한국산학기술학회논문지
Vol. 11, No. 8 pp. 3012-3020, 2010

VPN(Virtual Private Network) SW의 시험사례분석

김경묵[1], 양해술[1*]
[1]호서대학교 벤처전문대학원

VPN (Virtual Private Network) SW's examination example analysis

Kyung Muk Kim[1] and Hae-Sool Yang[1*]
[1]**Seoul University of venture and information, Hoseo University**

요 약 VPN은 원격지에서의 접속에 안전성을 부여할 수 있어 원격지에서의 이동 사용자 지원이 필수적으로 요청되는 오늘날 기업의 기본 커뮤니케이션 수단으로 VPN이 자리매김하고 있다. 본 연구에서는 VPN 소프트웨어 분야의 기반 기술을 조사하고 VPN 소프트웨어 시장 동향 및 표준을 조사하며 VPN 소프트웨어의 평가모델을 개발하고자 한다. 이를 위해 VPN 소프트웨어의 특성을 조사/분석하고 시장 동향 및 표준을 조사/분석하며 이를 기반으로 VPN 소프트웨어에 평가항목의 도출과 평가모델을 개발한다.

Abstract VPN can give safety in connection in Timbuc-too, by corporation's basis communication means today that transfer user support in Timbuc-too is required compulsorily, VPN is activated. This research wishes to investigate base technology of VPN software field and investigate VPN software market trend and standard and develop estimation model of VPN software. For this special quality of VPN software investigation / analyze and investigate or analyze market trend and standard this to VPN software to base deduction of estimation item and estimation model develop.

Key Words : VPN, Software testing, Testing case

1. 서론

VPN(Virtual Private Network)은 이제 기업의 기본 커뮤니케이션 수단으로 완전히 자리매김한 모습이다. 민감한 정보를 노린 사이버 공격이 심화되는 오늘날, 업무환경의 변화에 따라 원격지에서의 접속 또한 급격히 증가하고 있다. 이러한 변화를 수용하기 위해서는 편리하게 원격지 접속을 지원하면서 동시에 높아진 사이버 위협에 대응한 보안 요구 또한 충족시켜야 한다.

이러한 요구를 수용할 수 있는 것이 바로 VPN이다. VPN은 원격지에서의 접속에 안전성을 부여할 수 있어 원격지에서의 이동 사용자 지원이 필수적으로 요청되는 오늘날 기업의 기본 커뮤니케이션 수단으로 VPN이 자리매김하고 있다.

본 연구에서는 VPN 소프트웨어 분야의 기반 기술을 조사하고 VPN 소프트웨어 시장 동향 및 표준을 조사하며 VPN 소프트웨어의 평가모델을 개발하고자 한다. 이를 위해 VPN 소프트웨어의 특성을 조사/분석하고 시장 동향 및 표준을 조사/분석하며 이를 기반으로 VPN 소프트웨어에 평가항목의 도출과 평가모델을 개발한다.

2. 관련 연구

2.1 VPN 시장동향

2.1.1 IPSec에서 SSL VPN으로 전환

VPN은 IPSec에서 편리성이 보다 강화된 SSl(Secure Socket Layer) VPN으로 진화하고 있다. 기존 IPSec VPN

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.
(NIPA-2010-(C1090-1031-0001))
*교신저자 : 양해술(hsyang@hoseo.edu)
접수일 10년 06월 08일 수정일 (1차 10년 07월 30일, 2차 10년 08월 04일) 게재확정일 10년 08일 10일

기술은 확장성이 취약한 반면, SSL VPN은 사용자 또는 그룹별로 세분화돼 안전하면서 편리한 원격 액세스 방식을 제공하는데 있어 강력한 위력을 발휘한다. 이러한 이점을 갖는 SSL VPN은 사실상의 표준 접속 제어 메커니즘으로 발전하고 있다. SSL VPN은 최신 바이러스 백신 소프트웨어의 존재 여부와 연결 단말의 환경을 검사하는 등 사용자의 보안 상태를 검사하고 신뢰도 수준에 따라 액세스 권한을 동적으로 조정할 수 있어 보다 안전한 접속환경을 구현할 수 있다. 또 위치나 연결 장치와 상관없이 사용자에게 안전한 액세스를 동적으로 프로비저닝할 수 있어 관리 측면에서도 보다 유용하다[4]. NAT (Network Address Translation), 방화벽 트래버설(Firewall traversal)등과 같은 운영체제 조정, 혹은 네트워크 환경변경이 사용자나 IT 담당자의 개입 없이 투명하게 바로 처리할 수 있는 것. 더불어 모든 사용자에게 기업 표준 구성의 PC를 제공할 필요가 없기 때문에 하드웨어 비용도 절감할 수 있는 장점이 있다.

