행하도록 해준다[13].

이러한 정책 기반 IDS의 표준 프로토콜로는 COPS, IAP/IDXP, SNMP 등이 있으며, 다음과 같은 기능 및 특성을 가지고 있다.

- COPS(Common Open Policy System) : IETF의 COPS는 정책 기반 네트워크에서 정책서버(PDP)와 클라이언트(PEP) 사이의 정책정보의 전달을 위한 TCP기반의 간단한 질의/응답 프로토콜이다. 프로토콜 자체 수정 없이

확장을 통한 다양한 클라이언트 타입을 지원한다. COPS는 TCP 기반으로 상위 도메인의 정책 제공 및 통제 목적을 위한 정책 전달 프로토콜이다[14].

- Alert Protocol) : IETF의 IDWG에서 침입 경보 프로토콜(IAP)을 제안하였다. 침입 탐지 구성 요소들 사이(sensor/analyzer와 managers)에 침입 경보 데이터(Intrusion alert data)를 교환하기위한 응용 계층의 프로토콜이다. 전달되는 경보는 IDMEF(Intrusion Detection Message Exchange Format)에 명세 되어 있다. 현재 IDMEF의 메시지로는 Alert와 Heartbeat 두 가지가 정의되어 있다[15].

3.2 글로벌 네트워크 보안 관리 구조

네트워크상의 통신 및 시스템을 안전하게 보호하기 위해서는 네트워크 차원의 보안관리가 필요하다. 네트워크 차원의 보안 관리는 인접한 서비스 제공업자와의 보안관련 정보의 공유를 통하여 협력할 수 있어야만 가능하다. 네트워크 차원의 정보보호 서비스의 중요성이 증가하고 있어 수백 Mbps에서 기가급까지 처리 가능한 네트워크 정보보호 제품이 등장하고 있지만 개별 시스템 단위의 보안기능의 한계가 존재한다.

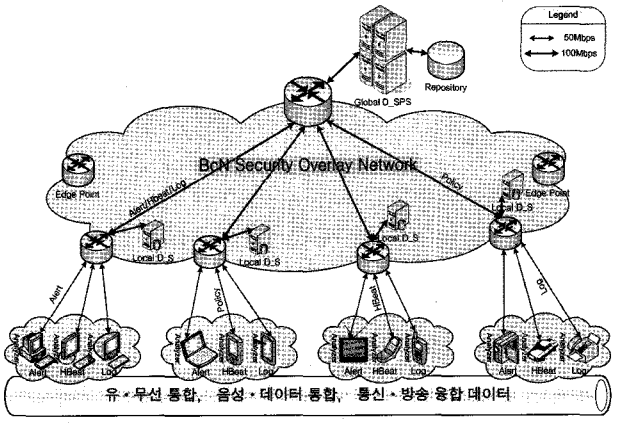
이러한 문제를 해결하기위해서 네트워크 차원의 종합적인 침입탐지 분석을 수행하는 글로벌 네트워크 보안관리 구조의 정립이 주요한 문제로 대두되고 있으며 분산 침입탐지시스템에 체계적인 정책 프레임워크와 종합적인 계층적 분석기법을 적용하여 글로벌 네트워크보안관리가 가능하다.

3.2.1 시스템 구조

네트워크 차원의 정보보호서비스를 제공하기위해 보안 노드를 광역 네트워크 전역에 조직적으로 분산시켜 이를 중앙에서 통합 관리함으로서 기존의 단일 환경의 정보보호서비스가 가지는 제약적인 문제점을 해결할 수 있다. 즉, 트래픽의 과다한 증가와 다양한 공격 유형에 보다 효율적으로 대응하기 위해서는 현재의 지역적 보안 환경을 광역적 보안 환경으로 확장하여 시스템 상호간의 조직적이고 유기적인 연동을 가능하게 하는 정책기반 프레임워크를 이용하여 네트워크를 보안관리 할 수 있다. 또한 다양한 정보를 수집하고 통합 분석하여 조기에 대응하기위해서는 계층적 통합 분석기법을 적용할 수 있다.

그러므로 정책기반 프레임워크에서 침입탐지 및 대응기능을 계층적으로 분리하고 광역 네트워크 전역에 조직적으로 분산시켜 이를 최상위의 정책서버에서 통합 관리함으로서 기존의 단면적이고 단일 환경의 제약적인 문제점을 해결 할 수 있고 계층적 분석을 통한 침입예측 및 환경에 적합한 대응정책의 결정과 인가가 가능할 것이며 글로벌 네트워크 보안 제어관리가 가능하다.

(그림 1)은 호스트 기반과 네트워크 기반 그리고 분산 침입탐지시스템과 중앙 집중 형태의 침입탐지시스템 관리 구조를 가지는 전역적인 네트워크 보안관리가 가능한 제안된 다중 도메인 보안관리 모델이다. 제안된 다중 도메인 보안관리 모델은 전역적인 침입탐지를 수행하기 위해서 IETF 정책 프레임워크를 기반으로 분석기, 지역적인 도메인 그리고 보안정책 서버로 구성되는 전역적인 도메인의 계층적인 구조를 가지고 있다. 가장 하위의 분석기는 각 도메인에서 다양한 형태의 침입을 탐지하는 에이전트들로 구성되어 있고 각 에이전트들은 그들의 특정한 탐지정보를 상위의 지역적인 도메인 매니저에게 보고한다. 에이전트들로 구성된 분석기에서는 수립된 보안정책을 기반으로 침입을 분석한다[11, 16].



