네트워크 보안 패러다임의 변화
Zero-trust 구현을 위한

소프트웨어 정의 경계
(**SDP** : **S**oftware **D**efined **P**erimeter)

기술백서

2020.05

since 1995
MLsoft

전통적 IT 보안 환경의 변화

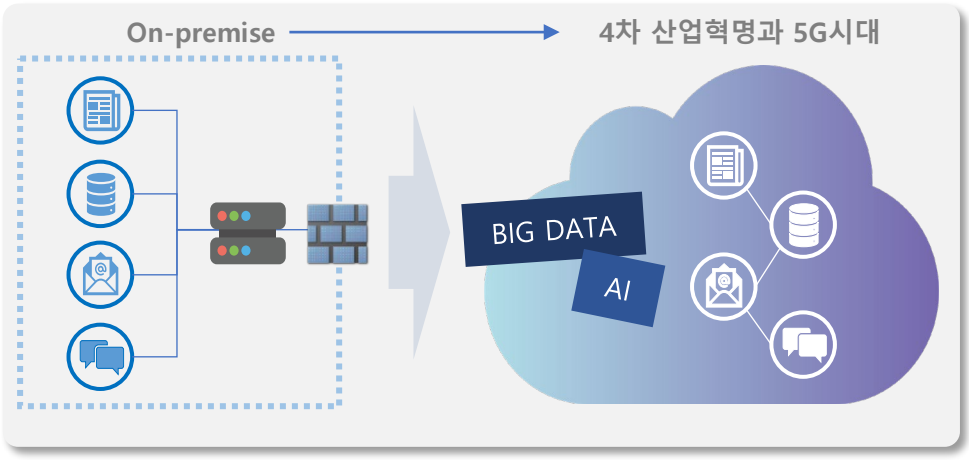
4차산업혁명에 따라 비즈니스 환경이 변화하고 있습니다.
이에 따라, 자연스럽게 IT환경과 IT보안 패러다임도 변화하고 있습니다.

본 문서를 통해 Zero-trust 구현을 위한 "소프트웨어정의 경계(SDP)" 기술에 대한 개념 및 구성, 활용방안을 알려드리려 합니다.

CONTENTS

정보보안 시장, 혁명이 시작됐다

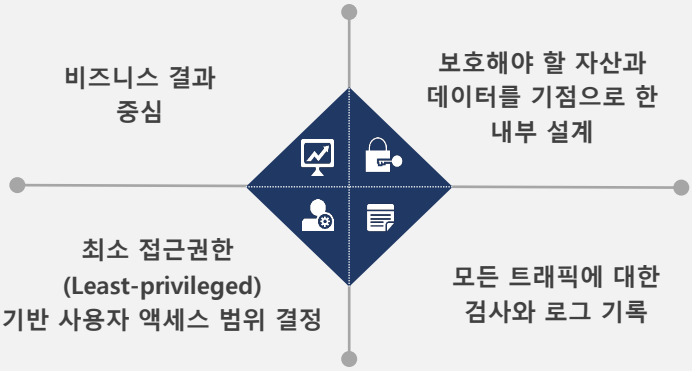
비즈니스가 클라우드로 확장되면서, 클라우드 환경에서는 전통적인 네트워크 경계 기반 보안 전략이 무용지물이 되고 있습니다.
4차산업혁명과 5G 시대를 맞아 Big Data와 AI를 이용한 초지능, 초연결사회로 급속히 변화하고 있으며, 기업의 전산망은 폐쇄적인 사내(On-Premise) 전산체계에서 개방적인 클라우드(Cloud) 체계로 전환되고 있습니다.



[그림1] 비즈니스 환경의 변화

이에 대한 성패는 초연결 인터넷망을 기반으로 하는 Zero-Trust 보안에 있다고 해도 과언이 아닐 것입니다.

Zero Trust 보안 전략 설계 4대 원칙



(출처 : 기업정보보안가이드 2019 v.14)

4차 산업혁명의 정의

"제4차 산업혁명(第四次 産業 革命, 영어: Fourth Industrial Revolution, 4IR)은 정보통신 기술(ICT)의 융합으로 이루어지는 차세대 산업혁명이다. 18세기 초기 산업 혁명 이후 네 번째로 중요한 산업 시대이다.
이 혁명의 핵심은 빅 데이터 분석, 인공지능, 로봇공학, 사물인터넷, 무인 운송 수단 (무인항공기, 무인 자동차), 3차원 인쇄, 나노 기술과 같은 7대 분야에서 새로운 기술 혁신이다."

* 출처 : 위키백과

"인간을 위한 현실과 가상의 융합"

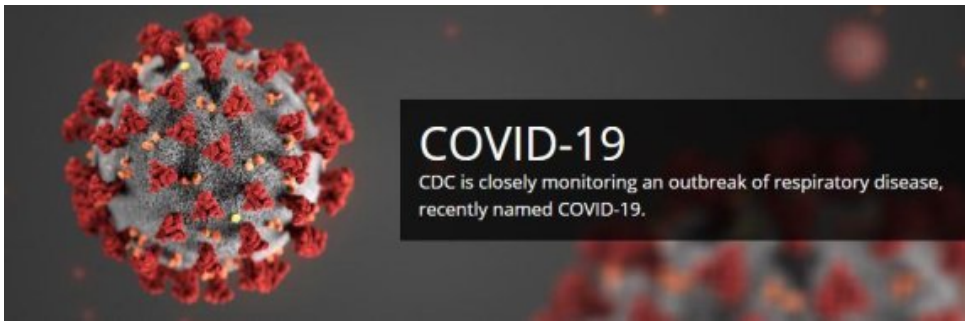
인간을 위한 : 가치 (AI - 예측, 맞춤)
현실 : Offline (IoT, Machine Learning)
가상 : Online (Cloud, Big data)
융합 : DT (Digital Transformation)
AT (Analog Transformation)

