DPI 기술 분석

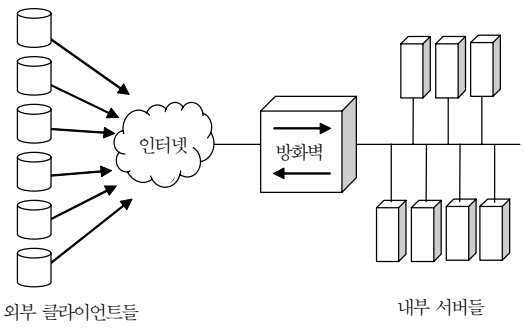
Analysis of Deep Packet Inspection Technology

신승원(S.W. Shin) 보안게이트웨이연구팀 연구원
강동호(D.H. Kang) 보안게이트웨이연구팀 연구원
김기영(K.Y. Kim) 보안게이트웨이연구팀 선임연구원
장종수(J.S. Jang) 네트워크보안연구그룹 책임연구원, 그룹장

과거의 패킷 필터를 기반으로 하는 단순한 방화벽은 더 이상 지능적인 해커들을 방어할 수 없다. 가트너에 따르면 현재의 방화벽의 기술은 패킷 필터에서 Application Proxy, Stateful Inspection을 거쳐 DPI로 진화하고 있다고 한다. NIDS나 NIPS를 떠오르게 하는 DPI 방식은 차세대 방화벽의 기술로 인정 받고 많은 연구와 개발이 진행되고 있으며, 실제 제품으로도 선보이고 있다. 본 논문에서는 DPI 기술의 정의와 알고리듬, 그리고 발전 방향에 대해서 알아볼 것이다.

I. 서 론

네트워크 보안을 위한 가장 기본적인 시스템은 방화벽(firewall)이다. 방화벽은 (그림 1)과 같은 형태로 구축되는데, 이와 같은 위치에서 방화벽은 자신이 보호하는 서버 그룹들로 전달되는 네트워크 패킷(packet)을 검사하여 패킷을 전달할지 여부를 결정하게 된다. 방화벽과 유사한 기능을 수행할 수 있는 NIPS(Network Intrusion Prevention System)가 등장하긴 했지만, 아직은 보조적인 역할을 수행하는 NIDS(Network Intrusion Detection System)에 대한 인식이 더 깊기 때문에 네트워크 보안에서 방화벽의 주도적인 역할은 아직 그 힘의 여지가 남아 있다. 그러나, NIPS와 같은 새로운 개념의 기술과 제품이 등장하면서 경쟁을 이루게 되면서 방화벽 역시 기존의 기술에서 많은 발전을 이루게 되었다. 본 원고에서는 이러한 발전 중에서 차세대 방화벽의 필수적인 요소로 평가 받고 있는 DPI(Deep Packet Inspection)에 대해서 알아볼 것이다.



(그림 1) 방화벽의 구성

II. 방화벽 개요

방화벽은 네트워크 보안을 위한 가장 기본적인 시스템이다. 방화벽은 (그림 1)과 같이 외부 네트워크와 내부 네트워크 사이에 위치하여 내부 네트워크와 서버들을 보호하는 역할을 하게 된다. 가트너는 기존의 방화벽을 다음의 세 가지로 분류하였다[1].

• Access Control List

방화벽의 초기 형태이며, 보통 라우터나 게이트웨이와 같은 형태로 구현되고, 5-tuple 정보들(Src/Dst IP Address, Src/Dst Port, Protocol)을 이용하여 관리자가 지정한 규칙을 기반으로 하여 네트워크 침입을 판단하는 시스템이다. 즉, 5-tuple 정보들을 검사하는 방식이다. 예를 들어, 이러한 시

스템의 경우, 보통 80포트(port)로 접속하는 HTTP 메시지나 110포트로 접속하는 POP 메시지는 내부 사용자들이 이용할 수 있게 하기 위하여 허용하고, 그 외의 포트들은 잘못된 접속이거나, 침입으로 간주하고 차단하는 방법 등을 이용한다.

• Application Proxy

각 업체들간의 정의에 논란이 있지만, 가트너에서는 이 시스템을 외부 네트워크와 서버 그룹들 사이에 위치한 소프트웨어 기반의 응용 프로그램으로 정의하고 있다. 즉, application proxy 시스템은 애플리케이션 계층의 정보를 바탕으로 침입 여부를 판단하는 것이다. 예를 들어, 웹 서버를 보호하기 위한 application proxy가 있다면, 이 시스템은 마치 자신이 HTTP를 이해하는 웹 서버처럼 행동하면서, 외부 사용자의 요구를 웹 서버 대신 자신이 받아들여서 침입 여부를 판단하게 된다. 이 경우 관리자는 웹 서버에 대한 침입을 막기 위하여 다양한 차단 규칙을 만들어 낼 수 있다. 특히 가트너의 정의처럼 소프트웨어를 기반으로 한 시스템의 경우 다양한 규칙을 만들어 낼 수 있다.

