한국형 네트워크 보안 시스템 성능 평가 방법론 설계

주 승 환* · 서 희 석** · 김 상 연***

A Designing Method of Performance Evaluation for Network Security Equipment of Korean Style

Ju, Seung Hwan · Seo, Hee Suk · Kim, Sang Youn

〈Abstract〉

With the advancement of network, privacy information as well as confidential information that belongs to government and company are exposed to security incident like spreading viruses or DDoS attack.

To prevent these security incident and protect information that belongs to government and company, Security system has developed such as antivirus, firewall, IPS, VPN, and other network security system.

Network security systems should be selected based on purpose, usage and cost.

Verification for network security product's basic features performed in a variety of ways at home and abroad, but consumers who buy these network security product, just rely on the information presented at companies.

Therefore, common user doing self performance evaluation for perform Verification before buying network security product but these verification depends on inaccurate data which based on some user's criteria.

On this paper, we designing methodology of network security system performance evaluation focused on Korean using other cases of performance evaluation.

Key Words : Network Security Performance Valuation, System Testing Methodology

Ⅰ. 서론

최근 IT 기술의 급격한 발전을 통하여 사용자는 시, 공간의 제약 없이 네트워크에 접속하여 원하는 정보를 얻을 수 있는 환경이 제공되고 있다. 그러나 네트워크의 고도화와 함께 바이러스 유포, 개인정보 침해 사고뿐만 아니라 최근 DDoS 공격 등과 같은 각 종 보안사고로 인해 개인의 정보뿐만 아니라 기업, 국가의 기말정보까지 공격에 노출되어 있다.

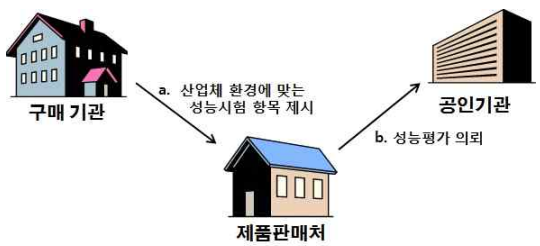
이러한 공격으로부터 개인정보 및 기업, 국가의 기밀정보를 보호하기 위해서 안티바이러스, 스팸, 스파이웨

*한국기술교육대학교 컴퓨터공학과 박사과정
**한국기술교육대학교 컴퓨터정보공학부 교수(교신저자)
***한국기술교육대학교 컴퓨터공학부 교수

어, 방화벽, IPS, VPN, UTM 등과 같은 네트워크 보안 시스템이 개발되었고, 네트워크 기반시설 및 국가 기관에까지 보급되었다. 따라서, 네트워크 보안시스템은 목적, 용도 및 비용 등을 고려하여 최적의 시스템을 선정해야 한다. 이를 위해서는 유사 시스템들 간의 기능이나 성능을 비교해서 보다 우위의 시스템을 선택할 수 있어야 한다.

네트워크 보안 시스템에 관한 기본적인 기능에 대한 인증은 국내외에서 다양한 방법으로 시행하고 있지만, 소비자 입장에서 볼 때 구매하려는 시스템의 "성능"에 관한 결과는 업체에서 발표하고 있는 정보에 의존할 수 밖에 없다. 네트워크 보안에 관련된 사항들을 객관적으로 평가할 수 있는 방법이 제시되고 있지 않은 상황이기 때문에 각 업체나 기관이 제시하는 방법들로 평가 할 수 밖에 없다[1]. 따라서 사용자들은 구매이전에 개별적인 성능 시험을 통해 네트워크 보안 시스템의 성능에 대한 검증을 수행하고 있다. 다시 말해서, 국내에서 정보보호 시스템은 공인기관에서 시스템의 성능을 수행하여 시스템의 성능을 평가 하고 있다. 그러나 성능평가를 수행하는 수행기관의 시험환경이 상이하고, 시스템을 구매하는 기관의 특성에 따라서 차별화된 성능시험 항목을 제시하고 있다[2-3].