(그림 1) 제안된 다중 도메인 보안관리 모델

분석기에는 다양한 침입을 탐지하는 에이전트들이 있다. 네트워크 기반 침입을 분석하여 경보를 발행하는 에이전트, 분석기의 현재 상태정보를 정기적으로 상위의 매니저에게 보고하는 에이전트 그리고 호스트 기반 로그를 바탕으로 정보를 전달하는 에이전트들이 있다. 각 분석기는 경보와 로그에 관한 메시지를 비동기적으로 그리고 분석기의 상태정보는 정기적으로 상위의 매니저에게 보고 하도록 하였다. 상위의 매니저는 보고받은 침입 탐지정보들을 분석하고 최상위의 전역적인 도메인으로 보고한 후 그들의 정보를 저장소에 기록한다. 최상위의 전역적인 도메인 매니저는 보고 받은 탐지정보를 기반으로 보안정책 서버를 통한 전역적인 보안정책을 수립 한 후 보안정책을 하위의 노드들에게 하달한다.

본 논문에서 제안한 통신 모델은 각 에이전트에서 독립적인 침입 탐지를 수행한다는 측면에서 분산 침입탐지라 할 수 있으며, 지역 도메인으로부터 경보나 다른 중요한 이벤트 데이터를 상위의 전역 매니저로 전송하여, 대규모 분산 시스템에서의 침입탐지시스템 사이의 정보 교환을 허용하는 구조를 취하고 있다는 것이 특징이다. 분산 침입탐지시스템 구조에서는 글로벌 네트워크 보안제어 프레임워크를 위해서 체계적인 보안관리가 가능한 정책기반 관리구조와 종합적인 보안 상황에 대한 판단과 수단을 제공하는 계층적인 침입분석기법을 분석한다[17, 18]. 제안된 다중 도메인보안관리 프레임워크의 주요 특징은 아래와 같다.

가. 글로벌 프레임워크

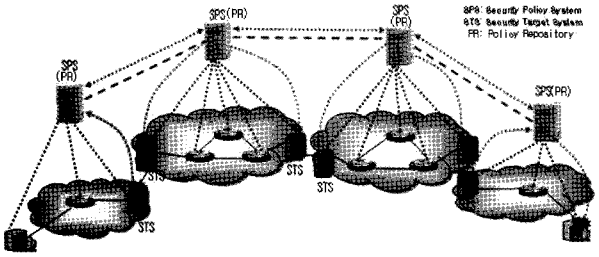
글로벌 네트워크보안관리 기술이란 지역망의 보안 관리방법을 보완하기위한 네트워크 차원의 보안 관리로써 망 인입점에서 유해 트래픽을 분석 및 차단하여 네트워크의 성능 저

하를 사전에 방지하고 네트워크의 자원 및 주요 통신 장비의 보호기능을 수행하는 것을 목표로 한다.

글로벌 보안관리 네트워크는 보안 오버레이 망의 구조를 가지며 인접 도메인과의 보안관련 정보의 교환 및 상호협력을 통하여 사용자가 사용하는 광역망에서 동일한 보안 서비스 품질을 유지할 수 있을 것이며 코어망의 보안성을 강화하고 사용자의 서비스 트래픽을 안정적으로 제공할 수 있다.

나. 보안정책기반 관리구조

구조적이고 체계적인 관리와 통합적인 관리를 제공 할 수 있도록 IETF 정책기반 프레임워크를 적용하여 네트워크를 보안관리 할 수 있다. 정책기반 네트워크보안관리 프레임워크는 네트워크 자원에 대한 운용 및 보안관리를 공통된 정책에 따라 일관성 있게 제어 할 수 있는 기능을 제공한다. 보안정책기반의 보안관리 프레임워크는 보안정책시스템(SPS)의 보안정책서버와 보안정책서버의 관리를 받는 다수개의 정책대상시스템(STS)으로 구성된 중앙 집중화된 관리구조를 갖는다. 여기서 보안정책 서버가 일관성 있는 정책으로 관리하는 영역을 도메인이라 하며 이 도메인에서 발생하는 모든 보안 관련 상황은 해당 도메인의 보안정책서버로 전달되어 체계적이고 종합적으로 관리되며 필요시 인접 도메인으로 전파할 수 있다. (그림 2)는 보안정책 관리 구조를 보여준다.



(그림 2) 보안정책 관리구조

이 정책 프레임워크에서는 보안정책시스템은 정책서버, 정책저장소로 구성되고 그리고 보안대상시스템은 정책대상의 기능 구성요소를 가진다. 정책서버는 크게 정책관리도구 및 정책 결정기능으로 구성되며 정책저장소는 정책서버와 독립적인 시스템으로 존재 할 수도 있다. 또한 정책대상은 정책을 실행하는 네트워크 시스템으로 자원관리관점에서는 경계라우터가 이에 해당된다.

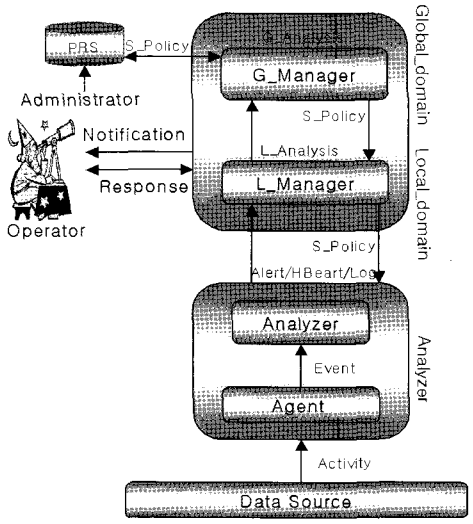
다. 계층적인 침입분석기법

보안에 관한 분석 장비들의 개별관리와 이들 간의 연동이 불가능함으로 네트워크 관리자들은 통합 관리의 어려움을 가지게 되고 보안시스템의 운용에 한계를 보이게 된다. 개별 보안 장비들은 단일 시스템 수준에서의 단면적인 침입분석을 수행하므로 네트워크 차원의 종합적인 침입분석과 예측을 수행할 수 없는 문제점을 가지게 된다.

