통합관제 보안관리모델의 성능분석

서정은* · 윤병민** · 허창우** · 김윤호**
* 한국화학연구원, ** 목원대학교 IT 공학부

Performance Analysis of Security Management model for Unity Control

Jeong-eun Seo* · Byung-min Youn** · Chang-woo Her** · Youn-ho Kim**
* Korea Research Institute of Chemical Technology, ** Mokwon University

요 약

본 연구에서는 한층 더 개선된 보안시스템을 구현하기 위해 현재 사용하고 있는 보안시스템에 대한 테스트를 실시하여 실제적으로 따르는 문제점을 분석하고, 그에 따른 대응책을 마련코자 하였다. 방화벽에서 처리할 수 있는 최대의 전송량을 측정하고자 테스트 모델을 구성하여 테스트를 실시하였으나, 테스트구간에서 전송된 Packet 수와 전송시간 측정만 기록되고, 최대 전송량 측정은 실현하지 못하였다. 따라서 보안업체의 협조를 얻어 Tool(스마트비트)을 이용한 테스트 결과를 얻을 수 있었으나, 실제 기관의 사례를 실사한 결과 많은 차이점을 가지고 있었다. 이는 기관별로 적용되고 있는 방화벽 정책(Rule 수)에 따라 방화벽의 처리성능이 가장 큰 차이점으로 분석된다.

ABSTRACT

In this study, the security system (Firewall and IDS) was installed in high speed information network and analyzed for a change in the speed of data transfer and the possibility of invasion. The selection of appropriate system, efficient detection and protection and surveillance method were suggested and analyzed. In order to do experiments, an experimental model was comprized to analyze the parameters that was affected by the detection and protection system in network. This will give a standard how much we can pull up the security system maintaining the network speed.

1. 서 론

본 논문에서는 웜 바이러스와 Network Scan 등 다향한 침해요소로부터 기관정보망의 효율적인 유지관리와 보호를 위한 방안으로 통합관제 시스템의 구축(Firewall, IDS, 관제시스템)모델을 설정하고 방화벽의 성능분석을 통해 인터넷 전용선의 속도에 따른 방화벽의 선택과 기관정보망의 보호를 위해 필요한 기술을 제안한다. 이를 위해 초고속 백본(Backbone) 기반에서 방화벽과 단계별 보안시스템을 구축하여, 데이터 이동에 대한 상태를 분석하기 위한 테스트밴드를 구성, 그 결과를 보이고, 성능분석에 의한 효율적인 보안관계모델의 구현 방법을 제시한다.

II. 침입차단/탐지시스템의 성능분석

방화벽은 크게 최근에 출시되고 있는 Switch 아키텍처와 기존의 대부분의 방화벽 시스템으로서 W/S에 Security Application을 설치하여 사용하고 있는 서버 아키텍처로 구분된다. 방화벽 설치에 따른 가장 큰 문제점은 방화벽 설치 후 방화벽의 Interface와는 별개로 전송속도(전송량)가 현저히 떨어지는 것이다. 테스트모델 구성은 표 1의 모델을 기반으로 아래와 같이 구성하였고, 모든 시스템의 정상 가동 상태에서 테스트를 하였다. 방화벽 설치 후 전송속도(전송량)는 그림 1과 같이 방화벽의 적용시가 비 적용시(약 60Mbyte) 보다 약 50% 이상 떨어진 30Mbyte정도를 나타내는데,원인은 W/S에 S/W를 설치(서버구조)한 것으로, 이 경우 Server의 I/O가 대부분 20~30Mbyte로 서버의 병목과 Security Application의 병목이 겹쳐지면서 약 30Mbps의 전송률을 나타냈다.

