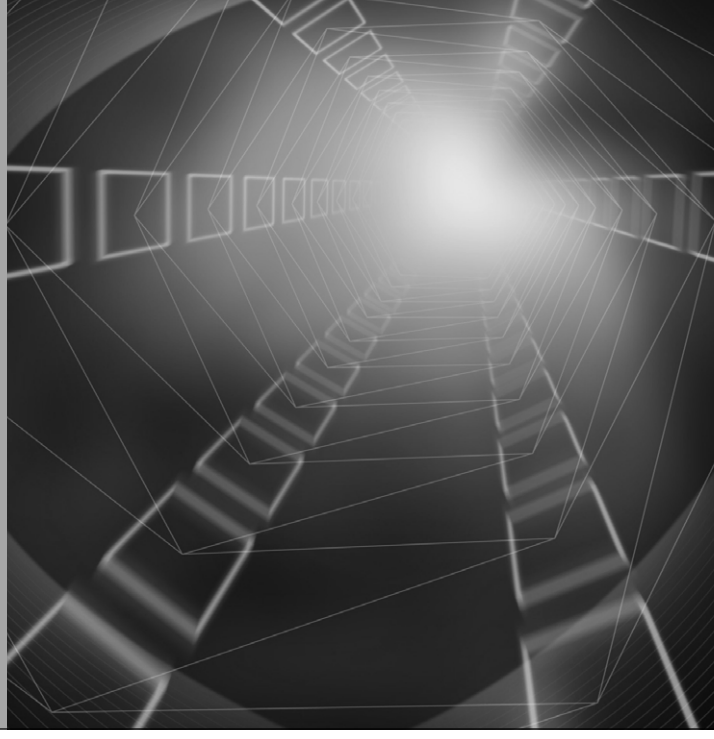
제8회 ION 2003 IPsec VPN 분야 시험 결과



김동호 / TTA IT시험연구소 네트워크시험센터
무선네트워크시험팀 선임연구원
김영진 / TTA IT시험연구소 네트워크시험센터
무선네트워크시험팀
박용범 / TTA IT시험연구소 네트워크시험센터
디지털홈시험팀 팀장

1. 시험 개요

인터넷 공중망을 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 송신측에서 수신측까지 터널을 형성한다는 의미로서 인터넷 네트워크상에서 외부의 영향을 받지 않는 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/암화화를 구현하는 기술로는 마이크로소프트(MS)사의 "PPTP(Point to Point Tunneling Protocol)", 베이네트웍스사의 "VTP(Virtual Tunneling Protocol)", 시스코시스템즈사의 "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 전세계적으로 매우 활발하게 노력하고 있으며, 국내에서도 지난 2003년 11월 TTA의 OpenLab에서 2002년 11월에 이어 두 번째로 IPsec 분야 VPN 단체 상호운용성 시험이 개최되었다.

한국정보통신기술협회(TTA)와 정보보호산업협회(KISIA) 공동 주최로 11월 17일부터 11월 22일까지 총 5일간에 걸쳐 실시한 이번 시험에는 IPsec 분야의 핵심 기술을 보유하고 있는 선도 기업인 ㈜퓨쳐시스템, 시큐아이닷컴㈜, ㈜어울림정보기술, 장미디어인터렉티브, ㈜시큐어소프트, ㈜인프니스, NetScreen Technologies 등 7개사가 참여하였다. 또한, 상용 시험기를 제조하고 있는 세계적인 시험기 제조회사인 IXIA, Spirent Communications, Matsushita Electric Works가 후원 기관으로 참여해 계측기 및 기술지원을 무상으로 제공하여 시험 수행을 지원하였다.

시험 내용은 상용 시험기가 제공하는 총 300여 개의 시험 항목에 대한 적합성 시험(Conformance Test)을 통한 IPsec Protocols에 표준에 따른 구현 여부를 체크하였다. 그리고, 별도의 독립된 장소에서 수행된 성능시험(Performance Test)을 통하여 각 회사 장비의 VPN 성능을 체크할 기회를 제공하였으며, 상호운용성 시험을 통해 서로 다른 업체 제품들간의 상호연동성을 검증하였다. 이를 위해 별도의 망을 구성하였으며, 망 구성에 대한 자세한 사항은 시험 환경구성에서 언급한다.