이러한 문제를 해결하기 위해서 보안장비의 분석과 이의 이벤트 정보와 경보정보를 기반으로 하여 네트워크 전반에 걸친 분석을 수행하도록 단순분석과 통계적 분석으로 이루어진 계층적인 분석기법을 사용한다. 계층적인 침입분석은 정책도메인 내에서 발생하는 모든 보안 이벤트정보를 수집하고 체계적인 관리를 통하여 전체 정책 도메인에 따른 보안상황의 분석을 수행함으로 종합적인 네트워크보안관리 프레임워크를 구축할 수 있다.

망의 인입점에 위치하는 보안 노드는 시그너처 기반의 침입탐지를 수행하는 비교분석과 트래픽 변화 유형을 모니터하는 관측분석을 통한 하위계층 침입분석을 수행한다 하위계층 침입분석의 결과를 기반으로 보안 노드에서 실시간 대응을 하거나 상위계층의 보안정책서버로 경보 정보를 전달함으로써 상위계층 침입 예측을 가능하게 한다.

(그림 3)은 제안된 모델의 계층적인 통신 프로세스를 보여준다.



(그림 3) 제안된 모델의 통신 프로세스

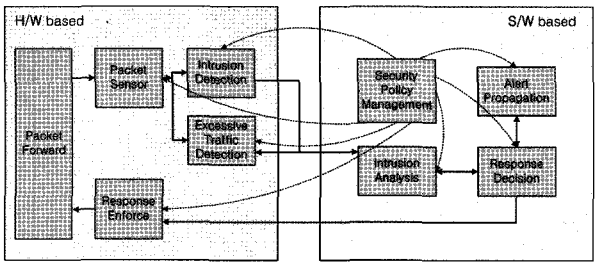
네트워크 전체의 보안관련 정보를 수집하고 관리하는 보안정책서버는 통계적 데이터를 기반으로 유사성 분석, 잠재성 분석과 침입 가능성 분석을 통하여 상위계층에서 침입 예측을 수행한다. 이를 토대로 네트워크 내에 적용할 대응정책을 결정하거나 침입의 징후에 대한 정보를 인접 도메인과의 통신을 통해 공유하여 글로벌 네트워크 차원의 침입 대응 체계를 구축할 수 있으므로 통합적인 보안관리가 가능하다.

3.2.2 노드 구조

인터넷의 폭발적인 사용의 증가로 정보통신의 인프라는 기가비트 이더넷 환경 같은 고속화와 대용량화로 네트워크 환경이 현실화되고 있으며 정확한 탐지, 나아가 예방까지 그리고 높은 성능을 기반으로 데이터를 처리할 수 있는 보안 기법들이 연구 중에 있다. 기가 급 침입탐지시스템 개발을 위한 구조와 시스템 성능을 예측하기위하여 시스템 성능분석에 대한 연구가 중요하다. 시스템의 성능은 칩 상에 구현된 하드웨어 특성과 그들에서 돌아가는 소프트웨어에 의존된다. 침입탐지 노드의 시스템 성능분석으로 시스템의 병목 현상을 규명

할 수 있고 이를 통하여 패킷 처리 과정의 문제점을 발견할 수 있으며 구조 개선이 가능하다. 아울러 효율적인 패킷 처리 알고리즘의 발견을 통한 침입탐지 성능의 개선이 가능하다.

본 절에서는 고속 네트워크 환경에서 침입탐지 및 대응을 제공하기위한 기가비트 침입탐지시스템의 보안 노드에 대한 구조를 분석한다. 네트워크 속도의 증가에 따른 침입탐지 기술도 상응하는 고속침입탐지 기술이 요구되며, 이에 따라 10G급 이상의 보안 어플라이언스 및 보안 엔진의 개발이 요구된다. 그러므로 시스템의 구조에 따른 성능분석 연구는 매우 중요하여 필수적으로 수행되어야 한다. (그림 4)는 고속으로 침입탐지 및 대응기능을 제공하는 기가비트 침입탐지시스템의 보안 노드 구조의 시스템 블록 다이어그램이다[19].



(그림 4) 보안 노드의 블록 다이어그램

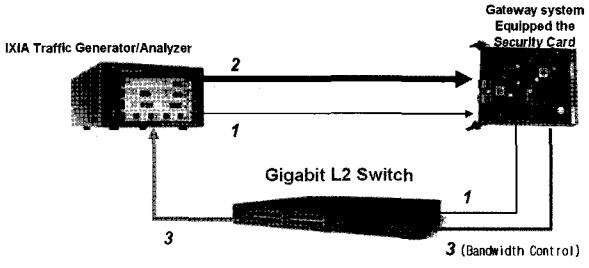
보안 노드는 하드웨어를 기반으로 하여 침입에 대해 고속의 시그너처(signature) 탐지를 하는 이더넷 인터페이스 보안 카드를 사용함으로써 네트워크 유해 트래픽의 검출 및 차단을 가속화시키며 기가비트 네트워크 속도를 지원할 수 있다. 또한 트래픽 모니터링뿐만 아니라 실시간 대응 기능을 지원하며 네트워크상에서 스텔스(stealth) 형태의 동작으로 자체 시스템 보안이 용이하다. 침입분석 후 유해한 트래픽이라 판정되면 피해를 최소화 하도록 즉각적인 대응 체계를 갖는 구조이다((그림 4) 참조).

