Solaris K4 방화벽에 대한 기능별 운영체제(32비트, 64비트)별 성능비교 연구

정회원 박 대 우*

A study on performance evaluation for Solaris K4 Firewall by functions and operating systems(32bit, 64bit)

Dae-Woo Park* ***Regular Member***

요 약

국가정보원에서 방화벽(Firewall)의 인증을 하고 있고, 여기에서 K4 등급을 받은 방화벽이 모든 공공기관에 설치되고 있다. Solaris를 운영체제로 하는 K4 방화벽의 기능에서 패킷필터링과 NAT, 프락시 및 인증서비스 기능 등에 관해 기능 설정 전과 기능 설정 후의 성능을 비교 평가한다. 그리고 기존 32비트 체제 방화벽성능에 비해 최근 인증을 받고 있는 64비트 체제의 Solaris 방화벽을 비교 평가하여, 32비트에 비해 64비트 체제의 방화벽이 2배 이상 성능 개선이 나타남을 평가한다. 그리고, 결론에서 K4 방화벽 및 대한민국 방화벽의 연구 및 개발에 방향을 제시하여 세계에서 경쟁력있는 시스템으로 도움이 되고자 한다.

Key Words : Firewall; K4; 32bit; 64bit; Information Security.

ABSTRACT

Korea National Intelligence Service has been issued on K4 Firewall Certificates, and these K4 Firewalls has been installing all Korean public organizer. I would evaluate the performance tests between the before setting and the after setting of Packet Filtering, NAT, Proxy, and Authentication services on functions of Solaris K4 Firewall System. Also I had been created by performance test between existing 32 bit and latest 64 bit K4 Firewall System on Solaris Operating System, So that the result of improved more two times passed rate on 64bit than 32bit on Solaris K4 Firewall System, At finally, I would conclude that the change direction will be useful for research and development on K4 Firewall System and Korean Firewall System which is a very competitive system in the world.

Ⅰ. 서 론

국내 인터넷 사용자는 2002년 12월 기준으로 인터넷 이용자수는 2,627만명(이용률 59.4%)로 2002년 6월의 2,565만명(58.0%)에서 62만명(1.4%)이 증가[1]하였다. 인터넷 사용자는 매년 증가하지만, 정보화의 역기능으로 인한 정보보호 침해사고도 매년 증가하여, 접수된 국내 침해사고도 2001년 5,333건이 발생했고, 2002년 1월부터 11월까지의 침해사고 접수도 13,127건으로 접수[2] 되고 있다. 이와 같이 불법적으로 정보를 취득하여 타인에게 해를 주거나, 네트워크 시스템을 손상하거나, 네트워크

*승실대학교 컴퓨터학과 통신연구실 (prof1@hanmail.net)
논문번호030054-0130 접수일자2003년 1월 30일

시스템에 장애를 유발하는 것이 침해사고이며, 정보보호 목적 중에 하나가 이들 사고로부터 정보자원을 안전하게 지키는 것이다. 이 목적을 달성하기 위한 대표적인 정보보호시스템 중의 하나가 방화벽 시스템 이다. 방화벽은 허가 또는 인증되지 않거나 비정상적인 사용자가 침입하는 것을 차단할 수 있다. 방화벽시스템은 외부와 방화벽 내부 네트워크의 연결하는 유일한경로(gateway)나, 혹은 중요한 정보 전송의 유일한 전송로에 설치되어, 방화벽시스템을 통과하는 통신 및 서비스를 감시하며, 허용되지 않는 침입을 차단한다.

본 논문에서는 현재 국가정보원에서 인증을 받아 모든 공공기관에서 사용하고 있는 K4 이상의 등급을 받은 방화벽[3] 중 범용적으로 사용되는 Solaris를 운영체제로 하는 방화벽의 성능을 비교 평가한다. K4 방화벽의 기능 중, 패킷필터링(Packet Filtering)과 NAT(Network Address Translation) 및 프락시(Proxy) 및 인증(Authentication) 서비스 기능이 네트워크 보안 정책에 따라 설정된 보안규칙설정에 따른 성능평가에서, 기능 설정 전 성능에 비해, 기능 설정 후에 얼마만큼의 방화벽 성능에 지연을 나타나는가를 비교 평가한다. 그리고 기존 사용되어오던 Solaris 32비트 체제 방화벽성능에 비해 최근 인증을 받고 있는 Solaris 64비트 체제의 방화벽 성능이 얼마만큼의 성능 개선효과가 나타났는가를 비교 평가한다. 그리고, 결론에서는 이러한 자료를 토대로 하여 앞으로 연구 개발될 및 국가정보원의 K4 방화벽 및 우리나라 보안시장의 대표가 되는 인증방화벽의 성능 개선에 도움이 되는 개선 방향을 제시 하여 세계적인 정보보호 제품으로써의 국내방화벽 기술의 우수성을 만드는 계기가 되고자 한다.