예를 들어, 산업체에서 시스템을 구매하는 경우 산업체의 환경에 맞는 성능시험 항목을 제시하고, 시스템 판매자가 공인기관에 산업체의 환경에 맞는 시험 항목에 대한 평가를 의뢰한다. 이는 각 구매자들에 따라서 요구하는 평가 항목이 다르기 때문에 성능평가를 수행하여



<그림 1> 국내 정보보호 시스템 성능평가 현황

시험기간 낭비 및 중복 투자비용이 발생하고, 빠르게 발전하는 네트워크 공격기법에 따라 짧은 생명주기를 갖는 정보보호시스템의 특성에 비추어 보면 치명적인 약점이 되고 있다[3].

본 논문에서는 국내 정보호호시스템 성능시험 기관의 시험 항목에 대한 분석과 해외 정보보호시스템 성능평가 기관의 성능평가 사례를 알아보고, 국내 현황을 반영한 한국형 네트워크 보안시스템 성능평가 방법을 제시한다.

Ⅱ. 국내 정보보호 시스템 시험 기관

2.1 한국정보통신기술협회(TTA)

한국정보통신기술협회(이하 TTA) 성능 시험 기관은 정보통신 시스템에 대한 제 3자 시험 인증 서비스를 제공함으로써 국내 정보통신 시스템의 시장경쟁력 향상을 목적으로 2001년 설립되었다. 성능평가 시스템은 소프트웨어, 네트워크, 디지털방송, 이동통신, 인터넷 전화, 통신 서비스 품질평가 장비 및 시스템에 대한 인증 서비스를 제공하고, 소프트웨어와 네트워크 분야에서 정보보호 시스템 성능평가를 수행한다. 소프트웨어에 대한 성능평가는 ISO/IEC 9126, 14598, 12119 등의 국제 표준에 의거한 평가 모델을 기반으로 국내 환경에 최적화된 기준을 도입하였고, 품질 특성을 평가하여 성능이 만족할 경우 GS(Good Softwore) 인증을 부여한다[4].

한국정보통신기술협회에서는 정보보호시스템의 성능시험을 위하여 "네트워크 보안 장비에 대한 성능 측정(TTAS. KO-12.0044) 표준 문서"가 제정되었다. 이 문서는 방화벽, IDS, IPS 장비에 대한 성능 측정 기준과 성능측정 방법에 대한 규격을 정의하는 것을 주된 내용으로 삼고 있다. 세부적으로는 패킷전송률, 지연시간 및 패킷손실률과 같은 필수 성능 측정 기준에 대하여 실제 네트워크 환경과 유사한 상황에서 다양한 인터넷 응용 트래픽과 복잡한 보안 정책 규칙을 적용하여 네트워크 보안 장비의 성

능을 측정하는 방법을 정의하고 있다. 대하여 네트워크와 정보보호 분야로 구분하여 성능시험 방법을 제시한다.

2.1.1 TTA의 성능시험 모델

<표 1> 방화벽 & IPS 성능시험 모델[4-5]

방화벽 & IPS	
네트워크 성능	- 패킷 크기 변화에 따른 처리율과 지연시간 - IPv4/6 트래픽에 대한 처리율과 지연시간 - TCP/UDP 트래픽에 대한 처리율과 지연시간 - 응용계층 트래픽에 대한 처리율과 지연시간
보안 처리 성능	- 접근 제어 리스트에 대한 처리율과 지연시간 - 시그너처 기반의 패턴 매칭에 대한 처리율과 지연시간 - 공격 트래픽 탐지/차단시 처리율과 지연시간 - 백그라운드 트래픽 부하에 대한 공격 트래픽 탐지율과 차단율
응용 처리 성능	- 최대 TCP 연결개수에 따른 TCP 연결 생성률과 해지율 - 최대 응용 트랜잭션 수에 따른 응용 트랜잭션 생성률과 해지율

