The Journal of Korean
Institute of CALS/EC
Vol 7, No. 3, Dec. 2002

K4 방화벽의 CPU 및 보안규칙의 증가에 따르는 성능평가연구

박대우*, 전문석*

A study on performance evaluation of K4 Firewall System with multiple CPUs and security rules

Daewoo Park, Moonseog Jun

Abstract

According as development of networks and increasing on internet service, For the performance increase of K4 Firewall require that hardware be installed of 2 CPU or 4 CPU instead of 1 CPU. Output of performance test among 1CPU, 2CPU, and 4CPU of K4 Firewall system has not any efficient about increasing multiple CPUs . K4 Firewall put performance on setting on demon of packet filtering rules and Network Address Translate and Authentication and Proxy services. Performance results that setting after security rules are less 2% Packet Filtering, 8%-11% NAT, 18%-20% Proxy and Authentication services than setting before security rules on K4 Firewall System. NAT and Proxy service have decrease of performance. This performance result comes in useful for research and development on K4 Firewall System.

키워드: 방화벽, K4, 다중CPU, 보안규칙설정, 정보보호

* 숭실대학교 컴퓨터학과

1. 개 요

인터넷의 발달과 더불어 정보화 사회에서의 정보는 국가의 이익과 경쟁력을 좌우하는 중요한 자산이 되고 있다. 그러나 정보를 취급하는 과정에서 발생하는 취약성을 이용하여, 인터넷에 연결된 호스트에 인증되지 않은 사용자가 침입하여 다른 사용자에게 해를 주고 있다. 이러한 침입자들은 불법적으로 다른 사람의 정보를 취득하여 해를 주거나, 네트워크의 시스템을 손상하거나, 네트워크 시스템에 장애를 유발시키는데, 이러한 폐해를 방지하는 것이 정보보호의 목적이다.

정보보호의 목표인 비밀성(secrecy), 무결성(integrity), 가용성(availability)[1]을 달성 하면서도, 정보보호 기술을 통하여, 허가 또는 인증되지 않거나 비정상적인 사용자에 대한 접근을 차단할 수 있는 가장 효과적인 정보보호제품 중 하나가 K4 방화벽 시스템이다. 방화벽은 외부와 내부 네트워크 유일한 경로(gateway)에, 혹은 중요한 정보매체에 대한 자료 전송 시 유일한 전송로에 설치되어, 양자간에 오가는 모든 통신을 감시하여, 외부로부터의 허용되지 않는 침입을 차단한다. 이로써 불법적인 네트워크 침입으로부터 내부 네트워크 시스템들을 보호하거나, 중요한 정보자원이 있는 호스트들을 보호한다.

이러한 K4 방화벽시스템을 설치하는 수요자들은 유일한 경로에 전송되는 최대 패킷 용량을 고려하여 하드웨어를 구성하는데, 현재 시장에서는 보통 CPU 가 한 개인 1 CPU 보다는, 2CPU 또는 4CPU 로 CPU 를 추가 확장하여 하드웨어 시스템을 구성한다. 이때 CPU 추가에 따르는 비용은 증가 하지만 비용 증가만큼의 성능에 대한 효율성은 검증된 것은 없이, 막연히 1CPU 에 비해서 2CPU 또는 4CPU 방화벽의 성능이 우수할 것이라고 생각하여 사용하고 있다. 따라서 본 논문에서는 CPU 를 추가하여 하드웨어를 사용할 경우, 방화벽의 성능과 효율성은 얼마만큼의 성능 개선이 이루어지는 가에 대한 비교 성능실험 평가를 한다.

또한 K4 방화벽에 패킷필터링 규칙설정 및 응용계층의 프락시 서비스와, NAT 및 인증관리 서비스 등 방화벽 보안 정책에 따라, 정보보호를 위해 필요한 방화벽 보안 규칙을 설정하는데, 이렇게 방화벽에 대해 보안 규칙을 설정하기 전과, 보안 규칙을 설정 한 후의 방화벽 성능결과를 비교 측정하여, 이 자료를 토대로 방화벽 성능 개선에 대한 방향을 제시 하고자 한다.

2. 관련 연구

2.1 방화벽의 평가 및 인증

대한민국에서 방화벽의 인증기준은 1998 년 2 월에 제정되어, 국가정보원에서의 정보보호 제품으로 인증하고 있는데, 인증 사 공식 제품명으로는 침입차단시스템이며, 현재에는 2002 년 8 월 5 일 개정된 정보보호시스템 평가 인증지침(정보통신부고시 제 2002-41 호)[2]을 사용하고 있다. 침입차단 시스템 평가기준은 보안기능의 신뢰성을 확인하기 위한 보증 요구사항으로 개발과정, 시험, 형상관리, 운영환경, 설명서, 취약성의

6가지 사항으로 이루어진다.

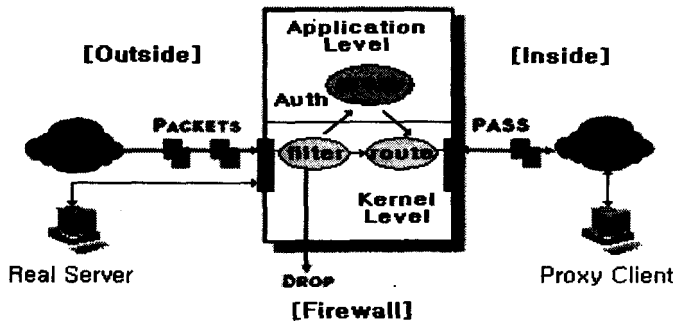
국가 정보원의 침입차단시스템 평가등급은 K1 등급을 최저단계로 하고, K2, K3, K4, K5, K6 그리고 K7 를 최고단계로 하여 총 7 단계로 구분하는데, 침입차단시스템을 통하여 전송되는 데이터를 암호화하여 기밀성 기능이 제공되는 경우에는 각 평가 등급에 E (Encryption) 자를 붙여서 K1E, K2E, K3E, K4E, K5E, K6E, K7E로 표기[3]한다.

