2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

네트워크 트래픽 상태 기반의 방화벽 시스템[1]

송병욱*, 김홍철, 박인성, 김상욱
e-mail:bwsong@woorisol.knu.ac.kr

Firewall System based on Network Traffic State

Byung-Wook Song*, Hong-Chul Kim, In-Sung Park, Sang-Wook Kim

요약

본 논문에서는 트래픽 상태를 기반으로 네트워크 패킷의 상호관계에 따라 트래픽을 제어하는 방화벽 모델을 제시한다. 기존의 방화벽은 단순한 필터링 메커니즘과 보안 정책으로 복잡하고 다양해진 네트워크 트래픽 패턴에 효과적으로 대응할 수 없었다. 그러나, 본 논문에서는 네트워크 트래픽의 정보를 정적인 상태 정보와 동적인 상태 정보로 구분하여 수집하고 이러한 정보를 보안 정책에 의하여 생성된 상태 그래프의 의사 결정에 반영함으로서 트래픽의 미세한 변화에도 효과적이고 다양한 대응을 할 수 있도록 하였다. 그리고, 트래픽 분석기, 네트워크 에이전트, 관리자 인터페이스로 구분함으로서 관리자 인터페이스의 형태와 위치의 독립성을 높임으로서 보다 효과적인 사용환경을 제공하도록 하였다.

1. 서론

네트워크 기술의 발전과 초고속 통신망의 비약적인 보급에 따라 인터넷의 사용이 대중화되고 상호 정보의 교류도 증가하고 있다. 그리고, 홈 네트워크 표준화와 함께 블루투스, 하비, 지니와 같은 홈 네트워크 기반 기술 및 응용 기술이 완성 단계에 이르게 되면서 네트워크를 통한 정보의 교류는 정부와 기업 등과 같은 기존의 사용자뿐 아니라 가정과 개인에 의해서도 활발하게 이루어지게 되었다. 그러나, 그에 따른 네트워크 침입과 정보 노출의 위험도 비례적으로 증가하게됨에 따라 방화벽, 침입탐지시스템과 같은 여러 가지 보안 솔루션들이 등장하게 되었다.

방화벽은 설정된 보안 정책에 근거하여 네트워크 트래픽을 감시하고 제어하면서 내부로 유입되는 부적절한 패킷을 제한함으로서 내부 네트워크의 호스트들을 보호하고, 네트워크 전반의 정보를 수집하여 관리함으로서 보다 효율적인 네트워크 관리를 위한 시스템이다. 그러나, 네트워크 트래픽의 형태가 복잡하고 다양해지면서 기존의 방화벽 메커니즘과 보안 정책의 형식은 한계에 이르게 되었다.

이에 본 고에서는 기존 방화벽 메커니즘의 문제점을 살펴보고, 상태 그래프를 기반으로 다양한 계층의 네트워크 정보를 수집하여 트래픽의 상호 관계를 고려하여 제어하는 방화벽 모델을 제시한다.

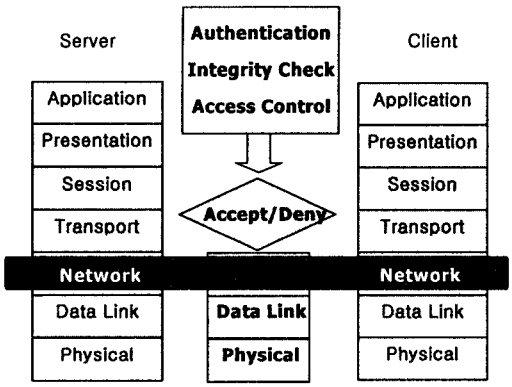
2. 기존 방화벽의 문제점

방화벽은 자료수집의 범위와 네트워크 트래픽 제어의 형태에 따라 크게 세 가지로 구분된다. IP 계층의 네트워크 패킷을 기반으로 주소와 프로토콜에 의한 단순 필터링 방식의 1세대 방화벽과 네트워크, 트랜스포트, 애플리케이션 등의 모든 계층을 대상으로 정보를 수집하고 다른 패킷과의 관계를 고려한 패킷 필터링 방식의 2세대 방화벽, 그리고 상태 기반의 필터링 방식인 3세대 방화벽이 그것이다.

1세대 방화벽은 필터링의 범위가 좁고 통제 방식이 간단하기 때문에 처리 속도가 빠르고 다른 서버 프로그램에도 영향을 주지 않아 대규모 네트워크에도 쉽게 적용할 수 있다. 그러나, 네트워크 트래픽의 패

1. 본 연구는 정보통신연구진흥원이 지원하는 이동네트워크 정보보호기술개발 연구의 일부분임

턴이 복잡해지고 네트워크 침입의 수준이 높아짐에 따라 빈약한 네트워크 정보와 단순한 보안 정책으로는 효과적인 트래픽 제어가 어려워졌다.



