AhnLab

Case Study

건설기업을 위한 IPSec VPN 구축 가이드

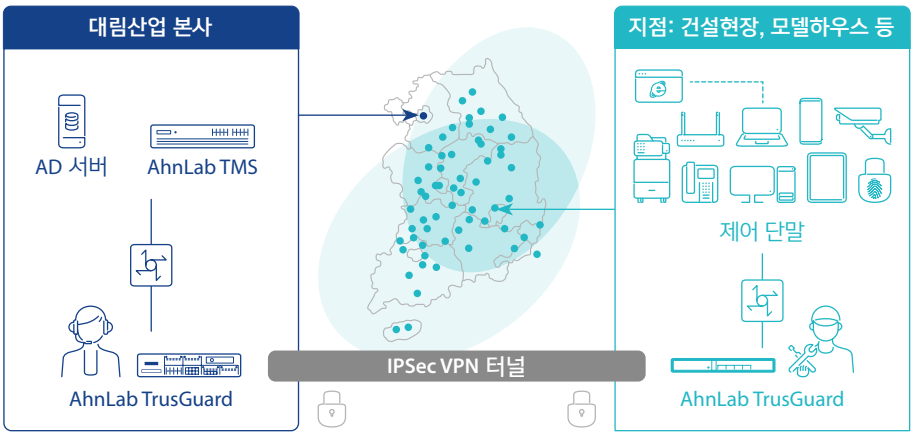
대림산업(현. DL이앤씨)은 AhnLab TrusGuard로 VPN을 구축해 본사와 여러 지점에 걸쳐 효율적이고 안정적인 네트워크 보안 체계를 구축했다.

개요

건설업은 일반 사무실과 비교했을 때 보안 운영 환경이 다르다. 특히, 건설현장은 장비와 인원의 이동이 계속되며, 장애 발생 시 대응에 어려움이 있다. 안랩의 차세대 네트워크 보안 솔루션 'AhnLab TrusGuard'는 'IPSec VPN with L2 Filtering' 기능을 필두로 다양한 네트워크 보안 역량을 지원해 탁월한 보안성과 편의성을 제공한다.

구축 사례

대림산업(현. DL이앤씨)은 2020년 9월, '전국 건설현장 VPN 구축 사업'에서 전국 대림산업 건설사무소에 AhnLab TrusGuard로 가상사설통신망(Virtual Private Network: VPN)을 구축했다. 이를 통해 본사와 여러 지점에 걸쳐 가변적인 현장 상황에 대응해 효율적이고 안정적인 네트워크 보안 체계를 마련했다.



AhnLab TrusGuard VPN을 통해 건설사무소 내부 네트워크 보안 인증, 미인가 단말 통신 제어, 네트워크 통합 중앙관리 등의 역량 확보

안랩은 대림산업 전국 건설사무소 네트워크 환경을 분석한 후 AhnLab TrusGuard로 VPN을 구축했다. 이를 통해 대림산업에 ▲건설사무소 내부 네트워크 보안인증 ▲미인가 단말(PC, 공유기 등)통신 제어 ▲네트워크 통합 중앙관리(차세대 네트워크 통합 위협 관리 플랫폼 'AhnLab TMS' 기반) 등 향상된 보안 기능을 제공했다.

대림산업은 AhnLab TrusGuard VPN 도입으로 건설현장에서 본사 네트워크 접속 시 미인증 단말의 접근을 제어하고 접속한 사내망 PC의 네트워크 보안도 강화하는 등 본사-사무소간 보안 수준을 한층 높였다. 또한 본사에서 수립한 VPN 보안 정책을 원격지의 건설현장에 일괄 적용해 전국 각지 건설현장의 보안 수준을 일정하게 유지할 수 있다.

"대림산업은 디지털 트랜스포메이션 기반 업무 혁신으로 건설분야 스마트화에 앞장서고 있다. 이번 사업은 디지털 혁신 기반 건설현장업무를 위해 대림산업 전국 각지 100여 개 건설현장에 네트워크 보안을 강화하고자 실시한 사업으로, 이번 VPN 구축으로 대림산업의 건설현장에서 주요 건설 데이터에 대한 보안은 물론 업무의 안정성도 높아질 것으로 기대한다."

– 대림산업 보안 담당자

도전 과제

IPSec VPN은 본사-지점 구성에서 보안을 위해 사용하는 통신 방식이며, 대부분 방화벽 제품에 일체형으로 제공된다. 방화벽은 Layer-3(IP 주소) 기반의 패킷 필터링을 제공하며 보안 운영 방식에 따라 다음과 같은 상황에서 L3 기반의 보안 운영이 어려울 수 있다.

