FreeBSD 커널 기반의 침입차단시스템 성능분석

박창서*

A Performance Analysis of Firewall on the FreeBSD Kernel

Chang-Seo Park*

요 약

인터넷을 통해서 침입하는 해커나 침입자로부터 기관의 내부 정보시스템을 보호하기 위하여 침입차단시스템(firewall)의 사용이 보편화되고 있다. 하지만 사용자 입장에서는 침입차단시스템의 성능을 확인 할 수 없을 뿐 아니라, 동작모드(브리지 모드(Bridge Mode), 게이트웨이 모드(Gateway Mode))에 따른 성능차이를 알 수 없다. 이러한 문제를 해결하기 위하여 본 논문에서는 침입차단시스템의 운영체제(Windows 2000, Linux, FreeBSD) 환경에 따른 성능을 분석하였다. 끝으로 FreeBSD 커널 기반의 침입차단시스템을 서로 다른 동작모드에서 성능을 비교하고 침입차단 정책수가 성능에 미치는 영향에 대하여 분석하였다.

ABSTRACT

The firewall is generally used to protect the internal information system from intruders and hackers who attack through the Internet. However, it is very difficult for a user to verify the performance of the firewall as well as the difference of the performance for the operating mode such as Bridge Mode and Gateway Mode. In this paper, the performance of a firewall on the operating systems of Windows 2000, Linux, and FreeBSD is compared. Finally, The performance of a firewall on the FreeBSD is compared at different operating modes and the effect of the number of rules by testing throughput of a firewall is analyzed.

키워드

Firewall, Bridge Mode, Gateway Mode, Throughput, Concurrent Connection Capacity

Ⅰ. 서 론

인터넷이 일반화 되면서 네트워크를 사용한 정보의 공유 및 전달은 개인이나 조직에 있어서 필수적인 사항이 되었다. 하지만 이에 따른 역기능으로 고의성 유무를 떠나서 데이터의 도난, 파괴, 바이러스 등 정보시스템의 침해가 급격히 증가하고 있다. 따라서 네트워크 보안의 가장 기본이 되는 침입차단시스템의 도입이 국내외적으로 급속히 늘어나고 있으며 그 성능도 기존의 100Mbps에서 1Gbps 이상을 지원하는 고성능으로 향상되고 있다.

침입차단시스템의 목적은 인가받은 사용자만 내부 네트워크의 자원에 접근할 수 있도록 허가하며 그렇지 않은 경우에는 접근시도를 차단하여 내부 네트워크에 있는 정보시스템의 자원을 외부로 유출되는 것을 막는데 있다. Cheswick과 Bellovin은 내부에서 외부로 모든 트래픽(반대의 경우도 포함)은 반드시 침입차단시스템을 통과해야하고 국지적인 보안정책으로 정의된 허가된 트래픽만

*동양대학교 정보통신공학부

접수일자 2003. 9. 22

통과를 허용하며, 침입차단시스템 자체가 외부의 침투에 대하여 견고해야 한다고 정의 하였다[1].

현재 사용되고 있는 침입차단시스템은 적용 기술에 따라서 크게 패킷 필터링 게이트웨이(Packet Filtering Gateway) 방식과 프록시(Proxy)를 활용한 어플리케이션 게이트웨이(Application Gateway) 방식으로 구분하나 대부분이 이 두가지 방식을 혼합한 하이브리드 게이트웨이(Hybrid Gateway) 방식을 채택하고 있다[2]. 또한 단순히 패킷의 헤더정보만을 이용하는 패킷 필터링 방식보다 발전된 방식으로 헤더정보와 함께 내용까지 해석하여 필터링하는 스테이트풀 인스펙션(Stateful Inspection) 방식을 사용하고 있다. 일부 프로토콜(Protocol)에 있어서는 패킷 필터링을 거친 패킷이 프록시를 거치는 투명한 프록시(Transparent Proxy)를 사용하기도 한다.

