IDG
Custom Solutions Group

IDG Summary | SSL VPN

SSL VPN 교체시 고려사항,
"다양하고 변화무쌍한 모빌리티를 생각하라"

국내 SSL VPN 시장은 2년 전부터 교체 주기에 접어들었다. 교체 연한을 넘긴 장비들은 성능적인 측면도 문제지만 무엇보다 호환성에서 관리자들을 힘들게 한다. 또한 나날이 강력해지고 지능화된 보안 위협과 임직원들의 다양하고 변화무쌍한 모빌리티 사용 환경은 기존 SSL VPN으로는 감당하기 힘든 실정이다. SSL VPN 교체 시 고려해야 할 사항과 조건에 대해 알아보자.

SSL VPN 교체시 고려사항, "다양하고 변화무쌍한 모빌리티를 생각하라"

이웅세 이사 | 델소프트웨어코리아 보안사업부

2015년 사이버 공격은 나날이 진화되고 공격 벡터의 종류는 일반적인 스마트폰, 태블릿뿐만 아니라 웨어러블(wearable) 기기, 전기 자동차, 사물인터넷(Internet of Things, IoT) 기기에 이르기까지 확장했다. 또한 오픈SSL에 대한 공격은 오픈소스 진영에 커다란 타격을 입혔으며 애플 또한 SSL 공격을 당했다.

델소프트웨어 시큐리티 사업본부가 발행한 〈2016 델 연간 보안 위협 보고서(Dell Security Annual Threat Report 2016)〉에 따르면, 지난해 악성코드 공격은 약 2배 가량 증가했으며 정부 단체 및 기관, 기업, 일반 개인에 이르기까지 많은 손해를 입혔다.

특히 2015년 4분기동안 SSL/TLS로 암호화된 HTTPS 연결은 전체 웹 상의 연결 내역 가운데 평균적으로 64.6%에 해당하며, 2015년 1월 HTTPS 연결은 지난해 같은 기간에 비해 109%나 증가했다. 게다가 2015년 매월, 2014년 같은 기간과 비교했을 때, 평균 53%의 증가 추세를 보였다. 이러한 성장과 함께 HTTPS 트래픽을 통한 공격 역시 급증하고 있다. 전세계적으로 SCADA(원격제어) 시스템에 대한 공격이 2배로 증가하고, 이미 스마트폰 전용 악성코드가 급증하는 상황에서 기업들은 기존 보안체계에 대해 변화를 고민하고 있다.

교체 주기를 맞이한 국내 SSL VPN 시장

국내 SSL VPN 시장은 교체 주기를 맞이하고 있다. 기업들은 2000년대 초반부터 특정 벤더의 SSL VPN을 많이 도입했는데, 이미 10년이 지나면서 교체 연한이 지난 경우가 많다.

일반적으로 공공기관의 장비 교체 연한은 4, 5년이지만 일반기업은 7년 이상으로 산정하기도 한다. 하지만 교체 연한을 넘긴 장비들은 하드웨어 성능적인 측면에서 너무 떨어져 다른 시스템의 발목을 잡는다. 이보다 더 큰 문제는 호환성에서 발생한다. 운영체제나 시스템은 지속적으로 발전하고 구 버전은 단종되고 있는데, 오래 전 도입한 SSL VPN은

이런 새로운 운영체제를 지원하지 않는 경우가 많다. 이로 인해 보안에 대한 관리포인트는 많아지며 관리자는 골머리를 앓게 된다. 특히 스마트폰의 경우 사용자의 교체 주기는 보통 2년인데, 교체할 때마다 운영체제와 애플리케이션들은 바뀌게 마련이며 이에 대해 기업의 보안정책 또한 빨리 업그레이드해야 한다.

모바일 시대의 위협 TOP 5

지금까지 IT 업계에서는 BYOD(Bring Your Own Device)라는 의미를 설파하면서 기업의 모빌리티 전략의 필요성을 얘기해왔다. 자신의 기기를 회사 업무용으로 사용한다는 개념의 BYOD는 직원들은 물론, IT 부서에서도 사용, 관리하기 불편하고, 귀찮은 것으로 인식되면서 도입율이 그리 높지 못했다.

