제6회 ION 2002 IPSec VPN 분야 시험결과

김동호 | TTA IT시험연구소 네트워크시험센터
네트워크장비시험팀 선임연구원
석동현 | TTA IT시험연구소 네트워크시험센터
테스트베드운영팀 전임연구원
장광익 | TTA IT시험연구소 네트워크시험센터
테스트베드운영팀 전임연구원
성종진 | TTA IT시험연구소 네트워크시험센터
테스트베드운영팀 팀장
박용범 | TTA IT시험연구소 네트워크시험센터
네트워크장비시험팀 팀장

1. 시험 개요

인터넷망을 이용하는 가상사설망(VPN: Virtual Private Network) 서비스의 핵심은 완벽한 보안환경을 제공하는 데 있다. 따라서 보안기능은 VPN 서비스의 가장 중요한 요소이며, 이러한 보안기능을 가능케 해주는 기술로는 크게 "터널링(Tunneling) 기술"과 "암호화(Encryption) 기술"을 꼽을 수 있다.

VPN에서 사용되는 터널링은 시작지점에서 목표지점까지 터널을 형성한다는 의미로서 인터넷 네트워크상에서 외부의 영향을 받지않는 가상적인 터널을 형성해 정보를 주고받는다는 뜻이다. 이는 네트워크상의 터널과 관련해 상호 약속된 프로토콜로 세션을 구성하고 이 터널은 다른 사용자로부터 보호를 받는다는 것이 터널을 구성하는 중요한 목적이다. 현재 터널링/암호화를 구현하는 기술로는 마이크로소프트(MS)사의 "PPTP(Point to Point Tunneling Protocol)", 베이네트웍스사의 "VTP(Virtual Tunneling Protocol)", 시스코시스템스사의 "L2F(Layer 2 Forwarding Protocol)" 등과 이미 표준화가 이뤄진 "L2TP(Layer 2 Tunneling Protocol)", "IPSec(IP Security Protocol)" 등이 있다. 그러나, 현재 관련 기술에 대해서 완벽하게 표준화가 완료된 것은 아니다.

이러한 배경으로 인해 제품을 직접 생산하는 벤더뿐만 아니라 학계와 연구소가 연계하여 IPSec 분야에서의 상호운용성 확보에 전 세계적으로 매우 활발하게 노력하고 있으며, 국내에서도 지난 2002년 11월 TTA에서 국내 최초로 IPSec 분야 단체 상호운용성 시험이 개최되었다.

TTA를 비롯해 개방형컴퓨터통신연구회(OSIA), 한국전자통신연구원(ETRI) 공동 주최로 11월 25일부터 11월 29일까지 실시한 이번 시험에는 IPSec 분야의

핵심 기술을 보유하고 있는 선도 기업인 ㈜어울림정보, ㈜리눅스시큐리티, ㈜시큐아이닷컴, ㈜시큐어소프트, ㈜시그엔, ㈜시큐어넥서스 등 7개사가 참여하였으며, 세계적인 VPN 장비업체인 CISCO systems와 NetScreen Technologies가 참여하였다. 또한, 상용 시험기를 제조하고 있는 세계적인 시험기 제조회사 3개 기업인 Agilent Technologies, IXIA, Spirent Communications가 후원 기관으로 참여해 계측기 및 인력을 무상으로 제공하여 시험 수행을 지원하였다.