운영체제(Operating System) 환경에서 보면 초기에는 마이크로소프트(Microsoft) 사의 윈도우(Windows)나 Unix의 Solaris 상에서 동작하는 어플리케이션 침입차단시스템이 대부분이었으나 최근에는 1Gbps이상의 초고속 네트워크 환경을 지원하기 위하여 운영체제의 커널(Kernel)과 같이 동작하는 Linux, FreeBSD 운영체제 기반의 침입차단시스템과 주문형 직접회로(ASIC)를 사용한 하드웨어 일체형 시스템, NPU(Network Processor Unit)를 사용한 하드웨어 일체형 시스템 등으로 발전하고 있다.

하드웨어 일체형(일명: Appliance Type) 침입차단시스템은 침입차단시스템에 대한 지식이 없는 사용자도 기존의 네트워크 장비(허브(Hub), 라우터(Router))처럼 손쉽게 다룰 수 있는 장점이 있는 반면에 침입차단시스템의 로그(Log)를 관리하는데 한계가 있다.

Linux나 FreeBSD 커널 기반의 침입차단시스템은 OSI(Open System Interconnection) 7계층(Layer) 중 2계층(Data Link Layer)에서 동작하는 브리지 모드(Bridge Mode)와 3계층(Network Layer)에서 동작하는 게이트웨이 모드(Gateway Mode)를 지원한다[3].

본 논문에서는 네트워크상에서 침입차단시스템이 트래픽 지연에 미치는 영향[4] 보다는 침입차단시스템 자체의 성능에 대하여 분석하였다. 따라서 운영체제 환경에 따른 침입차단시스템의 성능을 100Mbps 환경에서 비교 분석하였으며 1Gbps의 초고속 네트워크 환경을 지원하는 FreeBSD 커널 기반의 침입차단시스템의 성능을 동작모드에 따른 성능비교와 침입차단 정책수에 따른 성능을 분석하였다.

II. 시험 환경

2.1 환경설정

침입차단시스템의 성능을 분석하기 위하여 일반적으로 많이 사용되는 SmartBits 6000B을 그림 1과 같이 구성한다.

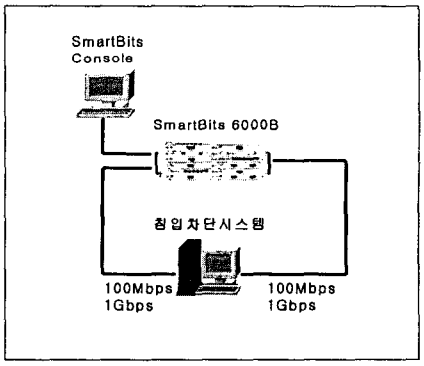

그림 1. 성능시험 구성도
Fig. 1 Configuration of the Performance Test

또한, SmartApplications/SmartFlow 소프트웨어를 사용하여 2계층(Bridge Mode), 3계층(Gateway Mode)의 Throughput 성능을 측정하고 Websuit/Firewall 소프트웨어를 이용하여 TCP 연결(Connection) 성능을 측정한다[5-7].

그림 1에서 침입차단시스템에는 100Mbps 또는 1Gbps를 지원하는 이더넷 카드(Ethernet Card)를 설치하며 SmartBits 6000B의 같은 속도를 지원하는 이더넷 카드(SmartCard)에 연결한다.

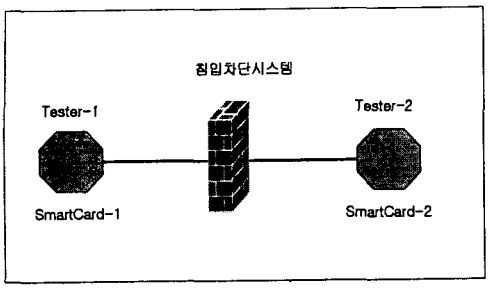

그림 2. 논리적 구성도
Fig. 2 Logical Configuration

그림 2는 1대1로 연결된 한 쌍의 침입차단시스템 포트간의 성능을 측정하기 위한 침입차단시스템과 테스터(Tester)간의 논리적인 구성도 이다.