하지만 기업 임직원은 자신의 스마트폰이나 태블릿으로 회사 메일을 보고, 노트북을 통해 회사 밖에서 회사 데이터를 사용하는 일이 일상이 됐다. 또한 현업 부서는 업무를 위해 IT 부서가 알지 못하는 클라우드 서비스를 제공받고 있다. 이런 모바일 기기와 클라우드 서비스 등을 통해 직원들은 언제, 어디서나, 필요한 순간에 업무가 가능하게 됐다. 이미 모바일 시대가 도래한 것이다.

모바일 시대의 사용자는 이미 인터넷, 이메일과 일정 관리를 위한 애플리케이션을 직접 사용하는 것에 익숙하게 되었다. 또한 애플리케이션을 통해 중요한 회사 업무를 하는 빈도가 지속적으로 증가하고 있으며, 이를 위한 모바일 기기를 사용자 스스로 선택하는 경향이 높아졌다. 이로 인해 기업들은 새로운 위협에 직면하게 됐다.

우선 사용자가 기기를 잃어버렸거나 퇴사한 직원들의 기기로부터 회사 정보가 유출될 수 있다는 점이다. 이는 기업의 중요 정보가 유출될 수 있는 심각한 사고임에도 불구하고 절반 이상의 기업이 이에 대한 보안 조치를 하지 않고 있다.

두번째 위협은 사용자 기기가 모바일 악성코드에 감염됐을 때다. 최근 미래창조과학부가 발표한 '2015년 정보보호실태조사' 결과에 따르면, 모바일 기기 사용자 10명 가운데 3명이 모바일 악성코드에 감염된 경험이 있다. 모바일 기기 사용자들이 경험한 보안사고는 악성코드 감염(32.0%), 스미싱 피해(28.9%), 개인정보유출(24.4%) 순이었다.

세번째 위협은 불안정한 애플리케이션을 통한 정보 유출이다. 모바일 기기 자체는 안드로이드든 iOS든 애플리케이션에 취약할 수 밖에 없는 구조적인 특성

표 1 | 모바일 시대의 위협 TOP 5

분실 및 도난 기기 또는 퇴사한 직원의 기기로부터 회사 정보의 유출
모바일 악성코드(Malware)를 통한 정보 유출
불안정한 애플리케이션을 통한 정보 유출
모바일 기기, 운영체제, 설계 그리고 애플리케이션에서의 취약성
불안정한 와이파이 환경 또는 의도된 네트워크 침입

을 갖고 있다. 최근 버전이 업그레이드되면서 상당히 개선됐지만 위협은 여전한 상황이다. 또한 모바일 기기를 통해 공공 와이파이를 사용하는 경우, 자신도 모르는 사이에 악성코드가 설치되기도 한다.

MDM과 MAM의 한계

기업들은 이런 모바일 위협을 막기 위해 MDM(Mobile Device Management) 도입에 나섰다. 기업의 보안정책에 따라 사용자 기기를 관리한다는 MDM의 취지는 기업이나 관리자 입장에서는 매우 유익했다. 퇴사자나 기기 분실 시 해당 기기에 대한 보안정책을 통해 데이터를 삭제할 수 있었기 때문에 기업 정보 유출을 막을 수 있었다. 그러나 MDM이 단말기 내에 있는 개인 데이터에도 영향을 미칠 수 있다는 우려와 기기 사용이 불편하다는 점으로 인해 사용자의 업무 생산성을 저하하는 최악의 솔루션으로 인식됐다.

특히 2년마다 교체되는 사용자의 스마트폰을 제대로 지원하기 위해서는 MDM 솔루션도 그만큼 빨리 업데이트가 되어야 한다. 하지만 이를 제대로 지원할 수 있는 벤더나 수많은 관리포인트를 감당 할 만큼 역량을 갖춘 기업은 그리 많지 않았다. 이로 인해 MDM을 도입하고서도 운영하지 않는 기업들이 상당히 많은 실정이다.