[표 1] IPSec VPN과 SSL VPN의 비교

특성	IPSec VPN	SSL VPN
기밀성	잘 알려진 암호 알고리즘	잘 알려진 암호 알고리즘
인증방법	IPSec 프로토콜	LDAP, 래디우스, 액티브디렉토리, PKI, 보안토큰
보안적용 레벨	네트워크 레벨(호스트/프로토콜)	애플리케이션 레벨(URL, 파일 공유, 포트, 호스트)
접근 옵션	전체 네트워크	웹, 클라이언트/서버, 터미널 서비스 등
사용자 장비	제한적 장비(VPN 클라이언트가 설치된 PC만 접근가능)	모든 장비(웹 브라우저를 사용할 수 있는 PC, 모바일 기기 등)
고가용성(HA) 지원	가능	가능
확장성	제한적	좋다
도입 비용	고비용	비교적 낮음

2.1.2 NAC·WAF 보완

VPN은 최근 보안 시장에서 주목받은 네트워크접근제어(NAC), 웹 애플리케이션 방화벽(WAF) 등을 보완한다는 측면에서도 주목된다. NAC는 네트워크에 접근하는 단말의 물리적 위치에 관계없이 보안 검사를 수행함으로써 네트워크를 보호하며 NAC 환경에서 원격 접속 시 접속 단말이 악의적인 공격의 발원지가 되지 않도록 하는 VPN은 상호연동을 통해 NAC를 보조하는 역할을 충분히 수행할 수 있다.

특히 NAC의 표준화가 아직 현재진행형이란 점은 NAC를 보완하는 SSL VPN의 중요도를 높인다. WAF와 SSL VPN의 기능 통합도 흥미로운 점이다. 애플리케이션 단에서 보안이 적용되는 SSL VPN은 웹 애플리케이션의 보안성을 지켜주는 WAF와 유사한 측면이 있어 시너지 효과를 낼 수 있다고 평가되며, 이러한 점에 착안해 WAF와 SSL VPN을 통합한 솔루션도 출시되고 있다.

2.2 VPN 기술동향

2.2.1 네트워크 접근관리 기능의 통합

NAC는 IP관리, 사용자인증, 접근관리, 패치관리, 자산관리, 데스크톱관리 등 지사 네트워크 관리에 필요한 통합된 관리 기능을 정책에 의해 관리할 수 있어 엄격한 보안성을 지키면서도 관리의 효율을 극대화시킬 수 있다.

그러나 NAC 제품들은 별도의 센서 장비를 네트워크에 연결해야 하기 때문에 추가적인 하드웨어 도입 비용이 발생하게 된다. 관리 용이성 향상을 위한 NAC 도입에 인프라 교체와 같은 막대한 비용이 들어간다면 NAC 도입은 망설여질 수 밖에 없는 문제다. 이로 인해 구축된 VPN 장비를 활용하는 방안이 모색되고 있다. 예를 들면, VPN 장비에 NAC 센서기능을 추가, OS 업그레이드만으로 손쉽게 NAC 환경을 구축할 수 있게 하고 있다.

2.2.2 멀티터널링과 다이나믹 라우팅 호환

표준 IPSec 기반의 VPN 터널은 인터넷에 연결된 두 대의 장비간에 암호화된 세션을 연결하는 방식이다. 암호화된 VPN 세션은 인터넷에 연결된 많은 장비들을 경유하기 때문에 중간에서 통신 장애가 발생할 경우, 이를 감지해 터널을 끊고 새로운 경로로 연결되도록 해야 한다. 멀티터널링 기술은 이러한 문제를 해결하기 위해 개발됐으며, L4 스위치 없이 멀티터널링과 다이나믹 라우팅(Dynamic Routing)의 연동을 통해 비용절감을 이룰 수 있게 된다.

2.2.3 암호화와 멀티캐스트 라우팅

VPN을 통해 멀티캐스트 전송망을 구성하기 위해서는 멀티캐스트 패킷을 전송할 수 있는 GRE(G-eneric Routing Encapsulation)와 같은 별도의 터널링이 필요하다. 이는 IPSec VPN 터널이 포인트 투 포인트 네트워크로 구성돼 멀티캐스트와 같은 포인트 투 멀티포인트 패킷은 직접 전송할 수 없기 때문이다. 또한 초고속 인터넷망을 통해 멀티캐스트를 전송하기 위해서는 가상의 터널링이 필요하다. 하지만 복잡한 네트워크[5]에서 이중화 구성을 하기 위해서는 PIM- SM(Protocol Independent Multicast -Sparse Mode) 방식의 멀티캐스트 라우팅 프로토콜을 지원해야 한다.

PIM-SM은 연결된 모든 네트워크로 멀티캐스트를 전송하지 않고, RP(Rendezvous Point)에 멀티캐스트 그룹에

조인해 등록된 네트워크로만 멀티캐스트 패킷을 전송함으로써 허브 앤드 스포크(Hub -and-Spoke) 방식으로 구성되는 트래픽 병목 현상을 현저히 줄일 수 있다. 또한 라우팅에 의해 경로를 선택할 수 있어 다른 네트워크 장비와 연동한 이중화 구성에도 용이하다.

2.2.4 QoS로 멀티미디어 패킷 전송 보장

기업 내에서 발생하는 실시간 트래픽(영상, 음성)은 지연(Delay)에 민감하기 때문에 최대한 지연을 발생시키지 말아야 한다. 이렇듯 우선순위가 높은 클래스를 먼저 처리하는 방식을 PQ(Priority Queue)라고 한다.

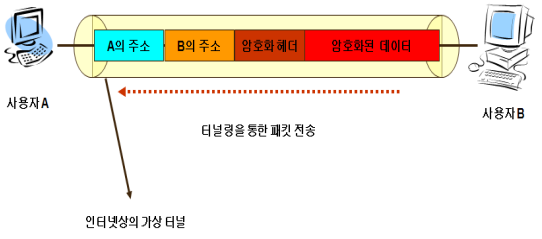
그러나 우선순위가 높은 클래스만 우선적으로 처리하면, 트래픽 병목이 지속적으로 발생할 경우에 클래스가 낮은 트래픽이 아예 처리되지 않을 수도 있다. 이와 달리 클래스별로 대역폭을 제한[6]하는 CBQ(Class Base Queue) 방식은 각 클래스별로 대역폭을 제한하는 방식이기 때문에 엄격한 QoS를 제공할 수 있지만, 트래픽 병목이 없는 상태에서도 클래스 정책에 제한되는 문제가 있어 대역폭을 효율적으로 사용하지 못하게 된다.

