혼합형 방화벽 시스템 구현 연구

Implementation of Hybrid Firewall System

정지문, 우성구, 이승호*, 최 성

Ji-Moon Jung, Sung-Gu Woo, Syng-Ho Lee*, Sung Choi

남서울대학교 컴퓨터학과

Dept. of Computer Science, Namseoul University

요 약

본 논문은 스크리닝 라우터에서 패킷 필터 규칙을 통과한 모든 트래픽이 베스천 호스트로 전달되도록 스크린드 호스트 게이트웨이를 사용하였으며, 스크린드 호스트 게이트웨이의 단점인 스크리닝 라우터의 경로정보가 내부 네트워크로 직접 전달되지 않도록 듀얼-홈드 게이트웨이를 사용하였다. 듀얼-홈드 게이트웨이에서는 두 개의 네트워크 인터페이스간에 트래픽이 직접 전달되지 않기 때문에 응용 게이트웨이 서버를 통해서 트래픽이 전달되고 모든 접속기록이 베스천 호스트에 기록되도록 하였다. 또한 외부 네트워크와 내부 네트워크 사이에 완충지역인 DMZ를 두어 공개 서버를 사용하기 쉽게 구현하여, 스크리닝 라우터와 스크린드 호스트 게이트웨이의 문제점을 해결하는 효과적인 혼합형 방화벽 모델을 제안하고자 한다.

Ⅰ. 서론

방화벽 시스템은 네트워크의 보안사고나 문제가 더 이상 확대되는 것을 막고 격리하려는 기술로서 특히, 한 기관 내부의 네트워크를 보호하기 위해 외부로부터 들어오는 불법적인 트래픽은 막고 허가되고 인증된 트래픽만을 허용하려는 적극적인 방어대책이다. 방화벽 시스템은 가장 효과적이고 비용이 비교적 저렴한 정보보호 기술이라 할 수 있다. 본 논문의 본론에서는 방화벽에 대해서 정의와 목적 그리고 시스템의 원리를 알아보고 시스템 침입유형을 파악하며, 방화벽 구축시 고려사항을 알아본다. 그 다음은 혼합형 방화벽 구현 모델링에 대해서 구현방법 및 설계를 한다.

Ⅱ. 본론

2. 방화벽

2.1 방화벽의 정의

방화벽(Firewall)이란 넓은 의미와 좁은 의미로 정의되어질 수 있는데 넓은 의미로는 인터넷(Internet) 같은 외부 네트워크에 연결된 내부 네트워크(예, LAN)를 외부의 불법적인 사용자의 침입으로부터 안전하게 보호하기 위한 정책 및 이를 지원하는 H/W 및 S/W를 총칭한다. 또 좁은 의미의 방화벽은 외부네트워크와 내부네트워크에 위치하여 외부로 부터의 침입과 내부로부터의 불법적인 정보유출을 방지하기 위한 네트워크의 한 구성요소(component)로서 H/W와 S/W의 조합으로 이루어지는 시스템이다.

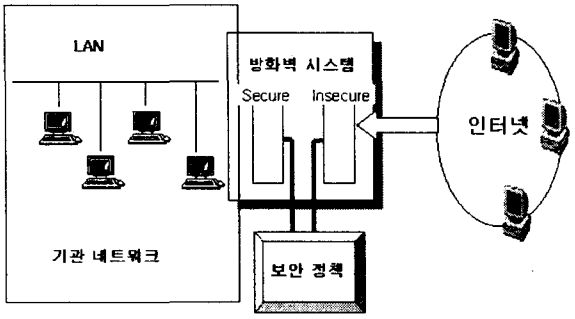
2.2 방화벽의 목적

방화벽의 목적은 정당한 권리를 획득하지 않은 사용자가 전용 네트워크의 자원에 접근하려는 시도를 막는 것과 중요한 정보가 허가를 받지 않고 네트워크를 통해 외부로 유출되는 것을 막는 것이다. 방화벽 시스템은 내부 네트워크 보호를 위해 현재로서 최선의 방법이지만 완벽한 보안을 해준다고는 보장할 수 없다. 그러나 가장 효과적이고 비용이 적게 드는 방법이라고 볼수있다.