이런 단점을 보완하기 위해 등장한 것이 MAM(Mobile Application Management)이다. MAM은 단말기 자체를 제어하는 것이 아니라 모바일 애플리케이션만 제어하기 위한 솔루션이다. 기업용으로 사용하는 애플리케이션과 저장 영역 이외 다른 기능들은 제어하지 않게끔 설계됐는데, 사용자 선호도 측면에서 MDM보다 높았다.

하지만 기기에 들어있는 애플리케이션 이외 다른 보안 관리는 되지 않아 전체적인 보안 문제를 해결할 수 없었다. 또한 여러 앱과의 호환성 문제와 가격적인 요소는 MAM 확산을 더디게 하는 이유였다.

모바일 환경에 맞는 SSL VPN의 조건

모바일 보안에 있어 기업에서 필요한 것은 ▲모바일 기기를 통한 정보 유출 방지 ▲모바일 기기를 통한 접속, 통제에 대한 제어 ▲통합된 보안 정책 제공 및 관리 등 3가지 요소로 구분할 수 있다. 이 3가지 요소에 공통적으로 들어가는 것이 바로 모바일 네트워크다. 모빌리티를 통한 내부 접속이 업무 기본이 된 현실에서 모바일 네트워크 보안은 이제 필수요건이 됐다.

과거에 기업 사용자는 사무실에서 일했다. 말 그대로 회사 내부에서만 사내 데이터센터에 접속했으며, 고객 및 협력업체나 외부 접속이 필요한 외부 사용자들은 소수에 불과했다.

그러나 이제 업무 환경은 완전히 달라졌다. 임직원들이 집에서 재택근무를 할 때나 혹은 이동 중에나 공항, 출장지에서 메일을 보낼 때나, 외부 협력업체

들은 수시로 회사 내부망으로 들어온다. 이렇듯, 외부에서 내부로 접속하는 경우, 네트워크 보안이 필수적이다.

오래 전 IP Sec 프로토콜을 기반으로 한 SSL VPN을 활용해 본사와 지사간 네트워크를 내부 네트워크로 묶어 사용할 당시에는 보안 이슈가 그리 많지 않았다. 반면, 10여 년 전부터 도입해 온 SSL VPN은 접속하는 장소, 디바이스에 상관 없이 인터넷을 통해 내부 주요 서버에 접속할 수 있으며, 이 경우 안전한 데이터 전송, 네트워크 보안을 확보하는 것이 가장 관건이다. 임직원이나 협력업체가 회사 밖에서 언제, 어디서든 안전하게 필요한 업무를 수행할 수 있는 환경을 제공하는 것이다.

이를 위해서는 다양한 접속 환경을 지원하고 이에 대한 위협 감지 및 보호가 필요하다. 다양한 접속환경 속에서 우선 사용자가 어떤 접속 환경인지 파악하고 위협을 감지하고 내부에 할당된 리소스에 적절히 접속해 업무를 할 수 있도록 해야 한다. 감지, 보호, 연결하는 이 3단계가 SSL VPN의 기본 보안 단계다.

델소프트웨어는 모바일 커넥터를 사용해 PC든, 노트북이든, 스마트폰이든 제한이 없으며, 윈도우, 안드로이드, iOS 등 모든 운영체제를 지원한다. 또한 델 SMA 어플라이언스를 통해 보안정책에 근거한 사내 서버에 대한 접근을 유연하게 제어한다. 이와 함께 사용자 인증과 디바이스 인증 등을 통해 외부에서 들어온 접속 요청을 잘 연결하고 정책적으로 분리해준다.