따라서 트래픽 병목이 발생할 경우 우선순위가 높은 트래픽을 우선적으로 처리하는 PQ와 우선순위가 낮지만 최소한의 통신을 위한 대역폭을 할당해 줄 수 있는 CBQ를 동시에 지원하는 QoS 매커니즘이 요구된다.

2.3 VPN 핵심기술

2.3.1 터널링(Tunneling) 기술

터널링 기술은 시작 지점에서 목표 지점까지 가상적인 터널을 형성하여 정보를 주고받도록 하는 기술로서 가상의 터널을 만들어 제 3자의 접근을 막는 비밀 통로 역할을 한다. 다음의 그림 1은 패킷 사용시 터너링의 기술을 나타낸 그림이다.



[그림 1] 터널링 기술

즉, 송신자가 보내는 데이터 패킷에 보안 헤더를 추가하여 원래 패킷을 캡슐화하는 방식으로 사전에 약속된 수신자 이외에는 알아 볼 수 없도록 패킷을 전송하는 기술이다.

2.3.1.1 Client to Server 터널링

이동 사용자가 자신의 기업 LAN으로 접속하는데 사용하는 방식이로, MS사의 PPTP (Point-to-Point Tunneling Protocol) 또는 시스코의 L2TP(Layer 2 Tunneling Protocol)의 2계층 터널링 프로토콜을 이용하여 구현하는 기술이다.

2.3.1.2 Host-by-Host 터널링

기업의 여러 LAN을 상호 연결하기 위한 것으로 IPsec(IP Security), IETF IPsec WG에서 표준화, 3계층 터널링 프로토콜이다. 그리고 인증과 암호화 프로토콜 데이터 인증, 패킷 무결성, 데이터 신뢰성, 응답보고, 암호화 키 자동관리 및 SA(Security Association)등을 규정으로 하는 기술이다.

2.3.1.3 VPN공급 업체들의 터널링 구현 기술

(1) MS : PPTP(Point to Point Tunneling Protocol)

Microsoft에서 개발하였으며, 서버가 NT계열이어야만 하는 제약이 있다. 터널의 유지, 보수, 사용에 있어서 TCP를 사용하며, PPTP를 지원하는 소프트웨어가 설치되어 있어야 한다.

클라이언트 개시 VPN에 사용된다. 초기에 1:1접속의 단점이 있었지만 현재는 개선되어 다중접속 지원을 한다.

(2) 시스코시스템스사 : L2F(Layer2 Forwarding Protocol)

NAS 개시형 Protocol 으로, 하나의 터널에 다중접속 지원하며, 접속, 유지에 UDP 사용한다.

(3) L2TP(Layer 2 Tunneling Protocol)

PPTP와 L2F 의 장점만을 수용하여 개선한 Protocol 으로 Microsoft, Cisco 사 모두 지원 (호환성 우수)한다. PPTP와 유사한 캡슐화(encapsulation)를 가졌으며, IPSec을 이용한 암호화 가능, PPP가 지원하는 여러가지 프로토콜 (X.25, Frame Relay, ATM ,etc..)상에서의 구현 가능하다. 그리고 UDP 사용하고 RFC2661 표준화의 기능이 있다.

(4) IPSec(IP Security Protocol)

IETF에서 제안을 했으며, VPN 구현에 널리 사용된다. ISAKMP(Internet Security Association and Key Management Protocol)/ IKE (Internet Key Exchange)를 이용해 보안관련협상(Security Association Negotiation)과 키 관리를 한다.

IPv6에서는 기본적으로 포함되어 있으며, IPv4 에서도 보안성을 위해 사용 권장하며, IPSec의 헤더 AH, ESP를 통한 보안 구현한다.

2.3.2 MPLS

Cisco Systems 의 Tag switching 기술과 IBM 사의 ARIS(Aggregate Route-based IP Switching) 를 결합해 IETF에서 정한 표준으로 패킷에 새로운 레이블 정보를 추가하여 MPLS 네트워크 안에서 레이블 정보를 이용하여 스위칭 한다. 레이블 스와핑은 현재 부여받은 레이블이 다음 라우터에서 새로운 레이블을 부여받는 것으로 레이블 스와핑을 반복하여 목적지에 도착하며, ATM, PPP, MAC 등 다양한 2계층 프로토콜을 지원한다.

기존 인터넷에 그대로 적용 가능하며, 레이블을 이용한 새로운 라우팅으로 기존의 패킷 라우팅 개선하며, Qos, VoIP 등 부가서비스 가능, 일정한 대역폭 할당 가능, RFC1918(사설 주소 할당 가능), 레이블을 이용한 자체적인 터널링 가능하다.

라우팅 테이블의 수가 급격히 증가 - 기존 라우팅 테이블 외의 레이블 스위칭 테이블을 가져야 하며 이로 인한 관리 문제 발생을 한다.

IPSec VPN에 비해 라우터의 부하를 줄일 수 있지만 암호화 기능이 IPSec에 비해 취약하다.