2.3 방화벽 시스템의 원리

인터넷과 같은 거대한 외부 네트워크에 연결된 내부 네트워크의 모든 컴퓨터 시스템은 항상 해커에 의해 침입당할 수 있는 위험 지대(Zone of Risk)에 놓이게 되며, 각 시스템이 해커의 침입으로부터 자신을 개별적으로 방어하는 것은 현실적으로 불가능하다. 따라서 방화벽은 외부 네트워크에서 내부 네트워크로 접근하기 위해서는 반드시 방화벽 시스템을 통과하도록 함으로써 위험지대로부터 내부 네트워크를 분리하여 전체 시스템을 한꺼번에 보호하기 위한 "경계선 방어"의 개념을 사

용한다[그림 1]. 방화벽 시스템은 이러한 "경계선 방어"를 위해 "명백히 허용되지 않은 것은 금지된다"는 기본적인 원칙을 준수한다.



[그림 1] 방화벽 시스템에 의해 보호된 내부네트워크

3. 시스템 침입유형

인터넷의 시스템 침입유형은 표 1과 같이 분류할 수 있다.

[표 1] 시스템 침입유형

유 형	내 용
사용자 도 용	정당한 사용자의 권한을 도용하여 접근함 Packet Sniff, Crack등을 이용함
취약점 공 격	운용체제, 응용 프로그램의 취약점을 이용하여 공격함 Sendmail, NFS, Elm, TFTP등을 이용함
시스템 위 장	정당한 호스트로 위장하여 인증없이 불법 접근함 .rhosts, hosts.equiv 파일을 수정하여 접근함
데이터 주도공격	불법 프로그램을 이식함 Worm, ISS, SATAN등을 이용함
구조적 문제공격	시스템 및 프로토콜의 구조적 결함을 이용하여 공격함 IP Spoofing 이용함
서비스 방해공격	시스템의 정상적인 서비스를 방해하여 공격함 Mail Stome, Ping Flooding등을 이용함

4. 방화벽 구축 모델링

4.1 고려사항

방화벽 구축시 고려사항은 아래 표 2와 같다.

[표 2] 방화벽 구축 고려사항

구 분	내 용
자원 보호	H/W, S/W, 각종 중요한 정보, 시스템 사용자, 시스템 관리에 대한 문서
위협 존재	자원 및 정보에 대한 위협으로 어떤 유형의 위협이 존재하는지 파악
자원 중요도	자원의 손실 위험과 자원의 중요도를 정량화하여 값을 부여, 두 값의 곱으로써 라우터, 브리지, 서버등의 위험 가중치를 산출
사용자 인가	비인가된 외부인, 인가된 외부인, 내부인 등으로 구분, 접근범위 결정
요구되는 응용 및 서비스	Web, FTP, Telnet, Mail, News등과 같이 사용 가능한 응용 및 서비스들로 사용자의 인가범위에 따라 결정
비용대효과	다양한 형태의 실현 가능한 방화벽 시스템 검토