모빌리티 사용자를 위한 클린 SSL VPN 환경 제공

델소프트웨어 소닉월 SSL VPN은 EPC(End Point Control)를 통해 사용자의 기기를 식별하고 보안 상태를 탐지한다. 만약 스마트폰 사용자가 사내 네트워크에 접속할 때 해당 스마트폰이 루팅이나 탈옥이 되어 있다면 일반적으로 접근이 금지된다. 루팅이 된 스마트폰은 공공 와이파이로도 쉽게 악성코드에 감염되는 등 보안에 취약하기 때문이다. 기본적으로 안티바이러스, 안티스파이웨어 등 기본적인 보안 소프트웨어들을 탑재하고 있다.

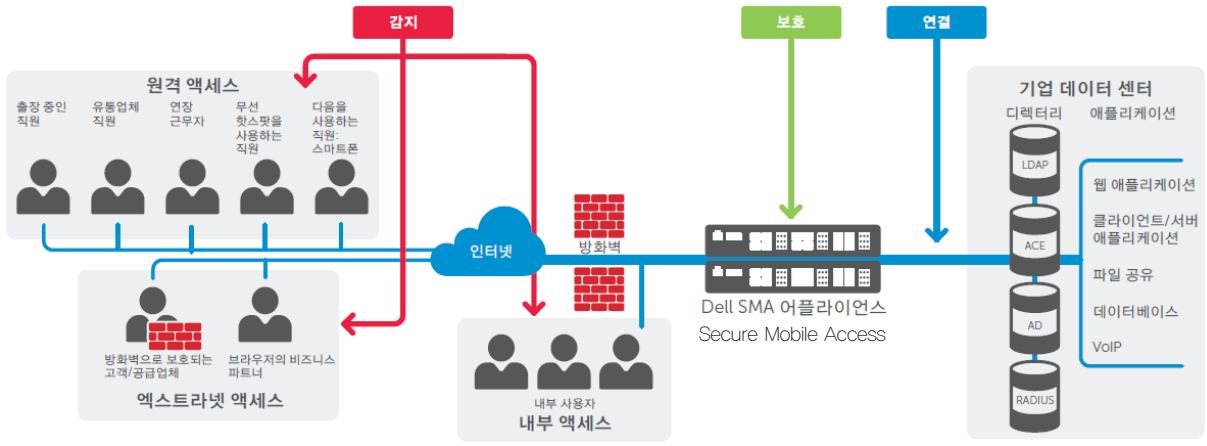
보호에 있어 사용권한 별 애플리케이션 접근 제어는 기본적으로 제공하며 특정 장비와 특정 사용자, 그룹을 관리하기 위해 관리자와 시리얼 번호와 장비 ID를 연계해 관리한다.

델 소닉월 어벤테일 유니파이드 폴리시(Dell SonicWALL Aventail Unified

표 2 | 모바일 보안 3요소에 따른 소닉월 SSL VPN

감지	EPC(End Point Control) : 엔드포인트의 식별과 보안 상태 탐지
보호	어벤테일 유니파이드 폴리시(Aventail Unified Policy) : 사용자 권한별 애플리케이션 접근뿐만 아니라 디바이스 접근 제어를 위한 강력한 엔진
연결	스마트 액세스(Smart Access)와 스마트 터널링(Smart Tunneling) : 모든 네트워크 리소스들의 사용자 보안과 접근 용이성을 제공하기 위한 전송 메커니즘

그림 | 모빌리티 사용자를 위한 클린 SSL VPN 환경 제공



Policy) 모델은 확장형 객체 기반으로, 모든 웹 자원과 파일 공유, 클라이언트 서버 자원의 관리를 한 곳에 통합함으로써, 단 몇분 이내에 정책 관리를 수행할 수 있도록 한다.

연결에서 DELL SMA 스마트 액세스(Smart Access)와 스마트 터널링(Smart Tunneling)을 통해 모든 네트워크 리소스에 쉽고 안전하게 접속을 제어한다. 이를 통해 델은 모빌리티 사용자를 위한 클린 SSL VPN(Clean SSL VPN) 환경을 제공한다.

교체 검토 시 SSL VPN 선정 기준, "호환성, 정책 연동, 그리고 모빌리티"

앞서 설명한 것처럼 기업들은 이미 10년 전부터 SSL VPN을 도입했는데, 오래된 SSL VPN의 경우 호환성 문제로 교체하려는 수요가 상당하다.