2.3.3 인증 및 암호화

터널링에 신뢰성 있는 보안 성능을 제공해 주는 기술이 인증 및 암호화 기술이다. 인증 기술은 사용자에 대한 인증과 전송된 데이터에 대한 인증으로 구분할 수 있으며, 사용자에 대한 인증은 VPN 게이트웨이로부터 이루어진다. 암호화 기술은 터널링을 통해 전달되는 데이터의 내용을 보호하기 위해 사용되는 기술로 이 과정은 암호 알고리즘과 키를 기반으로 수행된다. 인증 및 암호화 기술을 제공하기 위해서는 암호 알고리즘 등에 사용될 키를 협상하는 과정이 필요하며, 이를 수행하는 방법은 수동적인 방법과 자동적인 방법이 있다.

2.3.4 SSL VPN과 MPLS VPN

2.3.4.1 SSL VPN

암호화 인증 기능이 제공되는 SSL 프로토콜을 이용한다. SSL 프로토콜은 본래 웹을 기반으로 하는 통신을 보호하고자 사용되는 것으로 웹 브라우저를 이용해야 한다. 웹 어플리케이션만 지원 가능하다는 단점을 가지고 있어 각 어플리케이션이나 사용자 별로 수정해야 하는 불편함을 가지고 있다.

2.3.4.2 MPLS VPN

MPLS네트워크를 기반으로 해서 각 데이터 패킷에 레이블을 붙이고 이를 이용해서 트래픽을 분리하는 방식이다. MPLS 트래픽 엔지니어링 기능을 사용하여 서비스 품질의 차별적인 제공이 가능하고, 확장성도 보장 된다. 또한 서비스 사업자가 서비스를 운용 관리함으로써 고객 입장에서는 서비스를 아웃소싱할 수 있으며, 서비스 사업자의 경우는 여러 가지 부가서비스와 운용관리를 통합 지원함으로써 보다 고 부가가치의 서비스를 제공할 수 있게 된다.

3. VPN SW 품질 특성에 따른 수준 지표

본 연구에서는 품질 수준 지표를 소프트웨어 제품평가를 위한 국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 하여 구축하였다[1-3]. 즉, 주특성 6가지의 부특성에 대한 시험모듈에 일부가 표 2, 표 3, 표 4, 표 5, 표 6, 표 7과 같다.

3.1 기능성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 기능성의 5가지 부특성 중 사용자의 목적하는 바에 따라 적합한 기능을 제공하는 능력을 나태내는 적합성에 관한 시험모듈 표 2와 같다.

[표 2] 적합성 시험모듈

메트릭명			
	기능 정보 제공	계산식	기능 정보 제공 = B(문서에 언급된 기능 수)/A(프로그램에서 제공하는 모든 기능 수)
		결과 영역	0 ≤ 기능 정보 제공 ≤ 1
	경계값 정보 제공	계산식	경계값 정보 제공 = B(문서에 설명된 경계값 항목의 수)/A(프로그램 사용에 필요한 모든 경계값 항목의 수)
		결과 영역	0 ≤ 경계값 정보 제공 ≤ 1
	경계값 처리율	계산식	- 경계값 처리율 = B(각 항목별 테스트케이스 성공률의 합)/A(경계값 확인 대상 항목 수) - $B=\sum_{i=1}^{A}\frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 경계값 처리 기능 확인을 위해 수행한 테스트케이스 중 성공한 건수 - Total_TC : i 번째 경계값 처리 기능 확인을 위해 수행한 테스트케이스 수
		결과 영역	0 ≤ 경계값 처리율 ≤ 1

3.2 신뢰성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 신뢰성의 4가지 부특성 중 이전 버전에 대한 문제점을 해결하고 결함으로 인한 기능 장애를 피할 수 있는 능력인 성숙성에 관한 시험

모듈은 표 3과 같다.

[표 3] 성숙성 시험모듈

메트릭명	문제 해결 이력 정보 제공	계산식	- 문제해결이력 정보제공 = A(문제해결 이력 정보 제 공 여부)
		결과 영역	문제해결이력 정보제공 = Y or N or NA
	문제 해결률	계산식	문제해결률 = B(확인된 문제 해결 항목수)/A(시험 대상 문제 해결 항목수)
		결과 영역	0 ≤ 문제해결률 ≤ 1
	결함 회피율	계산식	결함 회피율 = 1- min(1, B(발견된 결함수)/A(단위 운용시간))
		결과 영역	0 ≤ 결함 회피율 ≤ 1

3.3 효율성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 효율성의 3가지 부특성 중 주어진 조건에서 기능을 수행할 때 반응시간, 처리시간, 처리율을 제공하는 능력인 시간효율성에 관한 시험모듈은 표 4와 같다.

[표 4] 시간효율성 시험모듈

메트릭명	평균 반응 시간	계산식	- 평균반응시간 = 1- min (1, B(반응평균시간)/A(반응평균시간의 한계값)) - B = $\frac{\sum_{i=1}^{n} T_i}{N}$ - Ti = i 번째의 테스트의 반응시간 - N= 반응시간 테스트 케이스 수
		결과 영역	0 ≤ 평균 반응 시간 ≤ 1

3.4 사용성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 사용성의 5가지 부특성 중 사용자가 제품을 활용하기 위한 방법이나 조건, 적절성 등을 파악할 숭 LtRP 하는 능력인 이해가능성에 관한 시험모듈은 표 5와 같다.

