韓國 컴퓨터情報學會 論文誌
第8卷 第1號, 2003. 3.

2003-8-1-1-6

IDS/Firewall/Router 통합 로그 분석기 설계

정 우 식* 도 경 화** 전 문 석***

Design of Log Analysis System for Enterprise IDS/Firewall/Router

Woo-sik Jung* Kyoung-hwa Do** Moon-seog Jun***

요 약

인터넷의 발전으로 내부네트웍을 보호하기 위한 보안제품들의 개발이 활발해졌다. 이에 따라, 여러 종류의 보안제품이 개발되었고 이에 따라 포맷이 다른 보안로그의 종류도 다양하다. 이는 각 시스템에서 발생된 로그들을 통합하기위하여 표준적인 포맷이 필요함을 의미한다. 따라서, 이러한 로그들을 수집하여 통합하고 연계성을 갖게 하는 것이 중요한 의미를 갖게 되었다.

본 논문에서는 기존의 보안로그 형태를 정형화하기 위하여 분석하며 이를 토대로, 로그수집 Agent를 이용하여 여러 시스템에 설치되어 있는 IDS/Firewall/Router의 로그를 수집, 분석, 정형화시켜 침입을 방지하고 침입자를 발견하는 로그분석기를 제안하고 설계한다.

Abstract

The growing internet business has required the acceleration of the development of security components. There are many different kinds of security components that have been developed in accordance with the appearance of various logs. Therefore, it is important that after the logs are collected they become integrated and need to . Once the data from the logs have been collected form the IDS/Firewall/Routers logs. It needs to be analyzed and formatted for standardization. This paper suggests designs that the log analyzation system could use in analyzing, detecting, and preventing intrusion in the various systems. Once the data has been analyzed it would be possible to prevent further intrusion as well as trace the intrusion back to the source.

* 동서울대학 컴퓨터소프트웨어과
** 숭실대학교 통신연구실
*** 숭실대학교 정보과학대학

접수일자 : 2003. 1.15
심사완료 : 2003. 3. 8

Ⅰ. 서론

인터넷의 발전에 따라 네트웍보안 제품의 개발도 활발해 졌다. 그렇게 때문에 네트웍보안 제품의 종류도 많다. 요즘은 네트웍제품의 통합화를 기대하고 있으나, 사실상 2개 이상의 네트웍 보안제품의 통합은 이루어지고 있지 않다. 뿐만 아니라, 그에 따른 보안로그도 그 종류와 양이 기하급수적으로 늘어나 있기 때문에, 그에 대한 관리가 시급하다. 따라서, 네트웍 보안 제품의 통합보다는 네트웍 보안제품의 보안로그의 수집, 통합 그리고 분석에 대한 중요성이 강조되고 있다.

이는 보안제품의 표준이 되어 있지 않아 침입에 대한 효율적인 결과를 얻을 수 없다.

보안로그의 종류는 기본적으로 라우터에서 발생되는 패킷의 접근에 대한 로그와 방화벽에서 발생되는 로그 그리고 IDS에서 발생되는 로그들을 대표적으로 볼수 있다. 또한, 이러한 보안로그들은 침입의 관점에서 볼때, 연계성을 갖는다.

본 논문에서는 각 네트웍에 설치되어 있는 보안제품들에서 발생되는 로그를 보안성이 가미된 로그에이전트(LogAgent)를 통하여 수집하고 로그 센터로 보내어 정규화하고 통합하여 분석하며 관리자에게 그래프를 통하여 로그를 제공하는 방법을 제안하고 설계한다.

2장에서는 라우터, 방화벽, IDS와 기존방법에 대해 관련 연구를 통하여 알아보고 3장에서는 제안한 IDS/Firewall/Router 로그분석기의 요구사항에 대해 설명한다. 4장에서는 제안한 IDS/Firewall /Router 로그분석기를 설계하고 5장에서는 이에 대한 기본적인 평가를 수행하며 마지막 6장에서 결론을 내린다.

Ⅱ. 관련 연구

1. IDS/Firewall/Router의 로그 특징

IDS/Firewall/Router의 로그는 제품과 개발형태에 따라 다르나 로그의 내용은 아래와 같다.

• IDS(Intrusion Detection System)

각 침입탐지시스템 제품의 이벤트 필드는 거의 유사한 형태를 지니고 있지만, 탐지된 공격 이름과 카테고리, 위험도 등은 각 제품별로 다르게 정의되어 로그를 남기고 있다. 내용은 정규화 과정을 통한 Mapping Table 을 이용하여 공격 시도날짜, 공격 시도시각, 공격 방법, 공격자 IP주소, 공격자 포트번호, 피공격자 IP주소, 피공격자 포트번호, 탐지장비, 추가정보, 프로토콜 등이다[1].