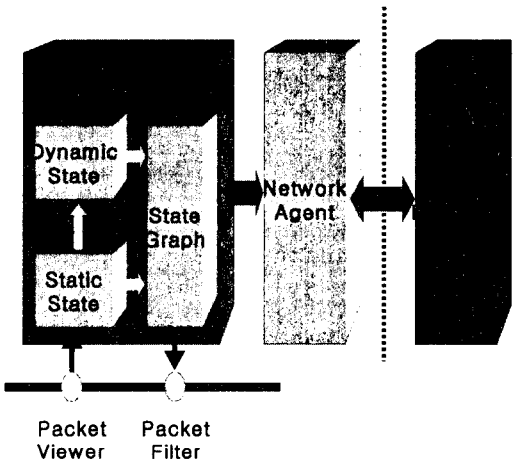
<그림 1> 일반적 방화벽 구조

2세대 방화벽은 수집하는 정보의 범위에 트랜스포트 계층과 애플리케이션 계층을 포함시키고, 패킷의 헤더 필드 뿐 아니라 실제 자료를 저장하고 있는 바디 필드까지 넓혀 광범위하고 입체적인 분석이 가능하다. 그러나, 패킷의 조사와 분석에 따르는 오버헤드가 너무 커 실제 방화벽으로서의 수행 효율이 낮고, 대규모 네트워크에도 적용하기 어렵다. 또, 모든 계층을 통제함에 따라 다른 서버 데몬의 수행에도 지장을 주게 되었고, 단순한 보안 정책 역시 패킷의 상호 관계를 파악하고 적용하기에는 무리가 따른다.

이와 같이 1세대와 2세대 방화벽은 적용되는 보안 정책과 필터링 룰이 네트워크 주소 또는 포트 번호와 같은 기본 패킷 정보의 조합과 허용과 거부만으로 나누어지는 단순한 통제 방식으로 구성되어 있기 때문에 네트워크 트래픽의 미세한 변화를 감지하여 다양하고 능동적인 통제 방식을 활용하한 효과적인 대응이 어렵다. 또, 네트워크 패킷간의 상관관계와 시간에 따른 변화로 이루어지는 네트워크 트래픽의 흐름을 읽어내지 못하기 때문에 복잡한 네트워크 트래픽의 유형을 감지하지 못한다.

3. 전체 시스템 구성

본 고에서 제시하는 모델은 <그림 2>와 같이 크게 네 부분으로 구성되어 있다. 트래픽 분석기는 수집되는 네트워크 트래픽 정보를 분석하고 관리자가 요구하는 정책에 의하여 네트워크 트래픽을 제어한다. 네트워크 에이전트는 트래픽 분석기와 관리자 인터페이스 사이의 통신을 전담한다. 관리자 인터페이스는 관리자에게 네트워크 트래픽의 상황과 통계적으로 가공된 정보를 여러 가지 관점에서 보여주며, 관리자가 의도하는 보안 정책을 트래픽 분석기에게 전달한다. 네트워크 트래픽 수집기와 제어기는 실제 게이트웨이를 통과하는 패킷을 읽어들이고, 설정된 규칙에 따른 필터링 작업을 한다.



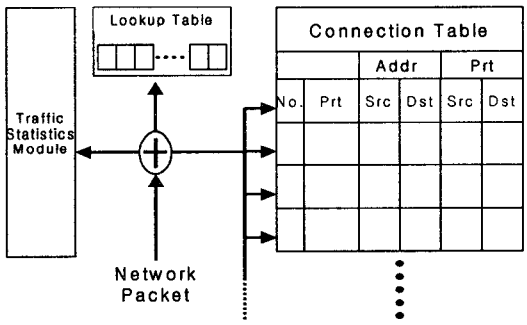
<그림 2> 트래픽 상태 기반 방화벽의 전체적인 구조

3.1 트래픽 분석기

트래픽 분석기는 수집된 네트워크 정보를 여러 가지 관점에서 분석하고, 관리자에 의하여 설정된 보안 정책과 필터링 규칙을 적용하여 트래픽의 흐름을 제어하는 모듈이다. <그림 2>에서 보는 바와 같이 트래픽 분석기는 크게 정적 상태 정보 수집기, 동적 상태 정보 수집, 상태 그래프로 나누어진다.