국가정보원에서는 2002 년 7 월 이후로는 정보보호 제품들에 대한 평가신청 및 평가를 위한 표준으로, IT 보안성 평가에 대한 국제표준의 ISO/IEC 15408 -1의 원본인 국제공통평가기준(Common Criteria for Information Technology Security Evaluation)을 국내 표준으로 제정하여 차후 정보보호시스템 공통 평가기준 을 적용하여 정보보호 제품에 대한 보안 인증평가를 실시 하려고 하고 있다. 정보보호제품의 보증 수준을 정하기 위한 공통 평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7 의 7 개의 등급으로 구분된다. EAL1 은 최저의 평가 보증등급이고, EAL7 은 최고의 평가 보증등급이다. [4]

국가정보원의 인증을 받아 사용중인 K4 등급 이상의 방화벽시스템은 인증신청인이 개발한 방화벽 소프트웨어를 운영체제와 하드웨어에 탑재하여 인증을 받거나, 하드웨어와 운영체제 및 소프트웨어를 일체형으로 하여 인증을 받는다. 일반적으로 국가 및 관련 공공기관에 설치되는 방화벽 시스템은 국가 정보원의 K4 등급 이상의 인증평가를 받은 소프트웨어 부분을 사용량과 전송용량 (Network Traffic) 을 고려하여 운영체제와 하드웨어 사양에 맞추어 설치한다.

2.2 K4 방화벽의 정보보호 서비스 내용

K4 인증 침입차단시스템의 방식은 조금씩 다르나, 정보통신망 침입차단시스템 평가기준에 의해 개발되며, 일반적인 모델은 (그림 1) 과 같이 하이브리드(Hybrid) 방식에다가 상태정밀검사방식(Stateful Inspection)[5]을 도입하고, 여기에 VPN(Virtual Private Network) 기능을 강화하여 사용하고 있다.



(그림 1) 하이브리드방식

K4 방화벽 시스템에서 제공되는 정보보호 서비스와 정보보안 기능은 각기 시스템의 특성에 따라 혼합되거나 각 기능과 연관되어져 사용 되고 있다. 이들 보안 서비스를 5가지로 크게 분류 해 보면 다음과 같다.

(1) 인증(Authentication)

방화벽을 통과하는 모든 접속에 대한 식별 및 인증에 이용되는 인증 자료를 처리하며, 보안관리자, 사용자, 사용자그룹에 대한 인증정보의 등록, 수정 및 삭제등에 대한 정보보호를 위해 S/Key와 같이, 일회용 패스워드[6]를 생성하거나, 접속 최대시도회수 및 암호변경주기 등을 통해 강력한 정보보호 서비스를 제공한다.

(2) 접근 통제(Access Control)

패킷필터링 규칙설정을 통해 위반사항에 대한 패킷에 대한 접근통제를 실시한다. 3계층인 네트워크층(Network Layer)의 IP의 헤더(header)와 4 계층인 전송층(Transport Layer) 인 TCP(Transmission Control Protocol), UDP(User Datagram Protocol)을 통해 패킷의 출발지 및 목적지, 서비스 포트(port) 번호 등을 이용 접근 통제를 하게 된다.

이때 임의적 접근통제(DAC: discretionary access control) 는 네트워크 단계에서 패킷필터링의 일괄적인 접근통제를 할 수 없는 부분을 보안 관리자가 각각의 게이트웨이 별로 특성에 따른 접근통제를 실시하는 것이며, 강제적 접근통제(MAC: mandatory access control) [7]는 주체 및 객체의 보안 레이블이 객체의 보안 레이블보다 높거나 같을 경우에 접근을 허용하는 것이다. 따라서 접근통제는 패킷 필터링, 상태정밀검사 방식, 프락시 서비스, 응용서비스통제 등을 통해 비인가자에 대한 침입을 차단한다

(3) 비밀보장(Data Confidentiality)

인터넷은 TCP/IP 프로토콜을 사용하기 때문에, 암호화 되지 않은 평문(Plain text) 형식의 내용이 노출되었을 경우 보안에 취약하다. 이러한 내용에 대한 암호화는 정보보호 서비스의 하나로, 인증 시 패스워드에 관한 암호화는 S/Key 등이 있으며, 전송내용에 대한 암호화는 RSA, 3DES, CAST, SEED, Bluefish, Twofish 등이 있고, 무결성 체크에 대한 암호화는 MD5, SHA -1[8] 등을 사용한다.

(4) 데이터 무결성 (Data Integrity)

방화벽 내에 무결성기능은 운용환경을 설정한 환경 DB(DataBase) 및 관련 보안자료의 추가, 수정 삭제 등이 발생 하였는가를 감시 하기 위해, 일정한 주기별로 DB 파일 변경 되었는가를 체크 하여 위반한 사항에 대해 보안 관리자에게 통보한다

방화벽 내에서의 전송 데이터에 대한 무결성은 VPN 기능을 도입하여 사용하며, 그림 2 와 같이 동작이 작동된다. 이의 과정 을 보면 다음 순서와 같다..

< Firewall A에서의 동작>

1. Host의 요청한 서비스가 NIC (Network Interface Card) 1에 도달하면 라우팅 테이블에 의해 목적지를 확인한다.
2. 목적지 IP 주소가 192.168. 50.200이면

터널링(Tunneling) NIC로 보내지고 해당 되지 않으면 NIC2 를 통해 공인망으로 보내진다.

3. 터널링 NIC로 패킷이 보내지면 터널링을 생성한다. 세션 키의 수동교환을 통한 연결 후 데이터의 무결성 정보를 확인한다.

4. 원시데이터를 SHA -1 알고리즘을 통하여 무결성 값을 생성하고, 원시데이터에 포함하여 압축한다.

