네트워크 보안 효율성 제고를 위한 보안 QoS(Quality of Service) 측정방법론 연구

노시춘*

요 약

QoS(Quality of Service)는 ITU-T Rec. E.800에 의해 서비스를 사용하는 형태, 특성 그리고 요구 수준에 따라 사용자의 요구에 부응하여 제공할 수 있는 네트워크 서비스의 성능지표로 표현된다. 네트워크를 활용하는 정보시스템에서 최종적인 목표는 요구되는 시간내에 목적하는 성능을 확보하는 것이다. 본 연구에서 제안하는 보안 QoS 프레임워크는 측정 메트릭스, 측정스케쥴, 측정도구, 측정의순서, 측정 결과분석에 관련된 사항으로 구성된다. 보안 QoS에서 네트워크보안의 정보보호기능과 시스템기능을 분리하여 관리하지 않고 연계하여 종합 메커니즘으로 구성및 적용할 경우 종합적인 정보보호 효율은 시너지효과로 나타난다. 본 연구는 정보보호기능과 제반 시스템기능을 연계하여 정보보호기능을 적용했을 경우의 연동메커니즘 구현방법 개발과 그 성과를 측정하기 위한 것이다. 본 연구에서 제안한 네트워크 보안 효율성 제고를 위한 보안 QoS측정방안 연구 방법론을 통해 체계적인 측정환경을 설계할 경우 운용시스템상에서 보안 효율성 측정이 가능함이 입증되었고 측정 메커니즘을 통해서 개선된 네트워킹기능과 정보시스템 기능을 위한 효율성제고 방법론 개발이 가능함을 보여주고 있다.

A Study of Security QoS(Quality of Service) Measurement Methodology for Network Security Efficiency

SiChoon Noh*

Abstract

QoS(Quality of Service) is defined "The collective effect of service performance which determines the degree of satisfaction of a user of the service" by ITU-T Rec. E.800.The final goal of information system is to secure the performance efficiency within the required time. The security QoS framework is the modeling of the QoS measurement metrics, the measurement time schedule, instrument, method of measurement and the series of methodology about analysis of the result of measurement. This paper relates to implementing issue and performance measuring about blended mechanism between networking technology and security technology. We got more effectiveness in overall network security, when applying and composing amalgamated security mechanism between network technology and security technology. In this paper, we suggest techniques being used on infrastructure system and also offers a security QoS methodology as a model of more effective way. Methodology proposed in this research has proven that it is possible to measure response time through the scheduled method.

keywords : Network Security, QoS, MOS, Measurement Methodology

접수일(2011년 3월 5일), 수정일(1차: 2011년 3월 18일),
게재확정일(2011년 3월 23일)

* 남서울대학교 컴퓨터학과

1. 서 론

인터넷이 빠르게 성장하고 트래픽이 급증함에 따라 인터넷 사용자에게 지속적이고 예측 가능한 end-to-end level의 Service Quality 제공이 과제로 등장했다. 인터넷상에서 QoS(Quality of Service)를 제공하고자 많은 방법들이 제안되었으나 보안기능 측면에서는 QoS서비스 도입연구 는 진전되지 않고 있다. 그 이유는 QoS서비스는 일반적으로 통신서비스 품질을 대상으로 개발되어 사용하며 이를 보안분야에 적용하는 방안은 기술적 제약과 QoS 수준 측정상의 문제로 용이하지 않다. 본 연구는 인트라넷 단위시스템별로 고객만족 측면에서 보안 QoS 서비스를 위한 품질평가 제도를 연구하여 제안하기 위한 것 이다. 특히 보안 QoS 만족도에 대한 평가 사양 및 운용방법을 개발 하므로서 QoS 측정/분석기능을 새로운 모델로 제안한다. 따라서 본 연구에서 제안하는 보안 QoS 관리체계는 통신관련 인프라시스템 운용에서의 QoS 보증을 위한 업무운용 제반 절차와 기준을 프레임워크화 하여 제도화하는 일련의 규격이다. 연구 순서는 QoS 정의,통신서비스 QoS 구조,IP 네트워크의 QoS 국제기준,보안 QoS측정방법론 설계,보안 QoS 측정방법 설계,제안방법 실험 순서이다[1].