• Stateful Inspection

라우터나 게이트웨이로 구현된 방화벽의 발전된 형태라고 할 수 있다. 처음 Checkpoint[2] 연구소에서 사용한 용어로, 현재는 대부분의 방화벽 업체에서 이 기술을 이용할 정도로 많이 이용되고 있다. 기본 방식은 access control list 방식과 유사하나, 결정을 패킷 하나 단위가 아닌 세션(session) 단위로 한다는 점에 차이가 있다. 예를 들어, 특정 외부 클라이언트가 방화벽이 보호하는 내부 서버로 접속하는 경우, stateful inspection을 지원하는 방화벽의 경우, 연결을 맺은 후 종료할 때까지의 세션 정보를 바탕으로 침입 여부를 판단하는 것이다.

가트너의 위와 같은 분류에 모든 방화벽들이 들어 맞는 것은 아니지만, 대부분의 방화벽에서 채용하고 있는 기술들은 위와 같은 것 중에서 하나를 지원하고 있다. (물론, 특정 방화벽들은 두 개 이상의 것들을 지원하는 경우도 있다.)

그러나, 이런 일련의 기술들만으로는 완전한 보안을 이루기가 쉽지 않다. 더욱이 간단한 메시지만을 전송하던 네트워크 환경이 점차 복잡하고 다양한 메시지 체계를 이루게 되면서 이러한 요구는 점점 늘어나게 되었다. 특히 웹 서비스(web service)로 발전되어 가는 웹 환경은 5-tuple 정보들만으로 상당한 정보를 얻을 수 있었던 과거의 환경을 벗어나 패킷 내부의 콘텐츠를 파악하여야 메시지 전달 체계를 이해할 수 있는 환경에까지 이르렀다. 대표적인 예로 XML 문서를 기반으로 하는 SOAP(Simple Object Access Protocol)과 같은 경우 5-tuple 정보들은 단순한 메시지 전달을 위한 것일 뿐 실제 그 패킷이 서버로 전달되어 행하여지는 행동은 내부 XML 콘텐츠에 포함되어 있다. 이러한 경우, 위에서 언급한 기존의 방화벽 기술들만으로는 해커 등이 XML 콘텐츠를 이용한 침입을 시도하였을 때, 이를 제대로 탐지해내어 제거하기가 쉽지 않다. 따라서, 기존의 방화벽을 발전시켜 왔던 학계와 연구소, 업체들은 이를 개선하기 위하여 DPI라는 기술을 개발하였다.

이어지는 III장에서는 DPI 기술에 대한 개요와 개념 그리고 기존 기술들과의 차이를 설명하고, IV장에서는 DPI를 실제 적용한 제품 및 연구 동향에 대해서 알아볼 것이다.

III. DPI 기술 개요

1. DPI란 무엇인가?

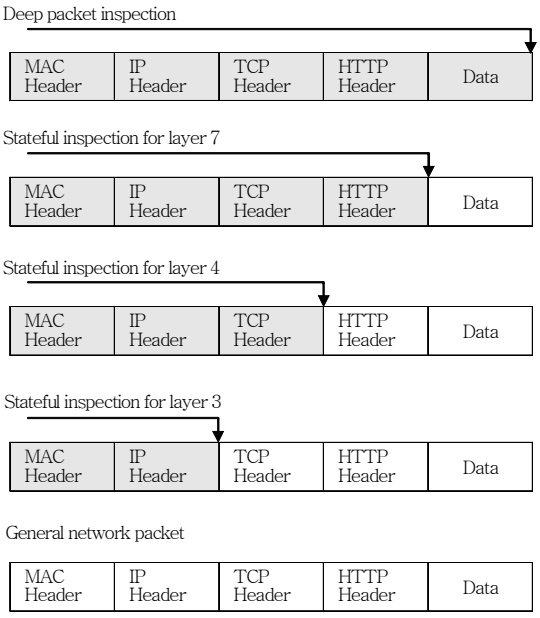
DPI 기술은 기본적으로 패킷 내부의 콘텐츠까지 파악한다는 것에 그 의미를 두고 있다. 동시에 클라이언트 서버 간의 패킷 통신의 규약에 대한 정보까지 파악하여 규약대로 통신이 이루어지고 있는지, 아니면 비정상적인 통신 형태가 이루어지고 있는지 파악할 수 있다. 먼저 DPI의 동작과 개념에 대해서 알아보자. DPI를 보면 방화벽이나 NIDS에서 정의하는 stateful inspection과 상당히 많은 유사성을 찾을 수 있다. (사실, 상당수의 회사에서 이 두 가지 개념을 혼동하여 사용하고 있으며, 구분한다 하더라

도 그 차이가 각양각색이다.) 그러나, 가트너에서 정의한 개념을 바탕으로 DPI를 정의해 본다면 stateful inspection과의 차이를 볼 수 있을 것이다.