표 1. 서버구조형 테스트모델 내역

구 분	장비(모델)명
Router	CISCO 7513 (RSP4, 256MB)
Firewall	수호신 3.0,(Server : SUN 250)
IDS	스나이퍼(K4, SUN O/S, 100Mbps)
Backbone S/W	CISCO Catalyst 6500
NMS	CISCO Works 5.1
인터넷전용선	45Mbps

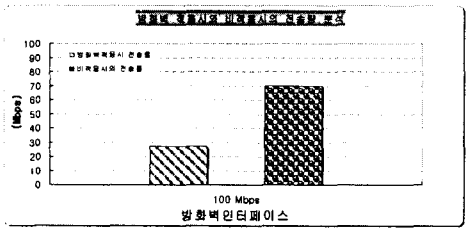

그림 1. 방화벽 적용후와 비적용후의 전송량 분석

그러나 W/S의 자체 테스트한 결과, 약 60Mbyte~70Mbyte 전송률을 보이는 것을 감안하면 서버형의 전송량 감소(약 50%)는 큰 걸림돌이 되고 있다. 결국 사용하고 있는 인터넷의 속도(45Mbps)에 비하여 방화벽에서 처리되는 전송량은 Interface를 100Mbps Full Duplex로 설정하였음에도 불구하고, 실제 전송량은 약 30Mbps 정도 나타내었다. 원인은 단순히 Server의 Interface 속도에 의한 것이 아니고, 방화벽 서버의 O/S 커널과 I/O, Load되는 방화벽 프로그램의 처리능력, 서버의 성능에 따라 그 결과가 각각 다르다는 것을 알 수 있다.

IDS의 모니터링 결과 여러 유형의 공격으로 트래픽이 가중되어 망 전체에 영향을 끼치고 있다. 동시에 많은 양의 웜 바이러스가 유입될 시 이를 처리하지 못하고 통과시키는 결과를 얻을 수 있었다. 이는 각종 침해 요인에 대해 IDS가 100% 차단하지 못하고 있으며, 방화벽과 IDS를 설치했다 하여도 침해방어에 안전할 수는 없다는 것을 말한다. 그 대안으로 인터넷 전용선의 속도를 근거로 한 이중화된 보안시스템 구조의 구성이 필수적이다. 특히 상황에 따른 변수는 있겠으나, 본 테스트에서는 CGI에 대한 공격이 가장 높게 나타나고 있어 결국 Web Server 구축 시 가장 많은 주의가 요구된다. 동시에 많은 양의 침해데이터가 유입 시 보안시스템의 병목 원인이 될 수 있는 바, 그 대안으로 보안시스템보다 그 처리능력이 우수한 라우터를 이용한 Access-list를 아래 표와 같이 적용시켜 성능분석을 수행하였다.

표 2. Access-list 적용

```
access-list compiled
access-list 5 deny    203.71.132.8
access-list 5 deny    203.241.123.65
access-list 5 permit any
```

웜 바이러스와 같이 대량 배포를 하는 사례의 경우, 탐지시스템을 이용하여 모니터링을 해 보면 특정 IP로부터 유입되고 있는 것을 발견할 수 있는데, 이런 경우 침입탐지시스템에서 처리를 하려면 많은 경우 자동 통과되거나, 네트워크에 많은 트래픽을 발산시켜 문제가 야기되는데, 이때 라우터에서 위의 예와 같이 Access-list를 이용하여 해당 IP를 차단하면 특정 Site (203.71.132.8등)에서 유입되는 침해정보를 근본적으로 차단하여 트래픽 양을 줄일 수 있었다.

III. 통합관제 서비스모델 구현 및 분석

테스트모델 구성과 테스트 결과에서 보듯이 인터넷 전용선에 근거한 방화벽의 선택과 효율적인 침해요인에 대한 방어대책을 강구하는 데는 여러 가지 제약이 따른다. 서비스 모델은 전용선의 속도가 45Mbps와 155Mbps 이상에서 적용될 수 있도록 100Mbps Dual 모델과 Gigabit 모델을 제시하고 단계별 조치사항을 제안하였다. 특히 100Mbps Dual 모델은 기존의 서버구조형 방화벽을 보존하고 문제점을 보완하는데 중점을 두었다.