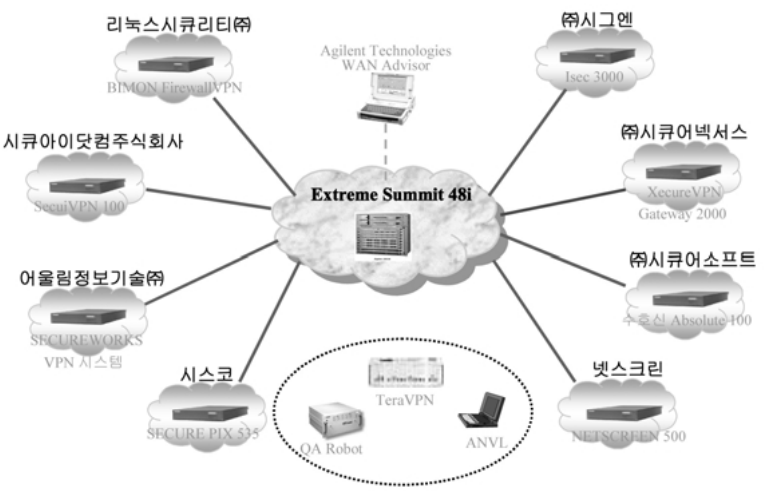
시험 내용은 상용 시험기가 제공하는 총 300여 개의 테스트 케이스에 대한 적합성 시험(Conformance Test)을 통한 IPSec Protocols에 대한 구현현황 체크와 각 제품들간의 상호운용성에 대해 검증하는 것 등이다. 이를 위해 별도의 망을 구성하였으며, 망 구성에 대한 자세한 사항은 시험환경 구성에서 언급한다.

2. 시험환경 구성

참여업체들의 장비는 IPSec 기반 VPN gateway 장비로 총 8개였다. 시험환경은 [그림 1]에 나타내었으며, 해당 업체들간의 보안을 위해 두 업체씩 Extreme Summit 48i Layer3 이더넷 스위치를 사용하여 VLAN(Virtual Local Area Network)으로 분리하였다.

3. 시험항목

금번 시험에서는 IPSec 신기술임을 감안하여 시험을 크게 각 장비들의 기능 적합성을 시험하는 적합성 시험(Conformance Test)과 호환성 및 연동성을 시험하는 상호운용성 시험(Interoperability Test)으로 나누어 수행하기로 결정하였으며, 그 중 적합성 시험은 자체 구성하여 시험을 하기에는 시간이 너무 많이 소요된다는 제약조건으로 인해 상용시험기인 Agilent Technologies QARobot 시스템 및 Ixia ANVL 시스템이 제공하는 총 450여 개의 테스트 케이스를 사용하



[그림 1] IPSec VPN 상호운용성 시험망 구성도

였다.

위와 같은 방법으로 최종 시험에 사용된 상호운용성 시험 항목은 아래와 같다. 각 항목은 별도의 망 구성을 요하므로, 전체 시험망에서 필요에 따라 망을 구성하여 독립적으로 활용하였다.

적합성 시험 항목

IPsec Core Protocol

▷ AH(MD5, SAH1), ESP(DES, 3DES), Pre-shared Key IKE, etc.

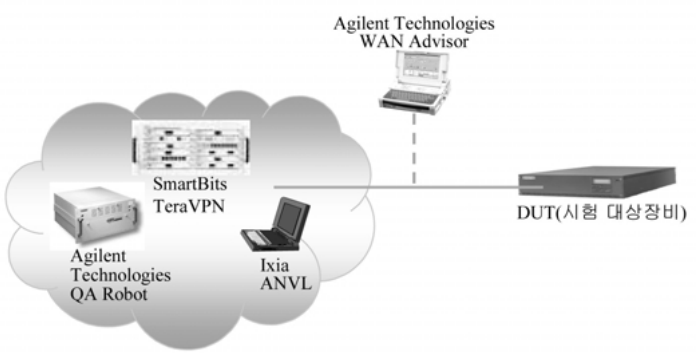
상호운용성 시험 항목

- Basic IPsec/IKE Communication
- IPsec Communications with Manual Key
  - ▷ IPsec/IKE with Pre-shared Seret
  - ▷ Interoperability for non-standard Encryption Algorithms(AES, SEED, BLOWFISH, etc.)
  - ▷ IPCOMP. Communications
  - ▷ AH/ESP/IPCOMP Combined Communication
- IPsec Fragment & PMTU Discovery
  - ▷ IPsec Fragment/Reassembly Issue
  - ▷ IPsec Path MTU Discovery
- IKE Proposal Exchange & ID Type
  - ▷ Phase 1 Multi-Proposal Exchange
  - ▷ Phase 2 Multi-Proposal Exchange
- IKE with PKI Certificate
  - ▷ X.509
  - ▷ CDP(CRL Distribution Point) and CA Revocation
- SA Expire & Re-Key Issue
  - ▷ Re-Keying when Lifetime/SA Expire SA Expire
- NAT-Traversal
  - ▷ Packet Fragmentation Problem with ESP-UDP
- Hub & Spoke VPN

4. 시험방법

시험 방법은 적합성 시험 방법과 상호운용성 시험 방법으로 나누어 설명할 수 있으며, 적합성 시험에서 사용한 시험망은 아래 [그림 2]와 같다.