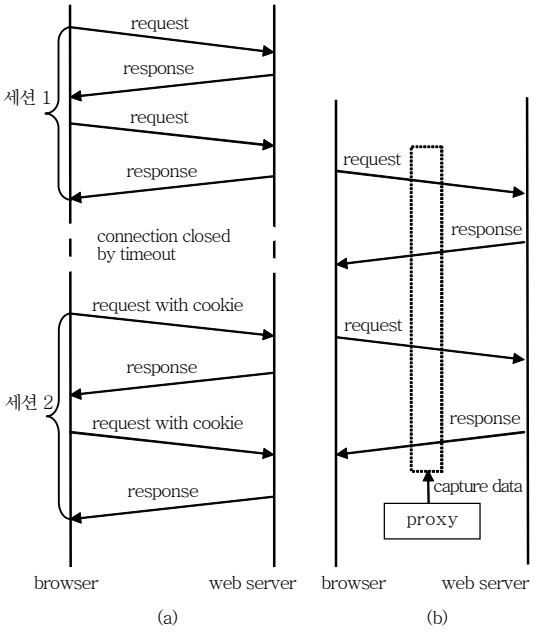
가트너에서는 DPI를 네트워크 전체에 대한 검사로 정의하고 있다. 또한, 순수하게 패킷 자체뿐만 아니라, 패킷을 주고 받는 애플리케이션 프로그램들의 동작에도 그 의미를 두고 있다. 그러나 이에 비해서 stateful inspection은 각 계층 상에서의 프로토콜의 세션을 유지하고 이에 대한 정보를 바탕으로 하여, 이를 분석하는 것을 의미한다. 만약, 4계층까지 지원하는 stateful inspection 기능이 있다면 이는, TCP 세션에 대한 정보를 유지하여 이를 바탕으로 네트워크 패킷의 이상 유무를 판별하는 것이다. 그러나, DPI는 네트워크 전체 계층에 대한 것 뿐만 아니라 패킷의 콘텐츠까지 검사하는 기능을 가지게 된다. (그림 2)를 보면 stateful inspection과 DPI의 적용 범위의 차이를 알 수 있을 것이다.

DPI는 동시에 단순한 패킷의 전달뿐만 아니라 그 동작에도 의미를 부여하게 된다. (그림 3)을 통해서 그 의미를 알아본다면 다음과 같다. (그림 3)의 (a)는 웹 브라우저와 웹 서버간의 연결을 의미한다. 이 때, 브라우저는 웹 서버에 연결을 맺고 웹 페이지를 전송 받은 다음 (세션 1 상태), 시간이 지나서 웹 서버에 의해서 연결이 끊어진 상태이다. 이 때, 웹 브라우저가 다시 쿠키(cookie)를 이용해서 웹 서버에 요청을 보내면 (세션 2 상태) 이는 웹 서버상에서는 같은 세션을 의미하게 된다. DPI의 경우에서는 HTTP 프로토콜의 내용을 파악해서 세션 1과 세션 2 모두 하나의 세션으로 처리하게 된다. 즉, HTTP 프로토콜 상에서의 세션의 의미를 가지는 것이다. 그러나, stateful inspection만을 지원하는 방화벽의 경우 이를 세션 1과 세션 2의 각각의 다른 세션으로 처리할 것이다. 따라서, 쿠키를 이용하여 공격을 시도하는 침입이 발생한 경우, 기존의 stateful inspection의 기술로는 그 침입을 탐지해 내기가 쉽지 않다. 그러나, DPI 기술을 이용하는 경우, 각각의 정보를 모두 분석하므로 침입을 탐지할 확률이 상대적으로 높다. 또한, (그림 3) (b)와 같이 브라우저와 웹 서버의 중간 단에 위치하여 서로 주고 받는 HTTP 프로토콜 계층의 내용을 파악 할 수 있기 때문에, application proxy가 할 수 있는 분석까지 가능하게 된다.

