선택이 아닌 필수!
도입 결정은 빠를수록 유리
SSL VPN 솔루션

글 | **송태호** (주)인성디지탈 주니퍼사업부 팀장 thsong@isd.co.kr

인성디지탈은 기업 정보시스템의 인프라가 되는 주요 업무용 소프트웨어, 그래픽, 보안, 백업 솔루션 제품군, 그리고 하드웨어 제품군 등 IT 전 부문에 걸쳐 고객이 필요로 하는 토탈 솔루션을 제공하고 있다.
소프트웨어와 네트워크 사업으로 시장 경험을 쌓아왔던 인성디지탈은 하드웨어 사업으로 그 영역을 확장함으로써 더욱 경쟁력있는 e-솔루션 사업 영역을 갖추고 IT 사업을 위한 새로운 도약을 준비하고 있다.

● 불과 몇 년 전만 해도 많은 정보를 가진 회사가 기업경쟁력의 우위를 점했지만, 이제는 더 이상 정보의 수가 중요하지 않게 되었다. 오히려 기업의 자산을 얼마나 잘 지키고, 권한있는 직원이 그 역할에 따라 시기적절한 접근이 가능한지가 기업 생존력의 관건이 되었다.

기업의 핵심자산을 지키기 위해선 보안의 핵심요소인 기밀성, 무결성, 가용성을 보장해야 한다. 물론 오프라인 시대에는 이러한 요소가 중요했으나 비즈니스 형태가 온라인으로 갈수록 이 세 가지 외에 인증, 부인방지, 접근통제, 책임 추적성 등의 요소까지 필요하게 되었다.

그 중에서도 기밀성과 가용성은 서로 상충되는 개념으로 둘 다 만족시키기가 어려웠다. 이러한 관점에서 SSL VPN은 바로 보안에 대한 일곱 가지의 모든 요소를 갖춘 차세대 접근 및 권한 관리 솔루션으로 기업의 핵심 자산에 대한 접근을 효과적으로 지키는 데 기여할 것이다.

기업 내 핵심 시스템을 안전하게 활용하기 위해서는 기업은 첫째, 사용자의 신원을 확실하게 증명하고 둘째, 정책 결정을 위해 사용자의 엔드 포인트에서 이뤄지는 작업 내역을 파악해야 하고 셋째, 해당 사용자가 사용하는 애플리케이션을 파악해야 한다.

또한 기업은 LAN 내외부의 모든 사용자에 대한 인증을 수행해야 하고 사용자 단말 장비의 계정과 보안, 시스템 상태 등을 확인하기 위해 엔드 포인트 시스템에 대한 조사를 실시해야 한다.

또한 관련 정보를 기반으로 정책을 작성한 후 이를 토대로 자원에 적합한 액세스 권한을 승인해야 한다.

최근의 환경은 오프라인 기반에서 인터넷 기반의 온라인 서비스로 비즈니스의 중심이 옮겨갔으며, 기업환경에서도 지점과 재택근무, 해외지사로까지 업무가 확장되어 갔다.

이렇듯 업무의 구성환경이 조직 내의 범위를 벗어나 협력사, 공급사, 파트너, 외주 업체, 아르바이트, 파견자 등등으로 다양하게 확대되었다. 이제 고객은 보안성을 높이면서 직원들의 편리성까지 만족킬 수 있는 솔루션과 서비스를 원하게 되었다. 〈표1 참조〉

주니퍼 SSL VPN 솔루션

주니퍼 네트웍스의 SSL VPN 장비를 이용하면 원격 · 모바일 직원, 비즈니스 파트너, 고객 등이 클라이언트 소프트웨어를 설치하거나 서버를 변경할 필요가 없으며, 지속적으로 유지보수를 하지 않고도 필요한 애플리케이션과 자원을 액세스 할 수 있다. SSL VPN은 외부 사용자와 내부 사용환경 사이에 설치되며 모든 표준 웹 브라우저에서 볼 수 있는 SSL을 사용해 안전한 전송을 제공한다.

주니퍼 네트웍스의 SSL VPN은 사용자와 자원 간의 모든 접촉을 중개하는 한층 강화된 플랫폼으로서 LAN에 보안 레이어를 추가하게 된다. 그리고 SSL VPN은 애플리케이션 계층에서 작동하기 때문에 다양한 접근 방식, 강력한 액세스 권한 관리, 매우 세밀한 감사 및 로그처리 등의 기능을 제공할 수 있도록 구성할 수 있다. 또한 익스트라넷 접근도 완벽하게 제공하며, DMZ 구축, 소프트웨어 구축, 사용자 정의 등은 전혀 필요하지 않게 된다.

