방화벽기술과 동향

지도교수 : 권 순 녀
연 구 자 : 강 범 준

< 목 차 >

요 약

방화벽은 보안의 가장 기본이자 중요장비로 매년 기능강화제품으로 다양한 솔루션이 등장하고 있다. 국내외의 다국적 기업들은 공기관 또는 일반인을 대상으로 그 규모는 매년 증가하는 추세이다. 인터넷을 통한 산업이 발전하면서 네트워크의 중요성이 강조되는 만큼 방화벽의 현재 단점과 한계점 들은 넘어서야할 문제이다. 네트워크 환경이 더욱 발전하고 공격자들의 공격의 다양화, 첨단화 되면서 이에 대한 방화벽 기술은 예측 및 방지에 중점을 두고 위협을 원천적으로 차단할 수 있는 전략이 필요하다.

주요어 : 방화벽, 패킷 필터링 시스템, UTM, 차세대 방화벽

1. 서론

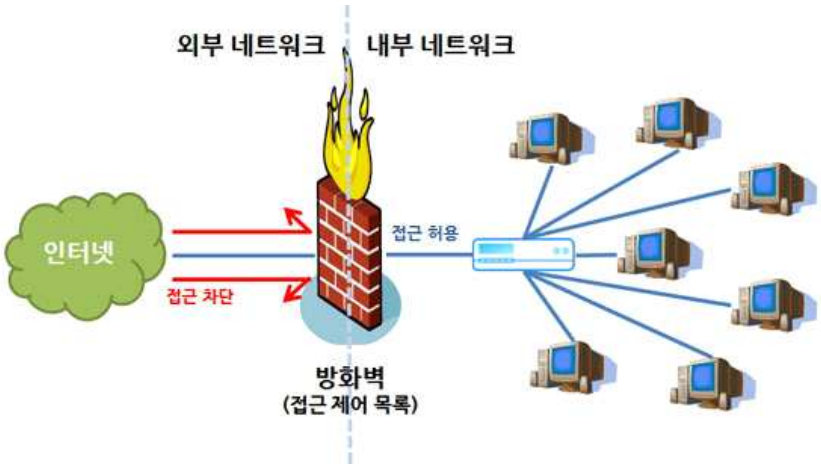
1.1 방화벽

방화벽(영어 : firewall)은 미리 정의된 보안 규칙을 기반으로 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템이다. 방화벽은 일반적으로 신뢰할 수 없는 외부 네트워크간의 장벽을 구성한다. 서로 다른 네트워크를 지나는 데이터를 허용하거나 거부하거나 검열, 수정하는 하드웨어나 소프트웨어 장치이다. 방화벽의 기본역할은 신뢰 수준이 다른 네트워크 구간 사이에서 신뢰 수준이 낮은 네트워크로부터 오는 해로운 트래픽이 신뢰 수준이 높은 네트워크로 오지 못하게 막는다. 흔히 네트워크 관리자의 입장에서 높은 신뢰도의 구간은 내부 네트워크 구간이라고 하고 낮은 신뢰도는 인터넷 구간 또는 외부 네트워크 구간이라고 한다. 대부분의 방화벽은 정책 기반의 방화벽으로 다양한 수준의 정책으로 네트워크 간의 트래픽을 제어한다.

1.2 방화벽 구성

1.2.1 동작원리

기본적으로 네트워크를 통해 들어오는 패킷에 대해 사전에 관리자가 설정해 놓은 보안 규칙에 따라 허용 또는 차단하는 기능을 수행한다. 일반적으로 내부 네트워크와 외부 네트워크 중간에 위치하여 이러한 패킷 제어 기능을 수행한다. 방화벽은 필요에 따라 여러 개를 배치하여 보안성을 강화할 수 있다. 외부 네트워크로부터 방화벽으로 들어오는 모든 접근 시도는 방화벽 내부에 사전 설정된 보안 규칙인 접근 제어 목록에 따라 내부 통과 여부가 결정된다. 기본적으로 방화벽은 모든 접근을 거부한 후 허용한 접근만 단계적으로 허용하는 방식을 따른다. 방화벽의 접근제어 목록 및 설정에는 보안과 관련된 상당한 지식과 함께 경험이 필요하므로 정확하고 체계적으로 이루어져야 한다.