* 출처 : KCERN

새로운 시장 "xTech"

4차 산업혁명에서는 AI와 Big-data를 이용해 새로운 시장인 핀테크, 밀리테크, 바이오테크, 에듀테크, 애그로테크 등의 xTech 기술에 의한 새로운 시장이 열리고 있습니다.

Post COVID-19



2019년 12월 중순,발병한 신종 코로나 바이러스(이하, 'COVID-19')로 인해 WHO는 전세계적 범 유행인 '팬데믹'을 선언하게 되었습니다. 또한 대한민국은 2020년 1월 최초 발병 후 소수 인원의 감염 보고가 유지되다가, 2월 중순에는 특정 종교단체의 집단예배로 인해 급격한 감염자 증가 사태가 벌어지게 됩니다.

이로 인해 직장 폐쇄 조치가 시작되면서 그 동안 소극적으로 관망하던 공공기관과 기업들은 임시방편으로 원격근무, 분산근무, 자택근무 등의 방안을 모색하게 되었습니다. 그러나, 어느 정도 진정국면을 지나고 있는 현 시점에도 이태원 클럽 발 2차 확산 감염 사태를 통해 언제든 COVID-19로 인해, 또는 그 비슷한 외부 환경요인으로 인해 업무 영속성이 심각하게 위협받을 수 있다는 것을 체험할 수 있었습니다.

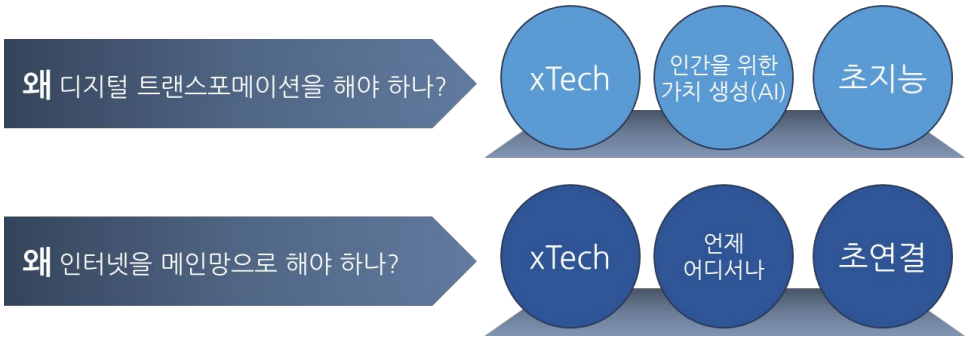
앞 장에서 말씀 드렸던, 4차 산업혁명과 5G의 초지능 • 초연결 시대와 더불어 Post COVID-19시대를 대비한 비즈니스 환경변화에 따라 기존 On-Premise 환경에서 Cloud로의 전환은 더욱 더 빠른 시간 내에 진행될 것으로 예상되고 있습니다.

[그림2] COVID-19 재택근무 관련 기사

왜 클라우드 인가?

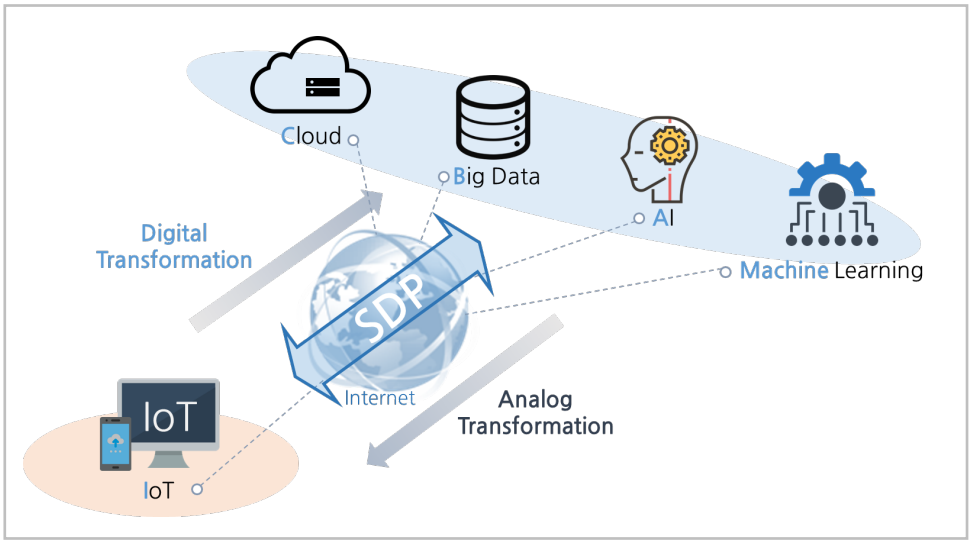
xTech를 담은 그릇, 활동 무대, 장터

- 비용절감을 위해?/ 살아 남기 위해?/ 비약적 발전을 위해?
- Big Data, AI/ Digital Transformation/ Internet/ IoT



ICBAM 과 네트워크 보안

현실과 가상의 융합의 구성요소인 ICBAM(IoT, Cloud, Big data, AI, Machine Learning)은 상호 Digital Transformation과 Analog Transformation이 이루어지며, 이 모든 것은 공개된 인터넷상에서 이루어지게 되며, 그에 따른 네트워크 통신 보안의 중요성이 더욱 강조되고 있습니다.