• Firewall

침입차단시스템에서 발생하는 이벤트는 트래픽 로그, 정책위반 로그, 관리자 로그 등이 있으며, 각 제품별로 필드의 형식과 정보가 다르다. 이 내용은 이벤트 날짜, 시간, 서비스 내용, 침입차단 상태정보, 출발지 IP주소, 출발지 포트 번호, 목적지 IP주소, 목적지 포트번호, 추가정보, 정책위반 사항, 정책위반 경고, 로그 기록 시간 등 이 있다[1].

• Router

네트워크 커넥션 장비의 상태를 감시하기 위한 이벤트를 수집하며 날짜, 시간, 로그 기록여부, 이벤트 명, 출발지 IP주소, 출발지 포트 번호, 목적지 IP주소, 목적지 포트번호, 그리고 패킷수, 지역주소, 지역포트 등이 있다.

2. 기존 보안요소들의 로그수집 및 분석 방법

사용되고 있는 보안 시스템들에 대한 로그의 수집 및 분석 방법은 아래와 같다.

• 침입탐지시스템(IDS)

침입탐지시스템에서 탐지한 이벤트 로그를 수집한다.

서버 기반과 네트워크 기반의 모두가 수집 대상에 포함되며, 이벤트 상태로그, 패킷정보로그, 침입 위반로그, 트래픽 로그, 관리자로그 등으로 분석한다.

• 침입차단시스템 및 가상사설망(Firewall, VPN)

침입차단시스템 및 가상 사설망의 이벤트를 수집한다. 이벤트에 대한 상태로그, 패킷정보 로그, 트래픽 로그, Alert 로그, Warning 로그 등으로 분석한다.

• 네트워크 장비(Router)

네트워크 커넥션의 근간인 각 장비의 상태를 감시하기 위한 이벤트를 수집하며 그 대상으로는 라우터, 스위치 등의 트래픽 상태 로그, 패킷 로그 등으로 분석한다.

Ⅲ. 제안한 IDS/Firewall/Router 로그분석기 요구사항

위절에서 보듯이 각 보안요소들은 각각 다른 형태의 로그를 발생시킨다는 것을 알수 있다. 이번 절에서는 실제 IDS/Firewall/Router의 로그의 특징을 분석한 것을 토대로 로그 분석기의 요구사항을 알아본다.

1. IDS/Firewall/Router의 로그분석기 요구사항

기존 로그분석기는 로그를 통합/수집하기 위하여 주기적으로 Telnet, FTP나 Tape 등을 사용하여 분석센터로 전송하였다. 전송한 로그를 통하여 원격 모니터링 및 호출기등을 통한 실시간 경고 그리고 그에 따른 대응체제들을 제공하였다.

기존의 여러 제품들이 있는데, 대부분 통합로그 수집, 검색, 분석 그리고 실시간 경고 등을 수행하도록 되어있다. 그러나 이러한 제품의 문제점은 관리가 가능한 보안요소, 다시 말해, 보안제품이 한정이 되어 있다는 것이다. 이는, 보안요소 마다 다른 형태의 로그를 제공하고 있기 때문이다.

따라서, 본 논문에서는 log Agent를 통하여 수집된 각 보안요소의 로그를 통합할 수 있는 단일화 포맷[2,3,4]을 제안한다.

2. Log Agent의 요구사항

로그 에이전트는 각 보안요소로부터 생성된 로그를 각 네트웍으로 부터 수집하여 통제센터로 전송한다. 대부분의 로그 수집 에이전트의 기능은 단순히 보안요소로부터 저장된 로그를 통제 센터의 요구에 따라 전송해주는데 의미를 둔다[7].

본 논문에서는 로그 에이전트의 기능에 제 3자로부터 로그를 변경할 수 없도록 보안 기능을 추가하기 위하여 데이터를 전송할 때 데이터의 암호화를 수행하도록 하고, 로그에이전트에 데이터 전송에 대한 수행을 통합 분석기에서 제어할 수 있도록 한다.

3. 로그 분석기의 요구사항

보안요소에 따라 상이한 로그들이 로그 에이전트를 통하여 수집되었을 때, 로그 분석기는 이러한 상이한 로그들을 단일화 하여야 한다. 이런 작업을 정규화한다구 한다. 또한, 정규화를 통한 로그 정규화와 필터링을 통한 로그의 분석 내용을 관리자에게 그래프 등을 통하여 알려주어야 한다[8,9].

