방화벽에서 바이러스 및 불건전정보 차단에 관한 연구

°송의*, 권석철*, 김남욱*, 이병만*, 송관호*
한국전산원*

The study on blocking virus and harmful information through firewalls

°Eui Song*, Seok-Chul Kwon*, Nam-Wook Kim*, Byung-Man Lee*, Kwan-Ho Song*
National Computerization Agency*

요약

외부의 불법 침입자로부터 내부 네트웍 보안을 위한 하나의 솔루션으로 방화벽이 제공되고 있다. 방화벽은 크게 패킷필터링 방식과 어플리케이션 방식의 방화벽으로 나누어지는데 어플리케이션 방식은 프락시 기능을 이용한다. 본 논문에서는 어플리케이션 방식의 방화벽에서 FTP Proxy, SMTP Proxy를 통한 파일전송시 바이러스 차단 및 HTTP Proxy를 통한 음란, 폭력물과 같은 불건전정보를 차단하는 방법을 제시하였다.

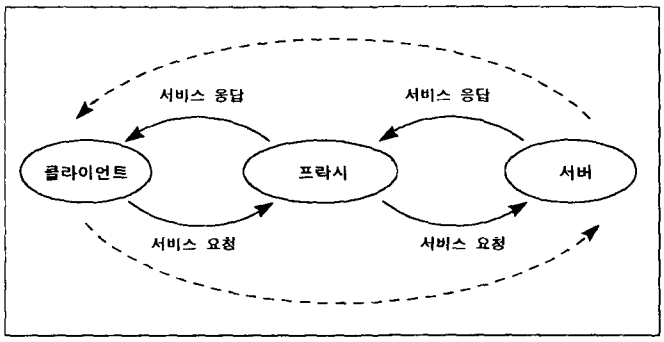
I. 개요

인터넷에 대한 관심 증대와 인터넷에 연결하는 호스트가 증가되고 있고, 이러한 인터넷을 통해 사용자들은 다양한 서비스를 받게 되었을 뿐만 아니라 유익한 정보를 얻을 수 있게 되었다. 그러나 인터넷을 통한 해커들의 침입으로 인한 피해도 크게 늘고 있고, 그 수법 또한 전문·다양해지고 있다. 인터넷으로부터 이러한 해커 및 불법 침입자의 차단을 막기 위한 대책으로서 방화벽은 하나의 솔루션으로 제공되고 있다. 국내에서는 외산 방화벽시스템을 도입하여 설치하고 있으며 국내 일부기관 및 업계에서는 국산 방화벽 개발을 하였거나 진행중에 있다. 이러한 방화벽들은 방화벽 관리자가 모든 내부 사용자들에 대해서 외부로 접속을 허용하도록 운영하고 있기때문에 내부 사용자가 인터넷을 통하여 얻는 정보가 사용자에게 유해한지를 알기란 어려운 일이다. 본 논문에서는 어플리케이션 방식의 방화벽에서 파일전송시 바이러스에 감염된 파일과 음란, 폭력, 마약 등 불건전정보를 차단하는 방법에 대해서 알아본다.

II. 방화벽 호스트에서 프락시(proxy)의 역할

방화벽은 외부로부터 불법침입을 차단하고, 내부로부터의 불법 정보 유출을 방지하는데 목적이 있는 네트웍보안 솔루션이다. 일반적인 방화벽의 방식은 크게 패킷필터링 방식과 어플리케이션 방식으로 나누어질 수 있는데, 패킷 필터링 방식은 네트웍의 OSI 7 계층 모델에서 제 3, 4 계층에 방화벽 기능이 들어가지만, 어플리케이션 방식은 제 7계층에 방화벽 기능이 추가된다. 어플리케이션 방식의 방화벽 구성 요소인 프락시의 특징은 클라이언트와 실제 서버사이에 존재하여 둘 사이의 프로토콜 및 데이터 relay역할을 하므로 이러한 프락시 기능에 바이러스 검색 기능을 추가함으로써 방화벽 상에서 바이러스 검색 효과를 부가적으로 얻을 수 있다. 이렇게 방화벽 상에서 바이러스 검색이 이루어지기 위해서는 기존의 프락시 서버가 바이러스 검색 모듈을 호출할 수 있도록 수정할 필요가 있다.