정적 상태 정보 수집기는 패킷 뷰어에 의하여 수집되는 네트워크 정보를 <그림 3>과 같이 커넥션 단위로 분류하여 관리한다. 커넥션은 TCP와 UDP 패킷으로 구성되는데, 커넥션에 등록되면 별도의 커넥션 정보 필드가 구성되고, 커넥션이 유지되는 동안 수집되는 패킷에 의하여 계속적인 정보의 갱신이 이루어지는데, 커넥션을 유지하는데 있어서 패킷의 역할에 따라 조사되는 정도가 달라지게 된다. 커넥션을 생성하거나 종료하는 패킷, 또는 윈도우 사이즈의 변경이나 라우팅 경로의 재설정 같은 커넥션 자체의 정보 변경을 위한 패킷의 경우 모든 필드의 정

보가 세밀하게 검토되며 조사된 결과에 따라 커넥션 정보를 갱신하게 되며, 커넥션 자체의 정보에는 영향이 없는 일반적인 데이터 패킷일 경우 기본적인 정보만을 얻게 된다. 그리고, 커넥션을 생성할 수 없는 ICMP와 IGMP 패킷은 수집되는 즉시 바로 처리된다. 트래픽 통계 모듈에서는 패킷이 커넥션에 미치는 영향력에 상관없이 전체적인 네트워크 트래픽이 형성하는 시간적 흐름에 따른 최대 트래픽량, 최소 트래픽량, 평균 트래픽량과 같은 통계적 정보를 수집하여 상태 그래프의 의사 결정에 기초적인 정보를 제공한다. 이러한 정보는 관리자의 실시간 네트워크 상태와 전체적인 네트워크의 흐름에 대한 이해를 위해 관리자 인터페이스에게도 제공된다.



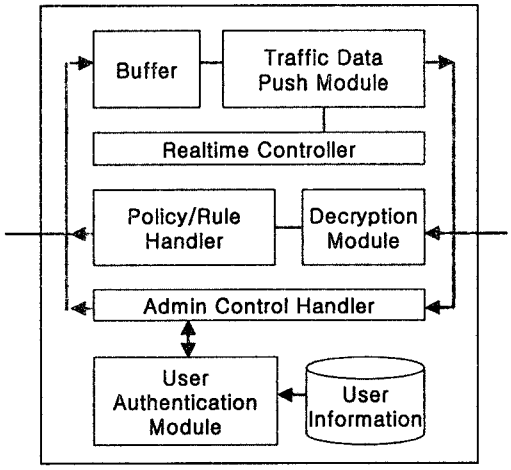
<그림 3> 정적 상태 수집기의 구조

동적 상태 정보 수집기는 네트워크 트래픽의 전체적인 흐름을 파악하기 위한 정보를 수집하는 모듈이다. 여기에서는 외부 및 내부 호스트의 네트워크 주소와 포트, 프로토콜, 커넥션의 종류에 따른 네트워크 정보를 수집하고, 네트워크 트래픽의 패턴이 따른 기존의 의사 결정 형태와 결과를 기록한다. 이러한 정보는 상태 그래프의 결과에 따른 트래픽 제어의 형태 결정에 참조된다.

상태 그래프는 보안 정책에 의하여 구성되며, 각 노드는 정적 상태 정보와 동적 상태 정보를 참조하여 보안 정책에서 결정된 임계치와 비교하여 상태 전이 또는 트래픽의 직접 제어가 이루어지게 된다. 보안 정책은 필터링 규칙에 의하여 이루어지는 정적 트래픽 제어와 상태 전이에 의하여 결정되는 동적 트래픽 제어로 구분된다. 트래픽 제어는 노드의 조건에 따라 결정되며, 허용, 거부, 반환, 기록, 보류 등으로 구분된다.

3.2 네트워크 에이전트

네트워크 에이전트는 트래픽 분석기의 외부 입출력의 담당하는 모듈이다. 이것은 독립된 데몬의 형태로 트래픽 분석기와 관리자 인터페이스를 분리하는 역할을 함으로서 관리자 인터페이스의 위치와 형태에 독립성을 부여하게 된다. 그리고, 트래픽 분석기에 접근하는 관리자 접속 요청에 대한 인증 단계를 담당하게 된다.



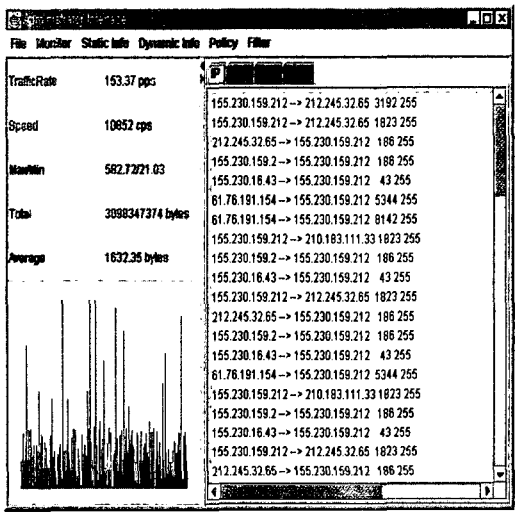
<그림 4> 네트워크 에이전트의 구조

네트워크 에이전트는 <그림 4>와 같이 크게 세 가지의 모듈로 나누어진다. 트래픽 데이터 푸시 모듈은 트래픽 분석기에서 수집된 네트워크 트래픽 정보를 실시간으로 사용자 관리기로 전달한다. 정책/규칙 핸들러는 관리자의 의하여 설정된 보안 정책 또는 필터링 규칙을 트래픽 분석기에 전달하게 되는데, 이러한 것들은 높은 보안성이 요구되므로 네트워크로 전송되기 전에 암호화되며, 다시 복호화 모듈에 의하여 복원된다. 관리자 제어 핸들러는 관리자의 요구 또는 의사를 전달하기 위한 것으로, 관리자의 권한에 따른 제한적 허용을 위한 인증 절차를 거치게 된다.