<표 2> 네트워크 보안 장비에 대한 성능 측정[6]

성능 측정 기준과 성능 측정 방법
패킷 크기 변화에 따른 처리율과 지연시간
IPv4/IPv6 트래픽에 대한 처리율과 지연시간
TCP/UDP 트래픽에 대한 처리율과 지연시간
응용계층 트래픽에 대한 처리율과 지연시간
액세스 제어 리스트에 대한 처리율과 지연시간
시그너처 기반의 패턴 매칭에 대한 처리율/지연시간
공격 트래픽 탐지 또는 차단시 정상 트래픽의 처리율과 지연시간
백그라운드 트래픽 로드 변화에 따른 공격 트래픽의 탐지율과 차단율
최대 IP 터널 개수와 IP 터널 생성률과 해지율
최대 TCP 연결 개수와 TCP 연결 생성률과 해지율
최대 응용 트랜잭션 생성률과 해지율

TTA는 방화벽, IPS 성능시험 모델은 아래 표 방화벽 & IPS 성능시험 모델 과 같이 최상위 정보보호시스템을 기점으로 2계층은 보안장비 성능시험 목표를 달성할 수 있는 광범위한 성능시험 특성을 제시하였다. TTA의 네트워크 보안 장비에 대한 성능 측정에서는 네트워크 보안 장비에 대한 성능 측정 기준과 시험 항목을 정의하였다.

실제 다양한 인터넷 응용 트래픽과 복잡한 보안 정책 규칙 적용에 따른 기본 보안 기능 처리 성능 및 응용 처리 성능에 대한 기준을 제시하였다.

2.1.2 TTA 보안 시스템 성능평가 현황

TTA에서는 네트워크 분야의 정보보호 시스템은 방화벽, IPS, VPN 장비에 대한 성능 시험을 수행하고, 스위치나 라우터 등의 일반적인 네트워크 장비 관점에서 성능을 측정한다. 따라서 방화벽, IPS, VPN 등 네트워크 정보보호 시스템 성능 결과는 네트워크 관점이었고, 보안 기능에 대한 성능 시험이 수행되지 않았기 때문에 정보보호 시스템에 대한 성능을 평가하기는 어렵다.

현재 수행된 TTA 검증의 경우 네트워크 관점에서 성능 측정과 적합성 및 상호운용성에 대하여 평가를 수행하였기 때문에 네트워크 보안 시스템에 대한 보안 기능 평가가 필요하다.

2.2 한국인터넷진흥원(KISA)

현재 KISA는 정보보호 기술 개발, 정보통신 기반보호, 정보보호호 평가 인증, 개인정보보호 업무 사업을 추진하고 있으며, 정보보호 평가 인증제도 활성화 및 국제화를 위한 CC(Common Criteria) 기반의 PP를 개발하였다.

PP는 안티 바이러스/스팸, IDS, 방화벽, IPS, VPN, OS 보안 시스템 등 14종의 시스템에 대한 평가를 수행하고 있으나, 시스템의 성능보다는 보안성에 초점을 맞추어 평가를 진행한다.

KISA가 사용하는 평가 과정 중 하나는 평가보증등급(EAL, Evaluation assurance levels)이다. 평가보증등급(EAL)이란 정보보호시스템 공통 평가 기준(CC)의 보증 요구 사항으로 이루어진 패키지로서, IT 시스템 또는 시스템의 평가 결과 보안 기능을 만족한다는 신뢰도 수준

을 정의한 것이다. CC 보증 요구 사항은 IT시스템 또는 시스템의 형상 관리, 배포 및 운영, 개발, 설명서, 생명 주기 지원, 시험, 취약성 평가 등을 포함하고, CC는 이를 7등급으로 구분하며, 등급이 높아질수록 보증 요구 사항은 강화된다.