[그림3] 인터넷상의 ICBAM

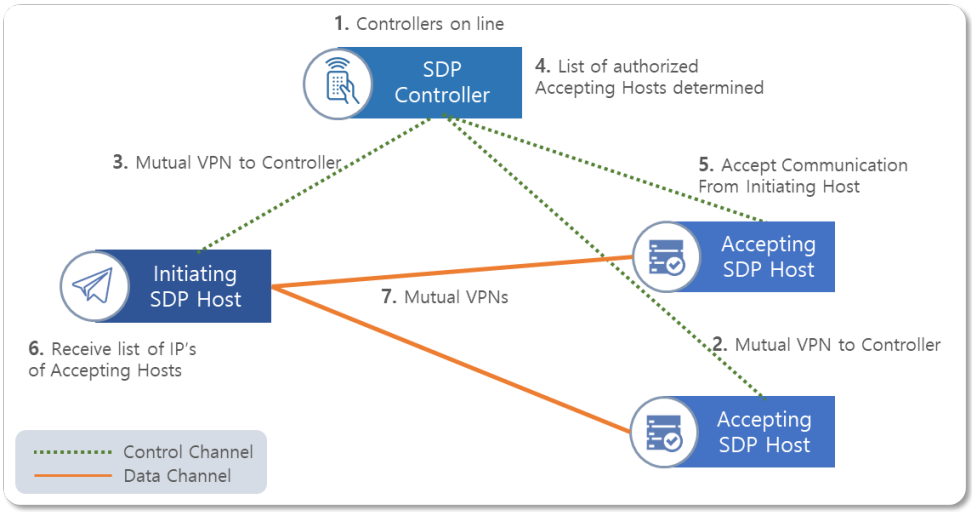
SDP 이해하기

소프트웨어 정의 경계

SDP (Software **D**efined **P**erimeter**)**

소프트웨어 정의 경계(Software Defined Perimeter, 약어로 SDP)란 '블랙 클라우드(Black Cloud)'라고도 불리며, 2007년경 미국방성의 GIG(Global Information Grid) 블랙코어 네트워크 우선권에 따라 DISA (Defense Information Systems Agency)에서 수행한 작업에서 발전한 컴퓨터 보안 접근 방식입니다.

SDP는 신원 기반으로 리소스에 대해 액세스를 제어하는 프레임워크로 네트워크 장치, 단말의 상태, 사용자 ID를 체크하여 권한이 있는 사용자 및 디바이스에 대해서만 액세스 권한을 부여하며 인증 받지 못한 단말기에 대해서는 그 어떠한 서비스 연결 정보도 얻지 못하게 되며, 인프라는 인증 및 인가가 되기 전에는 DNS정보나 IP주소를 알 수 없는 '블랙 클라우드(Black Cloud)' 네트워크로 동작이 되면서 해커들이 쉽게 보안을 뚫을 수 없도록 구성이 되어 있습니다.



[그림4] SDP Framework developed by CSA

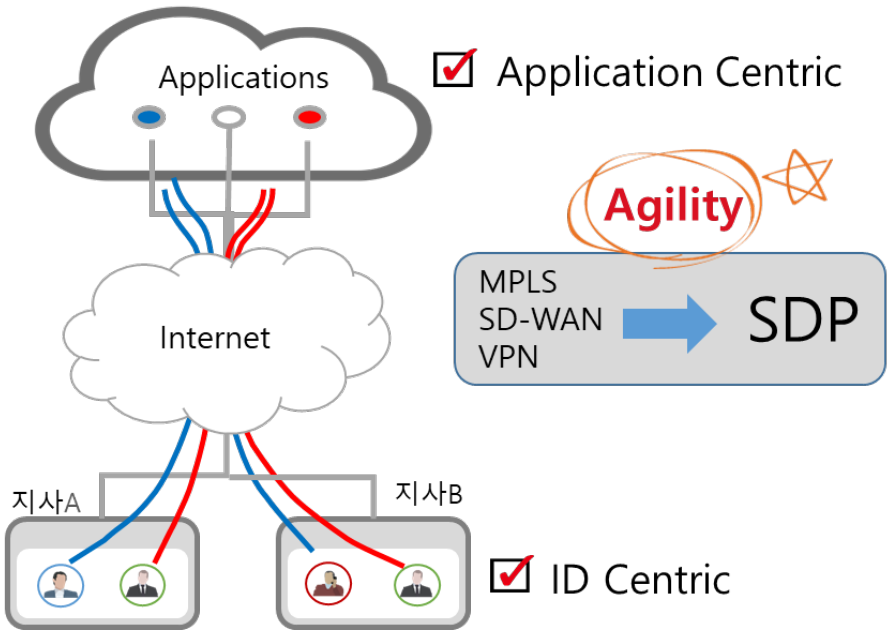
5개 계층의 보안 제어

소프트웨어 정의 경계 아키텍처는 단일 패킷 인증, 상호 전송 계층 보안, 장치검증, 동적방화벽 및 애플리케이션 바인딩의 5개 계층의 보안제어로 구성되며, 이러한 프로토콜들은 함께 공격자가 보호된 응용프로그램에 접근하는 것을 매우 어렵게 만듭니다.

