기업 내부 보안 시스템에서 보안성 개선 방안[1)]

유진근[0] 박근수
서울대학교 컴퓨터공학부
{jgyu[0], kpark}@theory.snu.ac.kr

Improving security on the Intranet security systems

Jingeun Yu[0] Kunsoo Park
School of Computer Science and Engineering, Seoul National University

요 약

인터넷 환경의 발달이 기업 내부까지 깊숙이 파고들어 기업 내의 각종 시스템 환경에 새로운 패러다임을 만들고 있다. 이러한 시스템의 활용적인 측면 뿐 아니라 보안적 관리도 중요해지면서 다양한 보안 시스템과 서비스가 내부 네트워크에서 운영되고 있다. 그래서 이 논문에서는 대기업을 모델로 하여 DNS(Domain Name System), 방화벽(Firewall), 침입 탐지 시스템(IDS)에 대하여 현 이용 실태를 파악해 보고, 각각의 개선 방향을 찾아본다.

1. 서론

인터넷 환경의 급속한 발달은 기업 내부의 네트워크 환경에도 많은 영향을 미쳤다. 메인프레임, 전용회선, client-server 전용 소프트웨어 등의 폐쇄된 형태로 구성되던 사내 정보 시스템을 인터넷에서 사용하는 TCP/IP open 환경과 웹이라는 다중 접속 소프트웨어를 통하여 기업 내의 자원과 비용을 효율적으로 사용하도록 변경시켰다. 이처럼 인터넷 환경의 축소판 구성이 사내에 들어서면서 인터넷 환경에서와 같은 정보 보안의 문제가 대두되게 되어 각 사업자들은 과거의 어느 때 보다도 내부 시스템의 보안에 신경을 쓰게 되었다. 과거의 폐쇄된 구조에서와는 달리 open 환경 시스템에서는 인터넷의 위협적인 요소가 바로 사내에도 위협적으로 작용하기 때문에 인터넷상에서 사용하는 각종 정보 보호 시스템과 기술이 사내에서도 그대로 사용 중에 있다.

이 논문에서는 대기업 A사를 대상으로 하여 내부의 정보 보호를 강화하는 방법을 찾아보고자 한다. 여기서 모델로 삼는 것은 대기업 위주의 모형이라서 중소기업의 환경이나 ISP(Internet Service Provider) 주변 환경과는 다소 차이가 있어 직접 적용하는 데는 적합지 않은 요소가 있을 수 있다. 그리고 여기서 택한 대기업 모델은 대략적으로 중앙에 정보 시스템 센터를 두고 지방에 다수의 지역 센터를 두고 운용하는 형태를 말한다. 내부의 사용자는 대략 수천 명 정도이고, 일반적으로 사용 중인 인터넷 환경이 사내의 인트라넷에 접속되어 있는 상황이다. 일부 정보 보호 시스템을 갖추고 있으며, 이를 전담으로 관리하는 부서와 인원이 구성되어 있고, 기업 내의 IT(Information Technology)부문 예산 중에서 일부분을 정보 보호 면에 투자할 여건을 갖춘 상태를 모델로 삼고 있다.

이 논문의 구성은 2장에서 사용 중인 DNS의 현재 상태와 보안성을 강화하는 방안을 검토하고, 3장에서는 방화벽에 대한 현황과 개선점을 알아본다. 4장에서는 IDS중에서 네트워크 베이스의 IDS에 대해서 현재의 문제점과 성능 개선을 위한 방안을 찾아본다. 5장에서는 결론과 함께 기업 내부의 정보 보호를 위하여 향후 지속적으로 관심을 가져야 할 부분에 대해서 알아보고자 한다.