4. 성능평가

4.1 보안 노드 성능 시험

(그림 5)는 보안노드(Gateway system) 성능 평가를 위한 IXIA 트래픽 발생기와 분석기, 기가비트 L2 교환기 및 보안 카드로 이루어진 테스트 베드를 보여준다.

<표 1>은 보안노드의 기능 중에서 비정상 트래픽 감지 및 대응 기능, 침해 탐지 및 차단 기능에 대한 성능시험 결과를 보여준다. 비정상 트래픽 감지 및 대응 기능에서 64, 1500 바이트의 침해 패킷에 대하여 다른 제품과 동일한 성능을 보여주었으며, 연결 설정 능력에서는 초당 더 많은 처리 능력을 보여주고 있다. 침해 탐지 및 차단 가능에서 처리 가능한 네트워크 용량과 시그너처 기반 탐지기능 모두에서 타사 제품과 비교하여 우수한 성능을 보여주고 있다.



(그림 5) 보안 노드 테스트 베드

〈표 1〉 보안 노드 시험 결과

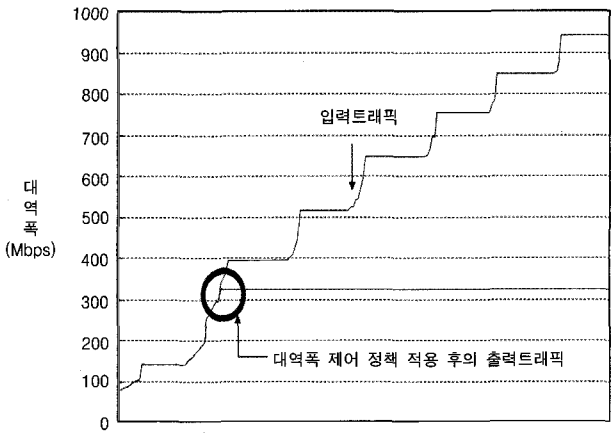
SSS 기능		계획 수준	결과 수준 (주1)	상용제품 비교(주2)	상용제품 비교2 (주2)
비정상 트래픽 감지 및 대응	처리가능한 Network Capacity	790 Mbps (64byte), 1 Gbps (1500 byte) Lossless	790 Mbps (64byte), 1 Gbps (1500 byte) Lossless	*AAHPS:* 790 Mbps (64byte) (주3), 1 Gbps (1500 byte) Lossless	*BAHPS:* 790 Mbps (64byte), 1 Gbps (1500 byte) Lossless
	Connection Setup 처리 능력	60000/s	64000/s	*AAHPS:* 54000/s	*BAHPS:* 25000/s
침해 탐지 및 차단 기능	처리가능한 Network Capacity	790 Mbps (64byte), 1 Gbps (1500 byte) Lossless	790 Mbps (64byte), 1 Gbps (1500 byte) Lossless	*AAHPS:* 600 Mbps (64byte), 1 Gbps (1500 byte)	*CAHPS:* 150 Mbps (64byte), 500 Mbps (1500 byte)
	Signature 기반 탐지 기능	100%	100%	*AAHPS :* 80%	*CAHPS:* 92%

(주 1) 시험장비 측정치
(주 2) Tolly Group Report no.204146 참조
(주 3) Gigabit Ethernet에서 64byte 패킷의 이론상 최대 bps

DDoS 공격에 대한 시험을 위하여 다음과 같은 시나리오를 수행하였다.

- 비정상 트래픽의 생성을 (그림 5)의 트래픽 발생기 포트 (2)로부터 40Mbps 단위로 1Gbps까지 증가시켰다.
- 비정상 트래픽((그림 5)의 3)에 대하여 rate-limiting 룰을 시행한다 : 보안 카드를 위한 룰의 생성과 실행은 정책 관리자에 의하여 시행된다.
- 트래픽 분석기 수신단에서 40Mbps에서 각 플로를 폴리싱한다.
- 비정상 트래픽만 폴리싱하고 정상 트래픽은 전송한다.

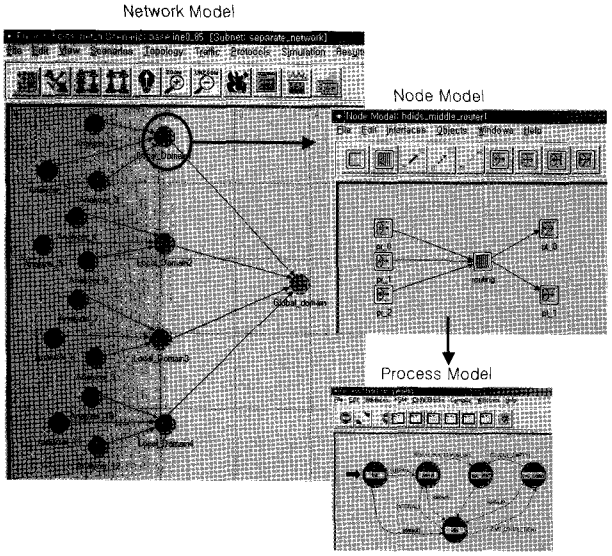
위의 시나리오에서 대역폭 제어기는 40Mbps 율에서 출력 트래픽을 제어한다. 그러므로 여덟 개의 플로 트래픽 합은 320Mbps가 된다. 출력 트래픽 율은 320Mbps이며, 정상 40Mbps 트래픽은 (그림 6)에서 보여주는 것과 같이 아무런 손실 없이 전송됨을 시험하였다.