2.2.1 KISA 보안 시스템 성능평가 현황

안티 바이러스/스팸, 방화벽, IPS, VPN, UTM 등 정보보호 시스템 전반에 걸쳐 보안성 평가를 수행한 KISA는 시스템의 성능 보다는 보안성을 중심으로 평가를 수행하고 있다. 인증 로그를 부여받은 시스템은 인증 등급에 따라 보안성을 검증 받았을 뿐 네트워크 관점의 처리량 및 지연율은 평가하지 않았기 때문에 네트워크 성능 시험을 위한 별도의 평가가 필요하다.

Ⅲ. 해외 정보보호 성능평가 시스템

3.1 Tolly Group

Tolly Group의 성능평가는 자체 시험 방법론과 공정한 성능 시험 원칙을 기반으로 성능시험을 진행하고 있으며, 독자적인 성능평가 방법론에 따라 성능을 측정한다. 현재 성능평가는 개발 업체 장비의 특성에 따라 QoS의 속성, 표준이나 프로토콜의 호환성, 웹 기반 관리, 보안 속성 등 장비 특정에 따라 다양한 성능 평가를 수행하고 있다.

Tolly Group의 성능 평가는 정보통신 장비에 대한 성능 시험을 수행하고 있으며, 정보보호 시스템은 안티 바이러스, 방화벽, IPS, VPN 등 장비에 대한 성능 평가를 수행한다[7].

Tolly Group의 성능평가 시스템은 방화벽, IPS, VPN 등 네트워크 기반의 정보보호 시스템을 중심으로 성능을 측정하고 있으며, 시험 요구자가 제시하는 항목에 따라 성능평가를 수행한다. 방화벽의 성능 평가는 처리량, TCP 연결 비율, HTTP 트랜잭션 비율, 방화벽 성능에 대하여 측정하였고, IPS는 네트워크 관점의 처리율, 지연율, 세션 비율과 보안 성능 측정을 위한 악의적인 공격의 탐지 및 차단 기능, 동시 세션 지원, 우회 공격에 대한 방어 기능의 성능을 평가하였다.

3.1.1 Tolly Group의 성능평가 현황

Tolly Group의 성능평가에서 방화벽, IPS의 성능 평가는 네트워크 성능과 보안 성능으로 구분한다. 네트워크 성능은 처리량과 지연율을 중심으로 수행하고 있으며, 보안 성능은 악의적인 트래픽 탐지 및 차단의 정확성에 대하여 성능을 평가한다.

VPN 장비는 IPSec 및 SSL(Secure Sockets Layer) 알고리즘 지원 여부와 터널링 설정시 처리율 및 지연율, 그리고 동시접속률 등에 대한 평가를 수행하였다.

성능 시험이 수행된 시스템은 성능 시험 기준에 따라 Tolly up to Spec, Tolly Verified, Tolly Tested로 구분하였다.

Tolly Group에서 제공하는 인증 서비스는 시스템의 성능 검증을 목적으로 수행하였기 때문에 동일 기능 시스템의 성능 비교가 아닌 요구자가 제시한 성능 시험 항목에 따라 수행하였고, 수행 결과에 따라 인증 로그를 부여하였다.

3.2 ICSA Labs

1991년에 설립된 ICSA는 안티 바이러스, 방화벽, IPS, VPN 등 정보보호 시스템에 대하여 인증을 실시하는 미국의 사설 성능 평가 기관이다.

각 시스템에 대하여 개별적인 평가 기준을 보유하였다. 정보보호 시스템 변화 대응에 따른 평가 기준 적시성 유지를 위하여 매년 기준을 갱신하여, 신규 평가 기준에 따라 성능 시험을 수행한다.

평가 시스템에 대해 객관성, 공정성, 신뢰성을 갖추어 평가를 수행한 결과를 통과 또는 실패로 분류하여 통과의 경우 인증 마크를 부여한다[8].