[사진 1]

1.2.2 기능

1) 접근 통제

허용된 서비스와 공개 서버와 같은 특정 호스트를 제외하고는, 외부에서 내부 네트워크에 접속하는 것을 패킷 필터링 등을 이용하여 통제하는 기능이 있다. 패킷 필터링은 내부 네트워크로 들어오는 패킷의 IP주소 혹은 서비스 포트 번호 등을 분석한 후, 외부 또는 내부 네트워크에 대한 접근을 통제하는 기능을 제공한다.

2) 사용자 인증

내/외부 네트워크 사이의 접속점이기 때문에 지나는 트래픽에 대한 사용자들의 신분을 증명하는 기능이 필요하다. 이는 ID/Password나 공개키 인증서를 이용한 사용자에 대한 식별기능과 이를 검증하는 인증 과정으로 이루어진다.

3) 감사 및 로그 기능

모든 트래픽에 대한 접속 정보 및 네트워크 사용에 따른 유용한 통계 정보를 기록하는 감사 및 로그 기능이 있다. 관리자는 사용자의 활동이나 인가되지 않은 외부로부터의 접근이나 침입 사건 등에 대한 로그 파일을 바탕으로 보안 기능과 보안 관련 데이터에 대한 안전한 보안 관리 기능을 제공한다.

4) 프라이버시 보호

내부 네트워크의 정보 유출 방지, 이중 DNS 기능과 프록시 기능 등을 제공함으로써 프라이버시와 관련된 정보의 노출을 막거나 정보를 공격자로부터 보호한다.

5) 서비스 통제

안전하지 못하거나 위험성이 존재하는 서비스를 필터링 함으로써 내부 네트워크의 호스트가 갖고 있는 취약점을 감소 시켜준다.

6) 데이터 암호화

방화벽에서 다른 방화벽까지 전송되는 데이터를 암호화해서 보내는 것으로, 보통 VPN의 기능을 이용한다.

2.방화벽 기술

2.1 유형

네트워크 계층과 전송 계층에서 수행되는 패킷 필터링 시스템과 응용 계층에서 수행되는 응용 게이트웨이 방식으로 구분된다. 패킷 필터링 시스템은 수신된 패킷의 TCP/IP 헤더 부분만 이용하여 침입 차단 기능을 수행하는 수동적인 침입차단시스템이라 할 수 있다. 응용 게이트웨이 방식의 침입차단시스템은 수신된 패킷을 응용 계층의 서비스 단위로 프록시 기능을 이용하여 침입 차단 기능을 수행하는 능동적인 침입 차단시스템이라 할 수 있다.

1) 패킷 필터링 시스템

스크린 라우터 혹은 패킷 필터링 라우터라고 불리는데 발신지 주소와 목적지 주소 그리고 사용하고 있는 세션과 애플리케이션 프로토콜을 기반으로 데이터의 흐름을 통제한다. 패킷 필터링은 내/외부 네트워크 경계 지점에서 패킷을 조사하여 혀용과 차단 여부를 결정하면 되므로 동작 방식이 매우 간단하여 구현하기가 쉽다. 또한 네트워크와 트랜스포트 프로토콜의 헤더 정보를 모니터링 하여 필터링 규칙과 비교하면 되므로 고속으로 처리할 수 있으며 사용자는 필터링 방화벽의 존재를 알지 못하는 상태에서 보안 서비스를 제공받을 수 있다. 하지만 패킷에서 헤더정보 외는 조사하지 않고, 다른 옵션들에 비해 상대적으로 낮은 보안을 제공하고 연결 상태를 추적하지 않는다는 단점도 가지고 있다.