2. DNS 개선

2.1 기존의 구성 및 운영 형태

현재 운영되고 있는 DNS 서버의 모습은 그림 1과 같이 내부와 외부에서 네임 쿼리가 있을 경우 이에 응답하고 있는 형태이다. 또, 시스템이 위치하는 곳은 일반적으로 외부에 공개되는 시스템들이 위치하는 DMZ[2)]에 위치하고 있으면서 내부와 외부 사용자로터 오는 쿼리에 응답을 하고 있다. 그래서 보통의 경우 내부 전용으로 사용되는 시스템들에 대한 정보와 외부

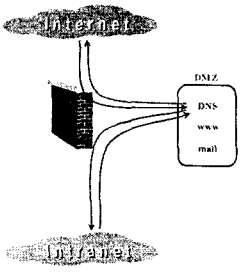

그림 1 기존 DNS 구성

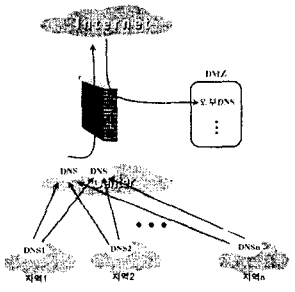

그림 2 DNS 개선안

로 공개되는 시스템에 대한 도메인 정보가 공유되고 있으며, 외부에서 쿼리가 가능하다. 이러한 구조에서는 외부에 공개되어야 할 도메인 정보를 관리하는 것은 문제가 되지 않겠으나 내부 전용으로 사용되는 시스템에 대한 도메인 정보를 외부에서도 찾아 볼 수 있는 기회를 제공하게 되어 내부 시스템에 대한 보안성을 약화시킬 수 있다.

그리고, DMZ는 중앙 전산 센터에 위치하게 되어 지역 사용자들은 지역에서 중앙으로의 네트워크를 거쳐 응답을 받게 되므로 지연을 감수해야만 한다. 더욱이 중앙의 DNS 서버가 외부의 공격을 받거나 시스템에 장애가 있을 경우 외부에 도메인 서비스를 제공하지 못할뿐더러, 내부 사용자들도 도메인 정보를 얻지 못하여 인터넷 접속에 지장을 받을 수 있다.

2.2 개선 방향

2.2.1 분산화, 이중화 구조

DNS의 문제점을 해결하기 위해서 우선 내부 도메인 정보 쿼리와 외부 도메인 정보 쿼리에 대한 응답 기능을 분산 시켜야 한다. 내부의 도메인 시스템은 내부와 외부의 도메인 정보를 resolving[3)] 할 수 있도록 해야 하고, 외부의 시스템은 인터넷에 공개되는 서버들에 대한 정보만 resolving하고, 내부 Intranet 시스템의 정보를 전혀 갖고 있지 않도록 구조와 환경을 바꾸어야 한다.

---

1) 본 논문은 2003년도 두뇌한국21 사업에 의하여 지원되었음.

2) DeMilitarized Zone : 내부 사용자와 외부 접속자에게 모두 접속을 허용하는 네트워크 Zone.

3) client로부터 도메인 쿼리를 받으면 DNS 서버들 간의 통신을 통하여 원하는 호스트의 IP address를 넘겨준다.

그리고, 내부 전용 DNS 시스템도 중앙 전산 센터와 지역 센터로 기능을 분산시켜 지역 사용자들에 대한 응답 속도를 향상시켜주는 것이 필요하다.

2.2.2 중앙 DNS의 개선

중앙 DNS중에서 외부 DNS는 역시 DMZ에 위치하면서 외부로부터 들어오는 쿼리에 응답을 해야 한다. 이때 사용하는 도메인 관련 소프트웨어는 최신의 버전을 사용하여 데몬의 취약점을 최소화시켜야 하고, 시스템 내부적으로 보관하고 있는 도메인 정보는 외부에 공개되어야 하는 정보만을 가지고 있도록 해야 한다.

중앙 센터에 있는 내부 DNS는 새로이 구성을 하여야 한다. 이 시스템은 내부의 사용자들이 이용하게 될 내부 시스템에 대한 도메인 정보를 갖게 된다. 그리고 지역에 분산되어 있는 DNS에서 요구하는 쿼리에 응답을 주어 내부 사용자가 이를 통하여 외부 인터넷에 접속하도록 한다.

2.2.3 지역 DNS의 개선

지역의 DNS는 지역 사용자들에게 접속 속도를 향상시켜 주는 주된 기능을 한다. 시스템을 구성할 때 캐쉬 기능 전용 서버로 구성하여 내부적으로 관리하는 도메인 정보는 갖지 않고 (이 기능은 중앙 센터의 내부 DNS에 위임) 사용자들이 사내외 시스템에 접속할 때 캐싱된 도메인 정보를 신속하게 제공한다. 그리고 이 지역 서버에는 forward[4][1] 기능을 살려서 지역 서버의 캐쉬에서 해결하지 못하는 도메인 정보는 중앙의 내부 서버를 이용하면 각 시스템 간에 기능과 정보를 효율적으로 이용할 수 있다.