5. UDP 패킷으로 변환 후 NIC2를 거쳐 목적지로 전송된다.

< Firewall B에서의 동작>

6. NIC2에서 받은 패킷의 출발지를 확인하고, 목적지 IP 주소가192.168.50.200이라면 터널링 NIC로 보내어진다.

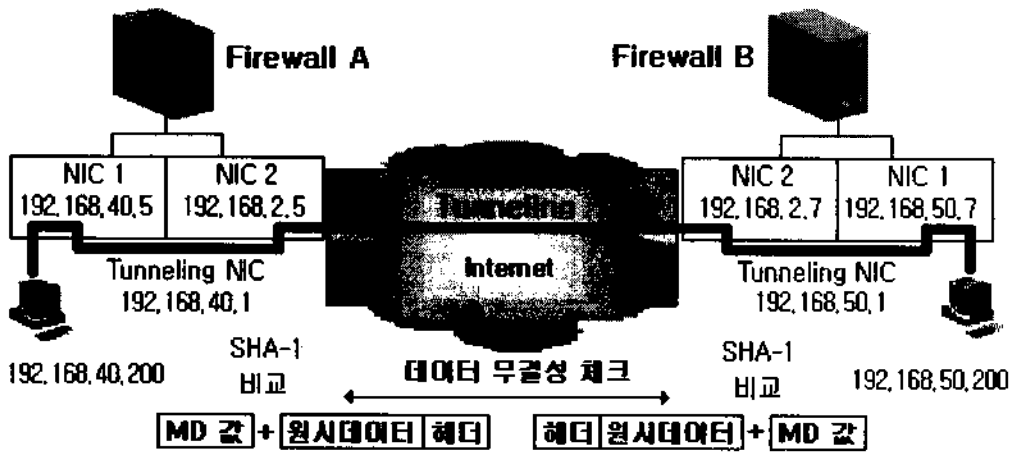
7. 무결성 확인 후 복호화하여 원시 데이터를 추출한다.

8. 원시데이터의 목적지를 확인하여 전송된다.

9. 작업종료 후 프로세스가 닫히면 세션도 닫히게 된다.

전송 데이터에 대한 무결성 검증은 상호 신분확인 및 데이터 무결성 체크 알고리즘을 이용한 데이터의 변조 및 위험성 방지와 데이터의 손실에 따르는 보안성을 높이며, 네트워크 계층에서의 VPN 터널링 방식인 IPSec 과 IKE 표준[9] 을 적용 하여 양 종단 간의 안전한 통신을 지원하기 위해 IP 계층을 기반으로 하여

터널 모드 AH (Authentication Header), 트랜스포트 모드 AH, 터널 모드 ESP (Encapsulation Security Payload), 트랜스포트 모드 ESP 의 4 가지 형태로 보안성을 제공 [10]하여, 어플리케이션[11] 에게 무결성, 인증, 비밀성 기능을 제공하고 사용자에게 투명하게 구현할 수 있다.



(그림 2) 방화벽 VPN을 통한 전송 무결성

(5) 부인방지 (Non-repudiation)

침입차단시스템은 통과하는 모든 트래픽에 대해 로그 파일(log file)을 기록할 수 있다. 이 로그파일을 토대로 한 감사기록 및 추적관리를 위해 날짜, 사용자, 기록형태, 호스트(host), 서비스,중요도, 사건형태 등을 기록하고, 또한 현재 접속되어 있는 사용자의 프로세스 관리와 실시간 내용조회를 통해 필터링(filtering) 하거나, 차단할 사용자를 강제로 차단시킬 수 있다.

2.3 K4 방화벽의 정보 보안 기능

또한 정보보안을 위한 K4 방화벽을 기능별로 크게 분류해 보면 다음과 같다. 이 기능들은 방화벽의 데몬을 통해 정보 보안 정책을 구현하는 보안 규칙들을 설정 할 수 있다.

(1) 패킷필터링 기능

방화벽 보안 정책에 입각한 패킷필터링 규칙설정을 통해, 불법적인 접근에 대한 패킷을 차단시키며, 네트워크층과 전송층에서 패킷의 출발지 및 목적지, 서비스 포트 번호, TCP Sync 등을 이용하여, 패킷의 ACCEPT, DENY, REJECT, MASQ, REDIRECT, RETURN 등[12]을 실행하게 된다.

(2) NAT기능

방화벽의 특정한 네트워크 인터페이스 카드를 거쳐서 전송되는 패킷을 검사하여 지정된 IP 와 목적 포트를 가지고 있는 경우에, 맵 테이블(Map Table)을 만들어 IP 주소를 변환 시킨다. 그러나 방화벽 외부망 사용자의 방화벽 내부 호스트로의 접근 시에는, 맵 테이블이 존재하지 않으므로 방화벽의 내부망에 접근 할 수 없다.

(3) 프락시

사용자가 접속하는 프락시에 대한 접속포트, 제한시간을 적용할 접근통제규칙 및 접속에 대한 환영, 거부메시지 등을 포함한 Telnet, FTP, HTTP, SMTP , PoP3, Rlogin, 네트워크 그룹 등 특정 프로토콜을 위한 프락시 서버가 작동하여, 프락시 서버의 보안기능에 의해 접근 허용을 결정한다.

(4) 사용자 인증기능

그리고, 방화벽을 통과하는 모든 사용자에 대한 식별 및 인증에 이용되는 인증 자료를 처리하며, 보안관리자, 사용자, 사용자 그룹에 대한 인증정보의 등록, 수정 및 삭제 등에 대한 정보와 접속 최대시도회수 및 암호변경주기 등을 통해 강력한 정보보호 서비스를 제공한다.

이러한 정보 보안기능들은 K4 방화벽 시스템에서 제공되는 정보보호 서비스와 함께, 방화벽 시스템의 특성이나 구현 방법에 따라 혼합되거나 연관 되어져 사용 되고 있다.