결국 DPI 기술을 채용한 방화벽 장비는 OSI-7



(그림 2) Stateful Inspection과 DPI의 비교



(그림 3) DPI의 세션 관리

계층 상의 모든 프로토콜에 대한 것을 그 동작의 의미까지 부여하여 검사를 하게 된다. 또한, 기존의 application proxy 상에서 존재하는 방화벽과 달리 (그림 4)처럼 DPI 기술을 채용한 방화벽은 각각의 프로토콜에 대해서 필요한 검사를 사용자의 지정에 따라서 다르게 할 수 있다.

이와 같이 DPI 기술은 애플리케이션 계층의 콘텐츠 및 프로토콜에 대한 정보를 바탕으로 좀 더 깊은 분석을 할 수 있다. DPI의 이러한 특성은 현재 네트워크 보안에서 많은 문제가 되고 있는 IDS Evasion[8] 방법을 이용한 침입 역시 탐지해 낼 수 있다. NIDS Evasion 방법은 IP 프로토콜 및 TCP 프로토콜의 내부적인 특성을 이용하고 있는데, 특히 IP 프로토콜의 fragmentation 기능과 TCP 프로토콜의 reassembly 기능을 악용하고 있다.

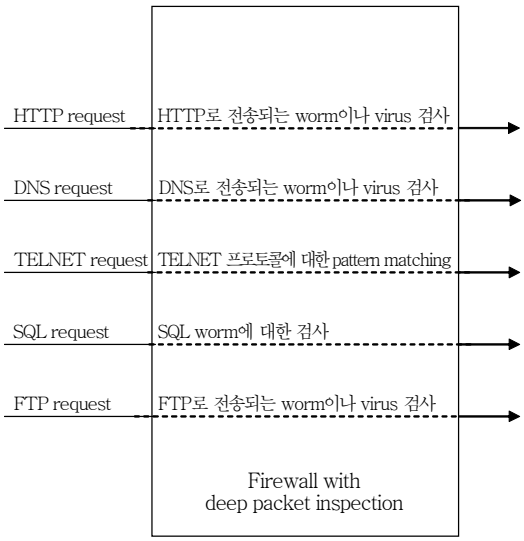
예를 들어, 어떤 네트워크 공격을 시도하는 사람이 어떤 웹 서버를 공격하여 모든 하드 디스크의 내용을 지우려 한다고 가정해 보자. 그리고, 침입을 시도하려고 하는 시스템이 windows NT 서버 하에서 구동되고 있는 IIS 웹 서버라고 한다면, 침입자는

GET/Catalog/Items/../../../../WINNT/SYSTEM32/CMD.EXE?/C+ format+ C:₩

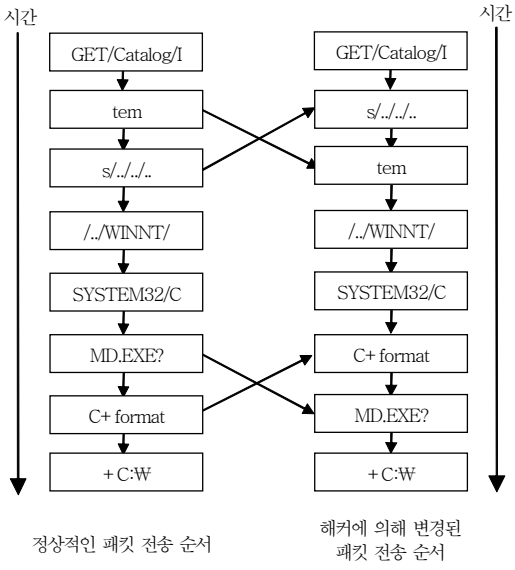
와 같은 HTTP 메시지를 전송하여 IIS 웹 서버가 설치된 시스템의 하드 디스크를 포맷하려고 할 것이다. 따라서, 공격자는 위의 메시지를 IIS 웹 서버로 보낼 것이고, NIDS의 탐지를 막기 위하여 메시지 전송순서를 임의로 변경할 것이다. 즉, (그림 5)와 같은 형태로 변경하여 전송할 것이다.

이렇게 메시지 순서를 변경하면, DPI 기능이 존재하지 않는 기존의 NIDS와 방화벽에서는 위의 메시지를 정상적인 통상 메시지로 간주할 것이다. 그러나, 만약 DPI 기술이 채택된 방화벽이라면, 위의 메시지를 (그림 6)처럼 모두 재조합하여 본래의 메시지를 만들어서 탐지하게 되므로 해커의 공격 의도를 파악할 수 있을 것이고, 바로 공격임을 알아서 차단하게 될 것이다.