SSL VPN을 교체할 때, 기업에서는 우선적으로 자사의 네트워크 사용 현황부터 파악해야 한다. 임직원들이 사용하는 네트워크와 기기들을 조사하고 이를 업무에 활용하고 있는지, 기업에서 지원하고 있는지 등을 파악해 자사에게 필요한 것이 무엇인지 알 필요가 있다. 일종의 수요 조사인 셈이다.

그리고 오래된 SSL VPN을 사용하는 기업이라면 가장 필요한 것을 꼽자면 단연 호환성일 것이다. 지원하는 운영체제는 단종되고, 지속적으로 발전하는데, 현재 SSL VPN은 이를 지원할 수 없는 상황이 발생한다면 관리자로서는 상당히 골치 아픈 일이다.

또한 보안정책과의 연동 문제다. 현재 기업을 대상으로 한 사이버 공격은 상당히 위협적이고 파괴적이다. 특히 공격자들이 기업 네트워크를 직접 공략하는 것이 아니라 방어에 취약한 개인 사용자나 협력업체 등을 해킹한 후, 정당한 권한을 획득해 침투하는 경우가 많아 보안 정책은 어느 때보다 중요해진 상황이다. 관리자뿐만 아니라 사용자들도 싱글 사인온이나 인증, 인가 등 기존 보안 시스템과 무리없이 연동되는 것이 거부감을 해소하는 데 도움이 될 것이다.

모바일 업무 지원, SSL VPN의 필수 요소

SSL VPN 교체의 필요성은 각 기업마다 다르겠지만 현재 수요뿐만 아니라 향후 5~7년을 내다보고 장비를 검토해야 한다는 점은 동일하다.

이런 점에서 모바일 업무 지원 여부는 상당히 중요하다. 임직원들은 이미 여러 대의 모바일 기기와 무선 네트워크를 업무에 사용하고 있으며, 외부에서 내부 시스템에 접속하는 경우가 일반화됐다. 수요 조사에서 현재 임직원들의 모바일 사용 현황이 낮다고 하더라도 향후 추세를 고려한다면 모바일 업무 지원은 필수 요소가 된다.

기업들은 보통 전통적인 SSL VPN과 모바일 기기만을 위한 SSL VPN을 별도로 구축하기도 한다. 하지만 비용 측면을 고려한다면 유무선 통합 SSL VPN을 도입해야 한다. 특히 MAM을 별도로 도입한다면 각 사용자당 MAM 라이선스 비용과 특정 업무용 모바일 앱의 네트워크 보안을 위한 SSL VPN 비용이 추가되지만 델의 경우 라이선스 추가는 전혀 없이, 고객은 구글 마켓이나 iOS 마켓에서 다운로드 받고 관리자가 유저당 라이선스 설정만 해주면 된다.

기업용 SSL VPN 전용 장비

모바일 기술이 진화하고 글로벌 시장이 성숙기에 접어드는 한편 재난 대비에 대한 관심이 높아짐에 따라 원격 접근 제어가 기업의 중요한 과제로 떠오르게 되었습니다. IT 부서에서는 사용이 간편하고 비용 효율적이며 안전한 원격 접근 시스템을 구축해야 하는 요구에 직면하고 있습니다. 클라이언트 기반 VPN은 사용하기 번거롭고 관리가 어려운 단점이 있으나, Dell™ SonicWALL™ Aventail™ E-Class Secure Remote Access (SRA)는 완벽한 기능을 제공하는 동시에 관리가 간편하며, 클라이언트를 거치지 않고 사용하거나 씬클라이언트 "인-오피스" 방식으로 단일 어플라이언스에서 최대 2만 여명의 모바일 엔터프라이즈 사용자를 동시 지원할 수 있습니다.