- DHCP로 인해 IP 주소가 유동적으로 변경될 경우, 그때마다 새로 보안 정책 적용 필요
- IP 주소가 아닌 단말을 기준으로 제어해야 할 경우, IP 주소는 단말의 고유한 값이 아니기 때문에 제약 발생

이러한 제약을 부분적으로 극복할 수 있는 방법으로 차세대 방화벽의 사용자 기반 제어와 디바이스 기반 제어가 있다. 하지만, 이 역시 다음과 같은 상황에서는 어려움이 있을 수 있다.

- 내부 직원이 아닌 협력사 직원 등 사용자를 정의할 수 없는 경우
- 비 윈도우 계열 OS 또는 IoT 기기 등 디바이스 기반 제어의 지원 OS가 아닌 단말일 경우

보안 담당자는 이와 같은 문제점을 극복하기 위해 Layer-2(MAC 주소) 기반의 보안 솔루션을 IPSec VPN과 함께 구축하게 된다. 이 경우에는 다음과 같은 운영 상의 비효율을 겪을 수 있다.

솔루션

AhnLab TrusGuard는 'IPSec VPN with L2 Filtering' 기능을 제공해 강력하면서도 편리한 보안 체계를 구축하도록 지원한다.

기능 핵심 포인트 1

L2 Filtering을 통해 같은 단말에 대해서는 항상 동일한 보안 정책을 적용할 수 있다.

- IPSec VPN과 L2 솔루션 추가 도입에 따른 구축 비용 증가
- 보안 운영 & 관리의 복잡성 증가

이를 해결하기 위해서는 단일 제품으로 L2 및 L3를 제어하고, 동시에 강력한 보안과 편리한 운영 & 관리를 제공하는 솔루션이 필요하다.

솔루션

AhnLab TrusGuard는 보안 운영상의 불편함과 비효율성을 모두 해결하여 보안 담당자가 보안성과 편의성에 대해 일거양득의 혜택을 누릴 수 있도록 IPSec VPN with L2 Filtering 기능을 제공한다.

특히 건설사의 경우, 새로 생기고 없어지기를 반복하는 다수의 건설 현장과 모델하우스 등에 대해 인가된 단말에 한해서만 네트워크 접근이 가능하도록 고도화된 보안 운영이 필요하다. 이와 같은 환경에 최적화된 AhnLab TrusGuard를 도입하면 강력하면서도 편리한 보안 체계를 구축할 수 있다.

주요 기능

L2 Filtering

AhnLab TrusGuard는 MAC 주소 기반의 패킷 필터링을 제공한다. 단말의 고유값인 MAC 주소를 통한 보안 적용은 IP 주소나 사용자와 무관하게 같은 단말에 대해 항상 동일한 보안 정책을 적용할 수 있다는 장점이 있다. 또한, 운영자가 원하는 기간 동안만 허용 & 차단 가능한 스케쥴링 기능을 제공해 더욱 유연하고 효율적인 보안 운영이 가능하다.

OUI-based Filtering 지원

수백~수천 여개 단말의 MAC 주소를 개별 관리하는 것은 운영자에게 큰 부담이 된다. 기업들은 대부분 정해진 몇 개의 업체를 통해 IT 자산을 도입하고, 같은 업체는 같은 식별 번호(OUI)를 갖고 있다. AhnLab TrusGuard는 개별 MAC 주소 뿐만 아니라 OUI 기반 패킷 필터링 기능을 제공해 다수의 단말에 대해서도 편리한 제어가 가능하다.