4.2 구현방법

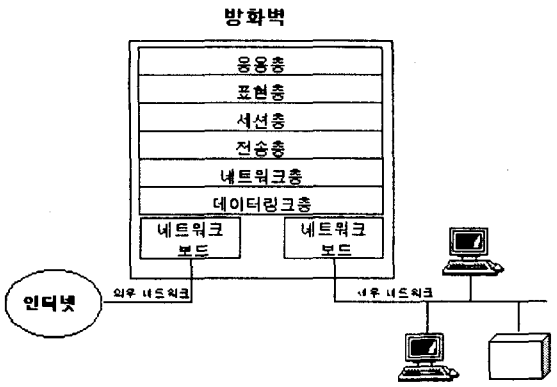
4.2.1 패킷 필터링

스크리닝 라우터를 사용하며, 스크리닝 라우터는 OSI 참조 모델의 네트워크 계층과 전송 계층에서 동작되기 때문에 이들 계층에서 동작하는 프로토콜인 IP, TCP 혹은 UDP의 헤더에 포함된 내용을 분석하여 동작한다. 특정 프로토콜을 기준으로 포트상에서 허용된 패킷과 금지된 패킷을 구별할 수 있는 라우터 기능을 패킷 필터링이라고 하며, 이와 같은 스크리닝 라우터를 패킷 필터링 라우터라고도 한다. 스크리닝 라우터는 네트워크 보안 경계영역을 침범하지 못하도록 하여 위험지역을 줄일 수 있는 장치이며 스크리닝 라우터 자체만으로 위험지역을 없앨 수는 없지만, 위험지역을 효과적으로 줄일 수 있다. 스크리닝 라우터의 장점으로는 라우터 하나로 내부 네트워크 전체를 동일하게 보호할 수 있으며, 필터링 속도가 빠르고 비용이 저렴하다. 단점으로는 네트워크 계층과 전송 계층에 대한 트래픽만 방어가 가능하며 보안 정책이 유연하지 못하고 패킷 필터링 규칙에 대한 검증이 어려움이 있다. 또한 접속기록을 할 수 없으며 패킷내 데이터에 대한 공격은 차단이 불가능하다.

4.2.2 응용 게이트웨이

가. 듀얼-홈드 게이트웨이

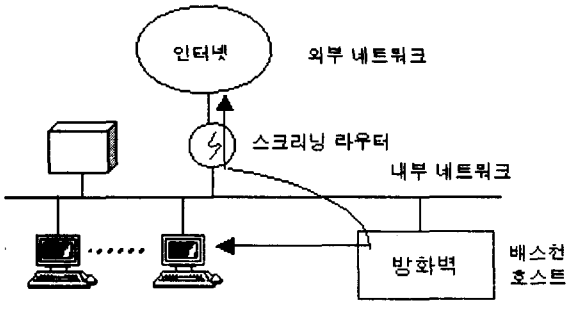
듀얼-홈드 게이트웨이는 그림 2와 같이 두 개의 네트워크 인터페이스를 가진 베스천 호스트를 말하며, 이들 인터페이스 사이에 라우팅 기능이 불가능하므로 외부의 신뢰성없는 네트워크로부터 내부의 네트워크를 분리시키는데 사용될 수 있다. 듀얼-홈드 게이트웨이는 TCP/IP 트래픽을 직접 통과시키지 않기 때문에 내부와 외부 네트워크간의 트래픽을 완전하게 막는다. 라우팅이 없는 듀얼-홈드 게이트웨이를 이용하여 인터넷 또는 내부 네트워크의 정당한 사용자들이 응용 서비스를 제공받는 방법으로는 첫 번째, 듀얼-홈드 게이트웨이에서 제공하는 Proxy 서버를 사용하는 방법과 두 번째, 응용 서비스를 제공해주는 듀얼-홈드 게이트웨이에 직접 로그인 한 다음 다시 내부 네트워크로 접근하는 방법인데, 이 경우에는 일회용 패스워드와 같은 강력한 인증 방법이 구현되어야 한다. 듀얼-홈드 게이트웨이의 가장 큰 위협은 외부로부터 직접 로그인을 허용하는 것이다. 이를 예방하기 위해서는 외부로부터의 신뢰성 없는 로그인에 대하여 강력한 인증이 요구된다.



[그림 2] 듀얼-홈드 게이트웨이

나. 스크린드 호스트 게이트웨이

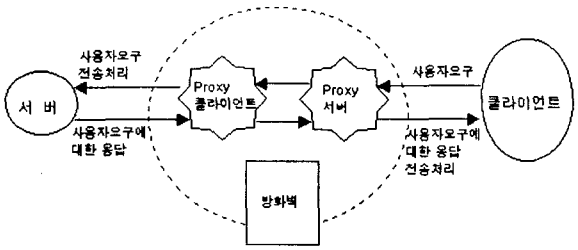
스크린드 호스트 게이트웨이는 스크리닝 라우터와 베스천 호스트를 혼합한 형태로서, 그림 3과 같이 스크리닝 라우터의 포트는 외부 네트워크와 내부 네트워크로 각각 연결되어 있으며, 베스천 호스트의 네트워크 인터페이스는 내부 네트워크에 연결되도록 구성된 종류이다. 스크리닝 라우터를 구성할 때 외부 네트워크로부터 내부 네트워크로 가는 모든 트래픽을 받은후, 트래픽에 대한 필터 규칙을 적용한 다음 베스천 호스트로 먼저 보내도록 해야 한다. 또한 베스천 호스트는 응용 게이트웨이 서버 기능을 사용하여 나가거나 들어오는 요청을 허용할 것인지 거절할 것인지를 결정해야 한다. 만약 스크리닝 라우터의 경로정보가 잘못 구성되어 내부 네트워크로 직접 보내지게 되면 베스천 호스트는 우회되므로 보다 더 안전한 방법으로 듀얼-홈드 게이트웨이를 사용한다.