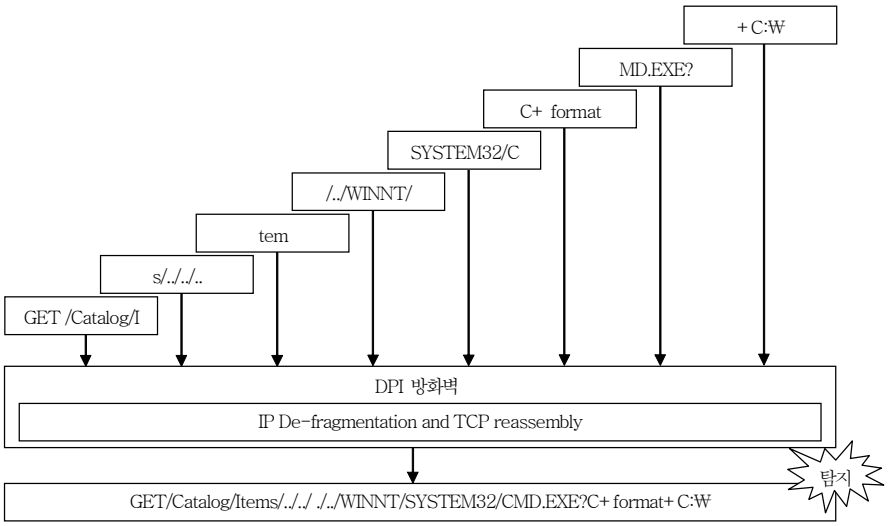
이렇듯 DPI 기술은 차세대 방화벽에서 기본적으로 갖추어야 할 기술로 인정 받고 있다[3]. 그러나, 모든 기술들이 그렇듯이 DPI 기술에 있어서 장점만 존재하는 것은 아니다. DPI 기술의 경우 많은 정보를 바탕으로 침입 탐지를 검사하기 때문에 상대적으로 많은 자원이 필요하게 된다. 특히, 5-tuple 정보만을 검사하던 초기의 방화벽 모델에 비해서 검사할 요소들이 수십 배에 이르기 때문에 많은 시간과 노력이 필요하게 된다. 이러한 검사 작업을 소프트웨



(그림 4) 방화벽 상에서의 DPI



(그림 5) 해커에 의한 패킷 전송 방식



(그림 6) DPI를 이용한 패킷 재조립

어로 행하는 경우 비교적 그 구현과 기술에 대한 검증에 걸리는 시간이 적게 소요된다. 그러나, 소프트웨어로 개발을 하게 되면 application proxy 계열의 방화벽에서 단점으로 지적했던 성능 문제가 더 치명적으로 다가오게 된다. 그렇다고 해서 ASIC이나 FPGA 혹은 네트워크 프로세서와 같은 하드웨어로 개발을 하게 되면 개발과 검증에 많은 시간이 소요되고 동시에 제품화에 성공하여도 비용 문제가 다시 발생할 수 있다.

2. DPI 기술의 장단점

그 동안, 앞에서 언급한 DPI 기술의 장단점을 분류하여 보면 다음과 같다.

• 장점

이러한 DPI 기술을 이용하면, 기존에 NIDS Evasion 기술들과 같이 방화벽이나 NIDS를 무력화시켰던 방법들을 이용한 공격들을 상당수 탐지할 수 있으며, NIDS나 방화벽에서 탐지할 수 없었던 상위 레벨의 프로토콜들의 취약점을 이용한 공격을 막아내는 것이 가능하다. 이 외에도 상위 응용 계층의 프로그램들에 대한 보안 역시 가능하게 할 수 있으며 worm이나 DDOS에 대한 공격 역시 더 확실하게 막아내는 것이 가능하다.

• 단점

가장 문제는 구현의 복잡함과 성능의 문제이다. DPI을 위해서는 상위 응용계층에서 지원하는 상당수의 프로토콜에 대한 분석이 이루어져야 한다 (HTTP, FTP, DNS, TELNET, etc.). 이러한 프로토콜은 그 표준에 대한 규약이 매우 복잡하고 양이 많아 구현에 어려움이 따른다. 그리고, 이런 분석이 복잡해지게 되면 성능에도 많은 문제가 따르게 된다. 소프트웨어로 개발을 하는 경우 개발의 어려움이 줄고, 시간도 단축되는 장점이 있으나, 역시 성능을 만족시킬 수 없기 때문에 대다수 방화벽 업체들은 하드웨어 방식을 이용하여 DPI 기술을 구현하는 방향을 선호하고 있다.