2) 응용 계층 게이트웨이

패킷을 응용프로그램 계층까지 검사한다. 회선 수준 프록시가 세션 계층까지 검사하는 능력을 가지는 반면에 응용프로그램 수준 프록시는 패킷 전체를 이해하고 패킷 내의 내용에 기반을 두어 접근 결정을 내린다. FTP GET 명령어와 FTP PUT 명령어를 구분하며, 세분화된 수준의 정보를 바탕으로 접근 결정을 내린다.

반면에, 패킷 필터링 시스템은 FTP 프로토콜 안에 사용되는 명령어가 아닌 단지 FTP 요청을 전체 허락하거나 거부한다. 응용 계층 게이트웨이는 응용 서비스마다 각각 다른 응용 게이트웨이를 구현하여 보다 안전하게 내부 네트워크의 시스템을 보호할 수 있다. 또한 응용 서비스 사용에 따른 기록 및 감사 추적이 가능하고 강력한 인증 서비스를 제공하며 융통성이 좋다는 장점이 있다. 응용계층 게이트웨이는 단순한 3계층 장비가 아니기 때문에 스푸핑 공격과 다른 정교한 공격에 대응할 수 있다. 패킷 필터링 방식에 비해 상당히 정교한 제어가 가능하다. 그러나 응용 게이트웨이 시스템은 높은 대역폭 혹은 실시간 응용프로그램에 일반적으로 적합하지 않다. 새로운 네트워크 응용프로그램과 프로토콜의 지원에 제한적이다. 응용 서비스별로 별도의 프록시를 필요로 한다는 단점을 가지고 있다.

2.1.1 프록시 방화벽

프록시(proxy)서비스는 호스트에서 실행되는 전문화된 애플리케이션이나 혹은 서버프로그램으로서 침입차단시스템에서 사용되는 베스천 호스트에 설치되어 운영된다. 프록시 서비스는 두 가지의 구성요소, 프록시 서버와 프록시 클라이언트를 필요로 한다.

장점으로는 가능하면 응용프로그램 계층까지 전체적으로 패킷의 정보를 검사하고 패킷 필터링 보다 나은 보안을 제공한다. 보호되는 시스템과 보호되지 않는 시스템 사이의 연결을 차단한다. 다만 몇몇 프록시 방화벽은 제한된 응용프로그램 번호만을 지원하며 트래픽 성능이 저하된다는 단점이 있다. 또한 응용프로그램 기반 프록시 방화벽은 확장성과 성능에 대한 논점을 일으키고 클라이언트/서버 모델을 깨뜨리며 보안을 위에서는 바람직하지만 몇몇의 경우 기능상의 단점이 있다.

2.1.2 스테이트 풀 인스펙션 방화벽

패킷 필터링시스템과 마찬가지로 동일한 패킷 정보를 검토하지만 TCP 연결에 관한 정보를 기록한다. TCP 순서번호를 추적해서 순서번호를 이용한 세션 하이재킹 같은 공격을 막는다. 네트워크와 전송계층에서 동작하며, 장비에 따라 조금씩 다르지만 연결이 시작되면 패킷의 모든 계층(모든 헤더, 페이로드, 트레일러 등)을 조사한다. 각각의 모든 통신 채널을 추적하는 상태 테이블을 관리한다. UDP와 ICMP와 같은 비 연결지향적 프로토콜을 추적하는 데이터를 제공한다. 패킷 안의 데이터 상태와 문맥을 갱신하고 저장한다는 특징을 가지고 있다. 패킷 필터링 방화벽과 동일한 성능을 수행하고 패킷에 대한 보안성을 높일 수 있으며, 네트워크 계층 이하에서 동작하는 Stateful Packet Inspector 모듈을 통해 전체 계층에 대한 상태를 조사할 수 있으며 사용자의 특별한 설정 없이 투명성을 제공한다는 장점이 있다. 그러나 SYN 패킷의 검사를 시작으로 상태 테이블을 유지시키는 방법을 사용하기 때문에 연결 요철의 첫 패킷 헤더가 공격당할 경우 잘못된 상태 테이블을 구성할 수 있는 단점이 있다.