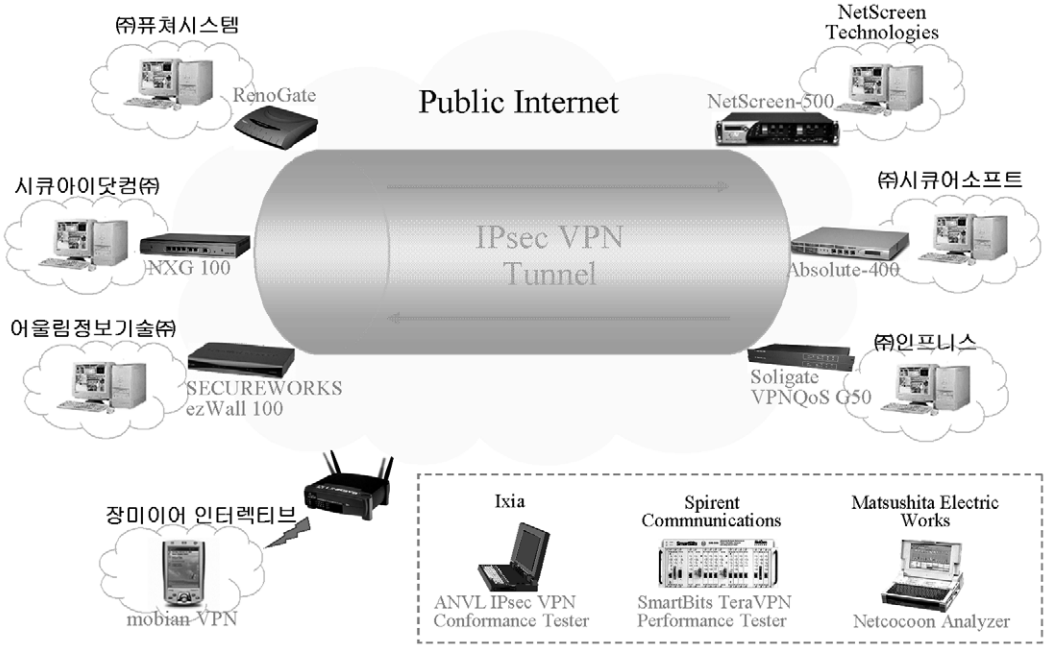
2. 시험 환경구성

참여업체들의 장비는 IPsec 기반 VPN gateway 장비 6개와 무선클라이언트 1개로 총 7개였다. 시험 환경은 [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. 시험 항목

금번 시험에서는 IPsec은 현재 표준화가 진행중인 신기술임을 감안하여 시험을 크게 각 장비들의 기능 적합성을 시험하는 적합성 시험(Conformance Test)과 호환성 및 연동성을 시험하는 상호운용성 시험(Interoperability Test)으로 나누어 수행하였으며, 그 중 적합성 시험은 상용시험기인 Ixia의 ANVL IPsec VPN 적합성 시험 시스템이 제공하는 총 300여 개의 테스트 케이스를 사용하였다.

위와 같은 방법으로 최종 시험에 사용된 상호운용성 시험 항목은 아래와 같다. 각 항목은 별도의 망 구성을



[그림 1] IPsec VPN 상호운용성 시험망 전체 구성도

요하므로, 전체 시험망에서 필요에 따라 망을 구성하여 독립적으로 활용하였다.

적합성 시험 항목

- IPsec Core Protocol
  - ▷ ESP(AES, 3DES), Pre-shared Key IKEv1, etc.

상호운용성 시험 항목

- Basic Communication[Pre-shared Secret, Main Mode(유선간)/Aggressive Mode(유무선간)]
  - ▷ IPsec :
    Protocol : ESP[RFC2406]
    ESP encryption : AES with 128-bit keys in CBC mode[RFC3602] and SEED
    ESP integrity : HMAC-SHA1-96[RFC 2404]
  - ▷ IKEv1 :
    Encryption : AES with 128-bit keys in CBC mode[RFC3602] and SEED
    Pseudo-random function : HMAC-SHA1 [RFC 2104]
    Integrity : HMAC-SHA1-96[RFC2404]
    Diffie-Hellman group : 1024-bit MODP [RFC2409]
- IPsec Communications with Manual Key
  - ▷ IPsec/IKEv1 Communications
  - ▷ IPCOMP. Communications
- 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
- SA Expire & Re-Key Issue
  - ▷ Re-Keying when Lifetime/SA Expire SA Expire
- NAT-Traversal
  - ▷ Packet Fragmentation Problem with ESP-UDP
- Hub-and-Spoke VPN

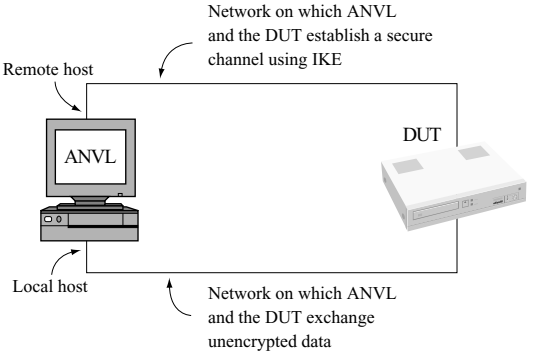
성능 시험 항목

- IPsec Tunnel Capacity
  - ▷ Tunnel(phase 1, phase 2) setup rate
  - ▷ Tunnel Capacity

4. 시험 방법

4.1 적합성 시험

적합성 시험에서 사용한 시험 구성도는 아래 [그림 2]와 같다.



