기업 분산 환경에 적합한 ESM 시스템 구현

강환창*, 박홍규*, 김일곤*, 최진영*
*고려대학교 디지털정보공학과
e-mail : hckang77@korea.ac.kr

Implementation of ESM System suited to Enterprise Dispersion Environment

Hwan-Chang Kang*,Hong-Kyu Park*,Il-Gon Kim*,Jin-Young Choi*
*Dept. of Digital Information and Engineering, Korea University

요 약

요즘 네트워크환경에서 기업네트워크의 보안은 가장 중요하게 고려되고 있는 문제 중 하나이다. 기업네트워크의 보안을 위해 활용하고 있는 VPN, IDS, Firewall 등의 다양한 솔루션들은 일관된 관리가 용이하지 않기 때문에 ESM 이 이용되고 있다. ESM 은 여러가지 보안 솔루션을 통합관리 해주므로, 솔루션의 낭비가 없고 효율적인 관리가 가능하다. 본 논문에서는 실제 운용중인 ESM 툴(Tool)에서 룰 설정의 중요성을 알아 보고 알려지지 않은 웜(Worm)이 들어 왔을 때 관제를 위한 룰설정 방법을 제시한다.

1. 서론

급성장하는 네트워크환경에서 대부분의 네트워크들은 인터넷, 인트라넷등의 네트워크 시스템 환경을 이용해 전 세계적인 형태로 확대되어 가고 있다. 이와 같은 기업 네트워크 규모가 증대되면서, 보안상의 취약점을 이용한 기업의 내.외부로부터 발생하는 공격 역시 증가하고 있는 추세이다.

대다수의 기업에서 이러한 공격을 방지하고 대응하기 위하여, 다수의 보안제품을 사용하여 방어하지만 이것을 적절하게 적용시켜서 효과적으로 이용하는데 있어서 많은 어려움을 겪고 있다. 그 이유는 많은 보안정책들을 제품에 맞게 적용시켜야 하고, 보안정책에 따라 보안제품을 어떤 방식으로 적용시키는가에 대한 명확한 해답이 없기 때문이다[1].

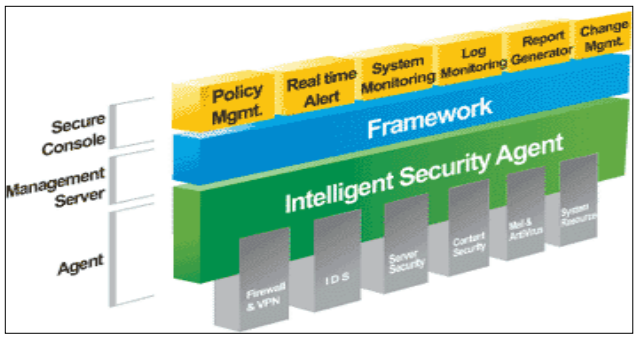
Enterprise Security Management (통합보안관리시스템 : 이하 ESM)은 이런 여러가지 보안제품들을 적용시키기 위해 개발 되었으며, 네트워크 시스템 자원을 분석하고 모니터링하며, IPS,IDS,VPN 등의 다양한 보안 솔루션을 통합관리 하여 보안관리의 효율을 극대화시킨다. 이 논문에서는 잘못된 룰 설정에 따른 로그 발생 추이를 확인하고, 알려지지 않은 웜이 들어 왔을 때 룰 설정 방법을 제시한다.

본 논문의 구성은 2 장에서 ESM 시스템을 설계하고, 3 장은 ESM 시스템 구현 환경 및 구현결과 이다. 마지막으로 4 장에서는 결론 및 향후 전망한다.

2. ESM 시스템 설계

2.1 ESM 의 구조

전체구조는 ESM Agent, ESM Management(이하 Manager)ESM Console 의 세부분으로 구성된다[2].



(그림 1) 효과적인 보안서비스를 위한 ESM 의 전체 구성도

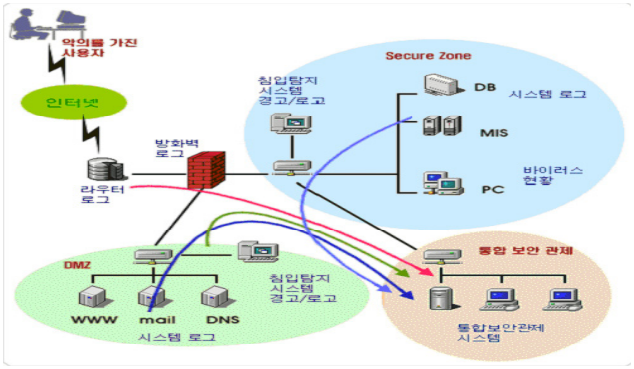
2.2 ESM Agent

주요기능은 events 수집, Normalization, Aggregation 의 기능이 있다. events 수집 기능은 보안 관련정보에서 발생하는 모든 이벤트 즉 네트워크 장비나 침입차단시스템, 침입탐지시스템,서버 보안시스템,UNIX 의 Syslog 메시지, Windows 의 이벤트 로그 등을 수집한다. Normalization 기능은 제품별로 각기 다른 형태로 수집되는 이벤트를 표준화하여 관리할 수 있도록 도와준다. 그리고 Aggregation 기능은 Normalization 작업을 통해서 얻어낸 결과와 불필요한 데이터를 제거하고 중복 이벤트 데이터를 축약 처리한다.