Ⅱ. 관련연구

1. 방화벽의 인증체계

대한민국에서의 방화벽은 제품명으로는 침입차단시스템이며, 이러한 정보보호제품으로써 정부차원의 인증은 국가정보원에서 시행하고 있다. 침입차단시스템에 대한 국가정보원에서 인증기준은 1998년 2월에 제정되었으며, 인증평가는 정보화 촉진 기본법 제15조를 근거로 하고 있다. 그 후, 몇 차례의 개정을 하여 현재 2002년 8월 5일 정보보호시스템 평가인증지침(정보통신부고시 제2002-41호)으로 개정[4] 되었다.

침입차단시스템 평가기준은 보안기능의 신뢰성을 확인하기 위한 보증요구 사항으로 개발과정, 시험, 형상관리, 운영환경, 설명서, 취약성의 6가지 사항으로 이루어 진다. 국가 정보원의 침입차단시스템 평가등급은 K1 등급을 최저단계로 하고, K2, K3, K4, K5, K6 그리고 K7를 최고 단계로 하여 총 7단계로 구분하는데, 국가 및 관련 공공기관에 설치 하기 위한 방화벽은 일반적으로 K4 등급 이상의 인증을 받은 방화벽을 채택하고 있다. 이 때 침입차단시스템을 통하여 전송되는 데이터를 암호화하여 기밀성 기능이 제공되는 경우에는 각 평가 등급에 E(Encryption) 자를 붙여서 K1E, K2E, K3E, K4E, K5E, K6E, K7E로 표기[5]한다.

국가정보원에서는 2002년 7월 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 공통평가기준을 적용하여 정보보호 제품에 대한 보안 인증평가를 실시 하려고 하고 있다. 정보보호제품의 보증수준을 정하기 위한 공통평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7의 7개의 등급으로 구분된다. EAL1은 최저의 평가 보증 등급이고, EAL7은 최고의 평가 보증 등급[6]이다.

2. K4방화벽의 기능

현재 사용되는 K4 인증 침입차단시스템의 형태는 조금씩 다르나, 정보통신망 침입차단시스템 평가기준

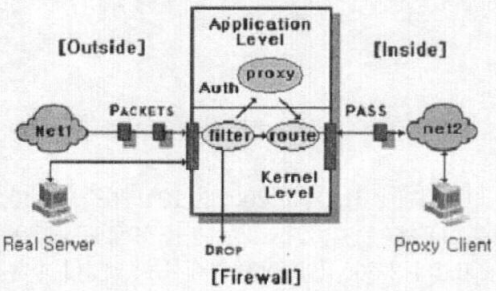

그림 1 하이브리드 방식
fig. 1 Hybrid type

에 의해 개발되며, 일반적인 모델은 그림 1과 같이 하이브리드(Hybrid) 방식에다가 상태정밀검사방식(Stateful Inspection)[7]을 도입하고, 여기에 VPN(Virtual Private Network)기능을 강화하여 사용하고 있다.

이러한 K4 인증 방화벽의 기능들을 크게 나누어 보면 다음과 같다.

1) 패킷필터링 기능

방화벽에서는 패킷필터링 규칙을 설정하고, 이를 위반하는 패킷에 대해 접근 통제를 실시한다. 3계층인 네트워크층(Network Layer)의 IP(Internet Protocol)의 헤더(header)와 4계층인 전송층(Transport Layer)인 TCP(Transmission Control Protocol), UDP(User Datagram Protocol)를 통해 패킷의 출발지 및 목적지, 서비스 포트(port) 번호 등을 이용하여 접근통제를 하게 된다. 이때 임의적 접근통제(DAC: discretionary access control) 는 네트워크 단계에서 패킷필터링의 일괄적인 접근통제를 할 수 없는 부분에 대해, 보안관리자가 각각의 게이트웨이 별로 특성에 따른 접근통제를 실시하는 것이며, 강제적 접근통제(MAC: mandatory access control)는 주체 및 객체의 보안레이블이 객체의 보안 레이블보다 높거나 같을 경우에 접근을 허용[8]하는 것이다. 따라서 보안관리자는 네트워크 보안정책에 따라 패킷필터링 규칙을 설정하여 비 인가자의 침입을 차단한다.

2) NAT 기능

방화벽의 특정한 네트워크 인터페이스 카드를 거쳐서 전송되는 패킷을 검사하여 지정된 IP와 목적포트를 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. 보안관리자는 Ipv4의 사용에 따른 부족한 IP의 부여 와 내부적 관리 및 보안을 위한 네트워크 시스템들의 그룹 관리를 위해 NAT 기능을 설정을 하고 있다.