2. 관련연구

2.1 QoS 정의

QoS는 소비자가 인지하는 품질을 의미하며 보통 무형적이고 확인이 어려운 특성을 지니는데 최근에는 매우 다양한 의미로 사용된다. Parasuraman, Zeithaml & Berry (1985,1988,1991)은 QoS를 "서비스 품질은 고객의 주관적 평가(Evaluation)에 의해 이루어지며, 지각되고 있는 서비스 품질이란 소비자의 기대와 지각된 서비스의 불일치 방향의 정도"라고 표현했다. ITU-T는 권고 E.800 (1994.8) 에서 "통신서비스 이용자의 만족도를 결정하는 서비스 성능들의 총체적 효과"로 표현했으며 ITU-T 권고 I.350에서 QoS는 "사용자가 느끼는 서비스품질로서 서비스 접근점에서 측정 가능한 사건 및 상태로부터 측정할 수 있어야 한다"로 표현했다. IETF는 서비스를 사용하는 형태, 특성, 그리고 요구 수준에 다른 사용자의 요구에 적응하여 제공할 수 있는 네트워크 서비스의 성능지표 이다. 일반적으로 QoS란 트래픽이 통신망에서 전달 되면서 예측가능하면서 동시에 최소한으로 보장되어야할 서비스 요구사항을 의미한다. 즉,사용자가 사업자가 제공한 서비스를 사용할 때 QoS는 망 사용자 입장 에서는 특정 서비스 사용에 만족하는 정도이나 망 제공자 입장 에서는Network Performance (NP)로 표현되고 어느 수준 이상의 서비스품질을 보장하도록 제어가 가능한 자원요소로써 측정 가능하고 정량적으로 표현될 수 있는 값이다[2][3][4].

2.2. 통신서비스 QoS 특성

QoS 서비스는 이용자간의 End-to-End QoS 서비스로서 만약 이용자간 일부 네트워크에서 QoS 기능이 제공되지 않는다면 End-to-End QoS 서비스가 제공될 수 없다. 따라서 End-to-End QoS 서비스가 제공되기 위해서 이용자의 Application부터 중간 경유되는 모든 구성요소들에서 QoS 기능이 제공되어야 한다. End-to-End QoS 서비스를 위해 QoS 관련 표준기술이 논의되어 왔다. 그러나, QoS 관계된 많은 기술 표준화 노력에도 불구하고 서비스를 네트워크에 적용하기에 적합하지 않아 End-to-End QoS 서비스가 제공되지 못했다. 더 큰 문제는 네트워크 장비가 End-to-End QoS 서비스와 관계된 많은 정보들을 유지해야 한다는 점이며, 이것은 결국 네트워크의 확장성을 가로막는 요소로 작용한다[2][4].

2.3 IP 네트워크 QoS 측정모델 국제기준

통신품질 평가를 위해서는 품질특징을 고려하여 전문화된 방법을 개발하여 사용한다. 측정목적은 통신 QoS 목표수준 달성을 위해 필요한 정보의 수집, 이를 통한 문제점 발견, 개선방안 도출 이므로 측정목적에 부합되는 사항들이 치밀하게 검토되고 결정되어져야 한다. QoS 평가 국제기준 으로 VoIP QoS 평가방법 유형과 품질평가 항목이 제시되고 있는데 주관적 방법으로 MOS(Mean Opinion Score)가 있으며객관적 방법으로 E-mode,PSQM Perceptual

Speech Quality Measurement , PESQ(Perceptual Evalutionof Speech Quality), PAMS(Perceptual Analysis Measurement System)가 있다. MOS는 ITU-T의 P.800으로 제시된 기준이며 평가자가 느끼는 품질을 5단로 평가한 평균값 이다. 서비스품질 평가에 사용되는 파리미터별 품질 산출방법 및 평가산식 종류는 e-model, r-value, rating factor,r-factor에 의한 MOS 값산출, 고객관점 가중치산출 방식 등으로 구분된다[7][8].

<표 1> IP 네트워크의 QoS 평가방법

평가 구분	평가 방법	ITU-T 권고	특징
주관 평가	MOS	P.800	평가자의 주관적 품질(5단계)
객관 평가	R 값	G.107	E-Mode 에 의한 품질 척도
	PSQM	P.861	원래 음성신호와 열화 음성신호 특성량의 차이에서 음성품질 추정
	PESQ	P.862	PSQM 모델의 개량 평가법

3. 보안 QoS 측정체계 설계

3.1 설계목표

전통적으로 네트워크 보안의 고객만족은 보안기능 자체만을 대상을 해석되고 관리되었다. 그러나 보안기능이 수행되는 과정에서 시스템 성능 영역, 보안기능 지원 영역, 네트워킹기능 영역등 의 연동 매커니즘 구조하에서 수행된다. 따라서 보안기능의 효율성은 이같은 연동 메커니즘이 효율적일 경우에만 가능하다[4][5]. 이제 보안기능의 효율성 제고를 위해서는 보안 영역의 소재만을 측정대상으로 할 것이 아니라 보안기능과 관련기능을 연계하여 고려하여야 한다. 예를들면 네트워킹기능과 정보보호기능은 기술영역으로는 별도의 카테고리 이지만 실제 운용시스템 상에서는 연동기능구조로 가동된다. 다양한 레이어별 네트워킹 공격에 대응하기 위해서는 양 기능 연동구도에 의한 단계별 차단을 실시해야한다. 연동구조기능은 보안기능, 시스템성능, 네트워킹기능, 보안 지원기능으로 구성되고 인트라넷 구조하에서 보안기능 수행과정은 스위칭 단계 -> 침입차단시스템 필터링 단계 -> 내부 게이트웨이 필터링 단계 -> 서버 바이러스월 차단단계 -> 자동화 방역 단계 순서로 이루어진다. 이를위해 보안 QoS 관리는 보안과 관련되는 연동기능의 QoS를 고려하여 제반 절차와 기준의 프레임을 개발해야 한다[6].