(그림 6) 대역폭 제어에 의한 과다트래픽 제어(320Mbps)

4.2 시뮬레이터 설계 및 구현

제안된 다중 도메인 보안관리 모델의 구현과 경보정보의 성능평가를 위해서 시뮬레이터 설계와 구현에는 OPNET Modeler를 사용하였다. (그림 7)은 구현된 시뮬레이터의 네트워크 모델과 하나의 노드 모델과 프로세스 모델의 예를 보여준다.



(그림 7) 시뮬레이터 구현에서 각 레벨의 모델 예

<표 2>는 본 IDS 평가 모델에서 적용한 이벤트별 데이터 크기이다. 시뮬레이터 구현에는 각 노드 이벤트 전송 율에서 분석기와 지역적인 도메인 연결은 50 Mbps, 전역적인 도메인과의 연결은 150 Mbps를 통하여 연결하였으며 각 분석기와 정책 서버에서는 데이터의 스케줄링과 처리를 위하여 유한버퍼를 사용하였다.

〈표 2〉 이벤트별 데이터 크기(단위 : 바이트)

이벤트 종류	Alert	HeartBeat	Log 데이터
크기	512	512	440

4.3 모의실험 및 성능분석

모의실험과 성능분석에서는 다중 도메인보안관리 모델을 대상으로 개발된 시뮬레이터를 이용하여 성능 모의실험을 통한 결과를 제시하고 분석한다. 에이전트가 탐지한 정보의 보고 및 보안 정책 서버의 보안 정책 하달은 독립적인 네트워크로 가정하여 모의 실험하였으며 성능분석은 두 단계에서 진행하였다. 첫 단계는 침입을 탐지한 분석기에서 최상위의 전역적인 도메인 보안 정책 서버까지 네트워크 수준에서 정보 전달에 따른 성능 분석이며 두 번째는 보안 정책 서버에서 분석기까지 보안 정책의 하달 성능을 분석한다. 성능 분석 파라미터로는 지연(delay)만을 사용하였다. 본 성능 분석에서 사용한 파라미터는 2.3절에서 기술된 성능 결정 요인들과 일반적인 네트워크 성능 분석 파라미터들을 고려하여 결정하였으며, 데이터의 표현 방법과 민감성에 대한 성능 분석은 수행하지 않았다.

4.3.1 성능평가 매개변수

매개변수별 성능 평가 착안점은 <표 3>과 같다.

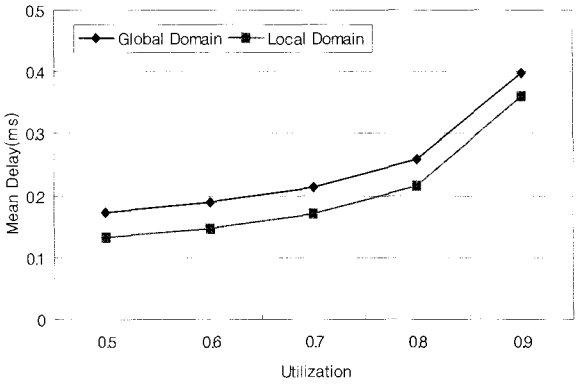
〈표 3〉 매개 변수에 따른 성능평가 항목

성능 평가 항목
네트워크 이용률의 영향
이벤트 데이터 형태와 크기의 영향
에이전트 수의 영향
데이터 생성빈도의 영향
핫-스폿의 영향
백그라운드 트래픽의 영향

4.3.2 성능 평가

가. 네트워크 이용률의 영향

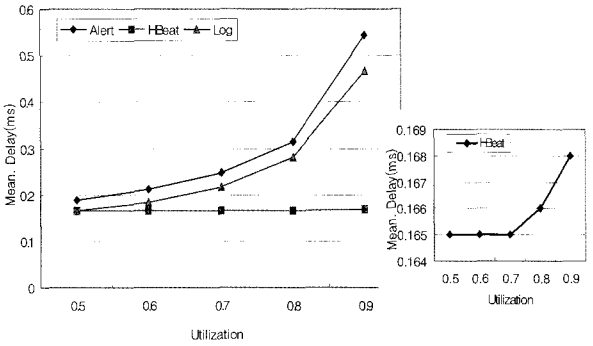
(그림 8)과 (그림 9)는 침입 탐지정보들을 전역적인 도메인 내 보안정책 서버에게 보고 할 때의 각 이벤트의 평균 지연 성능을 나타낸다. (그림 8)은 전역적인 도메인과 지역적인 도메인에서 입력 부하의 크기(즉 네트워크 이용률)의 변화에 따른 전송 패킷의 평균 지연을 보여준다. 지연은 이용률 0.7이상에서는 지수적으로 크게 증가하는 것을 볼 수 있다.



(그림 8) 네트워크 이용률에 따른 지연

나. 이벤트 데이터 형태와 크기의 영향

(그림 9)는 각 이벤트 종류에 따른 지연 성능을 나타낸다.