2.3 개선 효과

DNS의 보안 문제 중에서 가장 중요한 도메인 정보 spoofing[5] 문제를 해결하기 위해서 새로 등장한 개념이 DNSSEC[6]이다[2][3]. 하지만 이 문제를 해결하기 위해서 DNSSEC을 사용하기에는 현실적으로 많은 문제가 걸려서 아직까지 상용화가 되지 못하고 있다. 현재의 방법으로 완벽히 spoofing을 방어하지는 못 하지만, DNSSEC을 이용하는 것보다는 훨씬 효율적으로 DNS 체계를 이용할 수 있다.

외부에 공개되는 도메인 정보는 중앙 센터에 있는 외부 전용 서버의 정보이므로 외부에서 사내 시스템에 대한 도메인 정보를 찾아볼 수 없다. 또한, 공개된 외부 DNS 서버가 DOS공격을 받더라도 내부 사용자들은 내부 DNS 시스템을 이용해서 인터넷을 사용할 수 있다. 내부 DNS 서버의 정보는 인터넷상에 공개되어 있지 않으므로 DNS 서버의 보안성을 높일 수 있다. 내부 네트워크에서 지역 사용자들은 지역에 캐쉬 전용 서버를 사용함으로써 접속 속도를 향상시킬 수 있다.

그리고, 중앙과 지역의 시스템을 각각 복수의 장비로 운영한다면 worm 바이러스 등으로 인해 DNS의 자원이 급격히 필요할 때 많은 효과를 볼 수 있다(그림 2 참조).

3. 방화벽 개선

3.1 기존의 구성 및 운영 형태

방화벽 구간의 네트워크 구성을 보면 인터넷과 접속되는 구간이 있고, 외부에 서비스를 제공하기 위하여 설치된 DMZ 네트워크가 있고, 업무상 관련이 많은 외부 업체와 직접 접속하기 위한 Extranet 구간이 있고, 내부 사용자와 연결이 되는 Intranet 구간이 있다(그림 3 참조). 기존의 방화벽은 이 모든 방향의 네트워크를 한 곳에 집중 관리를 하고 있으나 여기에는 많은 문제점을 가지고 있다.

우선, 다양한 네트워크에 관련된 필터링을 수용해야 하므로 방화벽이 관리하는 rule의 개수가 많아져서 패킷을 처리하는데 지연이 발생할 수 있다. 또한, rule의 개수가 많아지면, 관리자

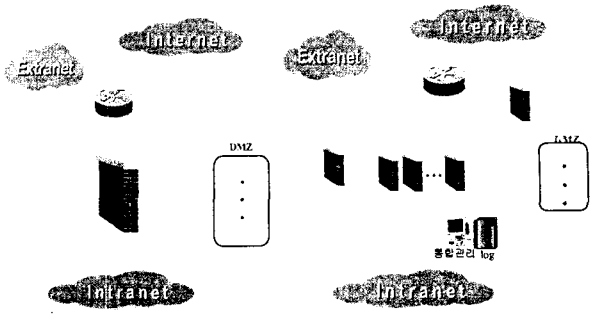

그림 3 기존 방화벽 구성

그림 4 방화벽 개선안

의 시스템 관리상 허점이 발생할 수 있다.

3.2 개선 방향

3.2.1 기능별 네트워크 분리

기업내외에 다양하게 요구되는 open 환경의 서비스를 충족시키고 늘어나는 트래픽을 적절히 처리하기 위해서는 방화벽 구간의 네트워크를 기능별로 구분 짓고 그에 따른 방화벽을 별도로 운영하는 것이 필요하다.

DMZ 네트워크는 외부에 공개되는 서비스와 시스템들이므로 방화벽을 거쳐서 인터넷과 연결이 되도록 DMZ 전용 방화벽 시스템을 운영하도록 하여야 한다.