2.3 ESM Management(이하 Manager)/Console

ESM Manager 는 ESM Agent 로부터 보고되어진 정보(로그정보, VPN 통신에 대한 정보, 트래픽 흐름 정보 등)를 적절히 DB 에 기록한다. Manager 에 수집된 이벤트 처리를 위한 구성이 ESM 성능에 영향을 미친다. Console 의 주요 기능은 각 단위 보안 시스템에서탐지한 내용들을 수치화하여 통계(Statistics) 보고하고, 보안 취약점이나 노출사항을 제거하기 위한 보안정책을 신속하게 도입할 수 있도록 한다.

2.4 ESM 시스템 배치 구조



(그림 2) ESM 시스템 배치도

2.5 ESM 시스템 주요 기능

주요기능은 다음과 같다. 보안감사를 위한 각종 정책들을 설정하고 정의, 각종 로그에 대한 모니터링 기능, 시스템 리소스 모니터링 기능, 위험 수위에 따른 실시간 경보 기능, 각종 보고서 생성 기능, 자동 업데이트 기능, 각종 보안 정보를 제공, 운영관리 및 경로추적 기능, 취약점 평가 기능등이 있다.

2.6 ESM 시스템의 장점

IPS 개념을 도입하여 불법적인 접근 시도시 능동적인 대처가 가능하다. 일반적인 ESM 의 사용자 인터페이스와 달리 친숙한 웹기반의 인터페이스 사용으로 사용방법에 대한 숙지가 용이하다. 시간 및 장소에 관계없이 고정된 ESM 서버에 접근하지 않고도 웹브라우저를 통해 관리 할 수 있다. 그리고 보안서비스를 실시간 통합 관리할수 있다[3].

3. 현재 사용되고 있는 ESM 시스템 구현 환경 및 구현 결과

3.1 ESM 시스템 구현 환경

ESM Manager Server 의 기종은 Sun Fire V480, O/S 는 Solaris8, Total HDD 는 120GB, CPU 는 1.2GHz, RAM 은 4GB 이다.

ESM DB 서버의 기종, O/S, HDD, RAM 은 ESM Manager Server 와 같고 CPU 속도만 1.05GHz 이다. 주요 Application 은 Oracle 이다.

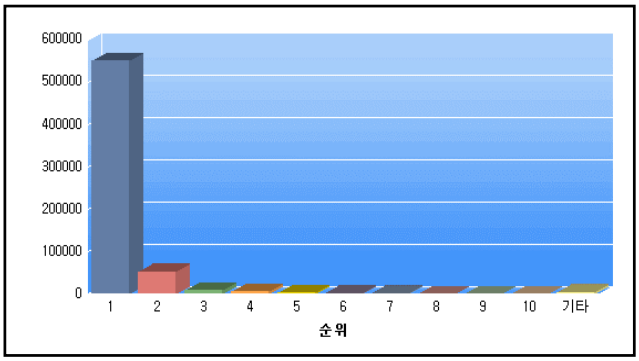
Agent 서버의 기종은 SUN E4500 이고 O/S 는 Solaris8, Total HDD 는 14GB, CPU 는 800MHz, RAM 은 1GB 이다.

3.2 ESM 시스템 구현 결과

(그림 3) 통합콘솔 첫 화면

위 (그림 3)은 각 지역 Internet Data Center(이하 IDC) 전체를 한 개 화면에 보여주고 있다. 왼쪽은 IDS 에서 탐지한 공격에 대한 각 리스트와 해당 건수를 표시하고 오른쪽은 방화벽에서 탐지한 공격에 대한 각 리스트와 해당 건수를 표시한다[4].

(그림 4)는 검색 - 보고를 보여준다. 내부 네트워크 IP 대역과 외부 네트워크 IP 대역을 구분하여 보고한다. 방화벽에서 발생하는 로그발생 드롭(Drop)이벤트 중 가장 많은 이벤트를 기록한 상위 10 개의 목적지 포트(Destination Port)를 기술한다.