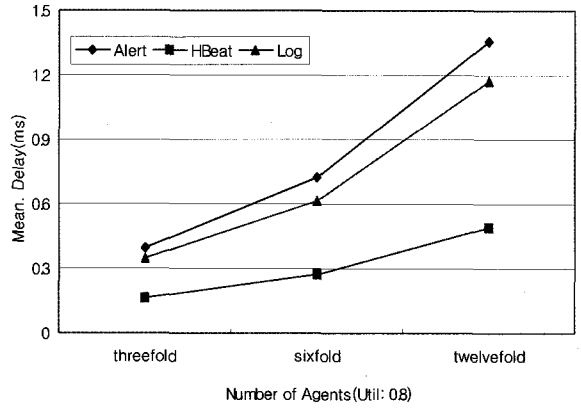


(그림 9) 이벤트 종류에 따른 지연

경보와 로그 이벤트는 지연이 이용률에 따라 증가하는 추이를 확연히 보이며 분석기 상태정보는 네트워크의 상태 변화에서도 정기적인 보고가 이루어지므로 가시적인 지연 성능은 이용률에 따라 다른 이벤트 데이터에 비하여 상대적으로 지연 변화가 작은 것으로 분석된다. 그러나 (그림 9)에서 상태정보를 좀 더 상세하게 분석하여 보면 지연이 미세하게 이용률에 따라 증가함을 보여준다.

다. 에이전트 수의 영향

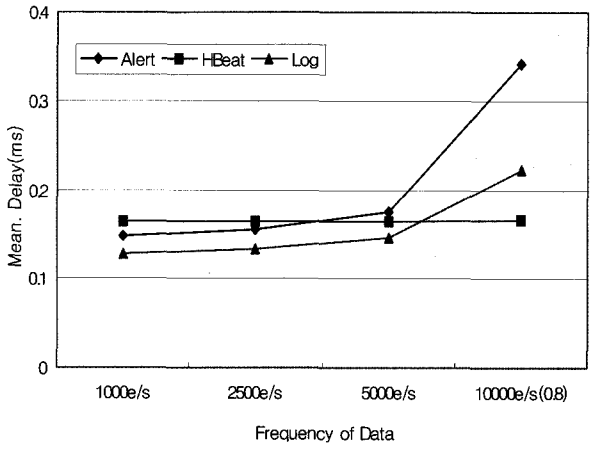
전역적인 보안을 위한 분산 침입탐지시스템에서 계위를 통한 통신 메커니즘을 결정하는 요인 중의 하나가 침입을 탐지하는 컴포넌트 수, 즉 에이전트 수이다. (그림 10)은 에이전트 수가 증가함에 따라 지연이 증가함을 보여준다. 에이전트 수를 3배, 6배, 12배로 증가시켰을 때 네트워크의 지연 성능이 크게 증가함을 보여준다.



(그림 10) 에이전트 수에 따른 지연

라. 데이터 생성빈도의 영향

이벤트의 발생 빈도가 증가하여 과다한 이벤트의 생성빈도를 가질 때 네트워크 성능에 미치는 영향을 분석하였다. (그림 11)은 데이터 생성빈도에 따른 지연 성능을 나타낸다.

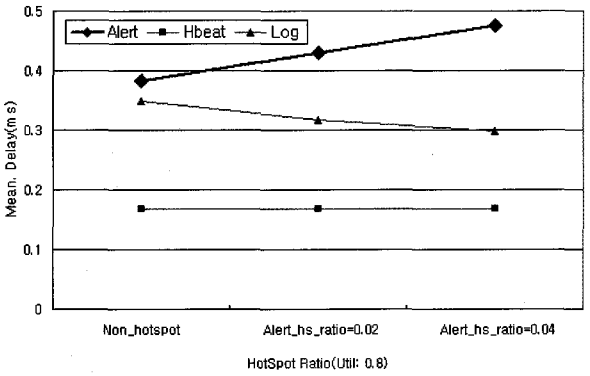


(그림 11) 데이터 생성빈도에 따른 지연

분산 서비스 거부 공격 같은 공격이 발생하면 다른 도메인에 존재하는 여러 에이전트들로부터 공격 발생으로 인한 이벤트의 빈도수가 과다하게 생성 될 수 있고 이것은 또한 네트워크 성능에 심대한 영향을 미칠 수 있음을 알 수 있다. 반면에 정기적인 상태정보의 전달 성능은 상대적으로 영향이 작음을 볼 수 있다.

마. 핫 스폿의 영향

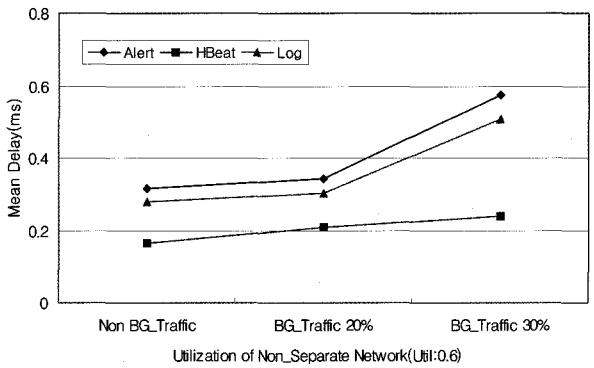
핫 스폿(Hot Spot)이란 특정한 데이터 형태의 이벤트가 집중적으로 발생하는 현상으로 핫 스폿을 이용하여 특정 부분의 네트워크에 미치는 성능을 분석 할 수 있다. (그림 12)는 경보 데이터의 핫 스폿 영향을 보여준다. 전체 네트워크 이용률을 일정하게 유지하고 (그림 12)에서는 경보 데이터의 핫 스폿이 증가할수록 경보 데이터의 지연은 증가하는 반면, 비 핫스폿 데이터인 로그 데이터의 지연 성능은 낮아짐을 또한 나타낸다. 상태 정보 에이전트는 정기적인 이벤트 발생으로 인하여 지연의 변화는 거의 없음을 보여준다.