3) 프락시 및 인증 기능

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

프락시 기능에 대한 접근 및 허용에 대한 인증은, 방화벽을 통과하는 모든 접속에 대한 식별 및 인증에 이용되는 사용자에 대한 인증 그리고, 보안관리자에 대한 인증 및 사용자그룹에 대한 인증정보가 있다. 방화벽에서의 내용에 대한 암호화와 함수는 정보보호 서비스의 하나로, 인증 시 패스워드에 관한 암호화 도구로는 S/Key 등이 있으며, 전송 내용에 대한 암호화는 RSA, 3DES, CAST, Bluefish, Twofish 등[9]이 있고, 무결성 체크에 대한 암호화는 MD5, SHA-1 등[9]을 사용한다.

4) 무결성(Integrity) 및 전송무결성(VPN)

무결성은 데이터의 내용이 정당하지 않은 방법에 의하여 변경 또는 삭제되는 것을 방지하는 서비스이다. 방화벽 내에 비전송 무결성기능은 선택한 영역에 대한, 운용환경 설정 환경DB 및 관련 보안자료에 대한 추가, 수정 삭제 등이 발생 하였는가를 감시 하기 위해, 일정한 주기별로 파일이 변경 되었는가를 체크 하여 위반한 사항에 대해 보안 관리자에게 통보한다. 방화벽에서 전송 데이터에 대한 무결성은 VPN기능을 도입하여 사용하며, 이런 과정을 거쳐, 데이터의 변조 및 손실에 따르는 보안성을 높이며, 네트워크 계층에서의 VPN 터널링 방식인 IPSec 과 IKE 표준[10]을 적용 하여 양 종단 간의 안전한 통신을 지원한다. 이때 IP 계층을 기반으로 하여 터널모드 AH(Authentication Header), 트랜스포트모드 AH, 터널모드 ESP (Encapsulation Security Payload), 트랜스포트모드 ESP의 4가지 형태로 보안성을 제공[11] 하며, 어플리케이션[12]에서도 무결성, 비밀성, 송신자 인증 기능을 제공하여 사용자에게 투명한 정보전송을 제공한다. 최근 VPN은 정보보호제품의 한 항목으로 분리해서 인증을 받게 될 것이다.

5) 관리 및 감사(Auditing) 기록기능

침입차단시스템은 통과하는 모든 송수신 트래픽에 대해 로그 파일(log file)을 기록 할 수 있다. 이 로그 파일에는 날짜, 사용시간, 사용자, 기록형태, 호스트(host), 서비스, 중요도, 사건형태 등을 기록하며, 이 기록을 토대로 한 감사기록 및 추적관리를 한다.

그리고 방화벽의 보안 관리자에게 침입이 발생하여 설정된 위험사항에 위배되거나 감사기록장소 소진 한도가 되면 E-mail이나 단문메시지 서비스 등을 이용하여 실시간으로 보안관리자에게 경보를 해준다. 보안 및 통계의 편리성을 위해 사용자 별 패킷 전송량 조회, 저장된 메일의 내역조회, 보안관리

자의 메일주소설정, 감사기록 장소관리, 보안데이터 및 감사기록 관리 기준설정 등을 제공하여 보안관리자에게 보안 기능 과 정책을 수행할 수 있도록 하는 관리자메뉴가 있다.

이들 K4 방화벽의 기능 설정에 대한 내용과 방법은 각 네트워크 시스템의 환경에 따라 다르다. 일반적으로 보안관리자는 각 네트워크 보안 정책에 따라 패킷필터링과 NAT, 프락시 및 인증관리 서비스에 대한 보안 관리규칙을 설정하며, 설정방법도 네트워크 상태 및 보안의 강도에 따라 수시로 변화시킬 수 있다.

그리고, 무결성은 중요파일에 의무적으로 설정되며, 전송무결성은 원거리에 떨어져 있는 네트워크 사이에서 설정되고, 관리 및 감사기록기능은 보안규칙설정에 따른 방화벽의 패킷로그 기록의 처리에 따른 상태와 결과에 대한 자료이다. 따라서 기능별 성능 비교 시에는 무결성, 전송무결성과 관리 및 감사기록기능을 제외한 패킷필터링과 NAT, 프락시서비스 및 인증관리에 따른 성능비교를 실시한다.

3. K4방화벽의 운영체제

K4 방화벽의 기능 평가는 한국정보보호진흥원(KISA: the Korea Information Security Agency)에서 담당하고 있다. 2003년 1월 27일 현재 평가 인증 후, 사용 중 이거나, 평가인증 중인 K4 인증 등급 이상의 침입차단시스템의 운영체제는 UNIX 계열의 Solaris 와 X86, IBM- AIX, HP-UX, 그리고 Windows 계열의 NT, Windows2000, XP 등[13]이 있다.