(그림 4) 검색 - 보고

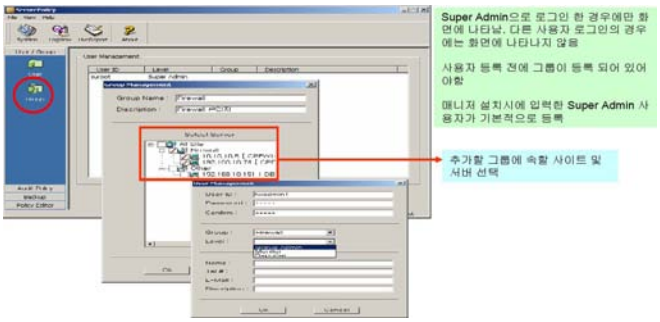
<표 1>처럼 이 정보를 통해 방화벽에서 드롭(Drop)된 이벤트중 어떤 포트(예:Port135)로 가장 많이 접근 시도 되었는지 알수 있다.

<표 1> 드롭(Drop) 이벤트

순 위	포트(Port)	발생건수	점유율
1	135	552,422	86.55 %
2	icmp	53,432	8.37%
3	1025	9,506	1.49%
4	1433	6,951	1.09%
5	4899	3,521	0.55%
6	3410	2,341	0.37%
7	139	1,921	0.30%
8	2745	1,368	0.21%
9	901	929	0.15%
10	6129	882	0.14%
기 타		5,033	0.79%
Total		638,306	

다음은 룰 설정 부분이다. ESM 에서 룰 설정은 보안 장비에서 어떤 로그를 수집할 것인지 그 수집대상을 설정하고(일반적으로 모든 로그 수집), 경보(Alarm)조건을 설정하는 것이다.

룰 설정은 보안감사를 위한 정책을 정하는 것이다. AuditPolice 에서 정책을 설정함으로써 에이전트(Agent)에 의해 수집된 정보들이 Manager로 전송되며, Log View 화면을 통해 실시간으로 모니터링되고 LiveReport 에서 보고서를 생성, Audit Policy 에서 정책이 설정되어 있지 않으면 Log View 및 Live 보고서가 생성되지 않는다.



(그림 5) 룰 설정(User/Group)

위 (그림 5)처럼 Super Admin으로 로그인 한 경우에만 화면에 나타난다. 다른 사용자 로그인의 경우에는 화면에 나타나지 않는다. 사용자 등록 전에 그룹이 등록 되어 있어야 한다. 메니저 설치시에 입력한 Super Admin 사용자가 기본적으로 등록된다.

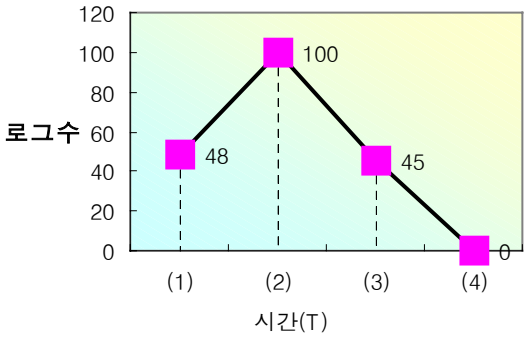
ESM 시스템에서 룰 설정의 중요성을 알아본다. 기존 사용하던 방화벽 및 IDS 는 현재 사용중이라도 ESM 에서 콘솔(Console)에 의한 룰설정이 필요하다.

최신의 알려지지 않은 웜(Worm)에 대한 관제가 어렵다. 그러므로 최신의 보안 정보 (예를들어 포트 정보등)를 바탕으로 관제 설정이 필요하다. 잘못된 룰 설정에 따른 불필요한 로그가 발생 할 수 있다.

<표 2> 잘못된 룰 설정에 따른 로그 발생건수

드롭(Drop)된 로그 건수 / 보안장비 경우의 수	로그가 중간 (Middle) (1)	로그가 피크 (Peak) (2)	로그가 중간 (Middle) (3)	로그가 제로 (Zero) (4)
방화벽의 룰 설정이 정확히 안 되었을 경우	48 건 /Min	100 건 /Min	45 건 /Min	0 건 /Min
IDS 의 필요없는 룰 설정이 되어 있을 경우	34 건 /Min	80 건 /Min	35 건 /Min	0 건 /Min

<표 2>는 보안장비의 룰 설정이 정확히 또한 불필요한 룰 설정이 없을 때 분(Min)당 로그 발생건수가 제로가 됨을 알수 있다. 방화벽의 룰설정이 정확히 안 되었을 때는 고객이 보안서비스 신청시 IP 를 정확히 모르거나 누락시킬 때, 대량의 웜이 외부에서 들어와 이상트래픽이 발생할 때, 외부에서 임의의 포트(Port)로 스캐닝 (Scanning)할때이다. IDS 의 필요없는 룰설정이 되어 있을때는 주로 오탐(Misuse Detection)설정이다. IDS 에서 오탐설정하는 경우는 취약점 정보 수집, 웜에의한 침입공격, 도스(Dos)등의 서비스 거부공격등이 있을수 있다. IDS 에서 오탐설정은 환경에 맞게 튜닝(Tuning)해야 한다.