2.4 인증 방화벽의 운영체제

K4 방화벽의 기능 평가는 한국정보보호진흥원(KISA: the Korea Information Security Agency)에서 담당하고 있는데, 현재 인증 후 사용 중 이거나 평가인증 중인

K4 인증 등급 이상의 침입차단시스템 운영 체제는 UNIX 계열의 Solaris 와 X86, IBM 의 AIX, HP-UX가 있고, Windows 계열의 NT, Windows2000 , XP가 있다.[13]

아래 < 표 1> 은 2002 년 11 월 27 일 현재 인증 평가 후 K4 인증 평가등급 이상을 취득하거나 평가진행 중인 방화벽 제품을 보여 주고 있다.

<표 1> K4 방화벽 제품명 및 운영체제

K4인증	평 가 제 품 명	운 영 체 제
평가완료	SecureShield-Firewall V1.0	Solaris 2.5.1
	인터가드 V1.5	Solaris 2.5.1
	수호신 V2.0	Solaris 2.5.1
	SecureWorks V2.0	Solaris 7 for x86
	수호신 V3.0	AIX 4.3
	SecureWorks V2.0	Solaris 7
	수호신 V3.0	Solaris 7 for X86
	매직캐슬 V1.0	Solaris 2.5.1
	수호신 V3.0	Solaris 7
	UniSecure Firewall V1.0	Windows NT 4.0
	SecuwaySuite 1000 v1.0	WindowsNT 4.0
	SecuwaySuite 2000 v1.0	WindowsNT 4.0
	SecureWorks V3.0	Solaris 8 for x86
	SecureWorks V3.0	Solaris 8
	화랑 3.0	Windows 2000
	SecureWorks V3.0	HP-UX 11.00
	REAL TIME F IREWALL V1.0	Windows 2000
평가 중	SecureWorks ezWall V3.0	SWOS
	SecuwaySuite 100 v1.0	Windows 2000
	UniSecure Firewall V2.0	Windows XP
	MagicCastle V3.0	Solaris 8

3. K4 방화벽의 성능 평가 방법

현재 평가 인증 중 이거나 인증 후 사용 중인 K4 인증 등급 이상의 침입차단시스템은 하드웨어와 운영체제에다가 개발한 방화벽 소프트웨어를 시스템으로 구성하여 평가를 받거나, 하드웨어 및 운영체제, 소프트웨어 일체형으로 평가하여 인증을 받는다. 하드웨어 및 소프트웨어 일체형은 전체 인증이 되므로 개별 성능을 비교 평가하기에는 부적절한 면이 있어, 소프트웨어로 인증 받은 제품을 대상으로 하여 운영체제와 함께 하드웨어에 인스톨 할 때 1CPU로 하거나, 2CPU 또는 4CPU로 확장하여 시스템을 구성한다.

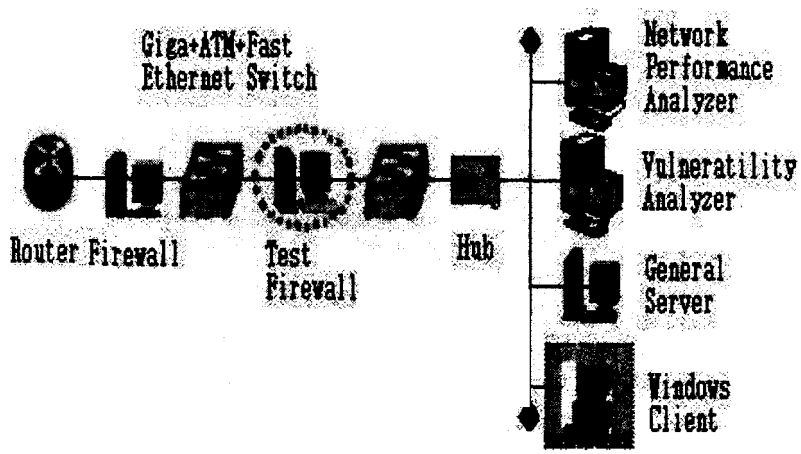
3.1. 방화벽 성능 평가 장비 구성

하드웨어 Ultra 80에 1CPU를 장착한 상태에서, 운영체제로는 UNIX 계열의 Solaris 2.8을 설치하고, 이를 성능 평가 장비인 SmartBit-2000 에서 패킷 생성 툴(tool)인 Smart TCP를 이용하여 네트웍 트래픽을 발생시킨다. 방화벽 성능실험을 한 방화벽 전용 성능 실험실[14] 에서 했으며, 테스트 장비 구성은 <그림 3>과 같다.

3.2. 방화벽 성능 평가 조건 및 방법

하드웨어에 운영체제를 설치 한 상황에서 K4 방화벽 소프트웨어를 인스톨하고, 방화벽 기능에 이상 없는지를 확인한 후, 전송부하에 대한 성능실험을 하였고, 실험의 조건은 다음 표 2와 같다.

평가 방법은 방화벽 운영시스템의 성능실험은 128Byte를 한방향 전송으로 할 때, 전송부하(packet load)를 50Mbyte에서 100Mbyte까지 실어 보낼 때 패킷손실율(packet loss)을 측정한다.



(그림 3) 방화벽 성능실험실 구성

<표 2> 성능실험조건

Test Duration	120 sec
Minimum Packet Load	50 Mbyte
Maximum Packet Load	100 Mbyte
Initial Rate	30 %

위 < 표 2> 의 성능실험에서의 결과 차이가 없을 때에는 패킷의 프레임 사이즈 (Frame Size) 별로 패킷손실율을 측정 하는 성능실험을 하였다. 실험 조건은 위와 동일한 하드웨어와 운영체제 그리고, K4 방화벽 소프트웨어를 인스톨하고 나서 성능실험을 하여 방화벽의 기능이 정상 작동 되는지를 확인하고 나서, 방화벽 성능 실험을 하였고, 실험 조건은 <표 3> 과 같다.