3.3 관리자 인터페이스

관리자 인터페이스는 트래픽 분석기를 직접적으로 제어하고 트래픽 제어에 필요한 보안 정책과 필터링 규칙을 설정하기 위한 도구이다. 주요 기능으로는

네트워크 트래픽의 실질적으로 파악하기 위한 실시간 모니터링, 트래픽 제어기에서 제공되는 네트워크 주소, 프로토콜, 트래픽의 종류에 따른 통계 자료의 시각적 표현, 현재 적용되고 있는 보안 정책과 필터링 규칙의 표시 및 설정, 내부 네트워크의 트래픽 상황 표시 등이 있다.



<그림 5> 관리자 인터페이스

관리자 인터페이스는 트래픽 분석기와 분리되어 원격에서 접속하여 제어함으로서 위치와 형태의 다양함을 얻을 수 있다. 때문에 관리자에게 기본적으로 제공되는 독립된 애플리케이션 외에 웹에서의 접근을 가능하게 함으로서 관리상의 편의를 제공한다.

3.4 네트워크 정보 수집 및 트래픽 제어

트래픽 분석기에 제공되는 실제적인 네트워크 정보를 수집하고 제어하기 위한 모듈로서, 네트워크 정보 수집은 libpcap을 사용하며, 트래픽 제어를 위한 패킷 필터링은 ip-chain을 사용하게 된다. 본 모듈은 트래픽 분석기와 독립적인 모듈로 존재하므로서 트래픽 분석기에 제공하고 네트워크 정보의 수집 경로와 트래픽 제어의 다양성을 높이고, 본 방화벽 시스템이 적용되는 운영체제의 폭을 넓힌다.

4. 결론

본 논문은 네트워크 트래픽의 상태를 일반적인 네트워크 정보를 통계적 방법으로 가공한 정적 상태와 네트워크 전체의 흐름을 파악할 수 있도록 네트워크 트래픽의 변화를 시간적 흐름과 연계한 동적 상태로 구분하여 수집하여 네트워크 정보의 다양성과 정확성을 높였다. 그리고, 이러한 정보를 상태 그래프의 의사 결정의 정보로 활용함으로서 복잡하고 다양해진 네트워크 트래픽의 패턴에 대하여 보다 효과적인 대응을 가능하게 했다.

또, 네트워크 에이전트를 트래픽 분석기를 분리함으로서 트래픽 분석기의 수행 효율을 높이고 관리자 인터페이스의 형태와 위치가 다양화되어 자체 제작된 애플리케이션뿐 아니라 인터넷을 이용한 관리가 가능하게 되어 보다 효율적인 사용 환경을 제공할 수 있게 되었다. 뿐만 아니라, 네트워크 패킷 수집기와 제어기를 독립된 모듈 형태로 구성함으로서 방화벽을 적용할 수 있는 시스템의 범위를 넓히고, 유지보수의 효율성도 높였다.

향후 과제로는 네트워크 트래픽 상태에 대한 정보를 다변화하고, 패킷 수집기와 커넥션 관리 모듈의 수행 효율을 높임으로서 보다 원활한 트래픽 제어가 가능하도록 하는 것과 보안 정책을 기술하는 형식의 구조화를 통하여 정책 설정의 다양함과 적용의 정확성을 높이는 것이다.

5. 참고문헌

[1] W. Richard Stevens, Unix Network Programming Networking APIs : Sockets and XTI, Prentice Hall, 1998

[2] W. Richard Stevens, Unix Network Programming Interprocess Communications, Prentice Hall, 1999

[3] D. Brent Chapman and Elizabeth D. Zwichy, Building Internet Firewalls, O'reilly, 1998

[4] Chris Brenton, Mastering Network Security, Sybex, 1999

[5] Michael Beck, Harald Bohme, Mirko Dziadzka, Ulrich Kunitz, Robert Magnus, Dirk Verworner, Linux Kernel Internals, Addison-Wesley, 1998

[6] W. Richard Stenvens, TCP/IP Illustrated Volume 1 The Protocols, Addison-Wesley, 1994

[7] http://firewall.com

[8] http://lists.gnac.net/firewalls/ : Firewalls Mailing List