3.2 설계조건

첫번째 조건은 네트워크보안 품질만족도 프레임 구조를 보안기능 단일 기능을 포함한 관련기능의 종합구조에 부합되는 다각적 측면의 기능을 설계해야 한다. 단일기능 측정 만으로서는 복잡하고 다양한 시스템 성능 관리에 한계가 있어서 측정자체의 의미와 가치 또한 한계일 수 밖에 없다. 두번째는 설계되는 프레임워크상 기능의 측정이 가능하여야 한다. 차단단계별, 차단 유형별, 성능측정을 통해서 시스템 효율을 분석할 수 있어야 한다. 시스템의 효율증진은 보안기능과 시스템 Performance가 연계로서 최종적이고 종합적인 성능향상이 이루어진다. 세번째 조건은 통합구조로 설계된 기능은 계량적으로 측정과 검증이 가능해야한다. 그 이유는 계량화 되지 못할 경우 QoS 파라메타별 품질달성 여부 및 수준평가 어렵기 때문이다[5][7].

3.3 전체적인 보안 연관기능 구조

전체적인 보안 연관기능 구조로서 본 연구는다음 <표 2>에서 제시한 네트워크 보안 QoS 종합구조 항목을 제시한다. 네트워크 보안 QoS는 ITU-T에서처럼 엄밀한 의미에서 QoS와 NP를 서로 구분하여 방법론을 새로이 제시하는 것이 바람직하다고 판단되어 본 연구를 통해 하나의 모델을 제시한다. 본 제안 모델은 향후 네트워크 보안 품질측정의 바로메타로 활용되어야 하고 세부적인 측정 메트릭스를 지속적으로 발굴해야 한다.

<표 2> 네트워크 보안 QoS 종합구조

보안 기능
• 악성코드 진단 • 악성코드 삭제 • 해킹차단 효율 • 보안취약점 검출 • 보안패치 이행율
시스템 성능
• Performance • 응답시간(Response Time) • CPU 부하율(CPU Utilization) • 시스템 프로세스(System Process)
보안지원 기능
• 트래픽 로드 밸런싱(Traffic Load Balancing) • 패킷필터링(Packet Filtering) 분담 • 차단 Rule 분담 • 정보 손실(Data_loss) 율
네트워킹 기능
• 지연(Latency) • 네트워크자원 이용현황(utilization) • 대역폭(Bandwidth) • 신뢰성(Reliability)

3.3.1 순수 정보보안 기능

정보보안기능은 인프라구조상에서의 • 악성코드 진단 • 악성코드 삭제 • 해킹차단 효율 • 보안취약점 검출 • 보안패치 이행율이 포함된다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통 경로별 차단, 방역 Zone별 차단으로 분류될 수 있다. OSI 계층별 차단은 OSI Layer2에서 Layer7까지의 계층별로 수행되는 차단 기능이다. 경로별 차단은 외부 라우터에서부터 최종 클라이언트까지의 트래픽 경로별로 수행되는 차단이다. 방역 Zone별 차단 기능은 각종 Resource별로 차단 기능이 수행되는 것이다[7].

3.3.2 시스템 성능

시스템 성능은 인프라시스템의 Performance, Latency, 응답시간(ResponseTime), CPU 부하율(CPU Utilization), CPU상의 시스템 프로세스(System Process)수로 대표된다. Performance는 인프라 구조에 의해 악성코드를 차단할 경우 부작용으로서 발생하는 시스템의 부하 수준이다. 응답시간(Response Time)은 호스트 접속 요구 패킷을 송신 개시하고 호스트로부터 응답시간 패킷을 수신 완료할 때까지의 시간을 의미하는 것으로 응답시간은 네트워크 전송시간 + 서버 처리 시간 + 클라이언트 처리 시간의 합계시간으로 산출된다. CPU 부하율은 차단 시스템 상에서 CPU 사용율을 의미한다. CPU 사용량의 증감은 트래픽 량과 악성코드 등 유해 트래픽의 발생에 의해서 좌우된다.

3.3.3 보안지원 기능

지원기능은 네트워킹 기능을 토대로 하지만 침입차단 기능 구현시 적용되어야 할 필수적인 효율성지원기능 또는 연관기능이다. 지원기능은 성격상 3개 세부 영역으로 분류되데 고가용성기능, 통합관리 기능 및 자동화처리와 실시간처리 기능이다. 지원기능은 보안 인프라 구현시 시스템 기능의 계속성과 안전성 그리고 효율 향상을 도모하기 위해 적용되어야 할 필수적인 기술 원리를 발굴 적용하는 방법론이다. 통합보안구조 설계의 경우 기본 기능인 침입차단 기능이 효과적으로 발휘되기 위해 주 기능에 부가하여 지원기능을 구조적으로 지원하여 효율성을 보장 한다.