현재 범용적으로 사용되는 침입차단시스템의 운영체제인 UNIX 계열의 Solaris K4 방화벽은 32비트 체제와 64비트 체제로 나누어 볼 수 있다. 즉, Solaris 2.5.1과 Solaris 2.6, Solaris 2.7 까지를 32비트 체제로 분류해 볼 수 있고, Solaris 2.8부터는 64비트 체제로 분류해 볼 수 있다. 위의 분류에서 Solaris 2.7을 32비트 체제와 64비트 체제로 혼용 작동시킬 수 있다고는 하나, 성능면에서의 정확성을 위해 Solaris 2.7을 성능 실험 비교 대상에서 제외 하였다. 그리고 Windows 계열은 아직 32비트 체제에 머물러 객관적인 성능 비교가 어려워 성능 실험 비교 대상에서 제외 하였다.

표 1은 2003년 1월 27일 Solaris K4 인증 방화벽 및 운영체제를 나타낸 것이다.

표 1 Solaris K4 방화벽 및 운영체제
fig. 1 Solaris K4 Firewall & Operating System

K4인증	평가제품명 및 버전	운영 체제
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
	SecureWorks V2.0	Solaris 2.7
	수호신 V3.0	Solaris 7 for X86
	매직캐슬 V1.0	Solaris 2.5.1
	수호신 V3.0	Solaris 2.7
	SecureWorks V3.0	Solaris 8 for x86
	SecureWorks V3.0	Solaris 2.8
평가진행	MagicCastle V3.0	Solaris 2.8
	EzoneWall-PlusV1.0	Solaris 8 for x86

4. Solaris K4 방화벽의 32비트와 64비트 차이점

현재 K4 인증 방화벽 중 운영체제가 Solaris인 방화벽은, 하드웨어에다 32비트 운영체제나 64비트 운영체제를 인스톨하고, 그 위에 방화벽 소프트웨어가 설치되어 방화벽 단독 기능만을 수행하는 정보보호시스템으로 운용되고 있다. 여기에서 성능 분석 대상이 되는 Solaris 운영체제는 32비트 체제에서 64비트 체제로 발전하면서, 크게 다음과 같은 3가지 차이점[14]을 개선 하였다.

첫째는 확장된 정밀도 (Extended Precision)

둘째는 확대된 데이터 집합체 지원 (Large Dataset Support)

셋째는 큰 가상주소 공간 (Large Virtual Address Space) 이다.

즉 기존 32비트 운영체제에 비해 정수 연산 성능과 실수 연산 처리가 64비트로 처리하면서 수학계산의 정밀성이 확장되었고, 64비트의 비동기적 입출력을 지원한다. 또한 부족한 메모리를 500 기가바이트 이상 1 테라바이트(Terabyte)까지 확장된 메모리를 통하여 대량의 데이터 집합체의 처리를 지원하여, 데이터 접근속도 향상 및 파일을 생성하는 데 걸리는 시간을 10배정도 향상시켰으며, 애플리케이션의 대형 복수 페이지 사용을 허용해 자원 효율성이 개선되고 오버헤드가 감소했다. 그리고 RM(Resource Manager)의 사용은 개선된 시스템 자원 할당 및 모니터링, 컨트롤 기능을 제공한다. 또한 쓰레딩 라이브러리 개선을 통해 Java 기반 애플리케이션 등을 처리하는 확장성과 성능을 개선하였고, RSMAPI(Remote

Shared Memory API) 클러스터 인식 에플리케이션이 클러스터링된 구성에서 이벤트에 응답하는데 소요되는 시간을 줄이고, NCA(Network Cache and Accelerator) 의 HTTP 요청에 액세스되는 웹 페이지의 인커널 캐시를 유지해 웹 서버 성능을 높였다. 또한 인터넷 키 교환(IKE)을 이용한 IPsec 은 서버와 통신 채널 간의 보안성을 높여 인가된 당사자만이 128bit로 암호화된 통신을 할 수 있게 한다.

이러한 64비트 운영체제의 개선된 성능의 우수성에도 불구하고 단점으로는 유닉스시스템 관리 방법의 한계에서 나오는 운영체제 및 보안정책 차원에서 root로 바로 접속이 되지 않게 하거나 telnet, ftp, rlogin등의 해당 데몬(daemon) 들을 제거하여 허가받지 않는 사용자들의 운영체제의 접속을 하지 못하게 한여야 한다. 특히 운영체제에 얹는 방화벽의 특성상 네트워크와 네트워크 사이의 유일한 연결통로(gateway)가 되어야 하므로 라우팅 테이블이나 방화벽 소프트웨어에 대한 관리자의 주기적인 보안관리가 요구되는 보안정책이 필요하다. 지금까지 K4 방화벽 소프트웨어 개발에서, 절차적(procedural) 언어로 구현되어있는 구조적 기법에 의한 프로그램의 수행은 함수나 서브 프로그램 단위로 순차적이면서 지역성을 잃지 않고 진행된 경우가 보통이었다. 이 경우에 반복적으로 참조되는 성질을 이용한 메모리 캐시의 적중률이 높아져 효율적이었다. 그러나 객체 지향 기법에서의 프로그램은 평면적, 병렬적으로 수행되는 성질이 강하여 페이지 폴트(page fault)의 빈도가 높아지고, 이는 페이지 교체와 메모리 캐시의 실패율 증가로 연결되어 CPU의 성능을 낮추는 결과를 가져온다. 이때 32비트 프로세서가 2단계 페이징(paging)을 갖는다면, 64비트 프로세서는 3단계 페이징 능력[15]을 갖는다. 따라서, 이론적으로 18exebytes까지 메모리의 확장이 가능한 64비트 프로세서는 요구 페이징의 부하를 현격하게 감소시킬 수 있어, 충분한 메모리의 활용과 CPU성능의 개선 효과가 64비트 방화벽 소프트웨어에 성능개선 효과를 제공하는 것이다. 아래의 표 2에서 Solaris 각 플랫폼(Platform)에 의한 하드웨어 MMU (Management Memory Unit)에서의 HAT (Hard Address Translation)단계 수행 능력을 보여 주고 있다.[16]