본 논문에서는 바이러스 검색 모듈을 추가하기에 용이한 어플리케이션 방식의 방화벽 시스템에 바이러스 검색 기능을 추가함으로써 바이러스를 차단할 수 있는 방법에 대해 기술하고 있다.

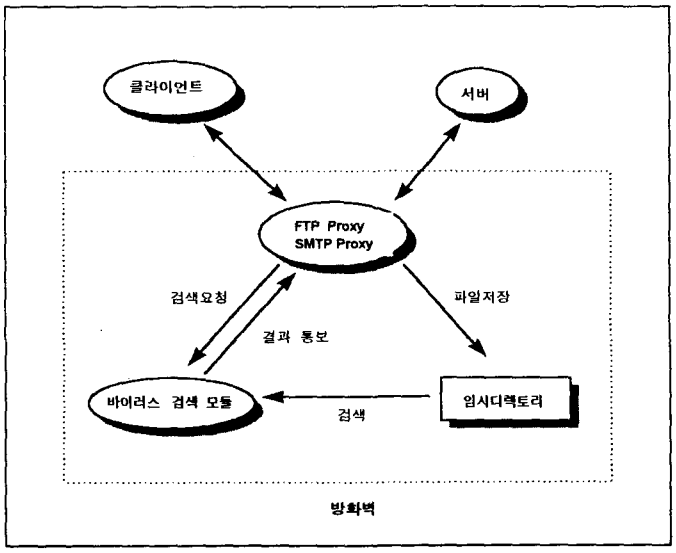


< 프락시 개념도 >

Ⅲ. 방화벽과 바이러스 검색 및 차단

과거에 PC의 바이러스는 디스켓 및 사내 네트웍을 통하여 확산되었지만, 현재는 인터넷을 통한 바이러스 감염이 확산되고 있는 상황이다. 지금까지는 서비스 요청을 한 클라이언트에서 각각 백신 소프트웨어를 이용하여 바이러스 감염 여부를 점검 하였지만, 이러한 점검 방법은 각각의 클라이언트에서 주기적으로 바이러스 백신 소프트웨어를 사용할 때만 바이러스 검출이 가능하므로 사용자가 스스로 대비를 하지 않는다면 그리 큰 효과를 얻지 못하고 있는 것이 사실이다.

따라서 네트웍 게이트웨이나 내부의 파일 서버 시스템에서 집중적으로 바이러스 점검을 하는 것이 더 효과적이라고 볼 수 있을 것이다. 더욱이 중앙에서 바이러스 점검을 할 경우, 새로 나오는 바이러스 패턴에 대한 데이터베이스의 갱신이 편리해 질 수 있다는 장점이 있다.



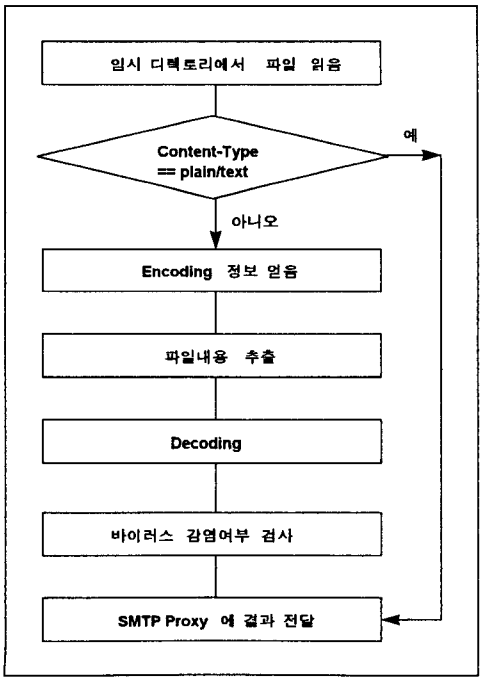
1. FTP(File Transfer Protocol)를 이용한 파일전송시 방화벽에서 바이러스 검색