100Mbps 하드웨어 구성은 인텔 CPU-PentiumIII 1.0GHz Single, RAM-512MB, 10/100Mbps Ethernet Card를 설치한 일반 PC를 사용한다.

1Gbps의 하드웨어 구성은 인텔 CPU-Xeon 2.0GHz Dual, RAM-1GB, 1Gbps Fiber Muti-Mode를 지원하는 Ethernet Card를 설치한 PC 서버를 사용한다. 테스트에서 1Gbps는 FreeBSD 커널 기반 침입차단시스템에 대하여 수행한다.

2.2 Throughput Test

Throughput 성능은 프레임(Frame) 손실 없이 전송 가능한 최대 전송률을 말하며 테스트는 단일 정책(Rule: All Pass)을 적용하였을 때 1대1로 연결된(UDP 1-Session Connection) 한 쌍의 침입차단시스템에 100Mbps 또는 1Gbps의 트래픽(Ethernet Frame)을 전송 하였을 때 프레임 손실 없이 전송이 가능한 최대 Forwarding Rate(Throughput)를 측정하는 것이다. 이 성능은 침입차단시스템의 패킷 처리속도를 객관적으로 비교평가할 수 있는 항목이다. 이 테스트에서 전송되는 트래픽의 IFG(InterFrame Gap)은 토폴로지(Topology)와 송신 SmartCard의 전송속도에 따라서 최소 IFG로 전송된다. 전송되는 프레임의 수는 설정된 테스트 기간동안 전송된 프레임이며 ARP (Address Resolution Protocol) 패킷과 라우팅 (Routing) 정보를 위한 메시지와 같은 운영 패킷은 포함되지 않는다. 테스트 절차는 초기 전송률 100%에서 테스트를 시작하여, 송신한 결과 프레임의 손실이 발생하면 전송률을 20% 낮추어 다시 수행한다. 반대로 테스트 결과가 손실된 프레임이 없으면 보다 빠른 속도로 Throughput을 찾기 위하여 BSA(Binary Search Algorithm)에 따라 전송률 증가를 결정(가장 최근 실패한 전송률과 성공률의 1/2 값)하여 반복 수행한다. 테스트 결과가 프레임 손실률이 0%가 될 때까지 반복 수행한다.

또한 테스트는 RFC(Requests for Comments)의 규정에 따라서 프레임 크기를 64, 128, 256, 1024, 1280, 1518 byets에 대하여 60초간 측정을 3회 반복하여 수행한 결과에 대한 평균치를 구한다.

2.3 Concurrent Connection Capacity Test

Concurrent Connection Capacity는 침입차단시스템에서 동시에 처리할 수 있는 최대 연결(Session Connection) 수를 테스트 하는 것으로 Connection Request를 테스트 시간동안 정해진 수만큼 계속 보내 침입차단시스템의 연결 여부를 분석한다.

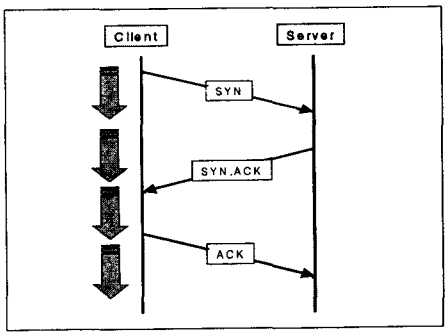

그림 3. TCP 연결 설정
Fig. 3 TCP Connection Setup

그림 3은 TCP 연결 설정이 3단계(Tree Way Handshake)로 이루어짐을 나타낸다. 클라이언트(Client) 쪽에서 침입차단시스템을 거쳐 서버(Server)로 Connection Request(SYN Segment)를 보내고 이를 받은 서버측에서 응답(SYN, ACK Segment)을 침입차단시스템을 통하여 보내준다. 이때 클라이언트 측에서 확인 응답(ACK Segment)

을 보내주면 이상없이 연결된 것으로 처리한다. 테스트에서 클라이언드와 서버는 SmartBits 시스템이 대행해주며 침입차단시스템의 Connection Request에 대하여 연결되는 최대의 동시 연결 수를 분석한다.