1) 작동원리

가)Stateful Packet Inspector는 데이터 링크 계층에서 SYN 패킷을 전송받으면 접근제어 정책에 의해 상태 테이블에 남겨 접근 허용여부를 결정한다.

나)만약, 접근이 금지된 패킷일 경우 로그를 저장하고 전송을 수행하지 않으며, 접근이 허용된 패킷은 네트워크 계층으로 전송시킨다.

다)SYN 패킷이 아닐 경우 상태 테이블의 패킷정보 여부를 검사하고 존재하면 네트워크 계층으로 패킷을 전송시킨다. 패킷정보가 상태 테이블에 존재하지 않을 경우에는 접근제어 정책에 따라 전송여부를 결정한다.

유형	출발지주소	출발지포트	목적지주소	목적지포트	상태
TCP	192.168.1.10	10001	201.10.120.21	80	established
TCP	192.168.1.11	10002	201.10.120.22	21	established
TCP	192.168.1.11	10050	201.10.120.22	20	established
TCP	192.168.1.12	10051	201.10.120.23	69	established

[표1]

2.1.3 UTM 방화벽

UTM(Unified Threat Management)은 물리적인 하나의 장비에서 여러 보안 기능을 통합적으로 제공하는 네트워크 보안 장비이다. UTM장비를 흔히 네트워크 방화벽이라고 하며, 방화벽, 가상사설망, 침입탐지 및 방지 등의 기능을 포함하고 있다. 각종 보안기능을 통합하여 관리, 설치하기 때문에 비용 절감의 효과가 있다. 진화하는 보안 위협 대응에 적합하고 실시간 긴급 대응 체계가 가능한 장점을 가지고 있다. 하지만 장애발생시 전체에 영향을 끼친다는 단점이 있다.

3. 방화벽 동향

3.1 한계점과 발전방향

이전에는 방화벽이 망 접점에 있으면서도 네트워크 장비에 비해 성능이 크게 떨어진다고 간주되어 성능 향상이 큰 문제점으로 부각되었다. 그러나 현재는 ASIC을 이용한 하드웨어 형태의 장비가 출시됨으로써 성능이 크게 개선되고 네트워크 장비와 비슷한 수준의 트래픽 처리 능력을 갖추게 되어 성능문제는 어느 정도 해결되었다고 볼 수 있다. 최근 등장한 UTM 등의 통합 위협관리 솔루션에는 방화벽뿐만 아니라 IPS, VPN, Anti-Virus 등 다양한 보안기능이 하나의 솔루션에 통합되어 복합 해킹 공격 등을 능동적이고 효과적으로 방어할 수 있다. 아래는 방화벽의 한계점이다.

가) 방화벽은 악성 소프트웨어 침투 방어에 한계가 있다. 방화벽은 패킷의 IP 주소와 포트 번호로 접근 제어를 하는 것이 보통이다. 바이러스, 웜, XSS코드 등과 같이 문서나 프로그램내부에 포함된 악성 소프트웨어를 탐지하여 방어하는데 한계를 가진다.

나) 방화벽은 악의적인 내부 사용자의 공격을 막을 수 없다. 방화벽은 보통 신뢰하지 않는 외부 네트워크로부터 신뢰하는 내부 네트워크를 보호하는 것이 주 목적이다. 따라서 경계에 대한 보안 정책을 수행할 뿐 내부 공격자에게 보안 정책을 적용할 수 없다.

다) 방화벽은 자신을 통과하지 않은 통신에 대한 제어 역시 불가능하다. 만약 내부 사용자가 방화벽을 통과하는 토신 신뢰가 아닌 무선이나 사설 통신 선로를 이용해 통신을 한다면, 공격자는 방화벽을 우회하여 내부 네트워크로 접속할 수 있다. 내부 사용자 역시 방화벽을 우회하여 외부로 허용되지 않은 접속을 시도할 수 있다.