<표 3> 성능실험조건

item	value
Test Duration	120 sec
Minimum Frame Size	64 byte
Maximum Frame Size	1518 byte
Initial Rate	30 %

방화벽 보안규칙 설정에 따른 성능 실험을 하기위해, 20 군데 이상의 현장을 둘러보면서 조사한 바 보안 규칙의 개수는 현장마다 다르고, 규칙 종류도 다양 하였으나 평균 50 개 미만이 대부분인 것을 감안하여 50개로 기준을 설정하였다, 각 보안규칙의 설정내용은 현 실무에서의 적용규칙을 최대한 반영하였다.

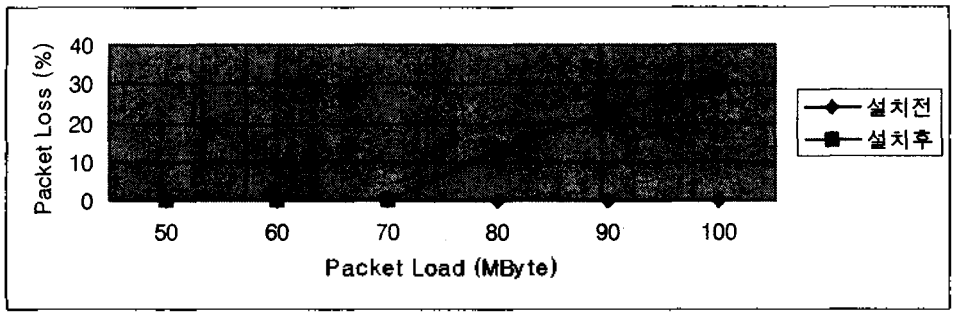
4. K4 방화벽의 성능 평가 및 비교

4.1 방화벽소프트 설치 전 후의 성능비교.

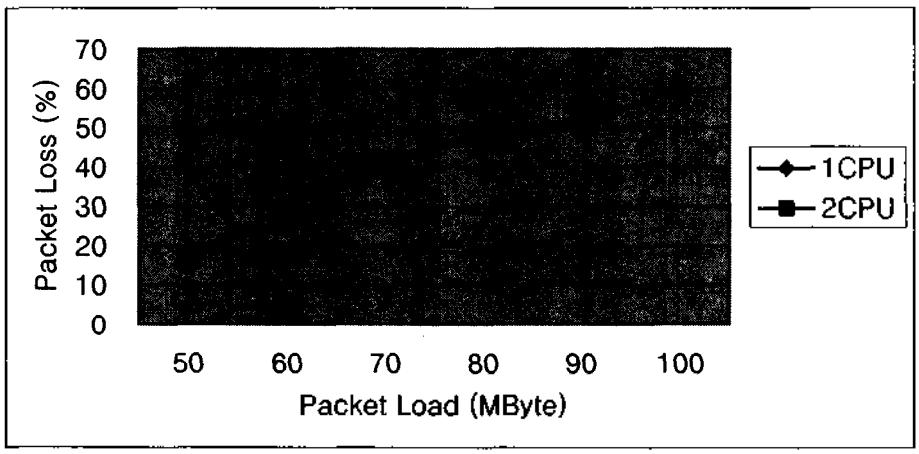
방화벽 소프트웨어 설치 전 성능 실험값을 얻고 난 후에, 이번에는 K4 인증을 받은 방화벽인 침입차단시스템 소프트웨어를 인스톨 한 후 성능실험을 하였다 성능실험의 조건은 표 2 와 같다. 그림 4 와 같이 방화벽 소프트웨어 설치 전 성능실험에서는 50Mbyte부터 100Mbyte 까지 패킷손실율이 발생하지 않았다. 또한 방화벽 소프트웨어 설치 후 성능 실험에서는 50Mbyte 에서 70Mbyte 까지 전송부하 실험에서는 패킷손실율이 나타나지 않았으나, 80Mbyte 전송시부터는 패킷손실율이 발생 하여, 100Mbyte에서는 30% 이르는 패킷손실율을 기록 하였다.

4.2 방화벽소프트 설치 전 후의 성능비교.

1CPU 하드웨어와 2CPU 하드웨어에 동일한 운영체제와 K4 방화벽 소프트웨어를 인스톨하고 나서, 성능실험 비교 값을 측정해 본 결과, (그림 5) 와 같이 패킷을 60Mbyte로 보냈을 경우에는 패킷손실율이 4.18% 의 차이를 보였으며, 90Mbyte 의 경우에는 패킷손실율이 1.68% 로 나타났다. 그러나 50Mbyte , 70 Mbyte , 80 Mbyte 100Mbyte 경우에는 패킷손실율이 0.5% 이내의 오차를 나타내었다.