ICSA 성능 평가 시스템은 안티 바이러스/스팸/스파이웨어, PC 방화벽, 응용 방화벽, 네트워크 방화벽, IPS, IPSec VPN, SSL VPN 등 정보보호 시스템에 대하여 전문적으로 성능평가를 수행한다[8]. ICSA 성능 평가는 호스트 인증의 신뢰성, 원격관리 안정성, 운용체계와 방화벽 모듈의 상호 연동, 모든 서비스에 대한 감사기록 저장 및 분석, 개발업체의 기술 지원 등에 대하여 성능평가를 수행한다.

합격된 시스템은 인증 로그를 부여하고, 결과를 ICSA 웹에 공개한다. 불합격된 시스템은 소정 기간 내에 수정된 시스템을 제출하여 재시험을 요청할 수 있으나 60일이 결과하면 모든 인증작업은 폐기된다.

ICSA 성능평가 기준은 매년 갱신되기 때문에 인증된 시스템도 변경된 기준에 따라 재인증을 권고하고 있으며, 재인증은 변경 부분에 대해서만 국지적 시험을 수행하기도 한다.

3.2.1 ICSA Labs의 성능평가 현황

ICSA은 정보보호 시스템에 대하여 보안 성능을 평가하는 전문 기관으로 안티 바이러스/스팸/스파이웨어, 방화벽, IPS, VPN 등에 대한 성능 평가를 수행하고 있으며, 성능 평가 기준을 ICSA에서 제시하고 있다[8].

ICSA 성능 평가는 보안 기능을 중심으로 평가를 수행하고 있으며, 네트워크 관점은 평가하지 않았다. 따라서 네트워크 성능 시험을 위한 별도의 인증 절차가 필요하다.

3.3 Veritest

Veritest는 미국 Lionbridge Technologies, Inc의 산하 기관으로 2001년에 Data Dimensions와 ST Labs을 합병하였고, 2002년 7월에 성능 시험 선도 기관인 Ziff Davis의 eTesting Lab을 합병하여 성능평가 분야를 확대하였다.

1992년부터 약 500여 회사 시스템에 대해 소프트웨어 분야별로 성능 시험을 실시하여 결과를 PC Magazine에 정기적으로 공표하는 등 소프트웨어 성능시험 분야를 선도하고 있다. 성능 시험은 완시스템 뿐만 아니라 개발 중의 시스템에 대해서도 성능 평가를 수행하고 있으며, 성능 시험 결과를 홈페이지에 게시하여 신청 업체들의 홍보 및 마케팅에 활용할 수 있도록 서비스를 제공한다.

3.3.1 Veritest의 성능평가 현황

Veritest의 성능 평가는 안티 바이러스/스팸 및 웹 보안 장비로 구분하였다. 안티 바이러스/스팸은 기능성, 성능, 사용자 수용 시험 등을 수행하였고, 웹 보안 장비는 기능성, 성능, 가용성 시험 등에 대하여 성능을 평가하였다[9].

Veritest 성능 평가는 유사한 기능의 시스템을 선별하여 기능, 성능, 가용성, 사용성 등의 성능 시험항목을 도출하였고, 시험 결과를 비교, 분석 결과에 따라 보고서로 작성하여 웹 환경에 공개하였다.

3.4 NSS Lab

1991년 영국에 설립된 유럽의 공인 기관으로 정보보호시스템 분야에 대하여 성능 시험 및 검증을 수행하는 공인 평가 기관이다. NSS는 성능 평가를 가장 뛰어나게 수행하는 곳으로 정평이 나있으며 방화벽, IPS, VPN, UTM 등 보안 시스템을 약 800개 항목으로 객관적으로 평가하여 성능 기준을 모두 통과한 시스템에 한정하여 인증마크를 부여한다. 정보보호 시스템에 대한 성능평가는 자체 지침을 기반으로 성능시험 시스템의 기능의 따라 항목 및 방법을 결정하였다. 각 시스템군은 성능 지침에 따라 네트워크 성능 및 보안 기능에 대한 평가를 수

행하였고, 성능시험 결과 NSS에서 제시된 모든 기준을 통과할 경우 인증 로그를 부여한다.