[표 5] 이해가능성 시험모듈

메트릭명	기능 이해도	계산식	기능 이해도 = A(제품설명서와 사용자 문서를 통해 이해할 수 있는 기능의 수)/B(전체 기능의 수)
		결과 영역	0 ≤ 기능 이해도 ≤ 1
	인터페이스 이해도	계산식	인터페이스 이해도 = A(인터페이스를 통하여 이해할 수 있는 기능의 수)/B(전체 기능의 수)
		결과 영역	0 ≤ 인터페이스 이해도 ≤ 1

3.5 유지보수성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 유지보수성의 5가지 부특성 중 발생하는 에러의 증상 및 장애원인을 진단하고 변경될 부분을 실벽 할 수 있게 하는 능력인 분석성에 관한 시험모듈은 표 6과 같다.

[표 6] 분석성 시험모듈

메트릭명	진단 기능 정보 제공	계산식	진단기능 정보제공 = A(진단기능에 관한 정보 제공 여부)
		결과 영역	진단기능 정보 제공 = Y or N or NA
	진단 기능 지원률	계산식	- 진단기능 지원 = B(각 항목별 테스트케이스 성공률의 합)/A(평가할 진단기능의 수) - B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 진단기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 진단기능 확인을 위해 수행한 테스트케이스 수
		결과 영역	0 ≤ 진단기능 지원 ≤ 1

3.6 이식성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 이식성의 5가지 부특성 중 제품이 요구하는 시스템 환경에 적응하는데 필요한 최소한의 조치만으로 이식될 수 있는 능력인 적응성에 관한 시험모듈은 표 7과 같다.

[표 7] 적응성 시험모듈

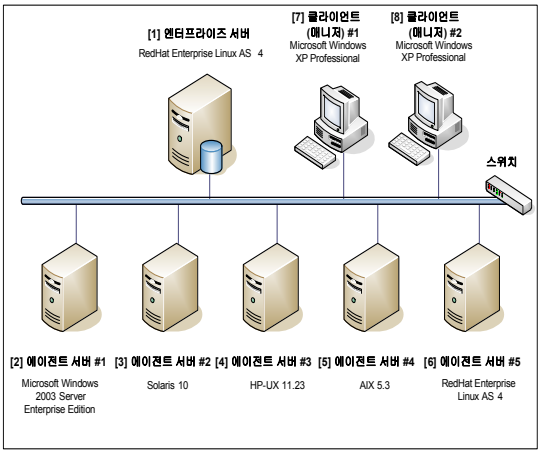
메트릭명	데이터 구조 적응 정보 제공	계산식	데이터구조 적응 정보제공 = A(데이터구조 적응에 관한 정보 제공 여부)
		결과 영역	데이터구조 적응 정보제공 = Y or N or NA
	데이터 구조 적응률	계산식	- 데이터구조 적응률 (DAR) = B(각 항목별 테스트케이스 성공률의 합)/A(평가할 데이터구조 적응시킬 데이터 항목수) - B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 데이터 항목 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 데이터 항목 확인을 위해 수행한 테스트케이스 수
		결과 영역	0 ≤ 데이터구조 적응률 ≤ 1

4. 시험사례에 대한 결함 및 평가방법 분석

4.1 시험을 위한 표준 환경 구축

VPN 소프트웨어는 저가의 고속 인터넷(공공망)을 사용하여 양쪽을 연결할 수 있으며, 재택 근무자나 출장중인 이동근무자도 회사로 안전하게 접속할 수 있다. VPN

은 한쪽에서 암호를 걸어 데이터를 보내고 다른 쪽에서는 그 암호를 풀어주는 방법으로 가상의 터널을 만들어 보안을 유지하며 시험 환경 구축은 그림 2와 같이 구축하였다.



[그림 2] 시험 환경의 구축

VPN 소프트웨어의 서버에 설치한 프로그램으로는 시험대상 엔터프라이즈 서버 모듈, DBMS : PostgreSQL v8.1.14를 설치하였고 에이전트 서버에 설치한 프로그램은 2 ~ 6번 서버에 시험 대상 에이전트 서버 모듈을 설치하였으며 클라이언트 7, 8 번에 설치한 프로그램은 엔터프라이즈 및 에이전트 서버의 환경설정과 로그 조회를 위한 매니져 프로그램과 일반 응용프로그램인 MS-office 2003, 한글 2002, 바이로봇 ISMS Client v3.5등을 설치하였다.

네트워크에 사용한 프로그램으로는 10/100M bps 스위칭 허브를 사용하였고, 성능측정도구로는 시험대상 제품의 자원 사용률을 측정하기 위해 TeamQuest v10.1을 1번 서버에 설치하였고 7번 클라이언트에는 TeamQuest view v10.1을 설치하였으며 가상 사용자 생성 및 부하 발생 프로그램인 LoadRunner v8.1은 8번 클라이언트에 설치하여 시험환경을 구축하였다.

4.2 결함내역 및 속성분석

4.2.1 결함 내역

"Ⅲ. VPN SW 품질 특성에 따른 수준 지표"에서 제시한 메트릭을 바탕으로 그림 2의 시험환경에서 시험한 결과 나타난 결함을 품질특성 및 결함속성별로 결함 건수 및 내역 등을 정리하면 표 8과 같다.