Ⅳ. 제안한 IDS/Firewall/Router 통합 로그 분석기 설계

1. 통합로그분석기 네트웍 구성도

다음은 제안한 로그 분석기의 네트웍 구성도이다[그림1]. 각 로그 분석기는 각각 다른 네트웍에서 IDS/Firewall/Router 등의 보안요소로부터 보안로그를 수집하고 인터넷을 통하여 통합로그분석기가 있는 네트웍으로 암호화된 보안로그들을 전송한다. 이렇게 전송된 보안로그들을 제안한 통합로그 분석기에서 정규화시켜 관리자에게 분석한 자료를 제공한다.

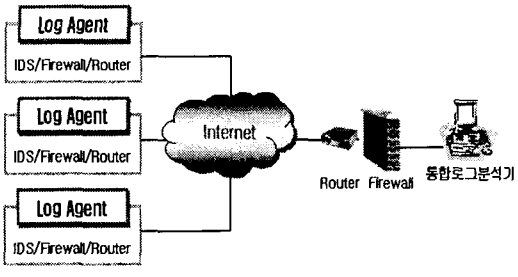

그림 1. 제안한 통합로그 분석기 네트웍 구성도
Fig 1. A Network Configuration of Proposed Enterprise Log Analysis System.

각 네트웍에서 로그에이전트로부터 전송된 IDS/Firewall/Router의 보안로그는 통합로그분석기를 통하여 저장되고 장비별로 로그 정규화를 통하여 경고로그를 필터링한다. 필털링한 로그를 정규화시켜 통합단일화 로그 저장소에 최종적으로 저장하게 되고 이를 그래프 등으로 분석하여 관리자에게 제공한다. 만약, 침입에 대한 징후로 밝혀지면, 관리자에게 알람을 통하여 알린다[그림2].

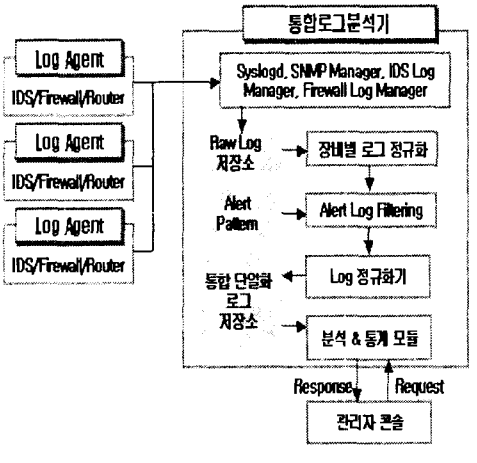

그림 2. 제안한 통합로그 분석기 전면도
Fig. 2. Configuration of Proposed Enterprise Log Analysis System

2. Log Agent 설계

로그 에이전트의 중요기능은 각 보안요소로부터 로그를 각 네트웍으로 부터 수집하여 통합로그분석기로 전달하는 것이다. 이는 이벤트 수집 기능과 정규화 기능을 수행한다. 특히, 보안요소인 IDS/Firewall/Router의 보안로그들을 수집하여 주기적으로 전송한다. 전송시, 각 데이터의 기밀성을 제공하기 위하여 SSH(Secure Shell)을 사용하거나, 암호모듈을 사용하여 데이터를 암호화하여 전송한다.

3. 로그 수집 모듈 설계

로그수집 모듈은 로그 에이전트에서 보내온 Firewall /IDS/Router 그리고 추가 보안장치로부터 전송된 보안로그를 기밀성을 위하여 SSH(Secure Shell)을 사용하여 데이터를 전송하고 이렇게 수집된 로그를 저장한다[그림3].

다시 말해, 각 로그는 각 로그에 합당한 로그 메니저를 통하여 필터링 되기 전의 로그를 나타내는 Raw log 저장소에 저장된다.