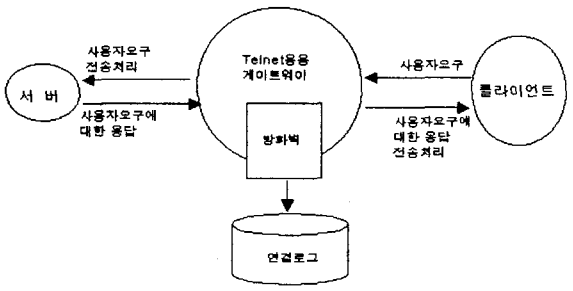
[그림 3] 스크린드 호스트 게이트웨이

다. 응용 게이트웨이 서버

응용 게이트웨이 서버는 방화벽 시스템에서 구동되는 응용 소프트웨어를 말한다. 축척-전달 트래픽뿐만 아니라 대화형의 트래픽을 처리할 수 있으며, 사용자 응용 계층에서 트래픽을 분석할 수 있도록 프로그램 된다. 응용 게이트웨이 서버는 사용자 단계에서 들어오고 나가는 모든 트래픽에 대한 기록을 관리하고 제어할 수 있으며, 해커 및 불법 침입자를 방어하기 위한 일회용 패스워드와 같은 강력한 인증기법이 필요하다. 응용 게이트웨이 서버는 사용되는 응용 서비스에 따라 각각 다른 소프트웨어를 구현하여 사용하기 때문에 높은 수준의 보안을 제공할 수 있다. 새로운 응용이 네트워크에 첨가되고 보호가 필요하다면 이를 위해 새로운 특수 목적용 코드를 생성해야 한다. 응용 게이트웨이 서버를 사용하기 위해서 사용자는 응용 게이트웨이 장치에 로그인하거나 서비스를 이용할 수 있는 특수한 클라이언트 응용 서비스를 가져야 한다. 각 응용에 따라 다르게 사용하는 특수한 게이트웨이 서버는 제각기 내부에 관리도구와 명령 언어를 가지고 있다. 응용 게이트웨이 서버는 그림 4와 같이 실제 서버의 관점에서 볼 때 클라이언트처럼 동작하며, 클라이언트 관점에서 볼 때는 실제 서버처럼 동작한다. 응용 게이트웨이의 구현 예는 Telnet 게이트웨이, FTP게이트웨이, Sendmail, NNTP News Forwarder등이 있으며 그림 5는 Telnet의 응용 게이트웨이 서버를 보여주고 있다.