- ✓ 단일 패킷 권한 부여(SPA)
- ✓ 상호 전송 계층 보안(mTLS)
- ✓ 장치 유효성 검사(DV)
- ✓ 동적 방화벽(Dynamic Firewall)
- ✓ 애플리케이션 바인딩(AppB)

민첩성

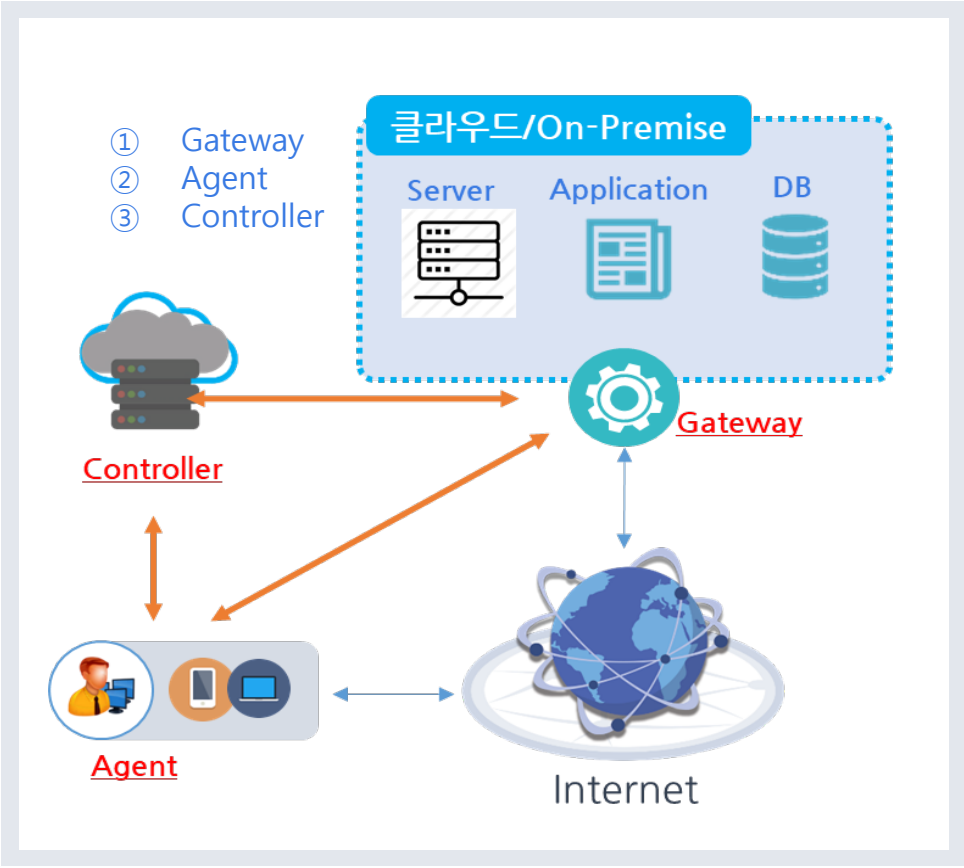
MPLS, SD-WAN, VPN등의 네트워크와 보안 환경 변경 시에는 Location, Hardware, Service-Provider 등의 제약조건이 발생합니다.
소프트웨어 정의 경계 아키텍처는 사용자는 ID Centric으로 서버부분은 Application Centric으로 구성되어 민첩하게 보안 환경 변경 관리 및 유지가 가능하게 만들어줍니다.



[그림5] SDP 민첩성

스텔스 (Stealth)

소프트웨어 정의 경계 아키텍처는 Server, App, Data등 중요 정보자원을 Gateway로 은폐하여 보호하는 방식이며, 사용자는 단말에 설치된 Agent를 통해 신원과 장비를 Control로부터 인증 받은 후에만 Gateway에 접속정보를 전달받아 Gateway로 접근할 수 있습니다. Gateway, Agent, Control로 구성되는 소프트웨어 모듈로 구축이 간편합니다.

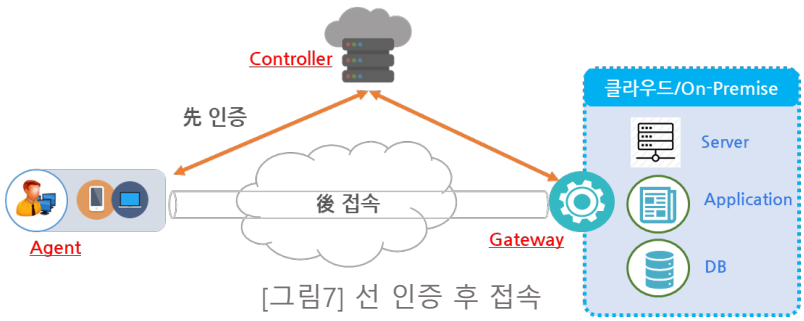


[그림6] 소프트웨어 정의 경계 구성

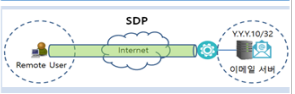
- 5개 계층의 보안 제어
- 민첩성(Agility)
- 스텔스(Stealth)
- **Next VPN**
- Zero Trust
- 신원 기반 네트워크 접속 통제

Next VPN

기존의 VPN은 '선 접속 후 인증' 방식으로 원격지 접속지 서버 정보가 노출 될 뿐만 아니라 VPN접속이후 내부 네트워크 상의 다른 네트워크 자원에 접근이 가능하게 되는 보안의 위협요소를 내포하고 있습니다.
소프트웨어 정의 경계 아키텍처는 '선 인증 후 접속' 방식으로 접속 서버가 노출되지 않으며, 접속 후에도 App-binding을 통해 지정된 서비스에만 접속하게 되어 기존 VPN을 대체 가능하게 됩니다.