[표 8] 결함 건수 및 내역

품질 특성	결함 수	결함 정도	결함요약	최종 결함수
기능성	8	L	경계값 처리 미흡	0
		M	그룹 설정 기능 오류	
		M	기능 정보 미 제공	
		M	기능 정보 미 제공	
		M	메모리 정보제공 오류	
		M	비밀번호 암호화 표시 기능 오류	
		M	잘못된 기능 정보 제공	
		H	터미널 제어기능 오류	
사용성	12	M	계정 추가일관성오류	0
		M	그룹 버튼활성화 오류	
		L	기능 설명중복 제공	
		M	기능명일관성오류	
		M	도움말과 프로그램화면 불일치	
		M	도움말과 프로그램화면 불일치	
		M	도움말 미 제공	
		M	도움말화면 표시 오류	
		M	메뉴일관성 오류	
		L	불필요한 정보 제공	
		M	세션 로그화면 표시 오류	
		M	잘못된 오류메시지 제공	
유지 보수성	9	H	로그 출력 오류	0
		H	로그 출력 오류	
		H	로그 출력 오류	
		H	로그 출력 오류	
		H	로그 출력 오류	
		H	로그 출력 오류	
		H	로그 출력 오류	
		M	설정 정보 미 제공	
		M	폴더 경로설정 오류	
이식성	1	H	프로그램설치 오류	0
일반적 요구사항	1	M	제품 식별정보 미 제공	0
합계	31			0

4.2.2 결함속성 분석

VPN SW를 시험한 결과 총 31개의 결함이 발견되었으며 사용성의 결함이 가장 많은 12건의 결함이 발견되었고, 유지보수성 9건, 기능성 8건 등 순으로 발견되었으며 최종 수정후 결함은 발견되지 않았다.

VPN SW의 기능성 결함을 살펴보면 그룹 설정 기능, 메모리 정보 제공 기능, 터미널 제어 기능 등 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 제품에서 제공하는 기능이 정상 동작함을 확인하였으며, 신뢰성 결함은 시험 기간 중 프로그램이나 시스템 운영에 치명적인 영향을 미치는 중대결함은 발견되지 않았으며 메시지 처리 등을 통해 사용자 오조작을 방지

하고 있다. 효율성은 명시된 시험환경(하드웨어 및 소프트웨어, 네트워크 환경)에서 제품 구동시 엔터프라이즈 서버의 CPU 사용률과 메모리 사용량, 응답시간은 로그 발생 및 수집, 로그 재연, 로그 검색 시 [1]번 엔터프라이즈 서버의 CPU 사용률은 약 1% 미만을 유지하였고, 메모리 사용량은 평균 122MB로 일정한 상태를 유지하였다. 에이전트 서버에서 발생한 로그가 엔터프라이즈 서버로 수집되어 매니저 프로그램에 , 되는 평균 응답시간은 Solaris 서버가 2.54초, HP-UX 서버가 1.86초, AIX서버가 2.35초, RHEL 서버가 1.95초로 나타났다. 사용성의 결함은 사용자 매뉴얼과 프로그램 도움말에 기능에 대한 자세한 정보를 제공하여 제품 학습 및 구동이 용이하였으며, 그룹 버튼 활성화 오류, 계정 추가 일관성 오류 등과 같은 사용성 결함이 발생하였으나 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 이상이 없음을 확인하였다. 유지보수성 결함은 하였고, 메모리, $초, RHE제공 등과 같은 유지보수성 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 정상 동작함을 확인하였고, 지보수 결함은 Solaris 서버와 Microsoft Windows 2003 서버에 제품 설치 시 필요한 라이브러리 파일이 제공되지 않아 설치가 정상적으로 완료되지 않는 지보수 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 제품이 정상적으로 설치됨을 확인하였고, 명시된 시험환경(하드웨어 및 소프트웨어, 네트워크 환경)에서 프로그램이 무리없이 구동됨을 확인하였다. 일반적 요구사항의 결함으로는 관리자 매뉴얼과 설치 매뉴얼에 제품 버전이 표시되지 않는 일반적 요구사항 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거쳐 최종적으로 제품에 대한 정확한 정보를 제공함을 확인하였고, 사용자 매뉴얼에 제품 기능에 관한 정보를 비교적 상세히 제공하였다.

[표 9] 결함 속성 분석

품질특성	결함요약	결함수	결함백분율
기능성	기능 오류	3	37.5%
	처리 오류	0	0.0%
	기능 및 정보 미제공	2	25.0%
	기능 및 정보 표시 미흡	1	12.5%
	기타	2	25.0%
신뢰성	종료	0	0.0%
	중지	0	0.0%
	오조작 방지	0	0.0%
	기타	0	0.0%
사용성	미제공	1	8.3%
	미흡	0	0.0%
	오류	7	58.3%
	기타	4	33.3%
유지보수성	기능 오류	0	0.0%
	미제공	1	11.1%
	기타	8	88.9%
이식성	설치 및 삭제 오류	1	100.0%
	미제공	0	0.0%
	기타	0	0.0%
일반적 요구사항	미제공	1	100.0%
	기타	0	0.0%

4.3 성능 시험 결과

4.3.1 성능 시험

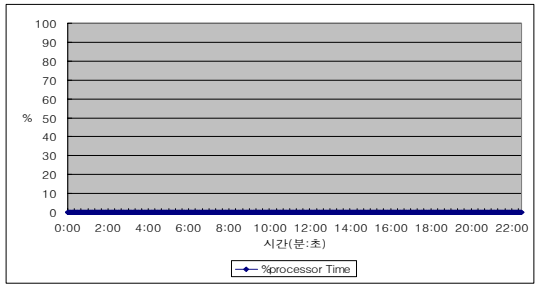
성능시험에서는 자원 효율성과 시간 효율성을 측정하였다.