현재 사용 중인 IPSec 기반의 VPN의 단점은 모든 리모트 접근에 대해 클라이언트 소프트웨어 및 관리가 필요하다는 점이다. 예전에는 불편함을 느끼지 못했으나 환경의 빠른 변화로 인해 사용자가 늘어날수록 비용 및 관리부담이 증가되었다.

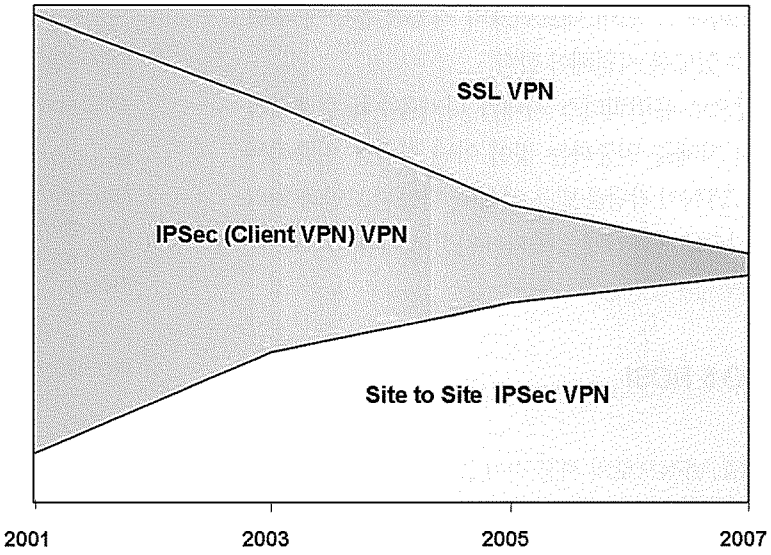
또한 구축 시 기존 네트워크의 Configuration이 고려되어야 하며, Home PC 및 협력사의 리모트 접근 곤란으로 생산성 저하를 유발하기도 하였다. 이에 대한 대안으로 SSL VPN은 기존의 문제를 상당 부분 해결하면서 보안성을 향상시켰다. <표2 참조>

주니퍼 SSL VPN 솔루션은 10명의 유저부터 5,000명까지 단일 장비에서 지원을 하며, 고객의 환경에 따라 여러 가지 선택사항을 조정하여 구성할 수 있기 때문에 비용을 절감할 수 있는 장점이 있다.

SSL VPN 시장 전망

향후 보안은 네트워크 계층 보다는 애플리케이션 계층 기반으로 발전할 것으로 예상된다. 기업 내부와 외부 사용자를 분리한다고 해서 현재 늘어나고 있는 모바일 사용자나 내부 직원들의 불법적인 행위, 퇴사자의 비인가된 접속 등을 차단하지는 못하기 때문이다. 이같은 문제점은 SSL VPN을 활용하면, 안전한 원격 접근은 물론 사용자의 권한 관리까지 관리해 안전한 통신이 이뤄질 수 있을 것이라 생각한다.

<그림1>VPN 시장



<표1>VPN을 고려하는 고객들의 요구사항

- 서비스 영역의 확장으로 인한 클라이언트의 보안성을 제공해야 한다.
- 엑스트라넷 상의 특정 클라이언트 접속을 제어할 수 있어야 한다.
- 클라이언트 상의 보안 애플리케이션 관리 및 적용 편리성을 제공해야 한다.
- 클라이언트 · 서버 기반의 응용 프로그램을 사용할 수 있어야 한다.
- 현재 응용 프로그램의 변경 없는 보안 서비스를 제공해야 한다.

현재 SSL VPN시장은 올해를 기점으로 하여 지속적으로 발전할 것이며 미래의 애플리케이션 접근 플랫폼을 확대시킬 것이다. 즉 모든 네트워크 장비에서 어떤 애플리케이션이든지 이용 가능하며, 트래픽을 처리하는 SSL기반 플랫폼이 데이터 센터의 에지에 배치될 것이다. 전 세계 어디서나 관리하고 확장할 수 있는 플랫폼은 사내 애플리케이션에 접근하고자 하는 사용자의 모든 요구를 처리하는 중앙 지점이 될 것이다.