[그림 2]에서 보는 것처럼 DUT(Device Under Test)는 시험 대상장비를 지칭하며, 본 시험에서는 해



[그림 2] IPSec 표준 적합성 시험 환경

당 참여업체의 VPN 장비가 해당된다. Monitoring 장비를 활용하는 것은 시험시 DUT에 문제점이 발생했을 경우에 보다 쉽게 문제점을 찾아내기 위함이다.

5. 시험결과 및 결론

적합성 시험을 수행한 결과 대부분의 업체가 IPSec Protocol 표준을 정확하게 이해하고 있었으며, 적합성 면에서는 상용서비스도 문제없는 수준임을 확인하였다. 상호운용성 시험 부분에서도 각 장비간 IPSec Protocol 호환성이 상당히 진척되어 있음을 확인하였다.

또한, 시험 도중 동종의 제품간 구현방법의 차이를 발견할 수 있었으며, 여기에 대해 심도있는 토론을 벌일 수 있었던 자리가 마련되었다. 이러한 자리를 통해 시험 도중 발견한 표준의 애매모호함을 곧바로 기술표준에 피드백할 수 있는 기회 역시도 얻게 되었다.

이러한 상호운용성 시험을 국내에서 개최하였다는 사실은 이 분야의 국내 기술이 일정 수준이상 성숙했음을 증명하는 것으로써, 지속적인 상호운용성 시험은 국내 기술력 보강은 물론, 현재 시장 성숙단계에 있는 IPSec 관련 시장을 확산시키는 촉매 역할을 할 것으로 사료된다.

한편, TTA는 2003년 국제 IPSec 상호운용성 시험의 공동개최에 대하여 의사를 타진하고 있으며, 이를 통해 관련 업체들의 기술력뿐만 아니라 시험 방법론 연구에서도 세계적인 수준으로 끌어올릴 수 있으리라 기대된다.

W3C, XML 관련 암호 승인

앞으로는 웹 문서의 중요 부분만 뽑아 암호화할 수 있게 될 전망이다. C넷(http://www.cnet.com)에 따르면 인터넷 표준화단체인 W3C가 확장성 표기언어(XML:eXtensible Markup Language)와 관련한 새로운 암호규격 2개를 승인했다. 새 암호규격은 'XML 암호구성 및 처리과정(XML Encryption Syntax and Processing)'과 'XML용 해독 전환 서명(Decryption Transform for XML Signature)' 등으로 두 규격 모두 웹사이트 보안개선 목적을 갖고 있다. 이번에 승인된 두 규격은 특히 XML로 제작된 웹페이지 문서의 일부분을 암호화할 수 있다. 즉, 기존 방식이 XML문서 전체를 암호화하는 반면 이번 규격들은 XML문서의 선택된 부분이나 요소의 암호화를 가능하게 한다. 이에 따라 이 규격을 활용하면 XML기반 전자상거래 사이트 구축시 웹페이지 전체를 암호화하지 않고 신용카드번호만을 암호화한 형태로 웹페이지를 구성할 수 있게 된다. W3C의 관계자는 "이번 규격들을 사용하면 웹 저작자에 의해 이미 보안성을 갖고 있는 XML문서의 일부분을 다시 암호화하게 되는 셈으로 암호기술을 두번 적용하게 되는 것"이라면서 "새 규격들이 XML은 물론 앞으로 특정 형태의 데이터 교환을 위해 만든 암호로 구축하는 웹사이트 발전을 한층 더 가속화할 것으로 기대된다"고 강조했다.