표 2 Solaris 메모리관리장치에서의 HAT 수행능력
table 2 Solaris MMU HAT implementations

Platform	No. of Contexts	Size of TLB	TLB Fill	Virtual Bits	Physical Bits
SPARC 1,2	8	64	Hardware	32	32
Micro SPARC	65536	64	Hardware	32	32
Super SPARC	65536	64	Hardware	32	36
Ultra SPARC I, II	8192	64 x 2	Software	44	41
Intel Pentium	-	-	Hardware	32	36

여기에서 64비트 체제의 Ultra SPARC I, II가 다른 플랫폼에 비해 TLB(Translation Look aside Buffer)에서 2배의 크기를 가지고, 44비트의 가상주소와 41비트의 실제주소를 사용하여 성능을 개선 시킨 것으로 나타난다. 여기에서 Solaris K4 64비트 방화벽은 32비트 메모리 어드레싱(Memory Addressing)을 64비트 메모리 어드레싱으로 활용하여 프로세서, 어플리케이션, 운영체제 등에서 메모리를 테라 바이트 수준까지 활용할 수 있는 능력을 가졌지만, 국내 방화벽 소프트웨어 개발은 64비트 어드레스 공간을 처리하지 못하고 있고, 실제 K4 64비트 방화벽에서의 각 기능에 대한 소프트웨어적인 모듈단위의 활용도에 대한 64비트 처리 체제로의 완전한 전환은 아직 이루어 지지 않고 있다.

Ⅲ. K4방화벽의 성능 평가 방법

현재 평가 인증 중 이거나 인증 후 사용중인 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 하드웨어와 함께 운영체제로 시스템을 구성한다.

1. 성능 평가 장비 및 프로그램 구성

K4 방화벽 시스템 평가에 쓰이는 하드웨어는 SUN Ultra 80에 1CPU와 메인 메모리 1024Mbyte, 32Giga 하드디스크에 32비트 운영체제로 Solaris 2.5.1을 설정하고, 64비트 운영체제로 Solaris 2.8을 설치하고,

각각에 K4인증을 받은 침입차단시스템 소프트 웨어를 설치하여 가동하고, 방화벽의 기능에 이상이 없는지를 실험한다.

기능에 따른 성능 비교 평가를 위해서는 안정성이 검증된 32비트 운영체제에서 평가하고, 운영체제에 따른 비교 평가에서는 32비트와 64비트를 차례로 설치 성능평가를 한 후 값을 비교 하였다. 성능평가는 방화벽 성능 평가 장비인 Smart비트-2000에서 패킷 생성 툴(Tool)인 Smart TCP 이용하여 네트워 트래픽(Network Traffic)을 발생시켰고, 성능 측정 프로그램은 Smart Applicat을 이용하여, TCP Flow를 발생시켜서 성능실험을 하였다.
성능 실험을 위한 방화벽 성능 실험에 대한 배치는 현장마다 다르나, 기본 형태의 현장배치는 그림 2와 같이 되어있다.

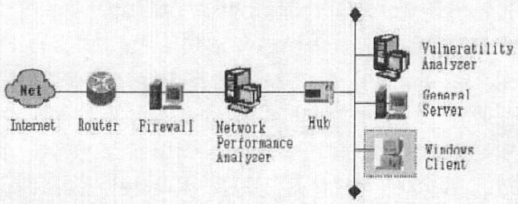

그림 2 방화벽 성능실험 배치도
fig. 2 firewall test arrangement

2. 성능 평가 조건 및 방법

성능 평가를 위한 실험조건으로 하드웨어에 운영체제를 설치 한 상황에서 K4 방화벽 소프트웨어를 인스톨하고, 방화벽 기능에 이상 없는지를 확인한 후, 전송부하에 대한 성능실험을 하였고, 방화벽에 대한 기본 보안 정책은 다음과 같다.