3.3.4 네트워킹 기능

네트워킹기능은 네트워크 인프라상의 통신트래픽 처리 기능이다. 네트워킹 기능은 OSI 7 layer별로 차별화된 네트워킹 기능구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅등 인터네트워킹 기능, 데이터 전송기능 그리고 패킷처리 기능을 수행한다. 다이어그램으로 본다면 이 네트워킹 기능 영역내에 지원기능과 침입차단 기능이 존재한다. 대역폭은 연결된 네트워크 구간에서 사용 가능한 트래픽의 양이다. 인터넷에서 사용하는 네트워크는 PSTN 망과는 달리 일정 전송속도로 음성패킷을 보내도록 설계된 것이 아니기 때문에 전송패킷의 속도가 인터넷의 대역폭에 따라 일정하지 않을 수 있다. 부하(Load)는 네트워크 트래픽의 분주(Busy)한 정도이다. 패킷 전송성능은 망 운영 센터에서는 네트워크가 잘 동작하는지를 감시하고, 패킷이나 셀이 설정을 잘못하여 폐기되거나 지연되는지를 분석하여야 한다[9][10].

3.4 단위기능별 QoS 측정기준

보안 프레임워크를 구현하는 방법으로서 보안기능 부분과 지원기능 부분의 성능이 발휘되며 이 성능을 측정하고 분석하기 위해 성능정보를 구성하고 정의해

야 한다. 성능정보 항목은 논문의 프레임워크에서 보안기능이 수행되는 과정에서 연동되어 수행되는 시스템 성능 영역, 보안기능 지원 영역, 네트워킹기능 영역이다[11].

3.4.1 보안성능 측정기준

◉ 보안기능

차단구조에서의 차단이 이루어진 실적을 계량화한 수치이며, 악성코드 차단, 해킹차단, 보안취약점 검출, 보안패치율, 보안효율로 구성된다.

- 차단건수 : 차단이 이루어진 악성코드 건수
- 차단율 : 차단건수 / 총발생 또는 침입건수
- 미차단율 : 미차단건수/총발생 침입건수

침입차단시스템 또는 클라이언트 방역솔루션의 경우에는 처리단위가 Packet Per Second(PPS) 또는 Byte Per Second(BPS)로 표현되기도 한다.

보안효율은 악성코드를 차단한 실적과 차단 행위 수행이 원인이 되어 Performance에 부작용이 발생한 상호 비율이다.

3.4.2 시스템 성능 측정기준

◉ Performance

인프라 구조에 의해 악성코드를 차단할 경우 부작용(Side Effect)으로서 발생하는 시스템의 부하 수준이다. Performance는 Latency, 응답시간 (Response Time), CPU부하율, CPU상의 시스템 Process 수이다. Performance는 부(-)가 지향 목표 수준이다.

- 측정단위 : 차단율, 응답시간 지연율(%) 상호 비교 분석 지수

◉ 응답시간(Response Time)

호스트 접속 요구 패킷을 송신 개시하고 호스트로부터 응답시간 패킷을 수신 완료할 때까지의 시간을 의미하는 것으로 응답시간은 네트워크 전송시간 + 서버 처리 시간 + 클라이언트 처리 시간의 합계시간으로 산출된다.

- 측정단위 : 초(second)

◉ CPU 부하율(CPU Utilization)

차단 시스템 상에서 CPU 사용율을 의미한다. CPU사용량의 증감은 트래픽량(Traffic Volume)과 악성코드 등 유해 트래픽의 발생에 의해서 좌우된다. 차단 기능의 수행을 통해 차단 시스템 CPU 부하율이 감소될 수 있다.

- 측정단위 : 백분율(%)

◉ 시스템 프로세스(System Process)

차단 시스템 상에서 수행되는 Process수를 의미, 시스템 상에서 생성된 Process가 Memory상에 Loading되면 Process가 가동된다. 시스템 부하의 수준에 따라 Process가 증가하거나 감소.

- 측정단위 : Process수

3.4.3 보안지원 성능 측정기준

차단 기능이 정상적으로 수행될 수 있도록 네트워킹 과정에서 지원 기능이 수행되며 지원 기능은 자동화 처리, 통합 처리, 실시간 처리 및 고가용성 처리 등으로 분류된다. 지원 기능은 모든 실적이 보안기능의 지원형태로 나타나므로 독립적인 성능 측정 분야가 될 수 없다고 할 수 있다.

◉트래픽로드밸런싱(TrafficLoadBalancing)

인프라스트럭처 가동시 차단단계에서의 트래픽 병목(Bottleneck)현상 방지를 위한 부하분산(Load Balancing)기능을 말한다. 기존 구조하에서 병목 현상은 스위칭, 패킷 필터링 단계에서 발생하여 시스템 전체 처리 지연의 요소가 되어왔다. 로드 밸런싱은 스위칭 단계에서 수행하므로 이 성능을 측정한다.