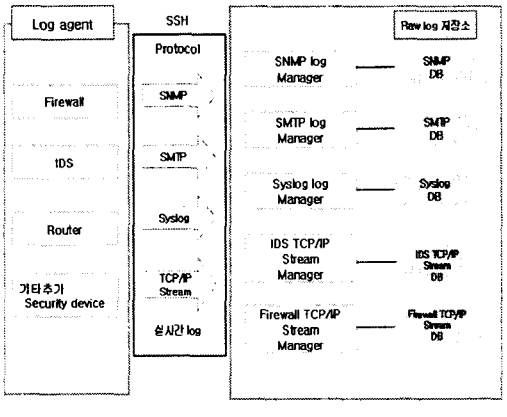

그림 3. 로그 수집 모듈
Fig. 3. Log Collection Module

4. 로그 필터링 모듈 설계

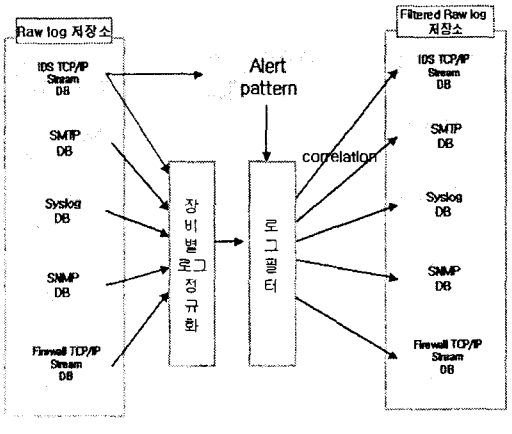

그림 4. 로그 정규화/필터링 모듈
Fig. 4. Log Normalization/Filtering Module

로그 필터링 모듈은 로그수집모듈로부터 저장된 각 Raw Log를 장비별 1차 로그정규화를 통하여 침입 패턴 데이터베이스(Alert Pattern DB)를 통하여 로그 필터링 작업을 수행한다[그림4].

기본 침입 패턴은 보안장비와의 비교를 통해서 보안 침해사항이 발생되었는지를 판단할 수 있는 기준이 되는 데이터베이스로의 삽입, 수정 및 삭제가 전체 시스템 메니져만이 가능하고 일반적으로는 읽기 속성만 갖는다.

5. 로그 정규화 및 분석 모듈 설계

로그 변환 모듈은 필터링된 로그를 정규화된 로그로 변환하여 통합변환 저장소에 저장한다. 통합로그변환 저장소에 저장된 로그는 로그분석 시스템을 통하여 로그를 분석하고 그에 따른 통계자료를 그래픽 형태 등으로 변환하여 관리자에게 제공한다. 또한, 침입에 대한 근거가 확실할 경우, 미리 설정된 알람으로 관리자에게 알린다[그림5].

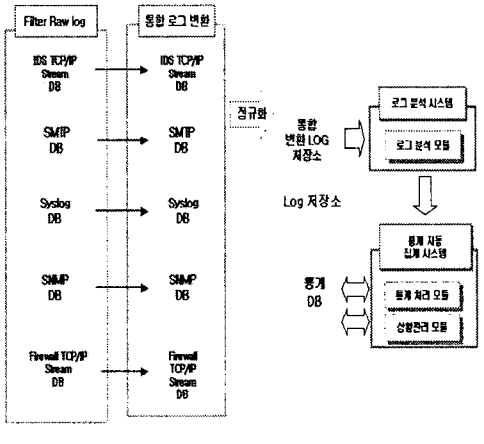

그림 5. 로그 정규화/분석 모듈 설계
Fig. 5. Log Normalization/Design of Analysis Module

V. 평가 및 실험

다중의 네트웍에서 발생하는 보안로그들은 그 종류와 형식이 매우 다양하다. 따라서, 본 논문에서 제안한 통합 로그분석기는 각 네트웍에 설치된 로그에이전트를 통하여 통합로그분석기로 보안로그를 보내게 되고, 이렇게 전송된 로그는 침입패턴DB를 통하여 필터링 되고 정규화 된 후에 분석되어 관리자에게 알리기 위하여 통계 시스템을 통하여 변환되어 그래프 형식으로 관리자에게 알려준다.

관리자가 관리를 위하여 접속할 때, 관리자 인증을 위하여 SSL을 사용하고 이는 처음에 로그인과 패스워드를 확인한다[그림6].

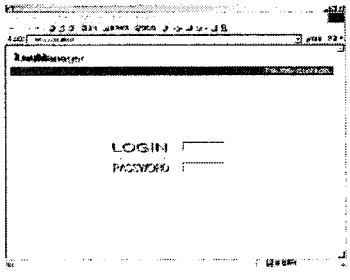

그림 6. 보안관리자 인증
Fig. 6. Authentication of Security Administration

관리자는 웹을 통하여 통합로그분석기에 접속하여 새로운 로그의 유입현황이나 이벤트 로그 혹은 로그분석 보고서 등을 확인한다[그림 7].