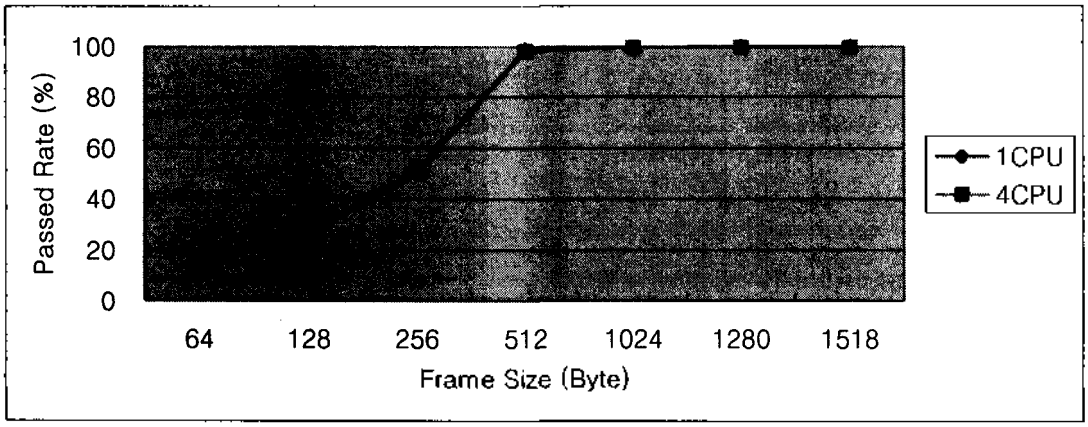
(그림 4) K4 방화벽소프트 설치 전 후 성능비교



(그림 5) 1CPU와 2CPU의 성능 비교

4.3. 방화벽 설치후의 1CPU와 4CPU 성능비교

위 하드웨어와 운영체제에서 4개의 CPU를 설치하고 표 2의 조건으로 방화벽 성능 비교 실험을 하였다. 그러나 결과의 차이는 나타나지 않았다. 그래서 다시 같은 조건으로 4개의 CPU를 하드웨어에 설치하고 표 3의 조건으로 성능실험을 하였다. 프레임 사이즈 별 성능 비교 실험에서 패킷손실율 측정 결과, 그림 6과 같이, 1CPU 하드웨어와 4CPU 하드웨어 설치 후에도 성능 실험 차이는 거의 없음을 나타냈다.



(그림 6) 1CPU 와 4CPU 의 성능 비교

또한 이 실험의 객관성과 검증성을 높이기 위해 같은 운영체제의 다른 제품의 방화벽 소프트를 설치한 후, 1CPU, 2CPU, 4CPU의 하드웨어를 추가하여 성능 비교 실험을 한 결과에도, 다른 방화벽제품 및 기능에 따른 1% -3%의 성능 차이 외에, CPU추가에 따르는 성능 실험의 결과값 차이는 거의 없었다.

4.4 방화벽 보안규칙 설정 전 과 후의 성능비교

K4 방화벽 성능 실험에서 방화벽 보안관리 데몬(daemon)에서의 보안규칙설정은 방화벽 패킷필터링 규칙 설정 전과 규칙 설정 후의 성능 실험을 하고, NAT 규칙 설정 후의 실험, 그리고 응용계층의 프락시 서비스 규칙설정 후의 성능실험을 하고, 이어서 사용자인증 등 인증관리 서비스를 통한 규칙설정 후의 성능실험을 통해서, 방화벽의 보안규칙 설정 전과 보안규칙 설정 후의 성능실험을 비교평가 하였다.

방화벽 보안규칙 설정에 따른 성능 실험을 하기위해, 방화벽 시스템의 기능이 정상인 것을 확인한 후, 그림 3 과 같은 실험실에서 아래(1) 환경에서 ① ② ③ ④ 의 보안 규칙을 차례로 적용 하면서 성능을 측정하였다 그러나, 여기에서의 환경 설정은 실제 업무 현장의 다양한 패킷이나 트래픽을 반영하기가 어려워, 이번에는 실제 K4 방화벽이 설치 운용되고 있는 (2) 의 현장에서 ① ② ③ ④ 성능을 측정 하였다.

실험 조건은 위의 표 2 와 같다.

(1) 실험실에서의 설정 전 후의 성능비교

① 패킷필터링 규칙설정: 규칙 설정 시 설정 전에 비해 성능 결과의 변화는 거의 없었다.

② NAT 규칙설정: ①에 더하여 주소변환(normal), 서버보안(redirect), 내부서

버(reverse) 규칙을 설정 때에 설정 전에 비해 약 1% 의 성능 결과 차이가 났다.

③ 프락시 서비스: ②에 더하여 게이트웨이, 접근통제 설정, 무결성 설정 등 규칙을 설정 때 설정 전에 비해 1%-2%의 성능차이가 났다.

④ 인증관리 서비스: ③ 에 더하여 사용자인증, 사용자 그룹의 규칙을 설정 때 설정 전에 비해 2% - 3%까지 성능차이가 나타났다.

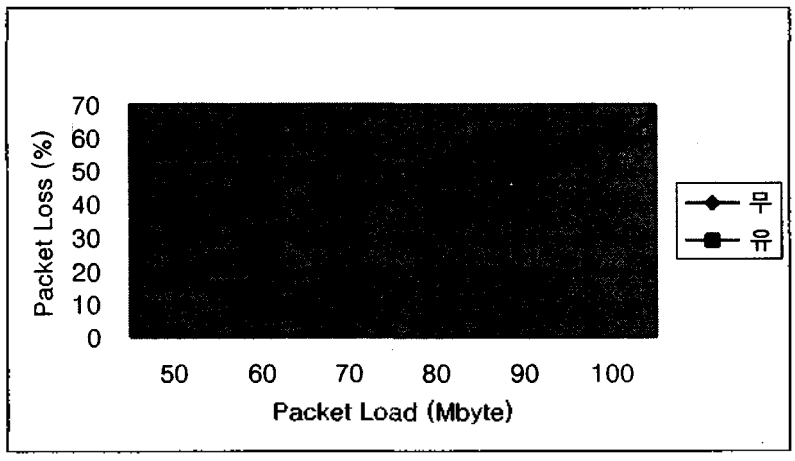
위 ① ② ③ ④의 보안 규칙을 설정한 후 실험실에서의 성능결과는 (그림 7) 과 같이 보안 규칙을 각각 50개 설정 때 규칙설정 전에 비해 약 2% -3%의 성능 차이 결과가 나왔다. 하지만 이 성능실험은 실제 업무 현장의 다양한 패킷이나 트래픽을 반영하기가 어려운 것으로 판명되어 다시 실제 업무 현장에서 성능 실험을 하였다.