보안시스템의 구축에 있어 반드시 고려해야 될 사항으로는 인터넷 전용선의 속도에 근거한 방화벽의 선택이다. 속도저하를 고려, 단순히 Interface의 속도에 의존하지 말고 전송량 측정을 통한 선택이 필요하며, 각종 웜의 유입에 대비 2~4배의 트래픽을 수용할 수 있는 디자인이 필요하다. 보안정책은 각 기관의 특성에 맞게 최소한의 설정이 필요하며, 보안정책 수가 많으면 프로세스가 증가하게 되고, 결국 방화벽의 성능을 떨어뜨리는 원인이 되며, 보안정책에 따라 방화벽 전송량은 많은 차이를 보일 수 있다.

가. Gigabit 방화벽에 의한 모델 설정

서비스 모델 구현에 필요한 구성요소와 단계별 조치방법은 표3과 같다. 방화벽과 IDS를 통합하여 1차 적인 차단과 탐지를 할 수 있도록 하고, Backbone Switch에 2차 탐지기능을 추가, 탐지 및 방어능력을 극대화하였다.

표 3. Gigabit 방화벽 모델 단계별 조치방법

구 분	서비스 모델 1
Interface	- 1Gbps
1단계 조치	- Access-List
2단계 조치	- Firewall / IDS
3단계 조치	- IDS
4단계 조치	- Secure O/S

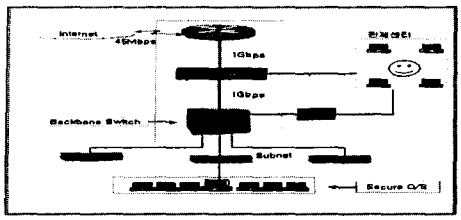

그림 2. Gigabit 방화벽에 의한 설정

나. L4 Switch를 이용한 방화벽 모델 설정

기존의 서버구조형 방화벽을 보존하고 문제점을 보완하는데 중점을 두었다. 구현에 필요한 구성요소와 단계별 조치방법은 표4와 같고 그림 2는 L4 witch를 이용한 방화벽 설정 시스템블럭이다.

표 4. L4 Switch를 이용한 단계별 조치방법

구 분	서비스 모델 2
Interface	- 100Mbps * 2
1단계 조치	- Access-List
2단계 조치	- Firewall * 2
3단계 조치	- IDS
4단계 조치	- Secure O/S

155Mbps 이상의 인터넷 전용선에서도 적용될 수 있도록 방화벽의 Interface를 1000 Base F로 설정 방화벽 설치로 인한 속도 저하문제를 해결하고자 하였다. 방화벽 단에 침입탐지시스템(IDS)을 추가하여 1차 탐지 및 방어를 하도록 하였고, Backbone Switch에 침입탐지시스템을 추가로 설정하여 2차 탐지 및 방어를 하여 1차 탐지 및 방어에서 통과된 침해 요소에 대한 조치를 담당하게 고려하였다.

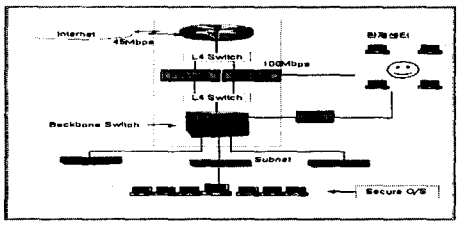

그림 3. L4 Switch를 이용한 방화벽 설정

모니터링을 한 결과, 방화벽의 CPU 점유율이 약 30%를 나타내고 있어 인터넷 대비 충분한 전송량을 처리하고 있다는 것을 추정할 수 있다. 또한 1차 IDS의 탐지건수가 70여건에 이르고 있으나, 2차 IDS의 탐지에서는 탐지가 되지 않고 있어 소수의 경우 1차 탐지에서 모두 처리됨을 알 수 있다. 그러나 대량의 침입 시에는 테스트 결과에서 알 수 있듯이 2차 탐지 및 방어를 할 수 있도록 설정하여야 차단할 수 있다고 판단된다.