[그림7] 선 인증 후 접속

구분	Site to Site VPN	Remote Access VPN	SDP
구성도			
철학(컨셉)	서로다른 양단의 네트워크를 가상 사설망으로 구성하고, 사용자 단말은 단순히 해당 네트워크를 사용하는 구성	사용자 단말과 특정 네트워크 그룹을 가상 사설망으로 구성	사용자 단말의 특정 프로그램과 사내의 서버 또는 서버내의 특정 프로그램과의 네트워크 경계를 만들어 사용
연결(노출) 범위	가상 사설망 내의 모든 서버 IP와 오픈된 서비스 포트 노출 (광범위 노출)	가상 사설망 내의 모든 서버 IP와 오픈된 서비스 포트 노출 (광범위 노출)	App to App 연결방식으로 권한이 없는 서버는 노출되지 않음
에이전트 프로그램	구성상 에이전트 불필요	에이전트 방식과 에이전트리스 방식 제공	제로트러스트를 위해 반드시 필요 (Application Binding 지원)
터널 생성	사용자 단말에서 터널을 생성하지 않음	사용자 단말과 VPN G/W간의 터널 생성	사용자 단말의 특정 프로그램과 SDP G/W 간의 터널 생성
서비스 대상	본사의 네트워크 자원에 연결하고자 하는 지사(지점) 사용자	외부에서 사내의 네트워크 자원에 연결하고자 하는 로밍 사용자	제로트러스트 환경에서 안전하게 사내의 특정 서버에 액세스하려는 사용자
인증 방법	선 접속 후 인증 방식으로 VPN G/W의 목적지가 노출됨 (채널 구분 없음)	선 접속 후 인증 방식으로 VPN G/W의 목적지가 노출됨 (채널 구분 없음)	선 인증 후 접속 방식으로 SDP G/W의 목적지 노출이 안됨 (제어 채널과 데이터 채널 구분)
방화벽 운영 방식	블랙리스트 방식, IP기반 정적 설정 (운영 및 관리가 어려움)	블랙리스트 방식, IP기반 정적 설정 (운영 및 관리가 어려움)	화이트리스트 방식, ID기반 동적 설정 (운영 및 관리가 쉬움)
취약점 및 보완 방법	신규 단말은 가상 사설망 이용에 특별한 제한이 없음으로 모든 서버에 접근이 가능하고 이를 보안하기 위해 별도의 솔루션(IPM, NAC 등)이 필요함	에이전트 프로그램과 ID/PW가 노출되면 타 장비에서 접근이 가능함	장비등록 단계에서 수집된 Device Key와 사용자 계정정보(ID/PW)가 일치해야 하고 HOTP 2차인증을 통과해야 연결이 허가됨