(1) 실제 현장에서의 설정 전 후의 성능 비교

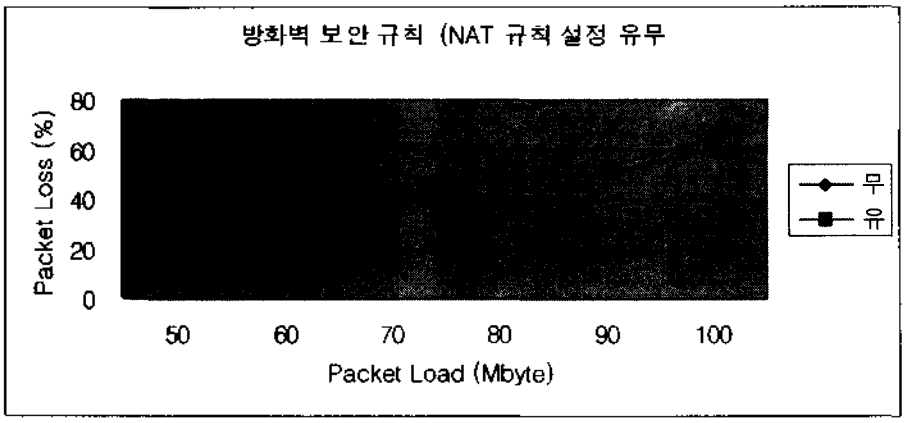
실제 업무 현장에 설치된 K4 방화벽에서의 패킷이나 트래픽을 대상으로 보안관리 데몬에서의 보안 규칙설정 전과 규칙설정 후에 성능실험에서 결과는 다음과 같았다

① 패킷필터링 규칙설정 : 50 개 규칙설정 시, 설정 전에 비해 성능 차이는 약 1% - 2% 였다.

② NAT 규칙설정 : ①에 더하여 주소변환(normal), 서버보안(redirect), 내부서버(reverse) 등의 규칙을 현장에 설정되어 있는 환경을 그대로 설정하고 실무를 감안하여 50 개 NAT 규칙 설정 때 그림 8과 같이 설정 전에 비해 약 8 -11%의 성능 차이가 났다.

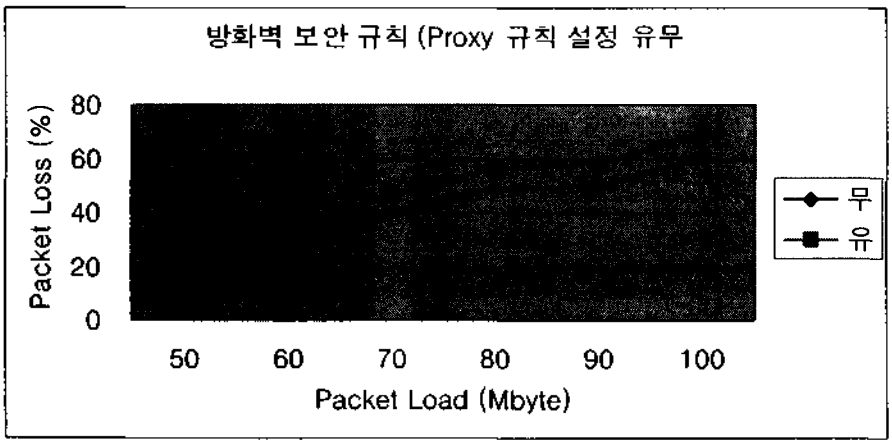


(그림 7) 보안규칙 설정 전 후의 성능 비교



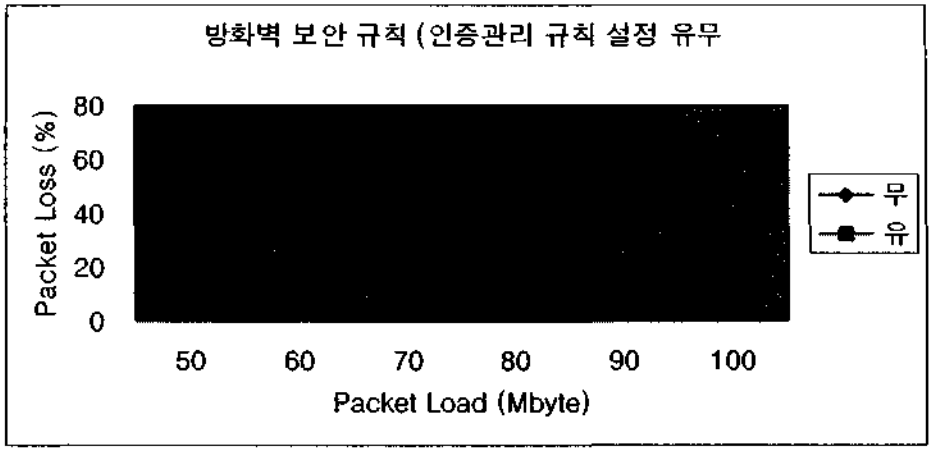
(그림 8) NAT규칙 설정 전 후의 성능 비교

③ 프락시 서비스 : ②에 더하여 게이트웨이, 접근통제설정, 무결성설정 등 프락시 규칙설정을 50 개 설정 때 그림 9 와 같이 설정 전에 비해 약 13% -16%의 성능 차이가 나타났다.



(그림 9) 프락시 규칙 설정 전 후의 성능 비교

④ 인증관리 서비스 : ③에 더하여 사용자 인증, 사용자 그룹 등 현장에 있는 인증관리 규칙 50 개 설정 때 (그림 10) 과 같이 설정 전에 비해 약 18% -20%의 성능차이가 났다.



(그림 10) 인증관리 규칙 설정 전 후의 성능 비교

5. 결론

위의 K4 방화벽의 성능비교 실험에서 나타난 결과 자료와 같이, 방화벽 소프트웨어를 인스톨하고 나서, 방화벽을 내부 네트워크 시스템의 게이트웨이로 설정 하면서부터 패킷손실율이 나타났다. 따라서, 방화벽 시스템을 채택할 때에는 일차로, 방화벽을 통과하는 네트워크의 트래픽에 대한 정확한 조사를 통하여, 향후 확장성을 고려한 최대 용량을 측정하여, 여기에 알맞은 방화벽 하드웨어 사양을 결정해야 한다는 결론을 얻었다.