III. 시험결과 및 분석

3.1 운영체제에 따른 성능분석

운영체제에 따른 침입차단시스템의 성능을 비교하기 위하여 100Mbps 환경에서 Windosw 2000, Linux Kernel 2.4, FreeBSD Kernel 4.5에서 Throughput 테스트를 단방향 성능(Uni-directional Throughput)으로 하였다. 테스트 모드는 3계층에서 동작하는 게이트웨이 모드에서 실시하였다. 그림 4는 운영체제에 따른 성능을 나타낸다.

여기서, Windows 2000에서는 패킷 필터링 방식을 사용하고 Linux나 FreeBSD는 스테이풀 인스펙션 방식을 사용하였으나 테스트 환경에서는 검색할 내용이 없음으로 성능에는 크게 영향을 미치지 않는다고 가정하였다.

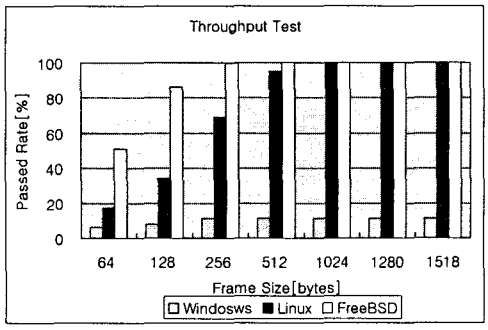

그림 4. 운영체제별 단방향 성능
Fig. 4 Uni-directional Throughput for Operating System

성능은 그림 4에서처럼 Windows 2000에서 침입차단시스템은 운영체제와 침입차단시스템 소프트웨어가 분리된 어플리케이션 형태로 성능이 좋지 않고, 일반적으로 Linux 커널보다 FreeBSD 커널이 크기가 작고 효율적이라는 것 반영 하듯이 FreeBSD 커널 기반 침입차단시스템이 최고의 성능을 나타내고 있다. 특히, 프레임 크기가 작은 영역에서 FreeBSD 커널 기반 침입차단시스템이 월등한 성능을 나타내고 있다.

3.2 동작모드에 따른 성능분석

동작모드에 따른 성능 분석은 OSI 7계층 중 2계층에서 동작하는 브리지 모드와 3계층에서 동작하는 게이트웨이 모드에서 100Mbps와 1Gbps 환경에서 각각 수행하였다. 그림 5는 동작모드에 따른 단방향 성능을 나타낸다.

2계층에서 동작하는 브리지 모드가 3계층에서 동작하는 게이트웨이 모드보다 성능이 우수 하였으며 프레임 크기가 작은 경우에는 100Mbps가 1Gbps 환경보다 상대적으로 효율이 좋게 나타났다.