- 측정단위 : 백분율(%)

◉ 패킷필터링(Packet Filtering)분담

패킷 필터링은 침입차단 시스템상에서 수행된다. 기존 구조상에서 패킷필터링역시 Main host로 집중됨으로서 시스템 병목 현상의 주 요인이 되어왔다. 패킷필터링 분담은 침입차단시스템의 기능구조이다.

- 측정단위 : 백분율(%)

◉ 침입차단 Rule 분담

차단 Rule이란 침입차단을 수행하는 과정에서 운용자에 의해 입력되는 차단기준과 규칙을 의미하며 이 Rule은 Rule Setting이란 절차에 의해 설정된다. 침입 유형이 다양해지면서 차단 Rule 또한 증가하므

로 Rule자체 기능에 의한 시스템 Performance가 지연되고 시스템 장애시 전 시스템 마비가 초래될 수 있다. 이 같은 Rule은 침입차단 시스템상에서 host간 분산시켜 집중화에 의해 위험을 분산한다.

- 측정단위 : Rule수와 백분율(%)

◉ 정보 손실 (Data_loss)율

에이전트 PC에서 송신한 패킷이 측정 목적지까지 왕복하지 못한 비율이다. 본 논문에서는 32byte의 ICMP ping패킷을 전송하여 타임아웃(10초)동안 응답을 받지 못한 패킷 비율이다.

- 측정단위 : 손실 패킷수/송신 패킷수

3.4.4 네트워킹 기능 측정기준

◉ 지연(Latency)

송신한 하나의 패킷이 측정목적지까지 왕복하는데 소요되는 시간을 의미한다. 통신 과정에서 음성과 데이타간 신호변환은 당연히 데이터의 감쇄, 지연,노이즈 가능성을 높이고 그로인한 latency와 jitter를 초래할 수 있다.측정 작업에서는 32bytes의 ICMP ping 패킷을 전송하여 측정 왕복시간을 측정한다.

- 측정단위 : micro second

◉ 네트워크 자원 이용 현황(utilization)

네트워크를 구성하는 링크나 노드의 자원 이용현황을 파악하기 위한 평가 항목. 특히 링크의 utilization 과 잠재적인 트래픽 병목 지점을 발견하고 예방 대책을 수립하는데 활용하기 위한 목적으로 개발이 필요하다.

- 측정단위 : 백분율(%)

◉ 대역폭(Bandwidth)

연결된 네트워크 구간에서 사용 가능한 트래픽의 양이다. 인터넷에서 사용하는 네트워크는 PSTN 망과는 달리 일정 전송속도로 음성패킷을 보내도록 설계된 것이 아니기 때문에 전송패킷의 속도가 인터넷의 대역폭에 따라 일정하지 않을 수 있다.

- 측정단위 : MB/S(%)

◉ 패킷 전송성능

망 운영 센터에서는 네트워크가 잘 동작하는지를 감시하고, 패킷이나 셀이 설정을 잘못하여 폐기되거나 지연되는지를 분석하여야 함

- 측정단위 : 백분율(%)

◉ 신뢰성(Reliability)

각 네트워크 연결 상태에 있어서 얼마만큼의 신뢰(비트에러율 등)를 유지하느냐가 수치로 표현된 것. 망 운영 센터에서는 네트워크 내의 장애를 신속히 발견하여 장애를 해결하도록 경보를 보내는 기능으로서 요구된다. 이를 위해 망 상태를 주기적으로 감시할 필요성이 대두된다.

- 측정단위 : 백분율(%)

3.5 보안 QoS 측정체계

보안 QoS 측정체계 설계 수행내용은 보안 QoS 측정체계 프레임워크 설계, 보안 QoS 측정방법,품질 파라메터별 QoS 측정기준, QoS 측정 체크리스트, 만족도집계, 가중치산정, 종합 만족도 MOS수준 산출 순서로 구성된다. 각 단계는 단계별 고유한 성격에 의거 계량화된 정량적 평가를 시행토록 설계한다. 이를위해 보안기능, 시스템성능, 네트워킹기능, 보안 지원기능 4개영역의 17개 항목 170개 세부항목을 체크리스트에 의해 점검한다. 집계된 측정점수는 가중점수를 반영하여 최종 평가점수로 집계된다. 평가점수는 5단계의 만족도 수준 등급이며 미흡, 기초, 보통, 정상, 성숙 으로 구분되며 종합만족도 MOS 수준으로 최종 결과가 산출된다. 종합만족도 MOS는 "2.3 IP 네트워크 QoS 측정모델 국제기준"에 예시된 ITU-T P.800 권고안으로서 평가자의 주관적 품질(5단계)이며 본 연구에서 품질목표 기준으로 인용하여 사용한다. 일련의 작업은 순서화, 계층화 되고 각 지표는 사전 설정된 지표를 준수한다.