Any_in(내부) —— Any anyTCP, anyUDP, Ping 허용
Any(외부) —— Any_inanyTCP, anyUDP, Ping 허용

평가 방법은 방화벽 기능에 대한 성능실험에서 128Byte를 한 방향 전송으로 할 때, 전송부하(packet load)를 50Mbyte에서 100Mbyte까지 실어 보낼 때 패킷손실율(packet loss)을 측정한다. 패킷손실율에 대한 성능실험조건은 다음 표 3과 같다.

표 3 패킷손실율 실험조건
Table 3 test condition of packet loss

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

방화벽 기능에 따른 성능 실험을 하기 위해 40군데 이상의 현장에 대한 보안규칙 설정을 조사한 바, 각각의 내부 시스템과 조직의 특성상 보안규칙 설정의 방법 및 보안규칙 설정의 개수와 규칙 종류도 다양 하였으나, 평균 50개 미만이 대부분인 것을 감안하여 50개로 기준을 설정하였다. 각 보안규칙의 설정내용은 현 실무에서의 적용규칙을 그대로 적용하고, 현장의 보안관리자 의견을 최대한 반영하였다.

32비트와 64비트의 운영체제별 성능평가 실험에서는 K4 방화벽의 기능 중, 패킷필터링과 NAT, 프락시 및 인증서비스 기능을 모두 적용한 후, 패킷의 프레임 사이즈(Frame Size) 별로 패킷손실율을 측정 하는 성능실험을 하였다. 즉 성능실험장치를 통해 128byte, 256byte, 512byte, 1024byte, 1280byte, 1518byte의 프레임 사이즈를 가진 전송부하를 100Mbyte로 생성하여 네트워크 트래픽(Network Traffic)을 발생시키고, 이를 32비트와 64비트의 각각 K4방화벽에 대하여 한 방향 전송을 시행하고, 이를 5회 반복하여 패킷전송율(Pass rate)을 산출한 후 평균 값을 계산하여 네트워크 처리율(Passed Rate)을 비교하였다. 실험 조건은 표 4와 같다.

표 4 네트워크 처리율 실험조건
Table 4 test condition of Passed Rate

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

Ⅳ. K4방화벽의 성능 비교

1. K4방화벽의 기능별 성능 비교

업무 현장에 설치된 K4 방화벽에 보안 규칙을 설정하지 않고, K4방화벽 시스템을 내부 네트워크 시스템들의 게이트웨이로 설정하자 설치된 K4 방화벽에 패킷손실율이 발생하였다.
K4 방화벽의 보안관리 데몬(demon)에서 보안 규칙설정 전과 규칙설정 후에 성능 비교 실험에서 결과는 다음과 같았다.

1) 패킷필터링 규칙설정 : 보안관리 데몬에 각 방화벽의 설정된 현장의 보안 규칙에 맞게 50개 규칙 설정 시, 설정 전에 비해 패킷손실율의 차이는 약

1%-2% 이었다.

2) NAT 규칙설정 : 1)에 더하여 주소변환(normal), 서버보안(redirect), 내부서버(reverse) 등의 규칙을 현장에 설정되어 있는 환경을 그대로 설정하고 실무를 감안하여 50개 NAT 규칙 설정 때, 그림 3과 같이 서버보안 및 내부서버 설정 시에 설정 전에 비해 약 8-11%의 패킷손실율의 차이가 났다.

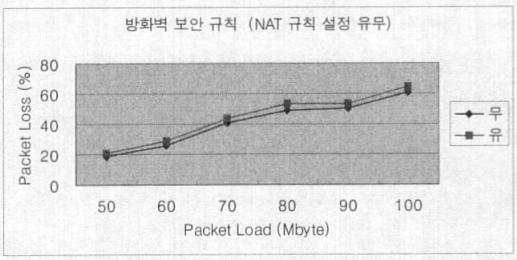

그림 3 NAT규칙 설정 전과 후의 성능 비교
fig. 3 performance before vs after NAT rules

3) 프락시 서비스 : 2)에 더하여 게이트웨이, 접근통제설정, 무결성설정 등 프락시 규칙설정을 50개 설정 때 그림 4와 같이 설정 전에 비해 약 13%-16%의 패킷손실율 차이가 나타났다.

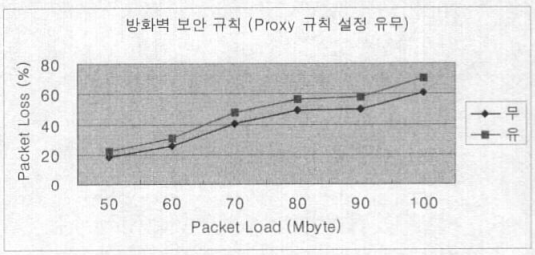

그림 4 프락시 규칙 설정 전과 후의 성능 비교
fig.4 performance before vs after Proxy rules

4) 프락시의 인증관리 서비스 : 3)에 더하여 사용자인증, 사용자 그룹 등 현장에 있는 인증관리 규칙 50개 설정 때 그림 5와 같이 설정 전에 비해 약 18%-20%의 패킷손실율 차이가 났다.