Active Directory 연동

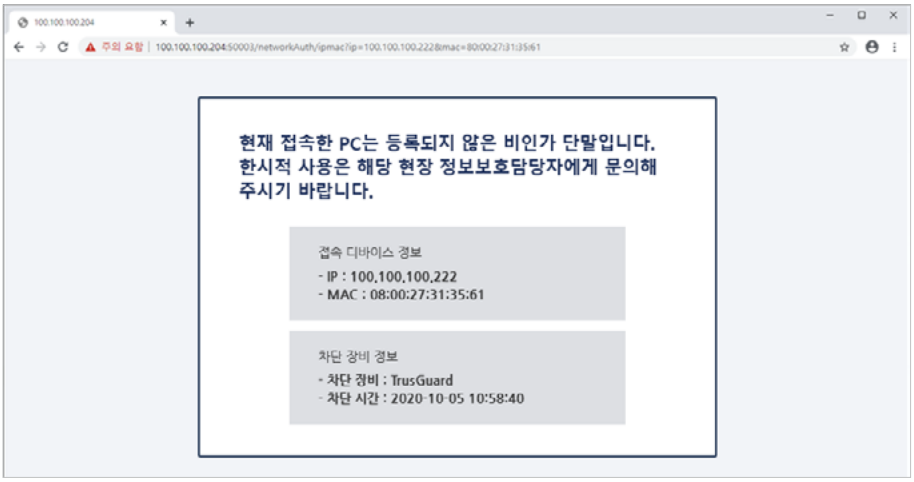
안랩의 네트워크 통합 위협 관리 플랫폼 'AhnLab TMS'(이하 TMS)는 본사의 AD로부터 네트워크 접근 허용이 필요한, 인가 받은 모든 단말에 대한 MAC 주소를 주기적으로 수집 및 업데이트한다. 이를 지점 VPN 장비에 전달함으로써 항상 최신의 보안 정책을 유지할 수 있다. 아울러, Windows AD는 물론 Microsoft Azure의 정식 호환 가능 VPN 제품으로 등록되어 Azure AD와의 연동도 가능하다.

기능 핵심 포인트 2

TMS를 활용해 인가 받은 모든 단말에 대한 MAC 주소를 주기적으로 수집 및 업데이트, 최신 보안 정책 유지가 가능하다.

차단 페이지 리다이렉트

지점에서 인터넷 접속 시, 미인가 단말인 경우 사용자에게 다음 그림과 같이 웹브라우저에서 차단 페이지를 리다이렉트하여 보여준다. 사용자는 단말의 IP 주소와 MAC 주소는 물론, VPN 지점 장비의 호스트명 및 차단 시각 정보를 출력하여 임시 허용 신청에 필요한 정보를 직관적으로 파악할 수 있다.



본사 운영자는 이 정보를 기반으로 임시 허용 여부를 결정하게 되며, 로그 기반의 원클릭 설정을 통해 편리하고 신속한 업무 처리가 가능해진다. 또한, HTTP와 HTTPS을 모두 지원해 모든 웹 트래픽에 대한 리다이렉트 기능을 제공한다.

다양한 부가 기능

이 외에도 AhnLab TrusGuard는 지점 VPN 장비의 설치 & 구축 현황 및 이력 관리를 위한 상세 메모 기능, 전국 모든 지점 VPN 장비의 운영 상태를 지도 상으로 한 눈에 파악할 수 있는 지점 모니터링 기능 등 여러 사용자 친화적인 기능들을 제공한다.

도입 효과

비용 절감

AhnLab TrusGuard는 VPN 기능은 물론 L2 기반 제어 가능도 함께 제공해 솔루션 추가 도입에 대한 비용 부담에서 벗어날 수 있다.

보안 운영 복잡성 해소

단일 제품으로 운영과 관리가 가능해 여러 솔루션을 구축하고 운영하는 방식에 비해 복잡성을 큰 폭으로 개선할 수 있다.

운영 편의성 향상

지점에서는 상황에 따라 특정 단말에 대해 임시 허용이 필요한 상황이 발생할 수 있다.

도입 효과

- 비용 절감: 추가 솔루션 X
- 복잡성 ↓: 단일 제품 운영
- 편의성 ↑: 원클릭 설정 가능

현장에서는 VPN 장비, 본사에서는 TMS를 통해 로그 기반 원클릭 설정으로 미인가 단말을 임시 허용할 수 있어 현장 및 본사 담당자의 업무 효율성과 편의성을 제고할 수 있다.

향후 로드맵

특허 출원

안랩은 'IP 레이어 방화벽에서 MAC을 통한 선택적 클라이언트 제어 방법' 명칭으로 특허 출원을 진행 중이다.

차단 페이지 커스터마이징

운영자가 원하는 디자인과 형식으로 차단 페이지를 새롭게 정의할 수 있는 기능을 제공할 예정이다.

DB 연동 범위 확대

AD 외에도 MS-SQL, My-SQL, Oracle 등 다양한 DB를 연동할 수 있도록 할 예정이다.

양자암호통신 기반 VPN 적용

기존 유사난수 기반 알고리즘의 보안성을 향상시킨 양자난수 기반 알고리즘의 VPN 기능을 제공할 계획이다.