이미 많은 지사를 가지고 있고 글로벌한 다국적 회사들은 SSL VPN을 활용해 회사 내외부의 모든 접근을 관리하고 있다. 이런 접근에 대한 전략이 자사에 적합한지를 파악하기 위해서는 네트워크 인프라의 네트워크 계층에 복잡성을 더욱 가중시켜 관리상의 포인트를 늘릴 것인지, 아니면 관리와 유지보수가 훨씬 간편한 환경을 구축할 것인지를 자문해 본다면 쉽게 결정할 수 있을 것이다. 많은 수의 관리자는 네트워크 장애가 발생하는 가장 큰 원인으로 네트워크와 보안의 복잡성과 연계성에 따른 문제를 든다.

현재 악성코드와 공격기법의 수준은 보다 정교해지고 직원들의 이동근무가 증가하고 있으며 광대역, 무선네트워크가 널리 보급되고 있다. 또한 기밀성도 유지하면서 속도와 편의성까지 요구함에 따라 이제 보안 우선 순위와 투자를 재평가하고, 네트워크 보안에 대한 기존의 인식

에 대한 재고가 필요하게 되었다. 또한 보안 운영을 간소화해 IT 팀이 네트워크의 지속적 운영에 주력할 수 있도록 지원해야 한다.

앞으로 유비쿼터스 시대가 다가올수록 현재처럼 장비 자체를 인증하는 것이 아닌 사람을 인증하는 SSL VPN이 각광을 받을 것이며, 다양한 보안과 편리한 기술들이 여기에 접목되어 나갈 것이다.

TCO & ROSI

SSL VPN으로의 시장 전이 중 가장 중요한 선택 요소는 가격이다. SSL VPN을 도입함으로써 사용자의 환경이 계속 바뀌는 원격 · 이동사용자 접속의 편리성과 업무의 연속성적인 측면에서 SSL VPN이 유리하다. 또한 비즈니스 파트너, 고객을 위한 접속이 필요한 경우 IPSec VPN과는 달리 중앙집중 관리가 가능하므로 관리비용 절감에 유리하다. 설치시간 면에서도 IPSec VPN보다 단축되고 유지하는 비용면에서도 상당한 이점을 제공한다.

SSL VPN 도입방안

사용자의 신원을 확인하는 방법은 날로 발전하고 있지만 인터넷을 접속할 수 있는 모든 컴퓨팅 장비에서 한 기업의 애플리케이션에 접근 권한을 부여하는 것이 과연 가능한가가 문제로 부각될 수 있다.

보안 문제는 단순히 사용자를 인증하는 것에서 나아가 운영체제, 브라우저, 애플리케이션, 심지어 네트워크의 유형 등 사용자의 컴퓨팅 환경에 내재하는 위험을 관리하는 차원으로 확대되야 한다. 공항이나 전시장의 키오스크, 호텔의 비즈니스 룸 컴퓨터, PDA 또는 친구의 가정용 PC 등과 같은 접근 장비는 트로이목마, 키입력 로거, 통제되지 않는 바이러스, 웜 등과 같은 위험에 노출돼 있다.

SSL VPN을 사용하게 되면 단순접속 제어뿐만 아니라 PC에 설치되어 있는 백신의 최신 버전까지 체크하여 웜 및 악성코드가 기업 내부로 유입되는 것을 방지할 수 있다.

도입방안으로는 첫째, 화상회의에 접목시킬 수 있다. 예전과 달리 비즈니스가 복잡해지고, 화상회의의 내용이 민감해졌기 때문에 회의내용도 외부에 노출될 확률이 높다. 이런 환경에서 주니퍼의 SSL VPN을 이용하여 동시에 10~250명의 사용자가 온라인으로 회의할 수 있도록 지원하는 IVE 플랫폼을 바탕으로, 플러그 & 플레이 장치를 이용하여 보안성은 높이고 비용은 절감할 수 있다.

둘째, 제조업체 위주로 생산에 관련된 업무를 아웃소싱하는 환경에 접목시킬 수 있다. 본사 측면에서는 하청업체에 특정 ERP 서버만 접속하게 해야 하며, 다른 서버로의 접근을 막아야만 한다. 이렇게 접근 권한 관리를 중앙에서 제어하기 위해 사용할 수 있다.