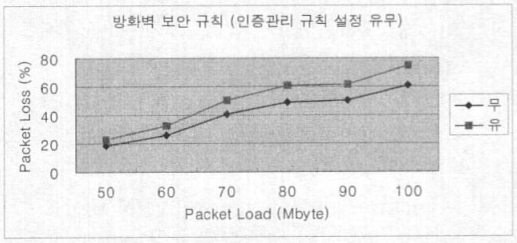

그림 5 인증관리 규칙 설정 전과 후의 성능 비교
fig. 5 performance before vs after Authentication rules

2. 32비트와 64비트 성능 평가

방화벽 설치전과 설치 후의 성능 실험의 결과 그림 6과 같이 128byte 한 방향 초당 트래픽 전송율은 32비트 체제는 70.31%, 64 비트 체제 에서는 97.69 %의 차이를 보였다. 256byte 성능 측정 에서는 초당 트래픽 전송율은 32비트체제는 87.62%, 64비트체제에서는 98.75%의 차이를 보였다. 그러나 512 byte 이상 에서는 99.81% 이상을 보여 하드웨어에 운영체제만 인스톨 시에 성능 차이는 작게 나타났다.

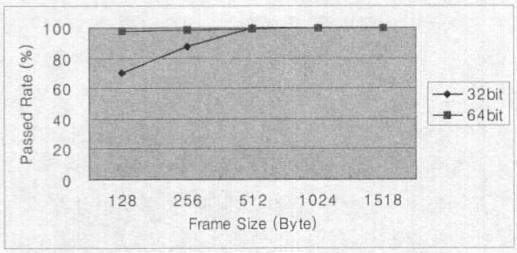

그림 6 방화벽소프트 설치 전 32비트와 64비트
fig. 6 performance 32bit vs 64bit before install Firewall S/W

K4 방화벽 시스템을 구축 후에 K4 방화벽 기능을 적용한 후의 성능평가 실험에서는 위 그림 7과 같이 32비트체제의 방화벽에서 성능 실험 결과는, 128byte에서 4.37%, 256byte에서 12.50%, 512byte에서는 19.37%, 1024byte에서는 25.61%, 1518byte에서는 27.49%의 네트워크 처리율을 보였으며, 64비트 체제의 방화벽에서는 128byte에서 30.67%, 256byte에서 56.97% 의 네트워크 처리율을 보였으며, 512byte이상의 패킷 크기에서는 패킷손실율이 적은 네트워크 처리율이 측정되었다.

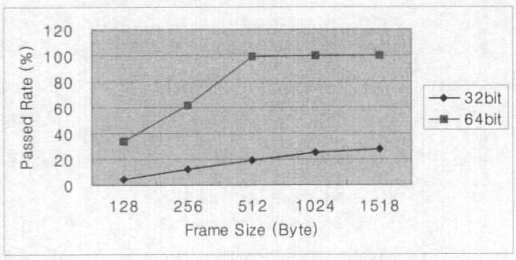

그림 7 32비트와 64비트 방화벽 성능 비교
fig. 7 performance 32bit vs 64bit of firewall

V. 결 론

위 Solaris K4 방화벽의 성능평가 실험결과에서, 방화벽시스템을 설치한 후 이를 내부 네트워크 시스템들에 대한 게이트웨이로 설정 하면서 패킷손실율이 발생한다. 따라서, 방화벽 시스템을 채택할 때에는 일차로, 방화벽을 통과하는 네트워크 트래픽량에 대한 정확한 조사와 함께, 조직의 보안정책 및 보안등급 그리고, 향후 확장성을 고려한 최대 용량을 측정하여, 여기에 알맞은 방화벽 하드웨어와 소프트웨어 사양을 결정해야 한다는 결론을 얻었다.

Solaris K4 방화벽 기능에 따른 실무현장의 성능실험에서, 패킷필터링 규칙설정 및 NAT, 그리고 프락시 및 인증서비스에 대한 기능설정 전과 보안규칙 50개 설정 후의 성능비교 실험 결과에서는 패킷필터링규칙 설정 후에는 약 1%-2%의 패킷손실율을 보였고, 추가로 NAT규칙 적용 중 주소변환 보다는 서버보안과 내부서버 설정 시 약 8%-11%의 패킷손실율이 나타났다. 거기에다 추가로 프락시 서비스에서는 13%-16%, 인증관리 설정 때 약 18%-20%의 패킷손실율이 나타나, K4 방화벽의 응용계층에서의 서비스가 방화벽의 성능을 저하 시키는 요인으로 발견 되었다.