기업간의 거래도 Extranet을 이용하여 처리되는 업무가 늘어나 별도의 네트워크로 분리하여야할 필요성이 있다. Extranet은 인터넷과 성질이 다르게 TCP/IP 이외의 프로토콜도 수용할 필요성이 있으므로 인터넷 구간과 구분지어 별도의 게이트웨이와 방화벽을 운영하여 업무의 효율성을 높이도록 하여야 한다.

그리고, 주 인터넷 트래픽이 처리되는 구간을 전담하는 방화벽 구조를 형성한다. 그리하여 주 방화벽의 rule을 감소시키고, 시스템의 자원을 확보하여 내부 사용자들이 사용하는 인터넷 구간의 병목 현상과 패킷 지연 현상을 제거하여야 한다.

3.2.2 Layer4 스위치를 이용한 부하 분담

인터넷 구간의 트래픽은 지속적으로 증가하고 있다. 이러한 대량의 트래픽을 중단 없이 처리하기 위해서는 대용량 처리 능력을 갖춘 방화벽을 갖추어야 하지만 단일 시스템으로 대처하기는 경제성, 시스템의 성능, 시스템의 관리 면에서 어려운 상황이다. 그래서 다수의 시스템을 병렬로 연결하여 트래픽의 병목 현상을 제거하고 방화벽 시스템의 장애 시 네트워크의 생존성을 제공할 수 있어야 한다. 이때, 근래에 생산되는 Layer4 스위치를 이용하여 방화벽 구간의 네트워크를 구성하면 방화벽의 효율성과 생존성을 확보할 수 있다.

3.2.3 별도의 로그 서버 운영

방화벽의 주요 기능은 필터링에 있지만, 방화벽의 활용성을 본다면 사후 로그 검색 기능이라고도 할 수 있다. 그 만큼 방화벽에서의 로그 저장 기능은 필수적인 요소다. 하지만, 기존 방화벽의 구성에서는 로그 저장을 방화벽의 내부 파일 시스템에서 관리하고 있어 방화벽의 장애나, 침해 시 로그 검색을 불가능하게 할 수도 있다. 이러한 상황에 대비하기 위해서는 별도의 로그 서버를 운영하여야 한다. 즉, 다수의 방화벽을 사용하더라도 별도의 외부 로그 서버를 구성하여 방화벽의 로그를 전용 네트워크를 통하여 로그 서버에 저장하여 본 방화벽의 장애 시 로그 검색, 관리에 대비하여야 한다.

3.2.4 통합 관리

이렇게 네트워크를 기능별로 구분하여 설치하고, 다수의 방화벽을 관리하고, 별도의 로그서버를 운영하기에는 복잡한 운영 과제가 뒤따르게 된다. 이러한 문제를 해결하기 위해서는 하나의 manager 시스템에서 다수의 방화벽을 통합 관리할 수 있는 시스템을 갖추어야 한다[4]. Manager 시스템에 전체 시스템을 관리하는 영역과 각각의 세부 시스템을 관리하는 영역을 구분하여 다수의 방화벽을 운영할 수 있도록 기능을 갖추어야 한다.

3.3 개선 효과

4) 자신이 알 수 없는 도메인 정보는 스스로 resolving 기능을 하지 않고 특정 서버에게 위임을 시킨다.

5) 도메인 네임과 연결된 IP address 정보를 조작하여 정상적인 서버 접속을 방해한다.

6) DNS 서버 간 통신을 할 때 PKI 방식의 인증과 전송 데이터의 암,복호화를 통하여 도메인 정보의 무결성을 보장하는 하나의 방법

네트워크의 분산으로 worm 바이러스 등으로 인해 인터넷 구간에 장애가 발생할 경우에도 Extranet 관련 트래픽은 정상적으로 소통될 수 있다. 그리고 방화벽 자체도 병렬 구조로 개선하면 병목 현상 제거 및 네트워크의 생존성을 확보할 수 있다. 다수의 방화벽을 통합 관리를 하면 시스템 관리에 효율성을 기할 수 있다(그림 4 참조).