[그림 2] 적합성 시험 구성도

적합성 시험기로 Ixia의 ANVL을 사용하여 표준에 정의된 서로 다른 인증 및 암호 알고리즘에 따른 각 Gateway의 IPsec 표준 적합성을 시험하였다. 이때 사용된 시험 항목 수는 300여 개이다.

4.2 상호운용성 시험

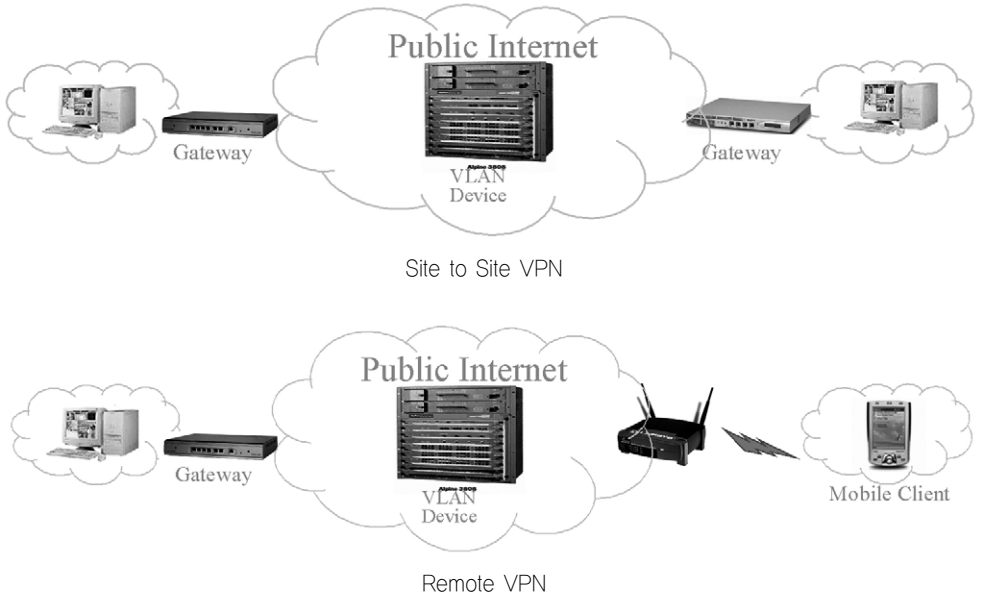
가. 기본 상호운용성

[그림 4]에는 각 VPN 업체들에 대한 상호운용성 시험을 위한 구성도이다.

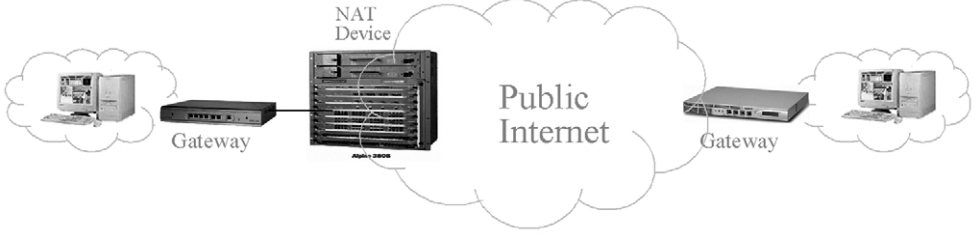
[그림 4]에서 볼 수 있듯이 Gateway들간의 상호운용성 시험은 Site to Site VPN 망을 구성하여 시험을 하였으며, Gateway와 Mobile Client 사이의 상호운용성 시험은 Remote VPN 망을 구성하여 IPsec 통신을 시험하였다.

나. NAT-T

[그림 5]에는 NAT-T를 시험하기 위한 구성도이다.



[그림 4] 기본 상호운용성 시험 구성도



[그림 5] NAT-T 시험 구성도

IPv4 주소의 부족을 해결하기 위한 방법으로 널리 사용되고 있는 NAT 장비가 VPN Gateway 사이에 존재할 경우에 대해 각 Gateway가 NAT 장비의 존재를 인식하고 정상적인 IPsec 통신이 가능하지에 대한 시험을 수행하였다.