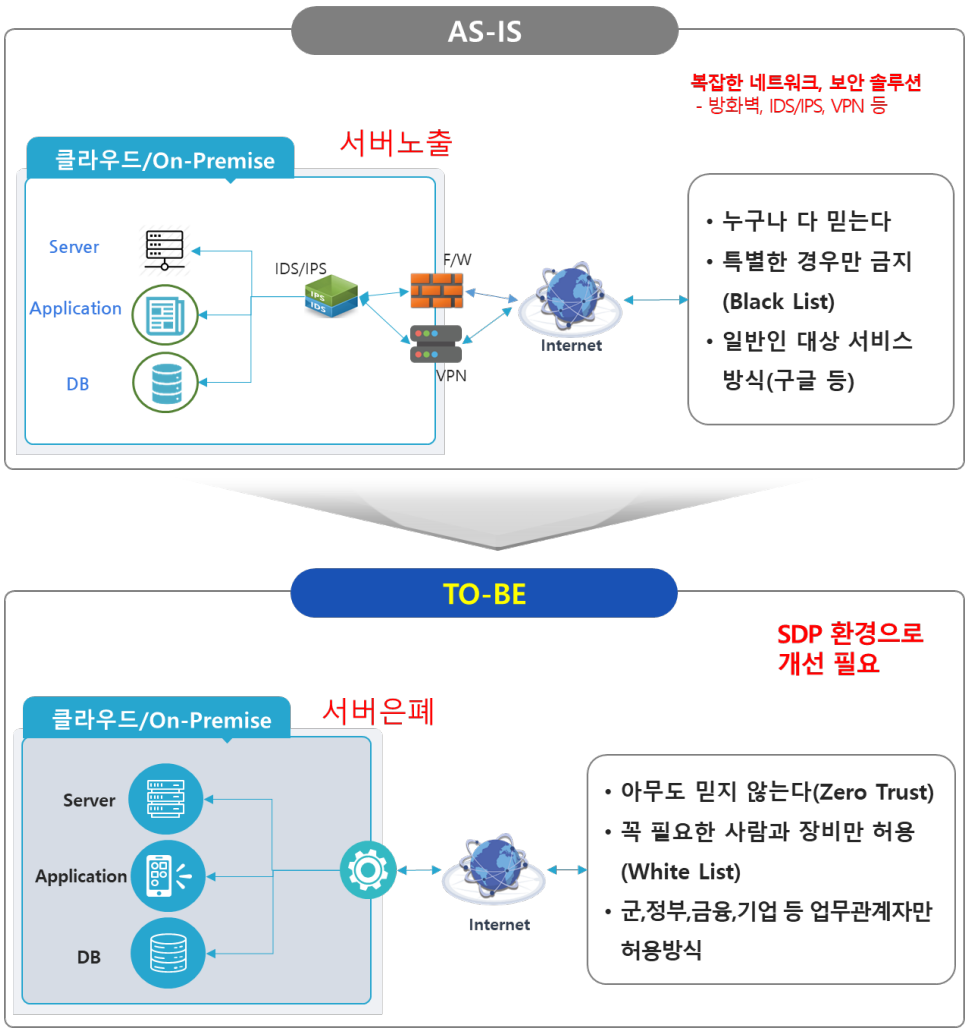
[표1] SDP VS VPN

Zero Trust

제로 트러스트 네트워크(Zero Trust Network), 또는 제로 트러스트 아키텍처(Zero Trust Architecture)라고도 알려진 보안 모델은 2010년 당시 포레스터 리서치의 수석 애널리스트로 재직 중이던 존 킨더박(John Kindervag)이 만든 모형이다

* 출처 : CIO KOREA

기업이 기존 레거시 시스템에서 하루아침에 제로 트러스트 기반의 네트워크 환경을 구성하는 것은 어려운 일입니다. 복잡하게 얽혀 있는 IT환경과 레거시 시스템들을 일시에 전환하는 것은 불가능하지만, 클라우드로 전환을 꾀하는 시점에서는 충분히 가능한 상황이며, 소프트웨어 정의 경계 아키텍처는 제로 트러스트 네트워크 모형 도입에 큰 기여를 할 수 있습니다. 제로 트러스트 모형에 가장 근간인 신원 기반으로 화이트 리스트의 사람과 장비만 허용하고, 대상 서비스를 숨길 수 있습니다.

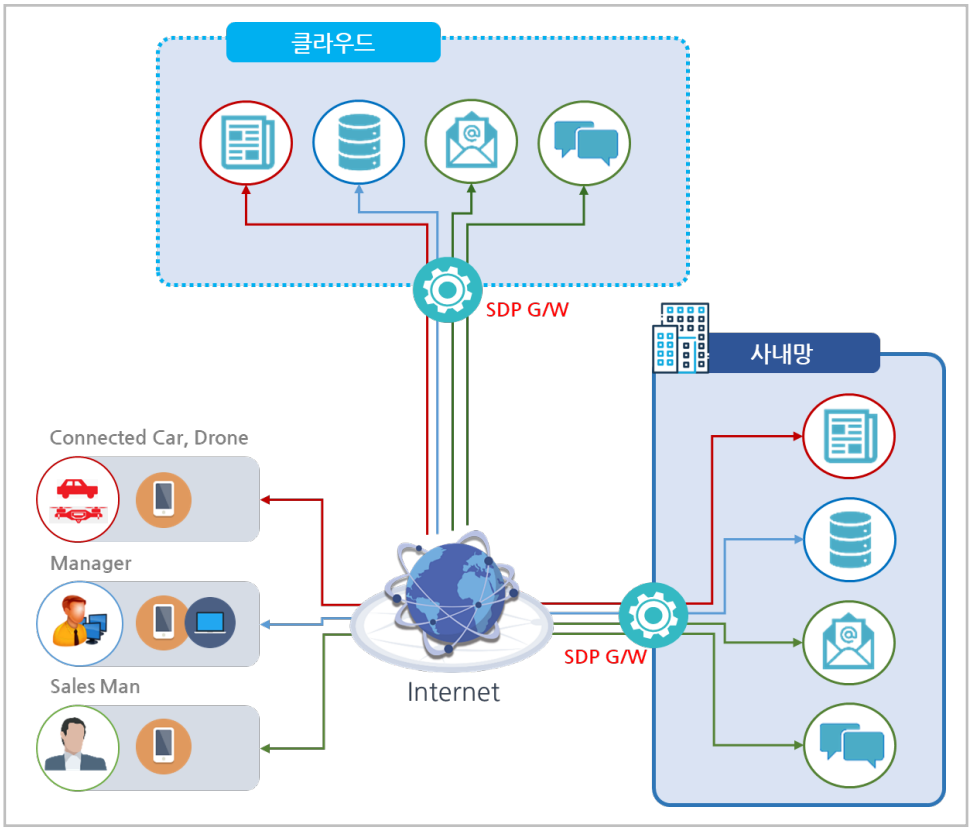


[그림8] SDP를 이용한 제로 트러스트 구성

신원기반 네트워크 접속 통제

다양한 임무를 수행하는 조직 구성원들은 PC, 노트북 등 뿐만 아니라, 모바일, 태블릿, RFID 리더, POS단말 등 다양한 엔드포인트 장치를 통해 조직 서비스망에 접속을 하게 되고, 업무 상황에 따라 빈번한 임무 변경, 조직구성이 변경되고 있습니다. 그리하여, 네트워크 및 보안 담당자들은 기존 레거시 시스템에서 빠르게 변화하는 환경에 맞게 설정하는 것 조차 엄청난 업무과중과 스트레스에 시달리게 되었습니다.