4. IDS(Intrusion Detection System) 개선

4.1 기존의 구성 및 운영 형태

IDS는 네트워크 베이스 모델과 서버 베이스 모델로 구분되지만, 여기서는 네트워크 베이스 모델을 위주로 살펴본다. 그림 5에서도 알 수 있듯이 IDS는 Intranet과 DMZ의 트래픽 중에서 비정상적인 패턴을 감지하기 위한 곳에 설치된다. 그리고 이 IDS는 공급사로부터 불법적인 형태의 패킷 정보를 다운받아 네트워크 상에 유통되는 패킷과 비교해서 불법 침입을 감지하여 관리자에게 경고한다. 하지만, 이러한 구조에서는 새로이

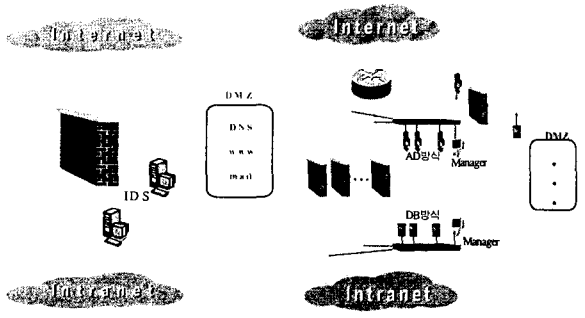

그림 5 기존 IDS 구성

그림 6 IDS 개선안

등장하는 불법 침입을 감지하는 데는 어려움이 있어, 실제상황에서 불법 침입을 감지하지 못하는 경우가 있다. 또, 대단히 많은 불법 유형의 DB와 비교하는 과정에서 처리 지연과 패킷 유실이 발생할 수도 있다.

4.2 개선 방향

4.2.1 부하 분산 구조

IDS가 도입되던 초창기와는 달리 현재의 트래픽은 위에서 살펴본 바와 같이 다양한 종류의 트래픽이 대량으로 전송되고 있다. 이러한 상황에서 IDS의 기능을 정상적으로 발휘하기 위해서는 시스템을 복수로 설치하여 부하를 분담시키는 구조로 형성하면서 시스템의 장애 시에도 침입 탐지 기능에 중단이 없도록 하여야 한다. 일반적으로 IDS가 침입을 감지하는 경우는 불법적인 패킷이 유입될 때지만, 근래에 들어서는 worm 바이러스의 패킷이 대량으로 발생할 때도 침입으로 간주한다. 이 경우 관련 네트워크에 갑자기 폭주가 걸리면 IDS의 성능이 제대로 발휘되지 않는 경우가 발생하므로 이를 위해서는 다수의 서버를 load-balance 구조로 구성하는 것이 필요하겠다.

4.2.2 복합 감지 방식 도입

현재 사용되고 있는 IDS는 비정상적인 패킷의 유형을 DB로 갖고 있으면서 전송되는 패킷과 비교하여 침입 패킷인지, 정상적인 패킷인지를 감지하는 DB검색 방식을 취하고 있다. 이러한 경우에 새로이 등장한 불법 패킷은 IDS에 감지되지 않고 통과하게 된다. 이 문제는 DB 검색방식의 IDS가 갖고 있는 태생적 문제라 할 수 있다.

이러한 문제점을 해결하기 위해서는 평상시 내부 사용자들이 사용하는 패킷과 외부에서 접속하는 정상적인 패킷에 대해서 학습 과정을 통하여 정상적인 패킷으로 분류하고 그 이외의 패킷은 불법적인 패킷으로 분류하여 침입을 감지하는 anomaly detection 방식 시스템 구성이 필요하겠다[5]. 이러한 anomaly detection 방식은 운영 초창기에는 오보의 확률이 높으나 시스템 교육을 통하여 차차 신뢰성을 확보할 수 있다. 이것은 지금까지 사용되어 온 DB 검색방식의 IDS가 불필요하다는 것이 아니고, 효율적인 침입 감지를 위해서는 두 가지 방식의 탐지가 병행되어야 한다는 것이다. 이렇게 하면 기존의 DB 검색 방식의 문제점을 해결하면서 효율적인 불법 패킷의 유통을 감지할 수 있겠다.

4.2.3 필터링 rule의 단순화

기존에 운영중인 DB 검색 방식에서는 매우 많은 불법 패킷의 유형을 보관하고 있으므로 감지한 패킷의 상태를 비정상적으로 판단하는 경우가 필요 이상으로 많이 발생한다. 하지만, 이러한 경보 중에서 실제 보안적 위협 요소에 드는 것은 극히 일부분에 지나지 않고, 대다수의 경보는 효용성 없는 경보가 되고 있다. 이러한 불필요한 경보를 막고, 시스템의 프로세싱 능력을 보호하기 위해서는 주기적인 모니터링을 통해서 IDS의 필터링 rule을 단순화하여야 한다[6][7].