IV. DPI 제품 및 기술 방향

1. 업체 동향

현재 많은 방화벽 업체들이 DPI 기술을 이미 채용한 제품을 출시하였거나, 채용할 계획을 발표하고 있다. NetScreen Technology[4], TopLayer Networks[5]와 같은 방화벽 전문 업체에서부터 로드 밸런싱을 전문으로 하던 Radware[6], F5 Networks [7]와 같은 업체에서도 DPI 기술을 채용한 보안 제품

을 발표하고 있다. 특히 Radware에서 출시한 디펜스 프로는 스위치 기반의 NIPS 제품으로 네트워크 장비에서 DPI 기술을 이용하여 네트워크 보안 기능을 지원하는 성공적인 사례로 들 수 있다. DPI 기술은 순수히 방화벽 업계에서만 이용되는 것은 아니다. 사실, DPI 기술 자체가 네트워크 침입 탐지를 위해 많이 이용되는 NIDS에서 이용하던 기술을 발전시킨 형태이기 때문에, NIDS에서 진화한 형태인 NIPS에서도 많이 채택되고 있다. 그럼, 현재 업계에서 DPI 기술을 이용한 제품들을 간단하게 살펴 보기로 하자.

가. Netscreen Technology

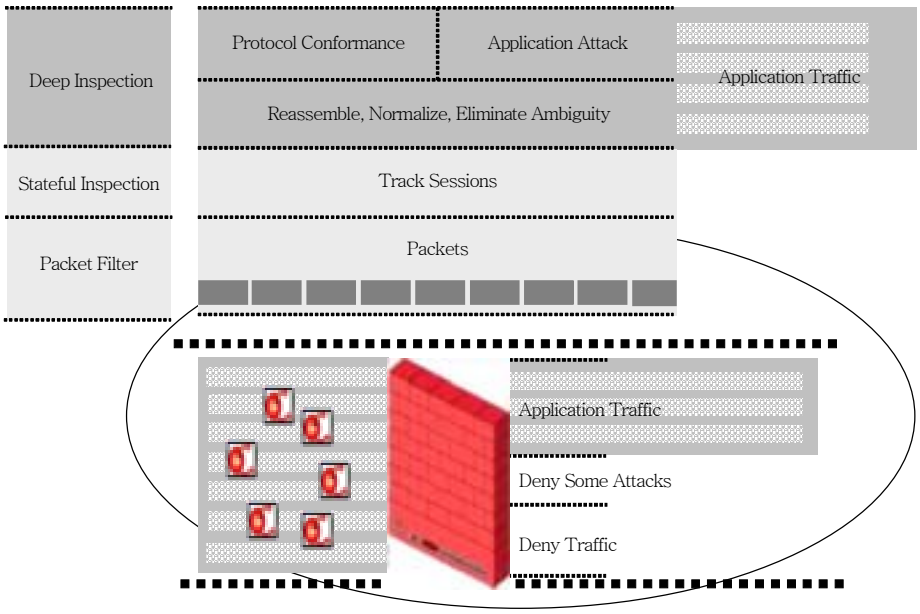
네트워크 보안 업체인 Netscreen Technology는 자사의 방화벽에 DPI 기술을 적용한 것을 가장 강조하는 업체 중의 하나이다.

Netscreen 사의 DPI 기술을 적용한 방화벽의 개념은 (그림 7)로 대변된다. Netscreen 사의 DPI 기술을 적용한 Netscreen-5000 방화벽은 DPI 기술을 충실하게 재현한 방화벽 중의 하나이다. (그림 7)에서 볼 수 있듯이 Netscreen-5000 방화벽은 DPI 기술을 적용하여, 애플리케이션 프로그램에 대한 공격과, 프로토콜 ambiguity 방지 및 IP 프로토콜에 대한 De-fragmentation 및 TCP 프로토콜에 대한 reassembly 등의 기술을 지원한다.

또한, DPI의 성능 문제를 해결하기 위하여 Application Specific Integrated Circuits(이하 ASIC) 기반의 DPI 전용 프로세서를 채택하였으며, switching fabric과 multi-bus 기술을 채택하여 내부 메시지 전송을 구현하였다.