3.4.1 NSS Lab의 성능평가 현황

NSS의 성능 평가는 방화벽, IPS, UTM 등 네트워크 기반 정보보호 시스템을 중심으로 성능을 측정하고 있으며, 네트워크 기반 성능 및 장비의 보안 기능에 대하여 평가를 수행한다[10].

방화벽, IPS는 NSS의 성능평가 지침에 따라 엔진의 공격 탐색, 기능성, 성능, 안정성, 가용성 등의 시험항목에 따라 성능을 평가하고 있으며, UTM은 보안 기능의 설정에 따른 네트워크 성능을 기준으로 평가를 수행한다.

NSS는 각 정보보호 시스템에 대한 자체 성능 평가 기준을 마련하고 있으며, 성능 평가 기준에서 제시한 항목 및 방법을 기반으로 장비의 성능을 측정하였고, 성능 시험 결과에 대하여 보고서를 작성하여 웹 환경에 공개하였다.

Ⅳ. 한국형 네트워크 정보보호 시스템 성능평가 방법론 설계

4.1 기존 성능평가 사례의 문제점

해외의 경우 NSS 그룹과 Tolly 그룹에서 네트워크 보안 시스템에 대한 성능 측정 작업을 수행하고 있다. 특히, NSS 그룹에서의 성능 측정 내역은 상세한 측정 기준 및 측정 방법에 기초를 하고 있고, 기가비트 방화벽 또는 멀티기가비트 방화벽 등의 시스템군에 대하여 동시에 많은 개발업체들이 참여하여 결과를 발표하고 있다. Tolly 그룹의 평가 내역은 상대적으로 작은 수의 필수적인 평가 기준들에 대해서 수행하고 있다. Tolly 그룹에서는 대개 한두 개의 시스템에 대한 성능 측정 시험을 하고, 이의 결과를 발표하고 있다.

하지만 Tolly Group의 성능평가는 요구자의 조건에 따라 시험 항목을 결정하기 때문에 동일 장비의 많은 성능평가를 야기할 수 있다. NSS Labs의 경우 객관적인 성능 평가 모델을 가지고 네트워크 보안 장비 성능평가를 하지만 업체의 성격에 따른(예를 들어 네트워크 성능보다는 정보보호 성능을 중시하는 업체나 정보보호 성능과 네트워크 성능을 동시에 요구하는 업체) 네트워크 보안 시스템 선택이 쉽지 않은 현실이다.

한국형 네트워크 정보보호 시스템 성능평가 방법론에서는 해외의 경우에서처럼 객관화된 형태의 기준과 측정 결과를 발표 할 수 있어야 하며, 성능 측정의 기준과 방법을 제시함으로써 개발업체와 사용자 모두에게 객관적으로 성능 측정 결과를 이용할 수 있도록 하는 것에 목적을 둔다.

4.2 한국형 네트워크 보안시스템 성능평가 방법론

4.2.1 네트워크 보안 시스템 성능시험 모델

방화벽에 대한 성능 평가는 방화벽의 기본적인 모듈, 로그 정보, 방화벽 설치 위치(가정, 중소기업, 대기업)에 따른 보안 기능을 평가한다.

<표 3> 방화벽 성능시험 항목

방화벽 성능시험 항목	
항목	내용
방화벽 처리량	- 4 계층 필터와 application payload signature에 기반한 7계층 필터로서 방화벽으로서 성능
TCP 연결 비율	- 4 계층 부하 분배기로 설정한 경우의 TCP 세션에 따른 연결 비율
HTTP 트랜잭션 비율	- 7 계층 부하 분배기로 설정한 경우 HTTP Get/Reply와 TCP로 구성된 HTTP 트랜잭션 비율
방화벽 성능	- 공격 트래픽을 막으면서 올바른 HTTP와 UDP 트래픽을 처리하는 성능