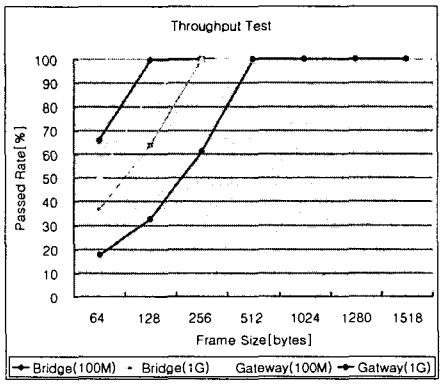

그림 5. 동작모드에 따른 단방향 성능
Fig. 5 Uni-directional Throughput for Operating Mode

3.3 정책(Rule) 수에 따른 성능분석

침입차단시스템의 성능을 보다 현실적인 환경에 근접하여 분석하기 위하여 침입차단 정책수에 따른 성능을 측정하였다. 1Gbps 환경의 게이트웨이 모드에서 허용정책(Pass Rule)을 정책 우선순위의 맨 마지막에 설정함으로써 정책수가 늘어남에 따른 침입차단시스템의 성능변화를 분석하였다. 표 1은 정책수에 따른 단방향 성능을 나타내며 그림 6은 결과를 그래프로 나타낸 것이다.

여기서, 정책수가 5000개 까지는 침입차단시스

템의 성능 거의 영향을 미치지 않음을 알 수 있다.

표 1. 정책수에 따른 단방향 성능
Table. 1 Uni-directional Throughput for the Number of Rules

구 분		Rule수					
		1-Rule	100-Rules	1000-Rules	3000-Rules	5000-Rules	10000-Rules
Frame Size [bytes]	64	18.26	18.26	18.26	18.26	18.26	18.26
	128	32.74	32.74	32.17	32.17	32.17	31.36
	256	61.06	60.53	60.00	60.00	58.97	42.59
	512	100.00	100.00	100.00	100.00	100.00	100.00
	1024	100.00	100.00	100.00	100.00	100.00	100.00
	1280	100.00	100.00	100.00	100.00	100.00	100.00
	1518	100.00	100.00	100.00	100.00	100.00	100.00

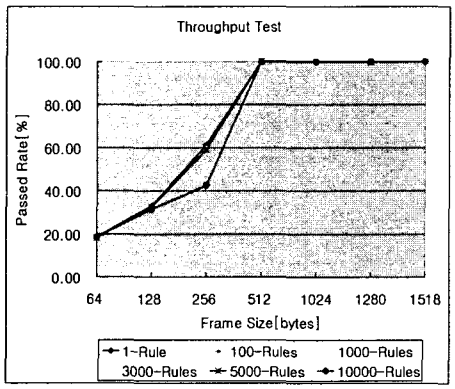

그림 6. 정책수에 따른 단방향 성능
Fig. 6 Uni-directional Throughput for the Number of Rules

3.4 Concurrent Connection Capacity 분석

침입차단시스템의 실제운영 환경에서 동시 사용가능한 사용자를 예측하기 위하여 1Gbps 환경에서 동시연결 세션 수(Concurrent Session Number)에 대하여 브리지 모드와 게이트웨이 모드에서 테스트를 하였다. 그림 7은 동시연결 세션 수에 대한 테스트 결과를 나타낸다. 게이트웨이 모드는 50만 세션까지 동시에 연결이 가능하고 브리지 모드는 60만 세션까지 연결이 가능함을 알 수 있다. 이는 3.2절의 성능과 마찬가지로 OSI 계층에 따른 성능차이로 볼수 있다. 일반적으로 하나의 웹페이지는 30-50 세션으로 이루어져 있으며 최근 급속히 성장하고 있는 P2P(Peer-to-Peer)를 사용하는 경우에는 1000 세션 이상이 요구되기도 한다.