또 기존의 32비트 체제의 Solaris K4 방화벽인 침입차단시스템과 Solaris 64비트 체제의 성능비교 실험의 결과에서 산출된 평균 값을 비교한 결과, 네트웍처리율에서 32비트체제에 비해 64비트 체제의 방화벽이 두배 이상의 성능개선이 이루어졌음을 알았다. 따라서, 당분간 국가정보원의 K4인증을 받은 64비트 체제의 방화벽이 주로 사용되어질 것으로 여겨진다.

현재 방화벽이 하드웨어와 운영체제 및 소프트웨어 각각으로 이루어진 하나의 시스템이란 점에서 Solaris 64비트 방화벽의 성능개선이 이루어진 기능 및 내용별 비교 결과의 분석은 향후 소스분석과 함께하는 성능분석으로 연구 되어져야 하겠다.

그리고, 차 후 인증되는 방화벽의 정보보호서비스 및 보안기능의 연구개발 시에는, Solaris 64비트 체제의 CPU 프로세서와 메모리 및 운영체제를 효율적으로 활용하여, 다중 패킷을 동시에 처리 할 수 있는 방법들이 연구 개발 되어야 하며, 또한 성능저하의 원인으로 밝혀진 응용계층에서의 너무 복잡한 서비스를 줄이고, 패킷필터링 부분에서의 필터링 모듈화와 운영체제의 일체화를 통한 보안기능의 강화가 기능개선의 한 방법이 될 것이다.

더욱이 다양한 멀티미디어 데이터의 전송에 따른 초고속 인터넷환경으로의 변환과, 대용량 트래픽을 감안할 때 기가비트(Gigabit) 방화벽에 대한 연구와 개발이 시급해 보이며, 특히 방화벽시스템의 내부에서도 하드웨어와 운영체제 및 방화벽소프트웨어가 하나로 통합된 전용방화벽시스템으로의 일체형 방화벽에 대한 연구개발이 세계와 경쟁할 수 있는 우수한 정보보호 제품으로써 대한민국 방화벽 기술의 우수성을 입증할 것으로 보여진다.

참 고 문 헌

[1] 한국인터넷정보센터, 2002년12월 *인터넷통계월보*,KRNIC, p2, 2002.12.

[2] CERTCC-KR통계, http://www.certcc.or.kr/, 2002. 11.

[3] 정보보호시스템인증제품, 평가인증제품현황, http://www.nis.go.kr/kr/security/info119/ product.html, 국가정보원 , 2002.11.

[4] 정보통신부고시, http://www.mic.go.kr/, *정보보호시스템평가인증지침*, 정보통신부, 2002.8.

[5] 정보통신부고시, *정보통신망 침입차단시스템 평가기준*, 정보통신부, p 1-2, 2002.2

[6] 정보통신부고시, http://www.nis.go.kr/, *정보보호시스템 공통평가기준*, 정보통신부, 2002.8

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

[8] 김재성, 홍기융, 김학범, 심주걸, 침입차단시스템을 위한 강제적 접근통제법설계, *한국정보처리학회*, 제5권 제4호, 1998.4.

[9] 한국정보보호진흥원, *정보보호개론*, 교우사, p17-42, 2000.7.

[10] http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-05.txt.

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

[12] 최준호, 김판구, 네트워크상에서의 바이러스 차단을 위한 방화벽시스템의 설계 및 구현,

*정보처리학회 논문지*C 제8-C권4호,2001.8.
〔13〕 한국정보보호진흥원, http://www.kisa.or.kr/, 평가체계, 시험평가, 평가인증제품 현황, 2002.11.
〔14〕 Sun Microsystems , http://wwws.sun.com/ software/solaris/faqs/64bit.html#0q0, 2002.11.
〔15〕 Daniel P, Bovet, Marco Cesati, Understanding the Linux Kernel, O'Really & Associates, p45-51, January 2001.
〔16〕 Jim Mauro, Richard MacDougall, SOLARIS Internals, *Sun Microsystems Press*, p190-194, 2001. August.

박 대 우(Dae-Woo Park) 정회원

1987년 2월 : 서울시립대학교 경영학과 졸업
1995년 2월 : 숭실대학교 컴퓨터학부 전산부전공
1998년 8월: 숭실대학교 컴퓨터학과 석사
2004년 2월 : 숭실대학교 컴퓨터 학과 박사
1987년 8월 : 동구여상 정보처리, 정보통신과 교사
2000년 2월 : Entrust-Korea 연구소 부소장
2000년 10월 : 매직캐슬정보통신 부사장 / 연구소장
2003년 3월 ~ 숭실대학교 겸임조교수

<주관심분야> 정보보안, 인터넷보안, 이동통신 및 보안, 정보보호제품, 무선방화벽, IMT-2000보안, 위성통신보안, Cyber Reality,