라) 방화벽은 전혀 새로운 형태의 공격을 막을 수 없다. 예측된 접속에 대한 규칙을 세우고 이에 대해서만 방어하기 때문에 새로운 형태의 공격에는 능동적으로 적용할 수 없다. 실제로 많은 해킹 공격이 방화벽을 우회하거나 통과하는데 성공하여 공격이 실행한다. 따라서 방화벽이 보안의 완성이 아니다.

3.2 방화벽 기술 전망

1) 차세대 방화벽

네트워크의 중요성이 강조되면서 방화벽만으로는 보안을 지키기 어려워지고 IPS와 UTM등 다양한 솔루션들이 등장하면서 방화벽 역시 차세대란 용어를 사용하는 기능강화 제품으로 진화했다. 차세대 방화벽의 기능으로는 이전 세대의 UTM방화벽은 IP, PORT를 기반으로 차단하는 정책을 사용했다면 이제는 특정 애플리케이션기반으로도 차단하는 것이 가능하다. 애플리케이션 제어기능은 세부적으로 사용가능한데, 예를 들어 페이스북 페이지까지만 볼 수 있는 정책이나, 사용자의 로그인까지만 허용하는 정책 등 정밀한 제어가 가능하다. 또한 사용자 ID기반 정책으로 세분화된 보안정책을 만드는 것도 가능하다. DLP(Data Loss Prevention)은 내부 정보 유출 방지 기능으로 데이터의 흐름을 감시하여 내부의 정보가 유출되는 것을 차단하는 기능이다.

[사진 2]

2) 웹 방화벽

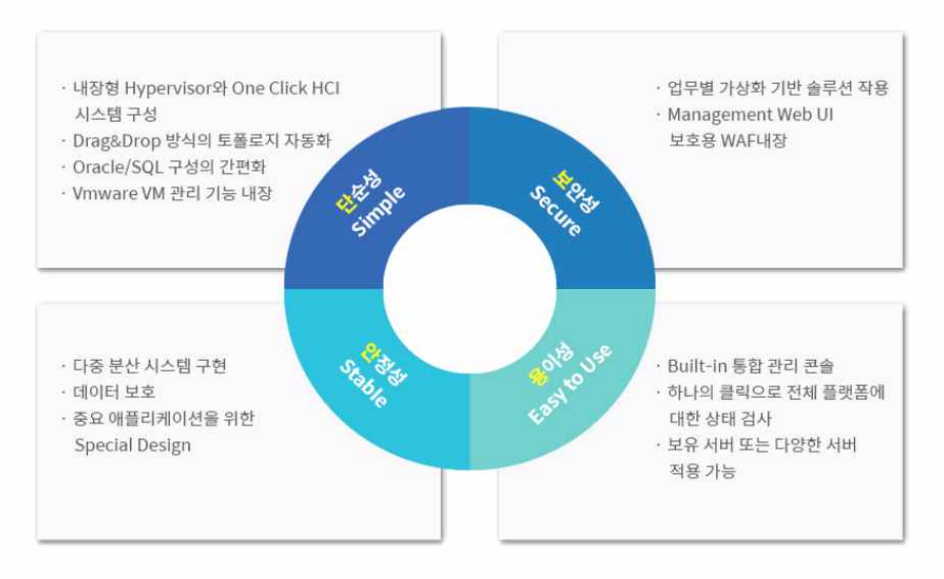
웹페이지 변조나 웹서버 공격은 꾸준히 발생하는 위협이다. 웹을 타깃으로 하는 공격은 일차적으로 웹 방화벽에서 방어해야 한다. 기존의 웹 방화벽은 운영이 까다로워 웹 서버에 설치만 하고 위협 탐지나 차단기능을 활성화하지 않는 경우가 많았다. 하지만 웹을 타깃으로 하는 위협이 많아지면서 위협에 대응할 수 있는 성능과 기능을 갖춘 웹 방화벽을 도입하는 추세이다. 또한, 클라우드 중심으로 변화하는 IT환경에서 웹 보안의 중요성을 빼놓을 수 없다. 다양한 기업에서는 클라우드를 지원하는 웹 보안 솔루션을 제공하고 있다. 웹 트래픽은 대부분 암호화 된다. 약 80% 이상 웹 트래픽이 암호화 돼있으며 대부분의 트래픽인 복호화해 분석하지 않는다. 암호화 트래픽에 악성코드가 있거나 중요정보가 유출된다 해도 보안 솔루션은 걸러내지 못한다.