3.5.1 QoS 파라메터별 MOS목표 설정

<표 3>에서 제시하는 MOS목표는 본 연구의 방법론을 적용하였을 경우 도출되는 목표치이다. 따라서 <표 3>에 구체적으로 제시되고 있는 값들은 본 연구에서 새로이 적용하고자 하는 사용자의 보안 QoS MOS목표 예시이다.

<표 3> 사용자의 보안 QoS MOS목표 예시

분야	QoS 파라메터	MOS목표(%)
보안 기능	• 악성코드 진단 • 악성코드 삭제 • 해킹차단 효율 • 보안취약점검출 • 보안패치이행율 합계	99
시스템 성능	• Performance • 응답시간(Response Time) • CPU 부하율 (CPU Utilization) • 시스템 프로세스(System Process) 합계	85
보안 지원 기능	• 트래픽 로드 밸런싱 (Traffic Load Balancing) • 패킷 필터링(Packet Filtering)분담 • 차단 Rule 분담 • 정보손실 (Data_loss)율 합계	85
네트워킹 기능	• 지연(Latency) • 자원이용 현황(utilization) • 대역폭(Bandwidth) • 신뢰성(Reliability) 합계	85
전체 평균	전체평균	88.50

QoS분야 파라메터별로 어느정도의 품질수준을 목표로 운용해야 하는가에 대한 수준 설정에 대해 국제적 표준으로 제시된 목표를 참조하되 각 운용시스템 환경을 고려하여 사용기관별 자체 목표 수준을 스스로 결정해야 한다. 본 연구에서 인용하는 품질목표는 ITU-T 권고 평가방법의 기준을 다음 표와 같이 예시한다. 이 예시는 보안기능을 대상으로 하는 것은 아니므로 보안 QoS는 사용부서가 스스로 결정 한다.

<표 4> 보안 QoS 점검방법

방식	사용방법	방법명칭	평가분야
수 동	체크리스트	기술보안관리 기능점검 보안이행체크 리스트점검	위협,취약점 보안기능보안관 기능 조사
자 동	침투테스트	측정 TOOL	위협,취약점
직접조사	직원면담,시스템 실사자료조사	현장실사	시스템,환경 보안체계조사

3.5.2 보안 QoS 점검방법 선정

자동점검은 실제상황점검, 상세점검, 특정취약점점검시 사용하며 수동점검은 전반적점검, 자동점검에 포함되지 못하는 항목 점검이다. 단기점검은 핵심단일종목 중점점검이며 직접조사는 수분야로서 자동점검,수동점검으로 상황파악이 곤란한 사례의 경우이다. 점검용 소프트웨어는방법론 개발시 공개용 소프트웨어 제품을 선정하여 방법론을 개발하며 실제업무 적용시는 공개소프트웨어를 업무사용도로 재구성 한다.

3.5.3 QoS 상세 체크리스트

측정 체크리스트는 품질 파라메터별 QoS 측정기준을 보안 QoS 점검방법에 따라 점검하는 상세내역이다. 작성분야는 보안기능, 시스템성능, 네트워킹기능, 보안 지원기능 4개영역으로 구성되고 각 영역별 측정 파라메타는 17개 항목, 170 세부항목으로 구성된다. 본 논문상에서는 QoS 영역별 상세 체크리스트 작성기준을 제안하고 기술은 생략한다.

<표 5> 4개영역 QoS 측정 체크리스트 구성

QoS영역	측정항목	세부항목	집계결과
보안 기능	5	50	건수, %,MS,초
시스템 성능	4	40	
보안지원 기능	4	40	
네트워킹기능	4	40	
종합만족도	17	170	

<표 6> 4개영역 QoS 측정 집계

QoS영역	측정 항목	세부항목	점수	집계 점수
보안 기능	5	50	1-100	
시스템 성능	4	40	1-100	
보안지원 기능	4	40	1-100	
네트워킹기능	4	40	1-100	
종합만족도	17	170	1-100	

3.5.4 QoS 측정값에 대한 가중치

<표 7> 5단계 가중치 기준

등 급	하	중하	중	중상	상
가중점수	0.1	0.15	0.2	0.25	0.3

평가지표의 동일 분류내 척도를 산출한 후 각지표의 중요도를 평가하여 중요도별로 가중 값을 부여한다. 가중치는 지표별 중요도 및 지표의 현실적 의미반영이 목적이며 기본 가이드라인은 다음과 같다.

- 가중치는 선택적 적용사항으로서 현장전문가 집단에 의한 진단평가와 협의결과 따라 적용여부, 대상, 적용수준을 결정한다.(델파이법 취지)
- 가중치 값은 진단평가 평가의 목적, 진단평가의 시기적특성, 업무성격, 업무규모, 업무프로세스 단계, 프로세스중요도 기준으로 부여한다.
- 적용된 가중치 값은 가변적인 데이터 값으로서 일정한 고정적인 개념이 아니다.
- 가중치 값은 동일구룹에 속하는 부여대상 전체를 대상으로 100%의 범위 값을 상대적 배분 한다.
- 가중치등급과 가중점수 종류는 단일가중치로 자산기준, 업무기준, 프로세스, 보안기능을 고려 한 한 종목을 선택하며 다중가중치는 자산 기준, 업무기준, 프로세스기준, 보안기능기준중 복수의 기준을 합산 또는 승산한다[9].