표 5. 테스트를 위한 구성요소

구 분	내 역
인터넷 속도	100 Mbps
방화벽/IDS	Absolute 500
2차 IDS	스나이퍼
Backbone S/W	CISCO Catalyst 6500

테스트 결과의 분석을 위하여 위 표 5와 같이 구성하고 모니터링을 한 결과, 방화벽의 CPU 점유율이 약 30%를 나타내고 있어 인터넷 대비 충분한 전송량을 처리하고 있다는 것을 추정할 수 있다. 또한 1차 IDS의 탐지건수가 70여건에 이르고 있으나, 2차 IDS의 탐지에서는 탐지가 되지 않고 있어 소수의 경우 1차 탐지에서 모두 처리됨을 알 수 있다. 그러나 대량의 침입 시에는 테스트 결과에서 알 수 있듯이 2차 탐지 및 방어를 할 수 있도록 설정하여야 차단할 수 있다고 판단된다.

L4 switch의 경우, 기존의 방화벽 시스템을 개선하기 위한 방안으로 제안하였으나, 장비 추가로 인한 비용 검토가 필요하다. 인터넷 전용선 속도는 45Mbps 급에서 적용될 수 있도록 하였고, 서버구조형방화벽 Interface(100BaseT) 1개의 속도로는 약 30Mbps의 전송량을 가지고 있어, 인터넷 속도를 유지하기 위해서는 L4 Switch를 설치하여 2개의 방화벽 시스템(100Base T)으로 구성하였다. 이렇게 함으로써 인터넷 전용선(45Mbps) 대비 방화벽에서 발생할 수 있는 병목현상을 L4 Switch에서의 Load balancing 기능에 의해 해결할 수 있었다. 그러나 단일 IDS 구조를 가지고 있어 침해요소의 대량 유입 시 피해가 따를 수 있다.

2개의 L4 Switch를 통하여 트래픽의 분산효과와 상호간 백업기능을 가질 수 있어 안정적인 서비스를 유지할 수 있는 장점이 있었다.

반면 별도의 Switch를 추가하지 않는 한 2단계 IDS 구성이 어려우며, 구성을 위해서는 반드시 통합형(Firewall+IDS)을 설치하여야 이중화 구성을 할 수 있다. 이 모델의 대안으로는, 기존 방화벽 시스템을 폐기하고, 최근 출시된 Switch 구조형 제품 중 통합형 100Mbps급을 활용하는 방법이 있다. 이것을 활용하면 1차 및 2차 IDS 적용과 L4 Switch 설치 없이도 초고속망(45Mbps급)의 인터넷 전용선을 활용할 수 있다.

V. 결 론

본 연구에서는 초고속 Backbone 망이라는 환경에서 각종 침해요인으로부터 정보망을 보호하고, 인터넷 전용선의 속도를 떨어드리지 않고 보안시스템의 구성방법을 제시하고자 하였다. 침해요인으로부터의 정보망의 보호도 중요하지만 그로 인해 전산망의 속도저하 문제를 해결해야 하는 것이 더 중요한 문제이다. 보안시스템으로 방화벽과 IDS의 설치는 필연적인바, 보안시스템 구축시 인

터넷전용선의 속도를 유지할 수 있는 보안시스템의 선택과 보안정책의 적용에 따른 병목현상을 최대한 고려하여야, 방화벽을 설치하면서 발생되는 속도저하와 안정적인 보안수준을 유지하는 방안이 될 것이다.

참고 문헌

[1] 박진수, "네 PC로 해킹하고 방어하기", (주) 사이버출판사 76판

[2] 호남네트워크 멤버쉽포럼 : forum.kjist.ac.kr

[3] 2002 정보시스템 해킹.바이러스 현황 및 대응 : KISA

[4] "방화벽 시스템의 구축과 운영", 한국전산원, 1996.

[5] Marcus J. Ranum, "Thinking About Firewall", Proceeding of Second INternational Conference on System on System and Network Security and Management, pp. 1-14, 1993.

[6] Mike Frantzen, Florian Kerschbaum, E. Eugene Schultz and Sonia Fahmy, "A Framework for Understanding Vulnera bilities in Firewalls Using a Dataflow Model of Firewall Internals", Computer & Security Vol. 20, No.3, pp.263-270, 2001.

[7] F.M. Avolio, D.M. Piscitello, "Intrusion Detection Joins Net Security Aresenal", Internet World, March 22, 1999.

[8] Karanjit S. Siyan & Chris Hare, "Internet Firewalls and Network Security", NRP, 1995