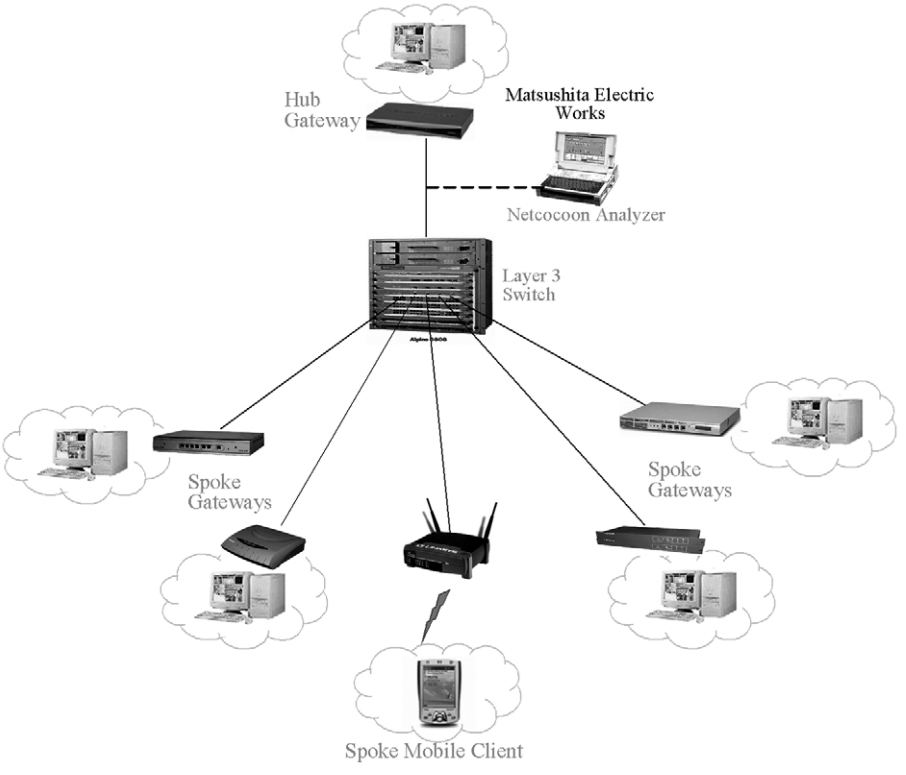
다. Hub-and-Spoke

[그림 6]에는 Hub-and-Spoke 시험을 위한 구성도를 나타내고 있다.

다수개의 VPN Gateway들이 존재하는 망 환경에서 두 Gateway들 간의 통신을 하기 위해 모든 Gateway를 Full-mesh로 연결하지 않고 모든 통신을 Hub Gateway를 거쳐 이루어지는가를 시험하였다.

5. 시험 결과 및 결론

제2차 VPN 상호운용성 시험 행사에서는 2002년 제1차 상호운용성 행사에 이어 IPsec의 표준 기능확인은 물론, IKE 암호화 알고리즘 및 각종 인증 알고리즘에서의 상호 동작을 확인하였으며, 특히 현재 국제적으로 크게 이슈가 되고 있는 NAT-T와 Hub and



[그림 6] Hub-and-Spoke VPN 시험 구성도

Spoke 통신 등 VPN 시스템의 핵심 기능과 최신 기술들에 대한 상호운용성을 검증하였다.

금번 VPN 단체 상호운용성 시험 결과, 참여한 업체 대부분의 장비들이 IPsec 기본 통신과 Hub and Spoke VPN 통신 및 무선 클라이언트와의 통신에는 큰 문제가 없이 상호운용이 되는 것을 확인하였다. 특히, 국내 표준 암호알고리즘인 SEED와 새로운 국제 표준 암호알고리즘으로 자리잡은 AES를 이용한 통신에 모든 업체들이 호환성을 확보한 것이 이번 상호운용성 시험 행사를 통한 가장 큰 수확이었다.

그러나, 현재 표준화가 마무리 단계에 있는 NAT-T의 경우에는 업체들이 서로 다른 버전으로 구현되어 있어 일부 업체들만 호환이 되었다.

따라서, 2004년에는 NAT-T 시험과 더불어 현재 표준화가 진행 중인 IKEv2에 대한 상호운용성 확보가 중요하며, TTA에서는 업체를 통해 이러한 요구가 있을 경우를 대비하여 시험 환경구축 및 상호운용성 시험 행사를 준비 중에 있다. 또한, TTA는 2004년 국제 IPsec 상호운용성 시험의 공동개최에 대하여 의사를 타진하고 있다.