소프트웨어 정의 경계(SDP)는 신원을 기반으로 네트워크 접속을 통제하므로, 이 문제를 손쉽게 해결할 수 있습니다. 단순히 사용자와 서비스를 맵핑하는 정책설정 과정만으로 접속 가능한 서비스를 제공하고, 과도한 권한을 가질 수 없도록 제한할 수 있습니다. 대규모 인사이동이 발생하더라도 인사시스템과 연동하여 즉시 정책이 변경이 되고, 권한을 부여하거나 회수할 수 있습니다.



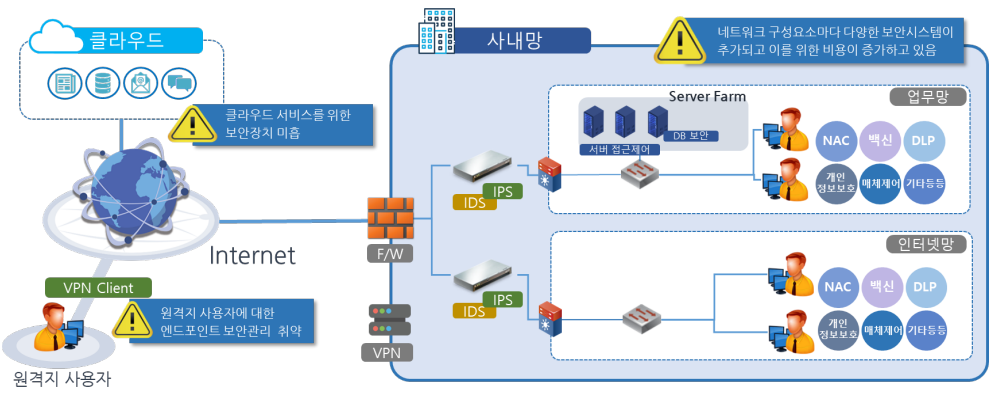
[그림9] 신원 기반 네트워크 접속 권한 통제

- **업무망과 인터넷 보안 환경 개선**
- 망 분리 체계 전환
- 각종 IoT 기기 보안 접속

업무망과 인터넷 보안 환경 개선

기존의 On-Premise환경에서 각 요소 및 단계마다 다양한 종류의 전용보안 시스템을 겹겹이 둘러싼 네트워크 중심기반의 보안체계를 구성하고 있습니다. 가령, 회사 내부로의 접점에는 외부 방화벽부터 Proxy, IPS , IDS, 물리적 망분리에 내부 방화벽까지 구성하고, 서버 단에는 서버접근제어, DB보안, 서버백신 등, 마지막 엔드 포인트 단에는 IP관리, NAC, 백신, DLP, 개인정보보호, 매체제어 시스템 등 다양한 보안솔루션과 시스템이 겹겹이 둘러싸고 있는 상황입니다.

물론, 기존의 이런 시스템들이 무용지물이라는 의미는 아닙니다. On-Premise라는 한정된 공간의 제한적인 사용자 접속을 통제하는 데에는 하나하나가 강력한 기능을 제공하여 지금까지 조직 내 중요한 보안을 책임져 왔기 때문입니다. 네트워크 또는 보안담당들은 대규모 인사인동이나, 지사나 지점의 이전, 증가하는 외근 사용자들의 IoT기기들에 대한 정책변경 및 보안관리를 위해 많은 밤을 지새우곤 해왔습니다. 더군다나, 4차 산업혁명 속에서 비즈니스 변화에 따른 민첩성을 더욱더 강요 받게 되어 앞으로도 더 빨리, 더 빈번하게 변경작업들이 이루어 질 것입니다. 잘 알 수 있다시피, 많은 보안사고는 이러한 과중한 업무 속에서 Misconfiguration 으로 인해 발생하기도 합니다.

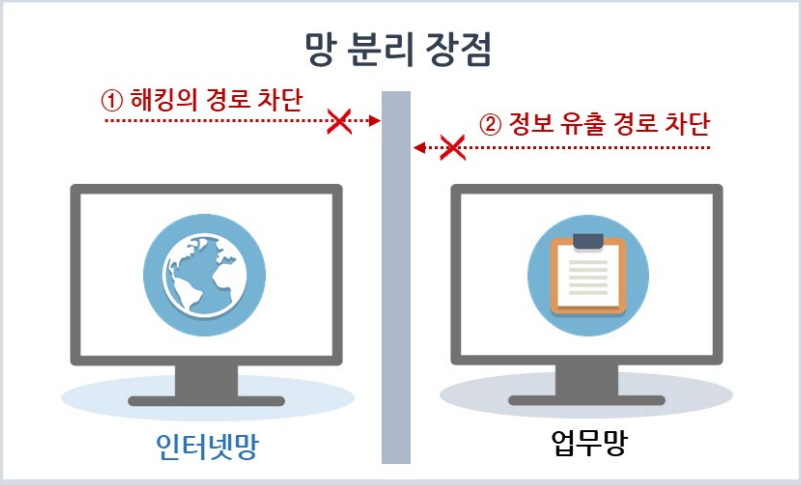


[그림10] 현재 보안시스템의 문제점

이런 상황에서 4차 산업혁명을 대변하는 AI와 Big data를 고려한다면, 클라우드 환경으로의 전환이 필수적 요소이고, On-premise환경과 다르게, 개방형 인터넷상의 수많은 서버들과 전세계 어디에 서든 접근하는 사용자의 접속을 제어한다는 것은 기존의 보안체계를 유지하는 것은 사실상 불가능하기 때문에 Network Centric 접속관리에서 ID Centric 접속관리로의 전환이 필요하게 된 것이며, **SDP는 이를 위한 최적의 네트워크 보안 솔루션**이라 할 수 있습니다.