<표 8> 4개 파라메타에 대한 가중치

QoS영역	측정항목	세부항목	점수	가중점수	최종점수
보안기능	5	50	1-100		
시스템성능	4	40	1-100		
보안지원기능	4	40	1-100		
네트워킹기능	4	40	1-100		
종합만족도	17	170	1-100		

3.5.5 QoS 수준 월간실적 집계

<표 9> 4개 파라메타별 QoS 만족도 집계식

영역구분	항목	산출식	합계
보안기능 만족도	만족율(%)	만족율(%) = 월 총 만족횟수 / 월 총 측정횟수 ×100	
	월 간 달성도	월간 달성도(%) = 100 - (94 - 국내구간 만족율) ×5	
	연 간 달성도	연간 달성도(%) = Σ월간 달성도 / 측정월수	
네트워킹기능 만족도	만족율(%)	만족율(%) = 총 만족횟수 / 총 측정횟수 ×100	
	분 기 달성도(%)	분기 달성도(%) = 100 - (89 - 해외구간 만족율) ×5	
	연 간 달성도(%)	연간 달성도(%) = Σ분기 달성도 / 측정분기수	

측정 QoS에 대한 만족도 집계는 4개 분야별로 나누어 산출한다. 보안기능 만족도의 경우는 만족율(%) = 월 총 만족횟수/월 총 측정횟수 ×100식으로 산출하며 월간 달성도(%) = 100 - (94 - 국내구간 만족율) ×5식으로 산출한다. 단,국내구간 만족율이 94%이상시 월간 달성도는 100이다. 연간 달성도(%)는 월간 달성도의 합계로서 = Σ월간 달성도/측정월수로 산출한다. 통신품질 만족도는 만족율(%) = 총 만족횟수/총 측정횟수 ×100 식이며,분기 달성도(%)는 = 100 - (89 - 해외구간 만족율) ×5 식으로 산출한다. 단, 통신품질 만족율이 89%이상시 반기 달성도는 100이다. 통신품질 만족도의 연간 달성도(%) = Σ분기 달성도/측정분기수로 산출할 수 있다.

3.5.6 최종 MOS 산출 및 비교분석

<표 10> 4개 영역의 보안 QoS의 MOS

평가분야	평가점수	목표점수	달성도	MOS 수준				
				미흡	기초	보통	정상	성숙
				1-20	21-40	41-60	61-80	81-100
보안 기능								
시스템 성능								
보안지원 기능								
네트워킹 기능								
전체평균								

종합만족도 MOS는 보안기능, 시스템성능, 네트워킹기능, 보안 지원기능 4개영역으로 구성되고측정점수, 가중점수, 평가점수로 집계된다. 평가점수는 5단계의 MOS 수준 등급으로 분류된다. 5단계 등급은 미흡, 기초, 보통, 정상, 성숙으로 구분되며 각각 1-100까지의 분포를 가진다. 평가점수를 운용목표와 비교하여 달성도를 분석 한다. 달성실적이 미진한 분야를 발췌하여 원인 분석 및 개선작업에 활용한다.

4. 제안방법 실험

4.1 실험 환경

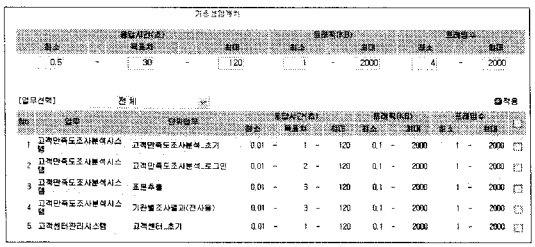
- 인용된 A기업 업무 환경과 인트라넷의 트래픽 처리 환경은 인트라넷 시스템내 접속 자원 규모이며

각종 서버 100대,클라이언트 PC 160대가 설치되어 있다.

- 인트라넷 시스템에서는 재무, 인사, MIS, 내부 관리 등 총 10종의 업무가 수용되어 있다. 트래픽 규모는 일간 약 5억 패킷이 처리되는 규모 볼륨이고 상시 3만 정도의 네트워크 세션이 접속되고 있다.

4.2 데이터 수집

- NP서버에서 주기적으로 측정시작지점으로 telnet을 접속한다. 측정주기를 일정시간으로 15분단위(매시 00분,15분,30분,45분)로하고 측정시작지점에서 측정대상지점으로 PING test를 실시한다. 측정조건은 100byte로 5개 packet 송출측정(time-out 2초)한다. 측정그룹별로 측정 실시후 접속을 해제한다.
- 실험에 사용한 작업은 단순 텍스트 기반 정적 html문서와 C++언어로 만든 간단한 CGI 동적 문서이다. 실험은 request가 클러스터링 그룹들 사이에 균일하게 분포되는 경우와 불균일하게 분포되는 경우로 나누어서 시행되었다.