또한 1 개의 CPU 를 장착한 하드웨어에서 2 개 CPU 로, 하드웨어 CPU 추가에 따른 방화벽의 성능 실험 결과는 예상 외로 성능 향상을 가져 오지 못했고, 또한 2 개 CPU 하드웨어에서 4 개 CPU 하드웨어로, CPU 를 2개 더 추가 하였을 때에도 성능 향상은 거의 없었다. 따라서 CPU 추가에 의한 하드웨어적 개선 방법은 CPU 추가에 지출되는 비용에 비해, K4 방화벽의 성능 개선에 영향을 주지 못 하였다.

또한 방화벽 보안관리 데몬에서의 패킷필터링 규칙설정 및 NAT, 그리고 프락시 서비스와 인증관리 등의 방화벽 보안규칙 설정 전과 보안규칙 50 개 설정 후의 성능비교 실험 결과에서는 보안 규칙 설정 전에 비해 실험실에서는 약 2% - 3 % 의 차이만을 보였으나, 실무현장의 성능실험에서는 패킷필터링규칙 설정 후에는 약 2% 의 성능 차이를 보였고, 추가로 NAT 규칙 중 주소변환 보다는 서버보안(redirect), 내부서버(reverse) 설정 시 약 8% - 11% 의 성능 차이가 나타났고, 위에 추가로 프락시 서비스는 13 - 16% 의 성능 차이가 나타났고, 위에 더하여 인증관리서비스의 경우에 18% - 20% 의 성능 차이를 발생하여, 응용계층에서의 서비스가 K4 방화벽의 성능을 저하 시키는 요인으로 발견 되었다.

따라서 이러한 성능 차이를 가져오는 요

인들에 대한 분석은 차 후에 좀더 연구 되어져야 하겠지만, 이 실험 결과를 놓고 분석해 볼 때, K4 방화벽의 성능개선을 위해서는, 다중 CPU 를 이용하여 패킷을 처리할 수 있는 패킷처리에 관한 운영체제와의 효율적 연구 개발방안과 함께 NAT 에서의 엔진 설계 부분의 개선 및 프락시 서비스의 엔진들에 대한 모듈 및 효율화 방안의 강구 그리고, 한 걸음 더 나아가 하드웨어와 운영체제 및 소프트웨어가 정보보호 제품 전용으로 통합된, 통합형 방화벽 시스템에 대한 설계 및 연구개발이 필요하다.

특히 차세대의 대용량 초고속 인터넷의 추세에서는 보다 근본적인 방화벽 내부의 패킷 속도를 향상시킬 수 있는 기가비트 (GigaBit) 방화벽에 대한 연구 및 개발을 통해서 세계 속에 뛰어난 품질을 가진 우리나라 방화벽의 성능개선이 이루어져야 하겠다.…

참고문헌

[1] 김명주, Security Expert, 영진닷컴, p 14-15, 2002.3.

[2] 정보통신부 고시, http://www.mic.go.kr/정보보호시스템평가 인증지침, 정보통신부, 2002.8.

[3] 정보통신부 고시, 정보통신망 침입차단시스템 평가기준, 정보통신부, p 1 -2, 2002.2.

[4] 정보통신부 고시, http://www.nis.go.kr/, 정보보호시스템공통평가기준; 정보통신부, 2002.8.

[5] 김재헌, 조자영, K4E 방화벽의 보안기술, 정보처리 제9권 제1호, 2001.1.

[6] 박창섭, 암호이론과 보안, 대영사, 1999.2.

[7] 김재성, 홍기용, 감학범, 심주결, 침입차단시스템을 위한 강제적 접근통제법설계, 한국정보처리학회,제5 권 제4호, 1998.4.

[8] 한국정보보호진흥원, 정보보호개론, 교우사, p 32-33, 2000.7.

[9]IETF, http://www.ietf.org/rfc/rfc 2401, 2402, 2406, 2408 .txt , Network Working Group Request for Comments 1998.11.

[10] ISTF -003, Implementation Technology for secure VPN in IP Layers, 인터넷보안기술포럼, 2001. 5.

[11] 최준호, 김판구, 네트워크상에서의 바이러스 차단을 위한 방화벽시스템의 설계 및 구현, 정보처리학회 논문지 C 제8-C권4호, 2001.8.

[12] 이준택, 배민호, 박미영, Securing Network & Building Firewall, 가남사, p281-283, 2002.4.

[13]한국정보보호진흥원, http://www. kisa.or.kr/, 평가체계, 시험평가, 평가인증제품현황, 2002.11.

[14] 한국정보보호진흥원, http://www.kisa.or.kr/, Test LAB3, 방화벽성능 실험실, 2002.5- 2002.11.

저자 소개

박 대 우

1987년 서울시립대학교 경영학과(학사)
1995년 숭실대학교 컴퓨터학부 전산부전공
1998년 숭실대학교 컴퓨터학과(석사)
2002년 숭실대학교 컴퓨터학과(박사수료)
1987년 동구여상 정보처리,정보통신 교사
2000년 Entrust-Korea 연구소 부소장
2000년 매직캐슬정보통신 부사장/연구소장
관심분야: 정보보안, 인터넷보안, 정보보호제품, 무선방화벽, IMT-2000보안, 위성통신보안, Cyber Reality,

전 문 석

1980년 숭실대학교 전자계산학과(학사)
1986년 University of Maryland Science(석사)
1989년 University of Maryland Science (박사)
1989 Morgan State Univ. 부설 Physical Science LAB. 책임연구원
1991년- 숭실대학교 컴퓨터학부 정교수
관심분야: 병렬처리, 암호화알고리즘 설계 및 분석, 정보보안, 인터넷보안, 침입차단 및 탐지 시스템 보안