셋째, ISP나 IDC 위주로 보안 관제 서비스에 응용할 수 있다. 즉 기존의 IPSec 고객이 관리상의 어려움을 이유로 자연스럽게 마이그레이션 될 것이다. 현재 호주를 비롯한 다양한 국가들의 통신사들은 고객의 글로벌한 경영을 지원하기 위해 기존 MPLS VPN 망에 대한 회선 서비스를 SSL

〈표2〉IPSec VPN vs. SSL VPN

	IPSec VPN	SSL VPN
기술 성숙도	높음	높음(더 오래되고 안정된 기술)
암호화 수준	강함	강함(IPSec과 동일)
취약점	터널이 셋업되면 해커가 쉽게 내부 망에 접근할 수 있음	One-way인증을 쓸 경우 암호 노출의 우려
Firewall, NAT 환경	어려움(IPSec 포트 개방 필요)	문제 없음 (HTTPS 443기본적 Open)
어플리케이션 접근제어	어려움(L3까지만 터널 그 이상 개방)	어플리케이션별 접근제어, 보안 우수
사용자 편의성	중간(별도 교육 필요, 클라이언트)	높음(교육 불필요, 웹 브라우저)
관리자 편의성	낮음(PC 클라이언트 설치 지원)	높음(클라이언트 설치 불필요)
인증방식	기본적으로 호스트에 대한 인증	사용자에 대한 인증
데스크탑 보안	보통 별도 클라이언트 프로그램으로 호스트 인증 수행	강력 Two-Factor 인증방식 사용가능 End Point Control (Host Checker) 기능으로 바이러스 여부 검사 후 접속 허용

〈표3〉주니퍼 네트워스의 SSL VPN의 가치

상당한 양의 총 소유비용(TCO) 절감
- 클라이언트나 서버 측에 하드웨어, 소프트웨어가 필요 없음
- 소프트웨어 배치, 통합 및 고객화 작업이 필요 없음
- 데스크탑 지원 비용이 대폭 절감
- 설치 비용의 절감

견고한 보안 아키텍쳐
- 보안 계층이 강화되어 모든 리소스에 대한 접근 중개
- 내부 자원에 대한 네트워크 계층 접근 개방 제거
- 강력한 인증 프로토콜 지원(RADIUS, AD/LDAP, CA, RSA, Netegrity, NIS, Local 등)
- 역할 기반의 역할 맵핑을 통한 정밀한 권한 부여 정책
- 수많은 서드 파티가 보안 검증
- 클라이언트 보안성 강화(호스트 체커, 캐시 클리너)

기업의 생산성 및 유연성 개선
- 어디서든 중요한 기업 정보에 안전하게 접근
- 별도의 구성이나 다운타임 없이 즉각적인 실시간 접근

관리 작업의 능률화
- Central Manager는 관리 업무를 쉽게 함.
- 관리 업무의 역할 기반 위임

엔터프라이즈 수준의 성능 확장성 및 고가용성
- 가장 복잡하고 요구사항이 까다로운 기업 환경에 맞게 적합한 설계

다수의 고객 옵션사항
- 애플리케이션 및 리소스 접근 옵션(Web, C/S, Server Initiate Application)
- 고 가용성 클러스터링 옵션
- 사이트 클러스터링 기능

사용자 한글 지원

VPN 서비스 망으로 전환을 했고, 기획 중에 있다.

고객 비즈니스의 다양화를 만족시키기 위한 일환으로 대형 SSL VPN 장비를 통해 여러 회사의 영업사원 및 해외 근무자들을 효율적으로 각 회사의 자원에 접근을 하도록 지원하고 있는 실정이다.

이제는 SSL !

불과 2~3년 전, ADSL의 안정화와 함께 인터넷의 광대역화에 힘입어 많은 기업들이 비용 절감을 위해 IPSec VPN 도입을 결정했다. IPSec에 대한 관심은 신문, 잡지 등의 미디어를 통해 그보다 1~2년 전에 나타나기 시작하였지만, 2002년에 들어서야 본격적인 구축이 시작되었던 이유는 다름 아닌 '기술에 대한 신뢰' 였다고 해도 과언이 아니다. 우리나라의 경우 새로운 기술을 도입할 때 해당 분야에서의 Leading Company의 사례 또는 타 기업의 도입 사례를 검토한 이후 도입을 결정하는 것이 일반적이다.

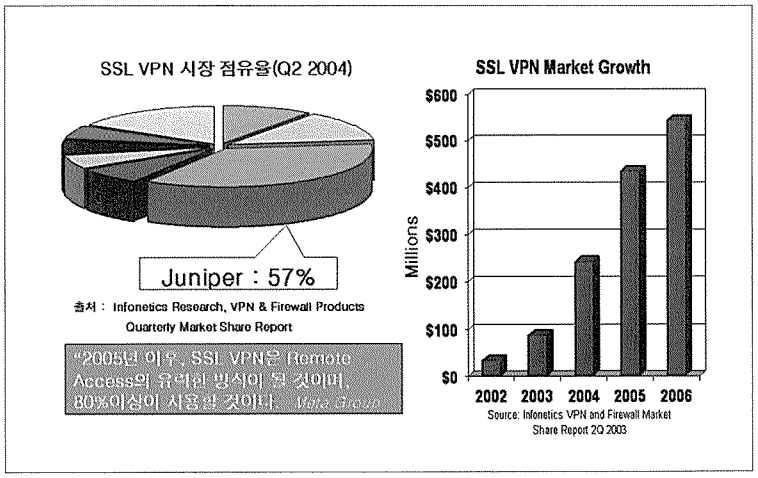
이제 SSL이다. 다수의 미디어들이 끊임없이 SSL에 대한 소식을 쏟아내고 있다. 2005년 현재 SSL에 대한 미디어의 홍보와 기업들의 관심은 이미 예정되어 있었다. 하지만 고객은 여전히 SSL을 어디에, 어떻게 사용할 것인지에 대해, 그리고 VPN이면 VPN이지 IPSec은 무엇이고 또 MPLS VPN, SSL VPN은 도대체 무엇이길래 다들 얘기하는지 모르는 경우가 많다.