IPS의 성능 평가는 기본 기능 및 장비 기능 평가로 구

<표 4> IPS 성능시험 항목

IPS 성능시험 항목		
항목	세부 항목	내용
네트워크 성능	- 처리량 - 지연율 평가 - 세션 비율	- IPS를 설치한 환경에서 네트워크의 처리량, 지연율, 세션 비율의 속도 및 손실 비율을 측정
악의적 공격방어	- 고가용성 - 보안성능 - 디지털 백신	- IPS의 최대 부하 상태에서 정상 패킷 처리 및 악의적 패킷의 탐지 및 차단 능력을 측정
동시 세션 지원		- 평균 백만개의 동시 세션과 초당 26,000개의 새로운 세션들을 지원여부 확인
우회성능		- 소프트웨어 또는 하드웨어의 실패에 응수하여 우회 성능을 제공

<표 5> VPN 성능시험 항목

VPN 성능시험 항목		
항목	세부 항목	내용
원격 접속	브라우저 기반 접근	- 브라우저 기반 원격 접속 기능 확인
	VPN 터널 지원	- SSL 기반 암호 터널링 지원 확인
	포트 포워딩	- 포트 포워딩 기능 지원 여부 확인
원활한 통합		- 백엔드 사용자 리포지토리와 통합 - 기존 방화벽 인프라와 통합 - 자가 서명 인증서 지원
접근 제어		- 접근 제어 및 단말의 보안 기능 확인 - 사용자 정의된 포털 레이아웃 - 사용자 정의된 포털 레이아웃, 포트 포워딩 및 접근 정책을 통한 세분화된 접근 제어
확장성	동시 터널 지원	- 최고 25명까지의 동시접속자 지원 여부 확인

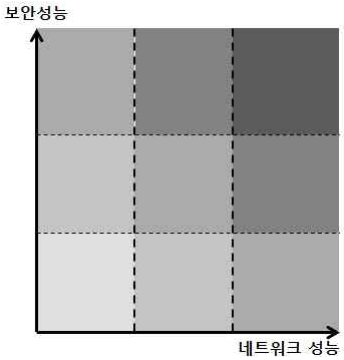
분하고 있으며, 기본 기능 평가는 관리 기능, 악의적인 데이터 탐색 및 인증, 트래픽 탐지, 로그 정보 저장 및 보고서 기능을 평가한다.

4.2.2 네트워크 보안 시스템 인증 방법

기존의 성능평가 방법에서 인증은 인증 기관의 평가 방법에 따라 3~4개의 등급으로 나누어 인증 로그를 부여하였다.

국내의 경우 성능평가를 요청한 구매자가 평가 요인을 선택하기 때문에 해당 평가 결과의 객관성이 부족했다. 이는 근본적으로 각 기업의 특성을 고려한 성능 평가 방법이 마련되지 않았기 때문이다. 어느 기업(구매자)은 보안성능은 어느 정도 갖추고 네트워크 성능을 중요한 이슈로 보안 시스템을 구매할 수 있고, 또 어느 기업은 네트워크 성능이 조금 보장되지 않더라도 높은 보안 기능을 요구할 수 있다[11-12].

한국형 네트워크 보안시스템 인증 방법론에서는 이러한 구매자들이 자신이 원하는 시스템을 조금 더 쉽게 고를 수 있도록 2-factor 인증을 제시하고자 한다.



<그림 2> 네트워크 정보보호 시스템 매트릭스

네트워크 정보보호 시스템을 보안 기능과 네트워크 성능 두 가지 기준으로 모두 평가하고 인증로그를 부여함으로써, 구매자의 성격에 맞는 시스템을 구매할 수 있도록 한다. 위 <그림2>는 보안성능과 네트워크 성능에 따른 정보보호 시스템을 나타내고 있다. 보안성능과 네트워크 성능 모두 우수한 제품이 가장 좋긴 하지만 제품의 가격을 고려하였을 때 기업의 입장에서는 그리 효율적이지 않다. 네트워크 정보보호 시스템을 보안 기능과 네트워크 성능 두 가지 기준으로 평가할 경우 구매자는 보안 성능과 네트워크 성능 관계에서의 Thresh-hold를

정하여 기업에서 필요한 네트워크 정보보호 시스템을 선택하는데 도움이 될 것이다.