(그림 12) 경보 데이터의 핫 스폿 영향

바. 백그라운드 트래픽의 영향

다중 도메인 보안관리를 위한 혼합형 IDS 평가 모델의 성능은 모두 독립적인 네트워크(separate-network)라는 가정 하에 분석하였다. 비 독립 네트워크(non-separate network)는 기존의 네트워크에서 사용하고 있는 트래픽이 있음을 의미하는 것으로 백그라운드 트래픽(background traffic)을 얼마나



(그림 13) 백그라운드 트래픽의 영향

사용하고 있느냐에 따른 영향을 분석한 것이다. (그림 13)은 백그라운드 트래픽을 사용하고 있을 경우에 대한 네트워크의 성능을 보여준다. 백그라운드 트래픽율이 증가할수록 상태 정보 데이터를 포함하여 모든 유형의 데이터에 대한 네트워크의 지연이 크게 증가함을 보여준다. IDS 정보를 일반 네트워크 트래픽과 같이 전송할 경우 암호화를 위한 지연도 추가되는 것을 고려하면, 보안 정보 전달을 위한 독립적인 네트워크의 사용이 장점이 많을 것으로 분석된다.

사. 결점 감내 구조와 분석

본 논문에서 제시한 다중 도메인 보안관리를 위한 혼합형 IDS 모델은 분산 IDS에서 중앙 집중형태의 보안 정책 서버까지 계층적으로 구성되어 전역적인 보안 관리를 하는 구조이다. 전역적인 도메인 내 정책서버는 단일화로 구성되어있다. 최상위 매니저인 정책 서버의 실패는 곧 모든 보안 정책의 실행이 불가능함을 의미하다. 그러므로 보안 정책 서버의 이원화를 통하여 결점에 적응하는 구조를 설계하고 구현하여 성능을 분석하였다. 각 지연 도메인 분석기에서 보고 받은 탐지 정보들을 지역 도메인 서버에서는 이원화 구조로 이루어진 전역 보안 정책 서버에게 보고하도록 되어있다.

결점 감내 구조에서는 각기 다른 연결(link)을 통하여 이원화된 보안 정책 서버에게 정보를 보고 한다. 근원지의 분석기 정보들은 주(primary) 보안 정책서버에 보고하고 지역적인 도메인 내 서버에서 복사된 패킷은 백업 보안 정책 서버에게 보고된다. 주 보안 정책 서버에 도달한 지연 성능은 단일 보안 정책 서버 시스템과 비교했을 때 네트워크의 성능에는 거의 차이가 없음이 분석되었다. 다만 보안 정책 서버의 이원화와 링크 추가에 따른 비용이 추가적으로 필요할 것이다.

5. 결론 및 향후 연구

BcN 전달망의 특징은 QoS 보장, 보안 기능 제공, IPv6 수용, 개방형 망 구조로 요약할 수 있다. BcN 환경에서는 보안 사고 발생 시에 그 피해가 전체적인 정보통신 인프라에 보다 빠르게 광범위하게 확산될 수 있기 때문에 더욱 심각한 통신 피해가 우려되고, 따라서 BcN을 위한 보안 대책이 적절히 수립되어야 한다. 그러나 국내에서 아직 BcN의 보안 관련 기술에 대한 참고문헌이 거의 없는 실정이다. 따라서 본 논문에서는 관련연구로써 BcN 보안 취약성과 요구사항에 대하여 살펴보고, BcN 인프라 보호 기술에 대하여 기술하였다.

BcN 보안을 위해서 개별 시스템 단위의 과대한 트래픽 분석과 다양한 침입 유형에 보다 능동적으로 대응하기 위하여 지역적 보안환경에서 광역적인 보안환경으로 적용하기 위한 글로벌 네트워크 보안제어 프레임워크 기술이 필요하다. 글로벌 네트워크 보안제어 프레임워크에서는 각 지역 망의 출력 트래픽들의 종합 분석과 망의 구성과 상태정보, 관리정보 및 통계정보를 다단계 분석으로 침입을 예측하고, 환경에 적합한 대응정책의 결정이 가능하게 된다. 이를 위하여 고속화 침입 탐지 엔진, 전달 정보를 축약하기 위한 기법 및 전달 프로토콜의 개발, 정보를 공유하기 위한 협력 메커니즘의 수립 그리고 종합적인 침입 대응 시나리오 등이 필요하다.

이러한 글로벌 프레임워크에서 컴포넌트 사이의 통신은 전체 시스템 기능성의 한 중요한 부분이다. 컴포넌트들은 통신 메시지를 통하여 시스템의 전반적인 상태를 얻을 수 있기 때문에, 통신의 붕괴는 전체 시스템의 오동작을 유발하거나 실패하게 만들 수 있다. 따라서 BcN 환경에서 다중 도메인 보안관리를 가능하게 하는 모델을 제안하였다. 제안한 통신 모델을 대상으로 모델링을 수행하고 시뮬레이터를 설계 및 구현하였다. 성능 평가를 위해서 글로벌 프레임워크의 통신 메커니즘을 결정하는 주요 요인인 침입을 탐지하는 컴포넌트의 수, 네트워크 이용률, 이벤트 데이터 형태와 크기 그리고 데이터 생성빈도 등에 대하여 모의실험을 수행하였다. 그 결과, 지나친 에이전트 수는 네트워크 성능에 영향을 미치는 것으로 분석되었다. 다음에 이벤트의 발생 빈도에 따른 네트워크의 성능을 분석하였다. 경보의 생성 빈도수가 증가함에 따라 과다한 트래픽이 생성되어 네트워크 성능에 심대한 영향을 미칠 수 있음이 분석되었다. 본 논문에서 제시된 결과는 종합적인 네트워크 보안관리를 위한 시스템 설계에 적용 할 수 있을 것으로 사료된다.