(그림 6) 방화벽의 룰 설정이 정확히 안 되었을경우 로그 발생 추이

(그림 6)은 **(1)** -> **(2)** -> **(3)** -> **(4)** 순서대로 방화벽의 룰 설정이 잘못되어 드롭(Drop)된 이벤트 로그수의 추이를 볼수있다 (로그수의 변화 48 -> 100 -> 45 -> 0). 방화벽의 로그수는 룰 설정이 정확히 안 되어 있을경우 즉 위에서 설명한 세가지 경우가 발생 하지 않을 경우에 제로(Zero)가 됨을 알수 있다.

그러나 시스템 관제시 최신의 알려지지 않은 웜이 들어올때라든지, 네트워크 사용량이 많은 유디피(UDP)패킷이 들어올 때, 서비스 성격을 파악하는데 시간을 필요로 하기 때문에 임계치 설정이 어렵다.

<표 3>알려지지 않은 웜(Worm)이 들어왔을 때 룰(임계치) 설정 방법

임계치 설정 / 룰설정 위치	(방법 A)의 로그의 갯수	(방법 B)의 로그의 갯수
ESM 시스템 (Manager)	100/초 ->200/초	200/초 ->100/초
각 싸이트(Site)의 IDS	200/초 ->100/초	100/초 ->200/초

<표 3>처럼 시스템 관제시 임계치를 서로 조정하여 관제할수 있다. ESM 시스템에서 웜(Worm)에 의한 로그의 갯수가 100 개의 로그에서 200 개의 로그가 들어왔을 때 알람이 울리게 하고, 고객 IDS 의 임계치는 상세하게 즉 200 개의 로그에서 100 개의 로그가 들어들어 왔을 때 알람이 울리게 설정할수 있다(방법 A)(방법 B)의 경우처럼 (방법 A)의 경우와 설정값을 반대로 설정할수도 있다. 일반적으로 (방법 A)를 많이 사용 한다.

ESM 의 알람 설정은 리얼 타임(Real Time)하게 보여주는 화면을 보고 다음과 같이 설정한다. 3 분당 CPU 사용률이 전체의 약 80%를 넘을 때와 3 분당 HDD 사용률이 전체의 약 80%를 넘을 때, 그리고 대량의 트래픽이 발생하는 경우에 알람이 울리게 설정한다.

4. 결론 및 향후 연구 방향

ESM 은 관리의 효율성을 한차원 높였다는데서 의의를 찾을수 있으며, 기업의 인력 배치 및 관리, 유지보수등 수많은 관리자가 해야 할 반복적이고 단순한 업무들을 자동화하고 단순화함으로써 비용절감 효과를 가져오며, 전사적인 차원의 관리로 자원의 낭비를 줄이고 효율적인 관리를 가능하게 했다. 또한 침입을 탐지하고 차단하는 과정이 능동화 되었으며 관리의 편의성을 도모하고, 각종 트래픽의 분석된 데이터를 시각화하여 그래프 형태의 보고서를 제공하며, 로그의 데이터베이스화로 필요할 때마다 확인 가능하게 되었다. 이로써, 관리자는 네트워크 시스템 현황 및 성능 분석과 사용현황 파악이 더 쉽게 되었으며, 불필요한 트래픽을 막고 다양한 로그기록을 이용하여 보다 안전하고 효율적인 시스템을 관리할 수 있으리라 기대된다. 본 논문에서는 잘못된 룰 설정에 따른 로그 발생 건수를 통하여 룰 설정의 중요성을 알아 보았다. 알려지지 않은 웜(Worm)등이 들어 왔을때 관제를 위한 룰 설정 방법을 제시했다.

향후 전망으로는 로그형식의 표준화가 요구되며, 알려지지 않은 웜에 대한 관제 및 ESM 이 보안장비 미설치 구간에 어떻게 하면 관제를 할수 있을것인가에 대한 연구가 이루어져야 한다. 또한 능동적인 대응이 자동적으로 실행되는 부분에 대한 연구가 필요 할 것이다.

참고 문헌

[1] 민동옥, 손태식, 구원본, 문종섭, ESM 시스템간 감사기록 교환방식에 관한 연구, 한국정보과학회 학술발표논문집 Vol.31,No.2, 2004 년

[2] http://www.igloosec.co.kr/products, 2004 년

[3] 박종혁, 효율적인 보안서비스를 위한 ESM 시스템의 구현,http://www.nanet.go.kr/dl/SimpleView.php, 2002 년

[4] IGLOO Security,Inc. http://www.igloosec.co.kr/

[5] http://www.oullim.co.kr/

[6] http://www.kisa.or.kr/

[7] http://www.kissc.or.kr