나. TopLayer Networks

역시, 네트워크 보안 전문 업체인 TopLayer Networks는 2003년도에 국내의 많은 사이트에 보안 장비들을 공급하였다. 그 중에서도 고속 ASIC 아키텍처 기반의 AppSafe 3500™은 DPI 기술을 이용하여, DDoS(Distributed Denial of Service) 공격 완화, VPN, 다수의 침입 탐지 시스템(IDS)을 위한 플로 미러링™ 및 방화벽 로드 밸런싱, VPN 로드 밸런싱, 서버 로드 밸런싱 등을 제공하는 다기능

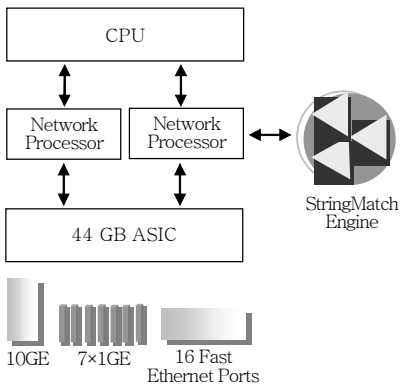


(그림 7) Netscreen사의 DPI 기술

보안 어플라이언스이다. 업계에서 유일하게 특허 받은 아키텍처를 통해 AppSafe 3500은 국제 표준화 기구(ISO)에서 정의한 OSI(Open Systems Interconnect) 모델의 7개 레이어에서 추출한 매우 상세한 네트워크 트래픽 정보를 사용할 수 있다. 기존 라우팅 및 스위칭 장비로는 네트워크를 통해 전달되는 정보 패킷을 자세히 모니터링할 수 없으며 보안 위협을 제대로 차단한다는 것이 불가능하기 때문에, AppSafe 3500의 ASIC 기반 설계는 매우 자세한 네트워크 세션 정보를 확보 및 검토하는 데 필요한 DPI 기술의 적용 및 연속 플로 분석을 지원할 수 있다. 뿐만 아니라 AppSafe 3500의 ASIC 기반 설계는 기가비트 속도로 트래픽을 처리 및 포워딩 할 수 있다는 이점을 제공한다.

다. Radware

Radware사는 본래 보안 관련 제품보다는 네트워크 로드 밸런싱 등을 위한 스위치 장비를 주로 개발하는 업체였다. 그러나, 자사의 스위치 제품에 보안 기능을 탑재하면서 보안 시장에 진출하게 되었고, 국내에서는 지난 2003년 1월 25일 인터넷 대란에서 worm의 확산을 막아내는 것을 입증하면서 많은 호응을 얻게 되었다. Radware에서 출시한 Radware Security-Switch 역시 이러한 제품군들 중의 하나인데, Radware사는 이 제품에 DPI 기술을 채택하였다. 이 제품은 3Gbps의 속도를 낼 수 있으며 이러한 속도를 유지하기 위해서 하드웨어 로직을 이용하여 DPI 기술을 구현하였다. Security-Switch 내에는 네트워크 패킷을 1차적으로 전송하는 44GB의 속도를 지원하는 ASIC으로 개발된 스위치가 있고, 이어서 전달된 패킷을 분석하는 네트워크 프로세서가 ASIC으로 구현된 string matching과 연계하여 DPI 기능을 수행하게 된다. 이에 대한 대략적인 내부 구조도는 (그림 8)과 같다.



(그림 8) Radware사의 Security-Switch 구조도

위와 같은 보안 전문 업체 제품들 이외에도 네트워크 스위치 장비 전문 업체인 F5 Networks에서 제작한 BIG-IP 5100이나 CISCO에서 제작한 방화벽 장비에서도 스위치 기능에 DPI 기능을 추가하여 보안 기능을 구현하였다. 또한, 국내 업체인 시큐어소프트와 Secui.COM과 같은 보안 업체와 그리고 LG 엔시스와 같은 네트워크 장비 업체에서도 DPI 기술을 빨리 적용할 것으로 보인다.

2. 학계 동향

보안 업체뿐만 아니라, 학계에서도 DPI 기술은 많은 관심을 끌고 있다. 특히, 네트워크 성능이 점차 진화화게 되면서 불거진 성능으로 인한 문제 때문에 많은 사람들이 고성능의 DPI 기술을 구현하는 데 많은 노력을 기울이고 있다. 앞장에서도 언급했듯이 DPI는 기존의 방화벽에 비해서 훨씬 더 많은 양의 데이터를 검사하기 때문에 더 많은 자원과 시간이 필요하게 된다. 따라서, 기가 급의 성능으로 진화하는 네트워크의 속도를 따라가기 위해서 많은 연구가 진행되고 있다. 이러한 움직임은 두 가지로 나누어 볼 수 있는데, 먼저 기존의 네트워크 프로세서를 이용한 DPI의 구현을 들 수 있고[9], 이어서 FPGA나 ASIC을 이용하여 DPI를 구현하는 기술을 들 수 있다[10].