FTP를 통해 파일 전송이 이루어질 경우, 클라이언트는 실제 서비스 서버에게 서비스를 요구하고 클라이언트의 요구를 받은 실제 서버는 요청 파일을 클라이언트로 전송하게 되는데, 이 경우의 전송 파일이 방화벽의 FTP Proxy를 통과하여 클라이언트로 전달된다. 이 경우 본 논문에서 제시한 수정된 FTP Proxy는 실제 서버로부터 받은 파일을 클라이언트에게 전달해 줌과 동시에, 방화벽 시스템 상에 설정해 놓은 임시 디렉토리에 파일을 복사하여 저장한다. 이러한 파일 저장이 완료될 시점이면 파일은 이미 클라이언트에게 전달되었을 상태이고, 방화벽의 임시 디렉토리에 남아 있는 파일에 대해서 바이러스 검색 모듈을 이용하여 바이러스 감염 여부를 검색하게 된다. 바이러스 검색 모듈은 FTP Proxy에 검색 결과를 통보하고, FTP Proxy는 통보된 검색 결과에 따라 파일에 바이러스가 감염되어 있으면 그 정보를 클라이언트에게 알려준다.

방화벽에서 사용하는 바이러스 검색 모듈은 내부의 UNIX 시스템을 파일 서버로 이용할 경우에도 응용할 수 있다. 사용자들은 파일 서버에 파일을 upload하거나 파일 서버로부터 download할 때 해당 파일의 바이러스 포함 여부를 확인할 수 있을 뿐만 아니라, 파일 서버 시스템 자체에서 파일의 바이러스 감염여부를 주기적으로 검사할 수 있도록 할 수 있다.

결국 외부로부터 내부 네트웍으로 전달되는 파일에 대한 바이러스 검사와 내부 네트웍에서 파일에 대한 바이러스 검사의 2중 검색 방법을 이용하면, 보다 확실하게 내부망으로 유입된 바이러스를 차단할 수 있게 된다.

2. 전자메일을 이용한 파일전송시 바이러스 검색



< 전자메일의 바이러스 검색 플로우 >

전자메일의 경우는 FTP와 비교할때 바이러스를 검색하기가 조금 까다롭다. 왜냐하면 전달되는 내용의 encoding/decoding 방법에 대해서 알아야하는 것이 추가로 요구되기 때문이다. 메일은 크게 헤더부분과 본문, 추가(attached)된 내용으로 나눌 수 있는데 헤더는 본문과 추가된 내용에 각각 붙여진다.

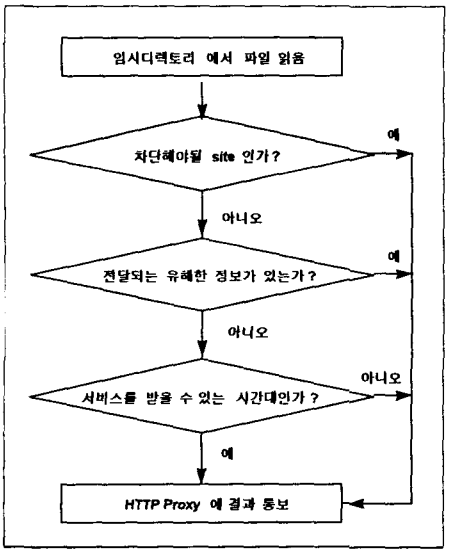
헤더의 내용 중에 Content-Type은 전달되는 내용이 텍스트 형태인지 아닌지에 대한 정보를 알려주고, Content-Transfer-Encoding은 전달되는 내용의 encoding 방법을 나타내고 있다. 따라서 전달되는 내용이 텍스트가 아니면 encoding정보를 얻은 다음 boundary 정보를 이용하여 순수 파일의 내용만을 분리한후 분리된 파일을 decoding하여 바이러스 감염 여부를 검사하면 된다. 검사후 바이러스가 있으면 메일을 송신자와 수신자에게 그 정보를 알려준다.

```
Content-Type: multipart/mixed; boundary="----------595E3D6A7A07"
This is a multi-part message in MIME format.
----------595E3D6A7A07
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
안녕하세요.
----------595E3D6A7A07
Content-Type: application/octet-stream; name="Esm.arj"
Content-Transfer-Encoding: base64
YOonAB4DAQAAAAKLi05VIQAAAAAAAAAAAAAAAAAAAAAAAEVT
bgAAGDqKgAeiLp+/9/9+GDqAAA=
----------595E3D6A7A07--
```

3. 불건전정보 차단

있기 때문에 방화벽에서 차단하는 것이 좋다고 볼수 있다.