(그림 1) 데이터 수집 및 분석 화면

4.3 분석결과

<표 11> 4개 영역의 보안 QoS의 MOS

평가분야	평가점수	목표점수	달성도	MOS 수준				
				미흡	기초	보통	정상	성숙
				1-20	21-40	41-60	61-80	81-100
보안 기능	97	99	97.0					*
시스템 성능	83	85	97.6					*
보안지원 기능	82	85	97.0					*
네트워킹 기능	83	85	97.0					*
전체평균	86.25	88.50	97.1					*

- 제안 보안 QoS 관리체계는 통신 인프라시스템 운용시의 QoS 보증을 위한 절차와 기준을 프레임워크화 하는 것으로서 분석 결과는 통신관련 인프라시스템 운용부서의 사용을 전제한다. 만족도 산출을 위해 보안기능, 시스템성능, 네트워킹기능, 보안 지원기능 4개영역에 대해 17개 항목 170개 세부항목을 체크리스트에 의해 점검했다. 점검방법은 "3.5.1 보안 QoS 점검방법"에 의거 자동점검, 상세점검, 특정취약점점검 및 을 실시했다.
- 측정점수에 가중점수를 반영하여 최종적으로 집계했으며 5단계의 만족도 수준 등급 미흡, 기초, 보통, 정상, 성숙 으로 표현된다.
- 4개 파라메타에 대한 만족도 집계값은 종합 효율 MOS값으로 산출했으며 측정결과 전체평균 MOS 값이 86.2로 측정되었고, 이는 목표88.5대비 97.1% 이며 양호한 QoS값으로 판단된다.

5. 결 론

희망하는 서비스 품질 수준은 사용자 마다 서비스 마다 다르기 때문에 QoS를 정의 하고 평가하는 척도(Measure)를 만드는 일이란 어려운 문제이다. 본 논문에서는 보안 QoS의 MOS 측정 기법을 사용한 인프라시스템에서 보안기능 만족도 측정 방법을 제안한다. 본 연구에서 제안한 방법론을 통해 체계적인 측정환경을 설계할 경우 운용시스템상에서 보안 QoS의 만족도 산출이 가능함이 입증되었고 만족도 측정 메커니즘을 통해서 개선된 네트워킹기능과 정보시스템 기능을 위한 효율성제고 방법론 개발이 가능함을 보여주고 있다. 정보시스템 인프라스트럭처의 효율성 여부는 사용자 또는 사용부서의 지속적인 진단과 튜닝을 필요로 한다.

참고문헌

[1] 나병윤, "시스템 및 네트워크 트래픽 모니터링, (주) PGPnet, 2003.
[2] 김태경 · 서희석 · 김희완, 서비스 응답시간 보장을 위한 패킷 손실에 관한 연구,2005
[3] 김태성,이금석, 웹 어플리케이션 응답시간 모 니

티링 API의 설계 및 구현,2000
[4] 장윤정, "L7 스위치로 네트워크 활용도를 높여라", 네트워크타임스, 2003.
[5] Sichoon Noh, Kuimam J.Kim, "Improved Structure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2003.
[6] Sichoon Noh, Kuimam J.Kim, "Improved Structure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2003.
[7] D. Yoon and K. Cho, "General bit error probability of rectangular quadrature amplitude modulation," IEE Electronics Letters, vol. 38, no. 3, pp. 131-132, January 2002.
[8] J. K. Kwon, S. Park and D. K. Sung, "Log-likelihood ratio(LLR) conversion schemes in orthogonal code hopping multiplexing," IEEE Comm. Letters, vol. 7, no. 3, pp. 104-106, Mar. 2003.
[9] Sichoon,Noh,Dong Chun Lee,"Multi-Level Protection Building for Virus Protection Infrastructure", SCIE LNCS 3036, 2004.6
[10] Sichoon,Noh,"Assurance Method of High AvailabilityinInformationSecurity Infrastructure System", SCIE LNCS 3794,2005.12
[11] Sichoon,Noh,"Building of an Integrated Multilevel Virus Protection Infrastructure", IEEE Computer Society,2005.12.
[12] Sichoon,Noh,Dong Chun Lee,Kuimam J.Kim "Protection Structure Building for Malicious Traffic Protecting in Intrnwt Systems",SCIE LNCS3981,2006.05
[13] ITU-T Rec. E.417, "Framework for the Network Management of IP-Based Networks,"Feb.2001.

[저 자 소 개]

노 시 춘 (SiChoon Noh)
1987년 : 고려대학교 경영정보학(석사)
2005년 : 경기대학교 정보보호기술(박사)
2002년 : KT 시스템보안부장
2004년 : KT 충청전산국장
2005년~현 재 : 남서울대학교 컴퓨터학과 교수
2011년~현 재 : 남서울대학교 IT융합연구소 연구위원
email : nsc321@nsu.ac.kr