[그림 4] 응용 게이트웨이 기능

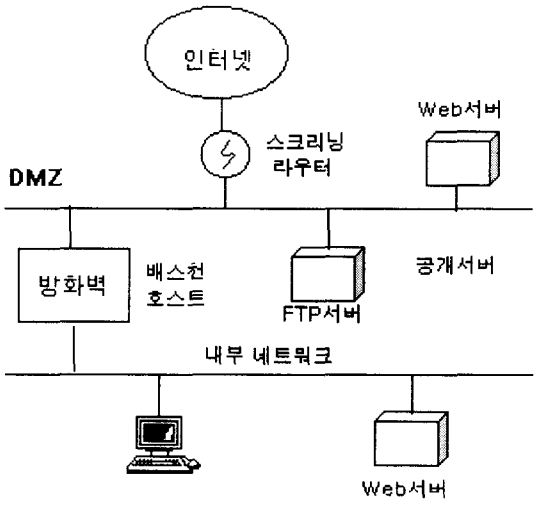


[그림 5] Telnet 응용 게이트웨이

4.3 혼합형 방화벽 설계

스크리닝 라우터의 기능은 네트워크층과 전송층의 트래픽만 방어가 가능하기 때문에 적절한 보안

정책을 수행할 수 없으며 접속기록에 대한 관리기능이 없다. 스크린드 호스트 게이트웨이에서 베스천 호스트가 하나의 네트워크 인터페이스로 구성되었을 때, 스크리닝 라우터의 경로정보에 이상이 발생하면 베스천 호스트의 기능이 우회되는 것을 방지하기 위하여 듀얼-홈드 게이트웨이를 사용한다. 듀얼-홈드 게이트웨이에서 두 개의 네트워크 인터페이스 사이에 트래픽이 직접 전송되지 않기 때문에 응용 게이트웨이 서버 기능을 사용하여 허가된 트래픽만이 전달되도록 하였으며, 또한 모든 접속기록이 베스천 호스트에 누적되도록 한다. 본 논문에서는 그림 6과 같이 스크리닝 라우터, 듀얼-홈드 게이트웨이, 스크린드 호스트 게이웨이, 응용 게이트웨이 서버의 기능을 가진 혼합형 방화벽 시스템으로 설계하였으며, 완충지역인 DMZ에는 내부 또는 외부 사용자가 쉽게 접근할 수 있는 공개서버들을 두었다. 스크리닝 라우터에서는 "명확하게 금지되지 않는 것은 허용한다."라는 방침에 따라 외부로부터 들어오는 프로토콜중에서 TFTP, Xdma, Ntp를 제외한 모든 패킷을 허용하도록 필터규칙을 적용하였으며, 모든 트래픽이 베스천 호스트로 전달되도록 경로를 설정하였다. 혼합형 방화벽 시스템의 모든 트래픽 경로는 스크리닝 라우터와 DMZ, 베스천 호스트를 반드시 거쳐야만 내부 네트워크로 접속이 가능하도록 하였다.



[그림 6] 혼합형 방화벽

Ⅲ. 결론

인터넷을 사용하는 대부분의 기관들이 안고 있는 문제점은 내부 네트워크의 구축 형태에 관계없이 외부 네트워크로부터 투명한 접근을 허용하고 있기 때문에 보안상의 많은 문제점을 내포하고 있는 것이다.

본 논문에서는 네트워크 계층과 전송계층에서 패킷 필터링을 하는 스크리닝 라우터의 단점과 하나의 네트워크 인터페이스로 구축된 스크린드 호스트 게이트웨이의 문제점을 해결해주는 듀얼-홈드 게이트웨이 및 베스천 호스트를 통과하는 응용에 대해 접속기록을 할 수 있는 응용 게이트웨이 서버로 구성된 혼합형 방화벽 모델로 제안하였으며, 외부 네트워크와 내부 네트워크 사이에 DMZ를 두어 모든 사용자가 공개서버를 사용하기 쉽도록 구현하였다.

본 논문에서 제안된 혼합형 방화벽 모델에 대하여 외부 사용자에 대해서는 DMZ에 있는 공개서버들만 사용이 가능하도록 하였으며, 내부 사용자에 대해서는 모든 접속이 가능하도록 하였다. 공개서버의 관리를 위하여 관리자만이 Telnet을 허용하도록 규칙기반을 적용하였다. 실험결과 DMZ에 있는 서버들은 모든 접속을 허용하였고, 내부 네트워크에 있는 서버들은 모든 접속이 거부되었음이 확인되었다. 그러므로, 혼합형 방화벽 모델이 내부 네트워크를 보다 안전하게 보호할 수 있는 것으로 입증되었다.

향후 내부 네트워크를 보다 더 안전하게 보호할 수 있는 새로운 방화벽 모델 및 접속기록에 대한 다양한 분석방법과 감사추적에 관한 연구가 이루어져야 할 것이다.

<참고문헌>

(1) 이선우, "전산망 보호와 방화벽 시스템에 관한 연구", 박사학위 논문, 97.2

(2) 이영웅"가상 다중세그먼트를 지원하는 방화벽의 설계 및 구현", 박사학위 논문, 99.2

(3) Robert S.Macgregor, Alberto Aresi, Andreas Siegert, "WWW.Security", Prentice Hall, 1996

(4) Simson Garfinkel, "Web Security & Commerce, O'Reilly & Associates, Inc., 1997

(5) Aviel D.Rubin, Daniel Geer, Marcus J.Ranum,"Web Secuirty Source Book", John Wiley & Sons Inc., 1997

(6) http://www.kisa.or.kr

(7) http://www.realseminar.co.kr

(8) http://webcomaprc.internet.com/chart.html

(9) http://www.trustedweb.com