4.2.4 다수 시스템에 대한 통합 관리

기업 내부의 대단히 많은 인터넷 트래픽에 맞춰 IDS를 운영하기 위해서는 IDS또한 다수의 시스템으로 구성되어야 한다. 이렇게 다수의 시스템으로 구성된 경우 관리자의 과오 방지와 업무의 효율성을 위하여 통합 관리가 필요하다. 즉, 수집된 패킷을 필터링 rule과 비교하여 원시 데이터를 만드는 agent와 이 결과를 수합하여 종합 메시지를 생산하는 manager를 관리하기 위해서 통합 관리 시스템이 필요하다.

4.3 개선 효과

DB 검색 방식과 anomaly detection 방식을 병행하여 침입 탐지를 함으로써 IDS 운영의 효율을 극대화 시킬 수 있다. 그리고 load-balance 구조와 통합 관리를 통하여 늘어나는 인터넷 트래픽에 유연하게 대처할 수 있고 시스템의 성능을 유지시킬 수 있다.

5. 결론 및 향후 연구

기업 내부의 네트워크와 시스템도 인터넷과 동등한 수준의 정보 보호 정책을 필요로 하고 있다. 이 중에서 인터넷 접속에 반드시 필요로 하는 DNS 서버를 외부용과 내부용으로 구분하고 내부용은 다시 지역의 사용자를 위한 형태로 구성한다. 그래서 외부에 필요 이상의 정보를 유출하지 않는 보안성을 갖추고 내부의 사용자에게는 접속 속도의 향상을 도모 하였다.

방화벽은 네트워크를 기능별로 세분화하고 기능에 따라 별도의 방화벽을 설치하였다. 주 인터넷 트래픽의 원활한 처리와 장애 시 네트워크의 생존을 위하여 병렬로 구성하여 통합 관리를 하였다. 그리고 사후 로그 검색의 중요성을 감안하여 별도의 로그 서버를 구성하여 활용성을 높였다.

IDS는 DB 검색 방식과 anomaly detection 방식을 복합 구성하여 불법 패킷의 감지 능력을 향상시켰다. 그리고 시스템의 확장을 용이하게 하고 부하량 폭주 시에 원활한 처리 능력을 확보하기 위하여 load-balance 구조를 갖추었다.

이 같은 개선은 추가적인 시스템이 필요하여 다소의 비용이 소요된다. 하지만 정보 보호의 중요성을 감안하여 기업의 IT분야 예산 중에서 일부분을 2-3년에 걸쳐서라도 꼭 투자해야 할 것이다. 그래야 점차 강조되는 정보 보호와 안정적인 인터넷 사용에 기여할 수 있겠다. 그리고 향후 연구로 바이러스 방역 체제, VPN(Virtual Private Network)운영 등에 관해서 개선 방향을 찾아볼 예정이다.

6. 참고 문헌

[1] Paul Albitz, Cricket Liu, DNS와 BIND 4판, p375-380, p436-515, 2002.1
[2] G. Ateniese, S. Mangard, A New Approach to DNS Security, CCS'01, Nov 5-8, 2001
[3] A. Lioy, F. Maino, M. Marian, DNS Security, Terena Networking Conference, May 22-25, 2000
[4] 이동명, 김동수, 정태명, 이종의 보안시스템 관리를 위한 정책 기반의 통합보안관리시스템의 계층적 정책모델에 관한 연구, 한국정보처리학회 vol8-c, No05 p607-614, 2001.10
[5] W.Lee, J.Stolfo, Data Mining Approaches for Intrusion Detection, the 7th USENIX Security Symposium, 1998
[6] K. Julish, M. Dacier, Mining Intrusion Detection Alarms for Actionable Knowledge, SIGKDD 2002
[7] 문종욱, 김종수, 정기현, IDS의 성능 향상을 위한 패킷 폐기 방안, 한국정보처리학회, Vol.9-c, No04, p473-480, 2002.8