3.1 차단방법



<음란정보 차단을 위한 플로우>

내부에서 외부로 접속을 시도할때는 불건전 사이트에 대한 URL(Uniform Resource Locator) Screening을 하고, 외부로부터 정보가 내부로 유입될때는 단어를 검색하여 차단하고자 하는 단어가 있으면 그 정보를 차단하면 된다. 이렇게 하기위해서는 별도의 차단 모듈 및 차단 관련 DB 구축이 필요하고, 기존의 HTTP Proxy를 수정해야한다.

내부 사용자가 외부의 웹사이트로 접속을 시도하였을 때 방화벽의 HTTP Proxy는 외부로의 접속허용 여부와 외부로부터의 HTTP Proxy로 들어오는 내용에 대해서 내부로 통과해야할지를 차단모듈에 요청한다. 차단모듈은 먼저 URL을 검사하여 또한 전달되는 정보에 차단해야 될 단어가 있는지를 검사하고 그 결과를 HTTP Proxy에 전달한다. 차단모듈로부터 결과를 받은 HTTP Proxy는 그 결과에 따라서 정보의 유입을 결정한다.

부가적으로 어떤 특정 시간에만 불건전 사이트를 볼 수 있도록 시간을 부여할 수 있다. 또한 외부로부터 내부 사용자에게 유입되는 정보의 내용 중에 차단하고자 하는 단어가 있는지 검색하여 확인되면 차단할 수 있다. 이러한 차단기능이 충분한 효과를 얻기위해서 차단하고자 하는 사이트의 지속적인 DB갱신이 필요하고, 단어검색을 하기위해서 빠른 알고리듬을 사용하는 것이 필요하다.

Ⅳ. 결론 및 발전방향

일반적인 방화벽은 외부로부터 불법 침입자가 내부망의 접근을 차단하기 위한 것이었지만 지금까지 살펴본 내용은 내부 사용자들이 외부로부터 정보를 가져올 때 파일전송을 통한 바이러스 , 웹을 이용한 불건전 정보 또는 불필요한 정보를 차단하는 방법에 대해서 살펴보았다. 특히 파일전송을 통한 바이러스 검색이 효과를 얻기 위해서 압축된 파일에 대한 검사가 필요하며 또한 바이러스 제작도구들을 분석하여 많은 바이러스 패턴들을 확보할 필요가 있다. 또한 웹을 이용한 불건전 정보를 차단하는 방법이 효과를 얻기 위해서 정보의 내용에 있는 단어 검색을 빨리 할 수 있는 알고리듬을 적용하는 것이 필요하다. 방화벽에서 바이러스 및 불건전정보를 효과적으로 차단하기 위한 방법과 이러한 차단 방법이 방화벽에 부하를 적게 하도록 하는 것은 앞으로 계속적으로 발전시켜야할 내용이다.

참고문헌

1. Karanjit Siyan and Chris Hare, "Internet Firewalls and Network Security", NRP, 1995
2. D. Brent Chapman and Elizabeth D. Zwicky, "Building Internet Firewalls", O'Reilly & Associates, Inc. 1995
3. William R. Cheswick and Steven M.Bellovin, "Firewall and Internet Security", Addision-Wesley, 1994
4. Marcus J.Ranum, "Thinking About Firewalls", proceedings of the Second World Conference on Systems Management and Security, 1993
   Available for FTP from ftp.tis.com:/pub/firewalls/firewall.ps.Z
5. 권석철, "컴퓨터 바이러스 예방과 치료", 크라운출판사, 1994
6. "컴퓨터 바이러스 감염 예방 시스템 개발에 관한 연구", 한국전산원, 1995
7. "인터네트", 342 - 351page, 정보시대, 1996. 10