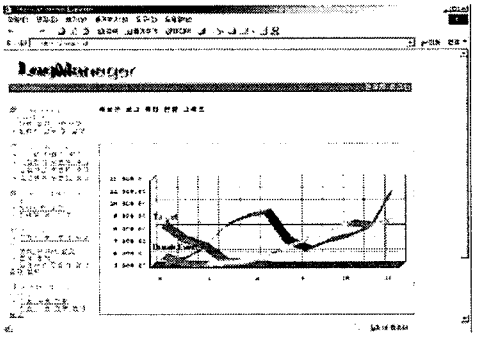

그림 7. 관리자용 웹 인터페이스
Fig. 7.Web Interface for Administrators

위 그림7.의 각 로그분석에 대한 항목은 Logmanager SecurePolicy, Log 상태보고, 시간이벤트 모니터링, 분석보고서, 시스템자원정보 모니터링 등으로 이루어져 있다.

Ⅵ. 결 론

본 논문에서는 통합로그분석기를 제안하여 IDS /Firewall/Router 등의 다양한 보안요소의 보안로그를 한곳으로 수집하여 효율적으로 네트웍을 보호할 수 있었다.

최근, 다양한 보안요소를 통합하는 작업이 수행되고 있으나, 이러한 작업은 2가지 이상의 보안요소를 통합하지 못하고 있다. 따라서, 이러한 통합로그분석기가 효율적인 보안요소의 관리에 도움이 될 것으로 사료된다. 또한, 효율적인 보안요소의 관리를 통하여 관리자에게 침입에 대한 통지를 미리 해 줄수 있음으로 해서 네트웍의 보안을 강화할 수 있다.

향후 연구방안은 이러한 통합로그분석기의 로그 에이전트의 기능을 강화시켜서 통합로그분석기의 정규화 부담을 나눌 수 있도록 하고 탐지 모듈을 향상시키도록 한다. 또한, 로그분석의 결과를 관리자가 요구하는 형태로 제공할 수 있도록 한다. 이러한 통합로그분석기는 향후 침입에 대한 방지와 침입의 결과를 찾는데 많은 도움을 줄 것으로 사료된다.

참고문헌

[1] kisa, 침입차단/탐지시스템 로그표준형식, kisa 표준문서, 2001.5

[2] ArcSight, Cot Correlation? Not Without Normarization, ArcSight Inc., 2002.

[3] Mark Handley, Vern Paxson, Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics, Usenix security'01, 2001.

[4] V. Paxson and M.Mandley, "Defending Against NIDS Evasion using Traffic Normalizers", presented at Second International Workshop on the Recent Advances in Intrusion Detection, Sept. 1999.

[5] James A. Hoagland, Stuart Staniford, Viewing IDS alers:Lessons from SnortSnarf, IEEE, 2001.

[6] Roesch, Martin, http://www.snort.org /.

[7] Midori Asaka, Atsushi Taguchi, and Shigeki Goto. The implementation of ida: An intrusion detection agent system. In Proceedings of the 11th FIRST Conference, June 1999.

[8] Teresa F. Lunt. Automated Audit Trail Analysis and Intrusion Detection: A Survey. In Proceedings of the 11th National Computer Security Conference, October 1988.

[9] Intellitactices, "Network Security Manager Administrators Guide", Version 3.2. 2001.

저 자 소 개

정 우 식

1980년 광운대학교 전산학과 졸
1982년 숭실대학원 전산학과 졸
1982 - 1984 한국전력공사 전자계산소 근무
1984.3 - 현재 동서울대학 소프트웨어과 교수
1997 - 현재 숭실대학교 전자계산전공 박사 수료
관심분야 :Network security, Software Engeering,Language 일반

도 경 화

1997년 : 건양대학교 컴퓨터공학과 졸업(학사)
1999년 : 숭실대학교 컴퓨터학과 졸업(석사)
2002년 : 숭실대학교 컴퓨터학과 수료(박사)
2001년~현재 : 숭실대학교 생산기술연구소 연구원
〈관심분야〉 네트워크보안(방화벽, IDS,ESM,VPN),스테가노그라피, 데이터 통신, 암호학

전 문 석

1980년: 숭실대학교 전자계산학과 졸업(학사)
1996년 : University of Maryland 전산과 졸업(석사)
1989년 : University of Maryland 전산과 졸업(박사)
1989년 : Morgan State University 전산수학과 조교수
1989년~1991년 : New Mexico State University 부설 Physical Science Lab. 책임연구원
1991년~현재 숭실대학교 정보과학대학 부교수
〈관심분야〉 컴퓨터 알고리즘, 병렬처리, VLSI 설계, 암호학