간단하게 세 가지의 기술을 구별하면 다음과 같다. 첫째, MPLS VPN은 Traffic Engineering 기술을 통해서 기존의 전용선 보다 다양한 서비스 형태를 제공할 수 있는 고급 전용선이라고 보면 된다. 물리적, 논리적인 인프라이기 때문에 기업의 입장에서는 End-to-End 보안 서비스를 받기 위해서는 IPSec과 결부되어야 하며, 주로 회선사업자의 VPN Managed Service에 사용되어지는 기술이다.

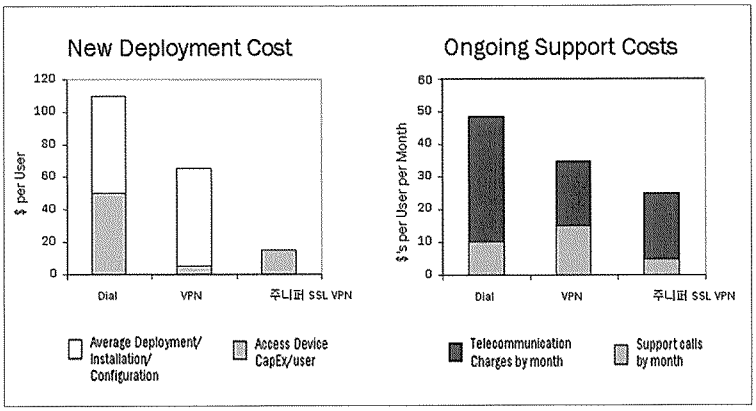
둘째, IPSec VPN은 인터넷을 통한 VPN의 표준 기술로서 기존의 전용선을 이용한 인트라넷을 인터넷을 통한 보안 터널링 구성으로 전환하는 기술로서 현재 가장 많이 사용되어지고 있다.

셋째, SSL VPN은 앞에서 살펴본 바와 같이 MPLS나 IPSec과 같은 네트워크 기반의 서비스 형태가 아닌 End-to-End 또는 End-to-Area 서비스 형태이다. 따라서 기존의 IPSec 기반에서 Dialup User가 내부자원으로 접근할 때 사용하는 IPSec Client VPN을 대체할 수 있다.

〈그림2〉세계 SSL VPN 시장



〈그림3〉TCO-Secure Access vs. Network-Layer VPNS



SSL은 궁극적으로 BcN(광대역통합망)과 유비쿼터스로 대변되는 미래의 분산컴퓨팅 환경에 가장 적합한 VPN 구성이라고 할 수 있다. 즉 분산되어 있는 서비스 자원들 및 브라우징 탑재만으로 경량화된 모바일 기기들의 이동성을 하나의 지점에서 모두 수용할 수 있는 설치의 간편성, 다양한 접근 개체와 대상 개체 간의 복잡한 식별 · 인증 · 권한 구조를 단일한 지점에서 효과적으로 수행할 수 있는 엑스트라넷 접근관리 구조(extranet access management infrastructure)를 제공함으로써 분산컴퓨팅 환경에 가장 적합한 보안 솔루션으로서 손색이 없다.

결론적으로 기업의 입장에서는 망과 망의 연결에서 MPLS 또는 IPSec VPN을, Client Access 및 Extranet Access와 관련해서는 SSL VPN을 구축하는 것이 가장 현명한 선택이 될 것이다. 이제 기업의 입장에서 SSL VPN을 도입하는 것은 어려운 선택이 아닐 것이다. 번거로운 관리에서 벗어날 수 있으며, 복잡한 접근관리를 한 번에 할 수 있는 방법이 있다. 도입 결정은 빠를수록 좋다. 제품 결정은 신중할수록 좋다. Users