[표 10] 성능 시험 내용

NO	내 용
no 1	대의 에이전트 서버(Solaris, HP-UX, AIX, RHEL)에 각각 25건의 로그를 발생하여 엔터프라이즈 서버(RHEL)로 로그가 수집됨 - 로그 발생 서버 : (3) ~ (60 에이전트 서버 #2 ~ 5 - 로그 수집 서버 : (1) 엔터프라이즈 서버 - 각 에이전트 서버당 로그 발생 건수 : 25건 - 엔터프라이즈 서버에 수집된 총 로그 건수 : 100건 로그 건당 명령어 입력 개수 : 10건
no 2	'no 1'에서 발생한 에이전트 서버(Solaris, HP-UX, AIX, RHEL)의 로그를 매니저 프로그램에서 각각 재연함
no 3	매니저 프로그램에서 엔터프라이즈 서버에 저장된 총 5,000건의 로그를 모두 검색할 경우
no 3	에이전트 서버에 접속하여 로그를 발생함 에이전트 서버에서 발생한 로그가 엔터프라이즈 서버로 수집되어 매니저 프로그램에 출력되는 응답시간을 측정함

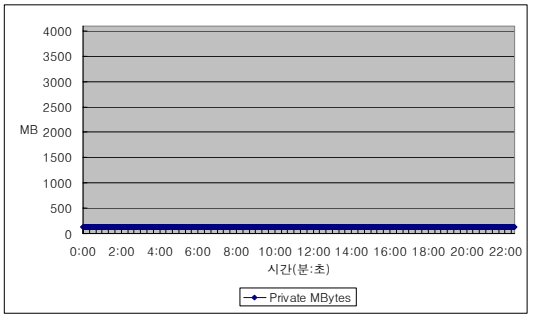
4.3.2 자원 효율성

CPU 사용률은 4대의 에이전트 서버(Solaris, HP-UX, AIX, RHEL)에 각각 25건의 로그를 발생하여 엔터프라이즈 서버(RHEL)로 로그가 수집될 경우와 로그를 매니저 프로그램에서 각각 재연할 경우, (1)번 엔터프라이즈 서버의 CPU 사용률이 약 1% 미만을 유지하였다.



[그림 3] CPU 사용률

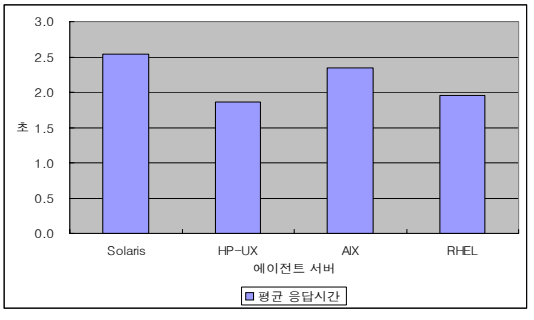
메모리 사용량은 4대의 에이전트 서버(Solaris, HP-UX, AIX, RHEL)에 각각 25건의 로그를 발생하여 엔터프라이즈 서버(RHEL)로 로그를 수집할 경우와 로그를 매니저 프로그램에서 각각 재연할 경우, 매니저 프로그램에서 5,000건의 로그를 검색할 경우, [1]번 엔터프라이즈 서버의 메모리 사용량은 평균 122MB로 일정한 상태를 유지하였다.



[그림 4] 메모리 사용률

4.3.3 시간 효율성

응답시간은 에이전트 서버에서 발생한 로그가 엔터프라이즈 서버로 수집되어 매니저 프로그램에 출력되는 응답시간은 아래와 같이 나타났다.



[그림 5] 시간 효율성

4.4 평가방법의 비교분석

표 11의 ISO/IEC 9126과 ISO/IEC 12119 기반의 품질평가에 대한 장단점과 기존의 평가 방법에 대해 기술하고 비교하였다. ISO/IEC 9126은 ISO/IEC 9126-2의 외부메트릭에 의한 평가와 ISO/IEC 9126-3의 내부메트릭에 의한 평가로 분류할 수 있다. 외부메트릭에 의한 평가는 국제표준을 기반으로 하여 상대적으로 높은 객관성을 가지며 실행 프로그램의 평가에는 적합하지만 라이프사이클 전반에 적용할 수 없다. 내부메트릭에 의한 평가는 높은 객관성을 가지며 실행 프로그램에 한정되지 않고 소프트웨어 개발 전 과정의 중간산출물 대상으로 하여 소프트웨어 라이프사이클 전반에 걸쳐 적용할 수 있지만 중간산출물의 품질 측정을 통해 최종 소프트웨어 제품인 실행 프로그램의 품질을 예측하는 수준에 그칠 뿐 확신할 수 없다는 단점이 있다.

ISO/IEC 12119 기반의 품질평가 방법의 경우에는 국제표준을 기반으로 하여 객관성을 확보할 수 있으며 소프트웨어의의 다수를 차지하는 패키지 소프트웨어의 평가에 적합하지만 기본적인 표준만으로는 일반적인 사무용 패키지 소프트웨어 중심으로서 다양한 소프트웨어 분야에 적용하기 쉽지 않다.