Ⅳ. 결론

본 논문에서는 국내외 정보보호 시스템 성능 평가 방법에 대해 언급하면서 한국형 정보보호 시스템 성능평가 방법론에서 각 평가 방법의 단점을 극복하려 하였다. 한국형 정보보호 시스템 성능평가는 객관화된 형태의 성능 측정에 관한 기준과 방법을 제시해야 할 것이다. 또한 기업에서 필요한 네트워크 정보보호 시스템을 선택하는데 도움이 되도록 네트워크 성능과 보안성능 각각의 정량적인 점수를 제공해야 할 것이다.

나아가 다양한 성능 측정 기준과 성능 측정 방법은 추가적으로 확장함으로써 한국형 네트워크 보안 시스템 성능평가 방법을 업그레이드 시켜 나가야 할 것이다.

참고문헌

[1] 정지환, 김상영, 황선명, “네트워크 보안성능 및 보안성 평가 방법에 관한 연구,” 한국멀티미디어학회, 2003년도 추계학술발표논문집 2003.

[2] NIST FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” 2004.

[3] NIST FIPS 200, “Minimum Security Requirements for Federal Informationand Information Systems,” 2006.

[4] ISTF-003, “IP 계층에서의 VPN 보안기술 표준,” 한국정보통신기술협회, 2001

[5] ISTF-004, “침입차단시스템 로그형식 표준,” 한국정보통신기술협회, 2001

[6] TTAS. KO-12.004, “네트워크 보안 장비에 대한 성능 측정 방법,” 한국정보통신기술협회, 2006

[7] Tolly Group, http://tolly.com., 2011.

[8] ICSA Labs, http://www.icsalabs.com, 2011.

[9] VeriTest, http://lionbridge.com, 2011.

[10] NSS Labs, http://www.nss.co.uk, 2011.

[11] 허수만, 서희석, “계약망 프로토콜과 DEVS 모델링을 통한 센서네트워크 보안 모델의 설계,” 디지털산업정보학회 논문지, 4권, 4호, pp. 41-49, 2008.

[12] 이기성, 김태경, 서희석, “DEVS 모델링을 이용한 보안제품 공동평가 통계,” 디지털산업정보학회 논문지, 6권, 2호, pp. 71-80, 2010.

■ 저자소개 ■

주 승 환
Ju, Seung Hwan

2011년 3월~현재 한국기술교육대학교 컴퓨터공학과 (박사과정)
2011년 2월 한국기술교육대학교 컴퓨터공학과 (공학석사)
2009년 8월 한국기술교육대학교 컴퓨터공학과 (공학사)

관심분야 : 모바일 보안, 보안제품 평가, 악성코드 분석
E-mail : judeng@kut.ac.kr

서 희 석
Seo, Hee Suk

2005년 3월~현재 한국기술교육대학교 컴퓨터공학부 (부교수)
2005년 2월 성균관대학교 전기전자및컴퓨터공학과(공학박사)
2002년 2월 성균관대학교 전기전자및컴퓨터공학과(공학석사)
2000년 2월 성균관대학교 산업공학과(공학사)

관심분야 : 네트워크보안, 보안시뮬레이션, USN
E-mail : histone@kut.ac.kr

김 상 연
Kim, Sang Youn

2006년 3월~현재 한국기술교육대학교 컴퓨터공학부 교수
2004년 KAIST (공학박사)
1997년 KAIST (공학석사)
1995년 고려대학교 (공학사)

관심분야 : 햅틱, 가상현실, 로보틱스
E-mail : sykim@kut.ac.kr

논문접수일 : 2011년 8 월 25 일
수 정 일 : 2011년 9 월 8 일
게재확정일 : 2011년 9 월 10 일