암호화 트래픽을 분석하는 솔루션도 있지만 고성능 장비로 비용이 많이 들며, 모든 장비마다 암호화 트래픽을 복호화 해 분석하고 다시 암호화하는 과정에서 리소스 낭비가 심해진다. 이와 같은 문제해결을 위해 네트워크 게이트에서 암호화 트래픽을 복호화 후 네트워크/보안 장비로 보내 분석하고, 분석 완료된 트래픽만 유입시키는 SSL 가시성 솔루션을 도입해야한다. SSL 솔루션은 암호화 트래픽을 복호화 하는 단순한 기능을 제공하는 것 같지만, 실제로는 다양한 인증서와 복잡한 예외처리, 국내 보안 솔루션 연동 등의 현실적인 문제도 해결해야한다.

3) 가상화 방화벽

단순히 방화벽을 가상화 하는 것이 아니라 서버, 네트워크, 스토리지 등의 인프라를 가상화 하여 관리하는 솔루션이다. 다중분산기술을 적용하여 데이터 안전성을 확보하고 네트워크 운영 환경을 고려한 유연한 자원 할당 및 자동화 기능을 지원한다. 서버 및 네트워크 구성과 보안 구축을 패키지 형태로 도입이 용이하며, 원 클릭으로 전체 플랫폼 상태를 검사할 수 있다.

또한, 가상 서버의 경우 Darg&Drop방식을 통해 즉각적으로 가상머신을 생성해 하드웨어 성능에 따라 무제한 생성이 가능하다. 물리적 서버 수량 감소에 따른 스위치 구성 간소화로 솔루션 도입 비용이 적게 들이고 필요한 공간 및 전력역시 줄어 운영비용 절감의 효과가 있다. 최근 VM없이 완전히 분리되어 운영되는 가상 방화벽 기술 발전으로 네트워크 유연성을 높이고 시스템 운영비용 절감에 효과적이다.



[사진 3]

4. 결론

꾸준히 발전하는 IT업계에서 보안의 기본인 방화벽 기술은 그 영향력이 점차 커지고 있다. 많은 기업들이 다양한 방화벽 보안 솔루션을 제공하면서 사용자들은 자신의 환경에 맞는 솔루션을 선택하고 있다. 하지만 국내 기술수준을 좀 더 고도화 할 필요가 있다.

국내 시장 활성화 보다는 글로벌 시장과 비교해 핵심기술 개발이 필요하다. 인터넷 침해 사고 위협 및 발생률이 늘어나는 만큼 기술 개발에 주력할 필요가 있다. 신종 공격 위험에 대한 침입 경로를 인식하고 변화를 수용할 수 있어야 한다.

향후 방화벽 시스템은 차단 기술보다는 예측 및 방지에 중점을 둔 각종 사이버범죄의 위협을 원천적으로 차단할 수 있는 개발전략이 필요하다.

참고문헌

1) https://it.donga.com/8810/
그림 1 방화벽 동작원리
2) 정보보안기사&산업기사 이론편 453-464p 방화벽
3) https://www.secui.com/product/virtualmax
가상화 & 보안 솔루션
4) http://www.cctvnews.co.kr/news/articleView.html?idxno=37738
그림 2 방화벽 시스템 기술 동향 및 기술 개발방안
5) https://www.pentasecurity.co.kr/
그림 3 차세대방화벽