E-Class SRA는 Windows®, Apple® Mac OS®, iOS, Linux®, 및 Google® Android 기기의 네트워크 자원에 대한 원격 접근을 정책에 기반하여 제어함으로써 생산성을 높이고 비즈니스 연속성을 보장합니다.

SonicWALL E-Class SRA는 인증된 사용자가 허가된 자원에 한해 접근하도록 제한합니다. 또한, Dell SonicWALL 차세대 보안 시스템을 Clean VPN™으로 통합 사용할 경우 중앙 집중형의 접근 관리 및 멀웨어 보호, 애플리케이션 제어 및 컨텐츠 필터링의 기능을 활용할 수 있습니다. 다계층의 보호를 제공하는 Dell SonicWALL Clean VPN™은 모든 종류의 인증 SSL VPN 트래픽이 네트워크 환경에 진입하기 전에 해독하여 위험요인을 제거합니다.

주요 기능 및 특장점

완벽한 iOS 및 Android 지원

Apple iOS 및 Google Android를 위한 통합 클라이언트 앱 SonicWALL Mobile Connect™는 스마트폰 및 태블릿 사용자들이 암호화 된 SSL VPN 커넥션을 통해 기업 및 기관의 자원에 대해 네트워크 레벨에서 접근할 수 있도록 지원합니다.

원격 지원

Dell SonicWALL Secure Virtual Assist는 기술 전문가들이 기존의 인프라를 활용해 안전하게 온디맨드 기술지원을 제공할 수 있도록 돕습니다.

안전한 엔드포인트 관리

Dell SonicWALL Aventail End Point Control™ (EPC™)은 업계에서 유일하게 Windows®, Apple Mac OS 및 iOS, Google Android, Linux 엔드포인트에 대한 단위별 접근 제어를 제공합니다. Device Identification을 통해 특정 장비와 특정 사용자 및 그룹을 관리하기 위해 관리자와 시리얼 넘버 및 장비 ID를 연계 시켜 관리합니다. Dell SonicWALL Aventail의 Virtual Keyboard는 보안되지 않은 엔드포인트 상의 키입력 Sniffer를 중단시킵니다. End Point Control을 통해 Android 시스템의 루팅 및 iOS 기기 탈옥 상태를 모니터링 할 수 있습니다.

정책 관리 간소화

상황 대응형 도움말 및 셋업 위저드를 통해 E-Class SRA 솔루션을 간편하게 설치하고 사용할 수 있습니다. 확장형의 객체 기반 Dell SonicWALL Aventail Unified Policy™ 모델은 모든 웹 자원 및 파일 공유, 클라이언트 서버 자원의 관리를 한 곳에 통합함으로써, 단 몇 분 이내에 정책 관리를 수행할 수 있도록 합니다. RADIUS, ACE, LDAP 혹은 Active Directory 인증 레포지토리를 기반으로 그룹 및 중첩 그룹을 이동시킬 수 있으며, Single Sign-On (SSO)과 포맷 기반 웹 애플리케이션을 지원합니다.

직관적인 관리 및 리포팅

Dell SonicWALL Aventail Management Console™ 은 중앙 집중형의 풍부한 모니터링 기능을 통해 감사, 컴플라이언스 준수, 관리, 자원 계획 등을 지원합니다. 관리자는 각 사용자, 시간, 처리량, 영역, 커뮤니티, 구역, 에이전트, IP 주소 별로 필터를 적용해 손쉽게 확인할 수 있습니다.

- 모든 종류의 엔드포인트에 대한 사용 편이성 제공
- iOS 및 Android L3 VPN 완벽 지원
- L3VPN access log 및 traffic log 지원
- 양방향(C→S, S→C) 접근 제어 정책 지원
- 모바일 단말 고유정보(UDID, IMEI) 모니터링 지원
- 모바일 단말 루팅 및 탈옥 상태 모니터링
- OTP(One Time Password) 서버 내장
- 모든 애플리케이션 플랫폼 접근
- 원격 지원
- 빠른 셋업 및 구축
- 손쉬운 통합 정책 관리
- 통계 및 레포팅 지원