본 연구의 평가 방법은 ISO/IEC 9126과 12119를 기반으로 핵심적이고 최적화된 평가가 가능하지만 범용적인 품질평가 표준을 기반으로 하여 VPN 소프트웨어의 특성을 수용하여 구체화하였으므로 고유의 특성에 대한 반영이 미흡할 수 있으므로 향후, VPN 소프트웨어의 관련 표준을 프레임워크로 한 품질평가 방법에 대한 연구가 추진되어야 할 것으로 생각된다.

[표 11] 평가 방법의 비교

평가방법 \ 구분		장점	단점	비고
ISO/IEC 9126 기반의 평가방법	외부 메트릭 기반	국제표준을 기반으로 하여 상대적으로 높은 객관성을 가지며 실행 프로그램의 평가에 적합	실행 프로그램을 대상으로 평가하는데 한정되므로 라이프사이클 전반에 적용할 수 없음	
	내부 메트릭 기반	높은 객관성을 가지며 실행 프로그램에 한정되지 않고 S/W 개발 전 과정의 중간산출물 대상으로 함	중간산출물의 품질로 실행 프로그램의 품질을 예측하나 확신할 수 없음	
ISO/IEC 12119 기반의 품질평가 방법		국제표준을 기반으로 하여 높은 객관성을 가지며 S/W의 다수를 차지하는 패키지 S/W 평가에 적합	일반적인 사무용 패키지 S/W 중심으로서 다양한 S/W 분야에 적용하기 쉽지 않음	평가대상 S/W의확대를 위한 연구 활발
본 연구의 평가방법		ISO/IEC 9126과 12119를 기반으로 핵심적이고 최적화된 평가 가능	범용적인 품질평가 표준을 기반으로 VPN 소프트웨어의 특성을 수용하여 구체화하였으므로 고유의 특성에 대한 반영이 미흡할 수 있음	

5. 결론

본 연구에서는 VPN 소프트웨어 제품의 품질 수준을

파악할 수 있는 지표를 국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 도출하여 지표산식을 정의하고 지표의 결과를 산출하기 위해 필요한 수집항목을 선정하며 수집과 분석을 통해 실질적으로 어떤 결함 유형들이 주로 발생하고 있는지를 확인하였으며 VPN 소프트웨어에 대한 시험 평가 모델을 개발하여 시험 및 분석하였다.

향후 실질적인 활용을 통해 고품질 소프트웨어의 개발을 촉진함으로써 높은 부가가치를 창출하고 국제적으로 경쟁력을 갖춘 제품의 개발을 지원할 수 있을 것으로 기대한다.

참고문헌

[1] ISO/IEC 9126, “Information Technology - Software Quality Characteris- tics and metrics - Part 1, 2, 3"

[2] ISO/IEC 14598, "Information Technology - Software product evaluation - Part 1, 2, 3, 4, 5, 6"

[3] ISO/IEC 12119, "Information Technology - Software Package - Quality requirement and testing".

[4] International Data Corporation(IDC), "Worldwide Security Appliance Forecast and Analysis 2003-2007, 2003.

[5] H.Otrok, A.Mourad, M.Debbabi, C.Assi, "Improving the Security of SNMP in Wireless Network", WirelessCom 2005, pp.MA6-4, 2005. 1.

[6] Bat-Erdene Munkhbayar, Esbold Unurkhaan, Tsogtsalkhan Anar, Damdinsuren Erdenechineg, "Network Security Mangement in MUST", ICEIC 2006, pp.227~230, 2006. 1.

[7] 한국정보통신기술협회, “소프트웨어 테스트 전문기술”, 기초과정편, TTA, 소프트웨어시험인증센터, 2006.

[8] 한국정보통신기술협회, “소프트웨어 테스트 전문기술”, 응용과정편, TTA, 소프트웨어시험인증센터, 2006.

[9] 양해술, “바이오 정보처리 소프트웨어 품질 평가 방법 연구”, 한국정보통신기술협회 최종보고서, 2004(11)

김 경 묵(Kyung-Mook Kim) **[정회원]**

- 1983년 2월 : 건국대학교 사학과 졸업(학사)
- 1985년 2월 : 건국대학교 서양사학과 졸업(석사)
- 2008년 3월 ~ 현재 : 호서대학교 벤처전문대학원 정보경영 전공 박사과정
- 2001년 3월 : KAIST 텔레콤 최고경영자 과정 수료
- 2004년 1월 ~ 2005년 12월 : 전자신문사 편집국 IT부 부국장
- 2005년 1월 ~ 2006년 12월 : 전자신문사 편집국 총괄 부국장
- 2007년 1월 ~ 2008년 12월 : 전자신문사 고객서비스국 국장
- 2008년 1월 ~ 2009년 4월 : 전자신문사 정보사업국 국장
- 2009년 12월 ~ 현재 : 지디넷코리아 편집국장 겸 상무

<관심분야>
IT정책 및 정보화 방법론, S/W공학(특히, S/W 품질보증과 평가 및 감리 컨설팅, SI), 품질경영.

양 해 술(Hae-Sool Yang) **[정회원]**

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 S/W공학 전공(공학박사)
- 1975년 5월 ~ 1979년 6월 : 육군중앙경리단 전자계산실 시스템분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대학교 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本 오사카대학교 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국소프트웨어품질연구소 소장
- 1999년 11월 ~ 현재 : 호서대학교 벤처전문대학원 교수
- 2010년 3월 ~ 현재 : 호서대학교 글로벌창업대학원 원장

<관심분야>
S/W공학(특히, S/W 품질보증과 품질평가, 품질감리 및 컨설팅, OOA/OOD/OOP, SI), S/W 프로젝트관리, 품질경영.