네트워크 프로세서를 이용하여 DPI를 구현하는 경우, 기존의 대량 생산되고 있는 네트워크 프로세서를 이용할 수 있으며, 개발에 드는 시간과 비용이 상대적으로 저렴하다는 장점이 있다. 그러나, 네트워크 프로세서의 개발 방법론이 아직 완전히 자리를 잡지 못하여, 개발이 일반 CPU나 소프트웨어에 비해서 상당히 어렵고, 각 회사마다 지원하는 기능과

표준이 없기 때문에 호환성의 문제가 발생할 소지가 있으며, 각 네트워크 프로세서의 성능과 지원 사양에 따라서 DPI의 성능이 크게 좌우된다는 단점이 있다.

FPGA나 ASIC을 자체적으로 개발하여 DPI를 구현하는 방법은 그 자유도와 성능에 많은 장점이 있다. FPGA 로직을 개발하면서 DPI에 적용할 수 있는 알고리듬이나 새로운 방법론을 자유자재로 적용할 수 있으며 동시에 성능 면에서도 만족할 만한 결과를 얻을 수 있다. 그러나, 이 방법은 개발을 주도하는 개발자들의 능력에 많은 부분이 좌우되며, 동시에 대량 생산을 하기 쉽지 않다는 점에서 단점을 드러내고 있다.

V. 결 론

DPI 기술을 살펴보면 그 기능과 적용 범위가 NIDS에서 이용하던 방법과 상당히 유사함을 알 수 있다. 현재 NIDS 업계에서 뜨거운 화제로 부상하고 있는 NIPS에 대하여 알고 있는 사람이면, DPI 기술이 NIPS와 많은 면에서 유사성을 지니고 있음을 알 수 있다.

처음 네트워크 보안이란 개념이 등장하면서 방화벽이 등장하고 NIDS가 등장한 후, 방화벽과 NIDS는 서로 상호 보완적인 존재로 인식되어 왔다. 그러나, 상호 보완적인 존재란 점이 부각되면 결국, 하나로 통합되는 것이 보통 기술의 발전 방향이듯이 방화벽과, NIDS는 점차 서로의 장점을 받아 들여서 하나의 통합된 형태로 발전되어 나가고 있다. DPI 역시 이러한 관점에서 파생한 기술로 봐도 무방할 것이라 생각된다. 방화벽의 패킷 차단 기술과 NIDS의 콘텐츠 검사를 통한 침입탐지 검사 기술의 통합은 서로 나뉘어져 존재하기 보다는 하나의 통합된 형태로 존재하는 것이 더 자연스러울 것이다.

또한, 실제 제품의 간단한 소개에서 볼 수 있었듯이 대부분의 제품들이 ASIC 기반의 하드웨어로 구현되어 있으며—물론 연구소나 학교 등지에서는 FPGA를 이용하는 경우도 있으나, 대량 생산을 목표로 하는 업체에서는 ASIC 기반의 구현이 더 매력적일 것이다—소프트웨어 기반의 구현 방법은 사라져 가고 있다. 따라서, DPI를 탑재하여 차세대 방화벽을 개발하고자 하는 곳이라면, 하드웨어에 대한 기술을 검토하는 것이 더 타당할 것으로 보인다.

참 고 문 헌

[1] R. Stiennon, "DPI: Next Phase of Firewall Technology," *Technology T-18-0340 Report*, Gartner Group, 21 Nov. 2002.

[2] Data Sheet and White Paper of SmartDefense, www.checkpoint.com

[3] Kristen Noakes-Fry, "Firewalls: Technology Overview," *Technology Overview DPRO-90318*, Gartner Group, 30 June 2003.

[4] A Technology White Paper by Netscreen Technology, "Netscreen's Deep Packet Inspection," www.netscreen.com, Oct. 2003.

[5] Data Sheet and White Paper of AppSafe, "AppSafe 3500," www.topayernetworks.com, 2003.

[6] White Paper, "Introducing 3-GBPS Security Switching," www.radware.com, 2003.

[7] Data Sheet and White Paper of BIG-IP, "BIG-IP 5100 IP Application Switch," www.f5.com, 2003.

[8] Thomas H. Ptacek and Timothy N Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection," http://www. insecure.org/stf/secnet_ids/secnet_ids.html

[9] 김대영, 조혜영, "하드웨어 기반 보안엔진 분석 기술," ICAT 2003, Apr. 2003.

[10] Sarang Dharmapurikar, Praveen Krishnamurthy, Todd Sproull, and John W. Lockwood, "Deep Packet Inspection Using Parallel Bloom Filters," Hot Interconnects 11(HotI), Stanford, CA, USA, Aug. 2003, pp.44-51.