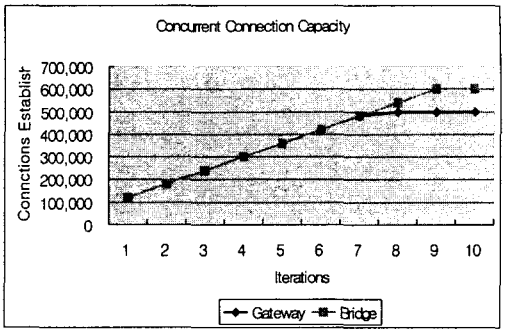

그림 7. 동시 연결 세션 수
Fig. 7 The Number of Concurrent Sessions

3.5 기타사항

그 외에 침입차단시스템의 성능에 영향을 미치는 요소에는 다음과 같은 것이 있다. 먼저, 동시연결 세션 수는 시스템의 RAM 크기와 관계가 있으며 패킷 필터링 성능은 CPU의 처리속도와 이더넷 카드가 설치되는 PCI버스 (Peripheral Component Interconnect Bus)의 속도에 영향을 받는다. 또한 FreeBSD 4.5 커널은 복수개의 CPU를 완벽히 지원하지 못해서 CPU의 수가 성능에 크게 영향을 미치지 않았다. 본 논문에서는 단방향 전이중방식(Uni-directional Full Duplex)에 대하여 테스트를 하였으며 양방향 전이중방식(Bi-directional Full Duplex)의 경우에는 성능이 프레임 크기가 작은 영역에서는 약 50% 정도 감소 하였다.

IV. 결 론

본 논문에서는 침입차단시스템의 성능을 객관적으로 분석하기 위하여 SmartBits를 사용하였다. 100Mbps 환경에서는 Linux나 FreeBSD처럼 운영체제의 커널에 포함되어 동작하는 침입차단시스템이 운영체제와 분리된 Windows 2000에서 보다 성능이 좋은 것을 알 수 있다. 100Mbps가 1Gbps 보다 상대적으로 프레임 크기가 작은 경우에 효율이 좋게 나타났다. 따라서 1Gbps 이상의 초고속 네트워크 환경을 지원하기 위해서는 프레임 크기가 작은 영역에서 패킷 필터링 성능을 향상 시켜야 한다. OSI 2계층에서 동작하는 브리지 모드가

3계층에서 동작하는 게이트웨이 모드보다 패킷 필터링 속도와 동시연결 세션 수 등에서 모두 좋은 성능을 가짐으로 부득이하게 게이트웨이 모드를 적용해야 하는 경우가 아니면 브리지 모드를 적용하는 것이 바람직하다. 또한 침입차단 정책수가 5000개를 넘어가면 성능에 영향을 미침으로 고속 알고리듬(Algorithm)이 요구된다.

본 논문은 1Gbps 이상의 초고속 네트워크를 지원하는 침입차단시스템 개발을 위한 기초적인 자료로 활용될 수 있을 것이다.

참고 문헌

[1] W. R. Cheswick and S. M. Bellovin, "Firewall and Internet Security", Addson-Wesley Publishing Com., 1994.

[2] 이준택, 배민호, 박미영, "네트워크 보안과 방화벽 구축", 가남사, 2002.

[3] 최준호, 김승영, 오준선, 편용현, "About FreeBSD", 영진닷컴, 2001.

[4] 정선이, 박정은, 유수연, 장성은, 채기준, 노병규, "네트워크 상에서의 침입차단시스템 영향력 분석", 통신정보보호학회 논문지, 제10권, 제4호, 2000.12.

[5] RFC 1242, "Benchmarking Terminology for Network Interconnection Devices", IETF, July 1991.

[6] RFC 2285, "Benchmarking Terminology for LAN Switching Devices", IETF, Feb. 1998.

[7] RFC 2544, "Benchmarking Methodology for Network Interconnect Devices", IETF, March 1999.

저자 소개

박창서(Chang-Seo Park)

1987년 광운대 전자통신공학과 졸업

1989년 광운대 전자통신공학과 공학석사

2000년 광운대 전자통신공학과 공학박사

1990년 5월-1996년 4월 LG소프트 과장

1996년 5월-1999년 2월 교보정보통신 팀장

1999년 4월-2001년 4월 에스큐브 연구소장

2001년 5월-2002년 2월 토탈시큐리티 대표이사

2002년 3월-현재 동양대학교 정보통신공학부 전임강사

※ 관심분야 : 정보보안, 시스템 및 네트워크 보안, 인트라넷 등