제품 세부 사양

	중소규모형 SSL VPN		대규모용 SSL VPN				
MODEL	SRA1600	SRA4600	EX6000	SMA6200	EX7000	SMA7200	EX9000
PERFORMANCE							
Concurrent users	Max 50	Max 500	Max 250	Max 2,000	Max 5,000	Max 10,000	Max 20,000
HARDWARE							
Form factor	1U	1U	1U rack-mount	1U rack-mount	1U rack-mount	1U rack-mount	2U rack-mount
Processor	X86 main processor	X86 main processor	Intel Celeron 2.0GHz	Intel i5-4570S 2.9GHz	Intel Core2 Duo 2.1GHz	Intel E3-1725 v3 3.5GHz	Intel Quad Xeon 2.46GHz
Memory	1GB	2GB	1GB	8GB	2GB	16GB	32GB
Interfaces	2xGbE	4xGbE	4xGbE	6xGbE	6xGbE	2x10GbE, 6xGbE	4x10GbE, 8xGbE
Power	Fixed power supply	Fixed power supply	Fixed power supply	Fixed power supply	Dual power supply, hot swappable	Dual power supply, hot swappable	Dual power supply, hot swappable

	가상화 기반의 SSL VPN
E-Class SRA Virual Appliance	
Hypervisor	ESG™ and ESX™ (version 4.0 and newer)
Operating system installed	Hardened Linux
Memory	2GB
Disk size	80GB
VMware hardware compatibility guide	http://www.vmware.com/resources/compatibility/search.php

주요 기능

인증
- AD/LDAP 그룹 정보 연동 지원
- One-Time Password 내장(OTP)
- Dynamic Group
- Dual/Stacked 인증
- Virtual Keyboard
- Password Management

Encryption
- ARC4(128), MD5, SHA-256, SHA-384, SSLv3, TLSv1, TLS1.2, 3DES(168,256), AES(256), RSA, DHE

지원 애플리케이션
- Proxy : Citrix(ICA), HTTP, HTTPS, FTP, SSH, Telnet, RDP, VNC, Windows file sharing(Window SMB/CIFS), OWA 2003/2007/2010
- NetExetender : Any TCP/IP based application(ICMP, VoIP, IMAP, POP, SMTP등)

웹 포탈 지원
- Web portal 커스터마이징
- 개인용 북마크 제공
- Smart Access
- On-Demand Tunnel
- Native Access Module
- Work Place Mobile

관리 및 운영
- Web 기반의 GUI 환경 제공
- Syslog 제공
- GMS와 연동(Heartbeat message)
- SNMP 지원
- User, memory, CPU, BW등에 대한 모니터링 기능 제공

L3VPN 전용 App. 지원
- 스마트 단말을 위한 L3VPN App. 지원
- 탈옥 및 루팅 여부 점검(E-Class)
- Android, iOS 단말에 대한 통합된 접근 제어 정책 적용
- Google Play, App Store를 통한 쉬운 설치 및 사용

iOS/Android 단말 상태 모니터링
- 탈옥 및 루팅 상태 확인
- Device ID (UDID) 확인
- Certificate 강제화
- OS version 제어

ActiveSync 지원
- 다양한 단말에서 ActiveSync 지원(email, 일정, 연락처 등)
- 멀티 플랫폼 지원(iPhone, iPad, Android, Windows Phone, Symbian등)
- Clientless Email, 일정, 연락처 지원
- Device ID 점검을 통한 보안 강화

기타
- Telnet/SSH 링크 추가 지원
- Telnet/SSH client 내장
- IPv6 지원
- HA 지원
- Load Balancing 지원
- Application offloading 지원

* 모델별로 제공되는 기능이 차이가 날 수 있습니다.

델소프트웨어코리아(주)
서울특별시 강남구 테헤란로 445 본솔빌딩10F
전화 번호 02-3420-9000 | 팩스 번호 02-569-3600
웹 사이트 www.software.dell.com
전자 메일 Korea.info@software.dell.com

DELL Software