향후 BcN 보안을 위하여 네트워크 간의 유기적인 협력을 통한 글로벌 대응 체계의 구축과, 네트워크 간 교환 되는 정보보호 관련정보의 표준화 및 교환 의무화를 위한 방안이 필요하다. 또한 안전한 광대역 통합망의 구현을 위하여 BcN에 관련된 보안 기술의 연구개발이 체계적으로 추진될 필요가 있다고 생각된다.

참 고 문 헌

[1] B. Gamm, B. Howard, O. Paridaens, "Security features required in an NGN", Alcatel Telecommunications Review, 2nd Quarter 2001, pp.129-133.

[2] 정보통신부 BcN 구축 기본 계획(2. 통합망 보안기능 고도화), pp76-83, 2004년 2월, 한국전산원.

[3] "Telecommunications and Internet Protocol Harmonization over Networks(TIPHON) Security; Threat Analysis", DTR/TIPHON-08002 V0.1.9 (2001-02-09).

[4] 서동일, 김광식, 장종수, 손승원, "IT 839 전략 추진을 위한 정보보호 기술개발 방향", 한국전자통신연구원 전자통신동향분석 제 20권 제 1호, 2005년 2월.

[5] Carl Endorf, Eugene Schultz, and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004.

[6] Eric Ahlm, Is Intrusion Prevention Changing Information Security?, Rev. Ver. 1.1, March 2004, Vigilar Inc..

[7] A White Paper by NetScreen Technologies Inc., Intrusion Detection and Prevention : Protecting your network from attacks, version 2.0, http://www.netscreen.com

[8] Ian Poynter and Brad Doctor, Beyond the firewall : The next level of network security, StillSecure, Jan., 2003.

[9] Top Layer White Paper, Beyond IDS : Essentials of Network Intrusion Prevention, pp.1-18, Nov., 2002.
[10] Neil Desai, Intrusion Prevention Systems : the Next Step in the Evolution of IDS, http://www.securityfocus.com/printable/infocus/1670, Feb., 2003.
[11] Diego Martin Zamboni, "Using Internal Sensors for Computer Intrusion Detection", Ph. D. dissertation, Purdue University, *CERIAS* TR 2001-42, August, 2001.
[12] Rajeev Gopalakrishna, "A Framework for Distributed Intrusion Detection using Interest-Driven Cooperating Agents", *CERIAS Tech.* Report 2001-44, Purdue University, 2001.
[13] Madalina Baltatu, Antonio Lioy, and Daniele Mazzocchi, "Security Policy System : status and perspective", pp.278-284, 1999.
[14] IETF, RFC 3084, "COPS Usage for Policy Provisioning (COPS-PR)", March, 2001.
[15] D. Curry, H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition", IETF Internet Draft, draft-ietf-idwg-idmef-xml-07.txt, Jun., 2002.
[16] IP Security Policy, http://www.ietf.org/html.charters/ipsp-charter.html
[17] 장종수, 김기영, 류걸우, "안전한 정보보호 인프라 제공을 위한 글로벌 네트워크 보안제어 프레임워크", *한국통신학회지*, 제19권 8호, pp.1146-1156, 2002년 8월.
[18] M. Stevens, Policy Framework Internet Draft, draft-ietf-policy-framework-05.txt, Sep., 1999.
[19] 김병구, 김익균, 이종국, 장종수, "고속 침입 탐지 및 대응을 위한 기가비트 침입탐지시스템의 구현", *제8회 COMSW 학술대회 논문집*, pp. 51-55, 2003. 7월.

장 정 숙

e-mail : jsukjj@cu.ac.kr
1989년~1991년 경일대학교 공과대학 컴퓨터공학과(학사)
1992년~1995년 대구가톨릭대학교 교육대학원 전자계산교육전공(석사)
1998년~2004년 대구가톨릭대학교 대학원 컴퓨터·정보통신공학 전공 이학박사
2004년~현재 대구가톨릭대학교 컴퓨터정보통신공학부 IT교수
관심분야 : 임베디드 네트워크 보안, BcN & QoS 보안, 홈네트워크 보안, 통신망 성능분석,

전 용 희

e-mail : yhjeon@cu.ac.kr
1978년 고려대학교 전기공학과(학사)
1989년 North Carolina State University Elec. and Comp. Eng.(석사)
1992년 North Carolina State University Elec. and Comp. Eng.(박사)
1989년 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년~1992년 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992년~1994년 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년~2003년 대구가톨릭대학교 공과대학장 역임
2004년~2005년 한국전자통신연구원 정보보호연구단 초빙연구원
관심분야 : 네트워크 보안, BcN QoS & Security, 통신망 성능분석

장 종 수

e-mail : jsjang@etri.re.kr
1984년 경북대학교 전자공학과(학사)
1986년 경북대학교 전자공학과(석사)
2000년 충북대학교 컴퓨터공학과(공학박사)
1989년~현재 한국전자통신연구원 정보보호연구단 네트워크보안그룹 그룹장
관심분야 : 네트워크보안, 웹서비스보안, Secure OS, IDS/IPS, Traffic Management