망 분리 체계 전환

망 분리란? 2013년 3월 20일 사이버공격 피해 사례를 분석한 결과로 개발된 **업무망과 인터넷망을 분리**하여 **해킹경로 차단 및 정보유출 방지**를 위한 보안 방식입니다.



[그림11] 물리적 망 분리 (예)

망 분리는 기존의 온 프레미스 환경에서는 최적의 보안 환경이라 할 수 있지만, 구축비용이 비싸고, 업무효율과 속도가 떨어지는 데다가 클라우드 환경에 적합하지 않는다는 단점이 존재합니다.

✓ 망 분리 구성에 높은 비용 발생

- 1인 2PC 구성으로 PC 및 SW구매 비용 증가
- 네트워크 이중구성 및 보안시스템 구축 비용 증가
- 관리포인트 증가로 관리비용 증가

✓ 업무효율 및 속도 저하

- 사용자 편의성 저하
- 작업공간에 대한 제약으로 효율성 저하

✓ 클라우드 환경에 부적합

- 업무 망 사용자의 클라우드 서버 이용이 제한적
- 전화하는 비즈니스 컴퓨팅 환경 변화 대응이 어려움

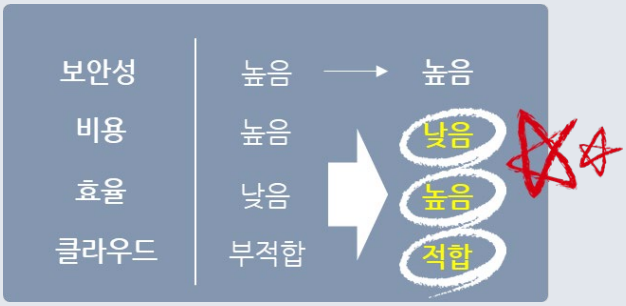
4 SDP 활용분야

그러나, 소프트웨어 정의 경계(SDP) 아키텍처를 이용하면 보안성은 유지하면서 비용을 절감하고, 업무효율을 높이면서도 클라우드 환경에 대응할 수 있습니다. 다만, 국내에서의 망 분리법에 의한 규제 대상 고객들은 법 개정 전까지 시간과 준비가 필요할 것으로 보입니다.

망 분리 대체 필요성

망 분리의 장점이자 목적인 높은 보안성을 유지한 상태에서

1. **구축 및 운영비용**을 낮추고,
2. **업무효율**을 높이고,
3. **클라우드 환경에 대처**가 가능한 방안 필요



망 분리는 대체 가능한가?

망 분리의 목적인 해킹경로 차단 및 정보유출 방지 역할은 충분히 대체 가능한 기술이 존재하며, 소프트웨어 정의 경계(SDP) 외에 Third –party 제품을 이용하면 망 분리 구성과 동일한 보안을 유지할 수 있습니다.

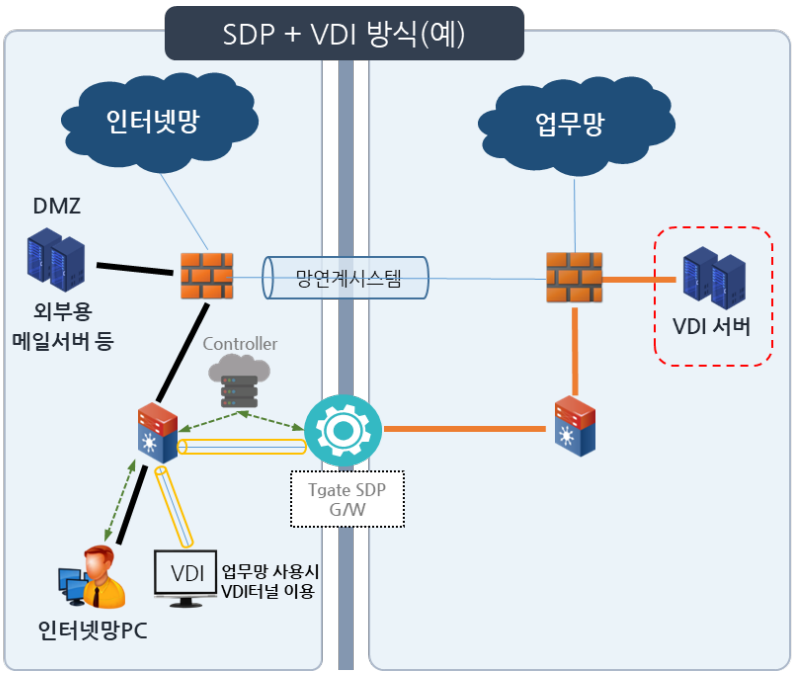
각종 IoT 기기 보안 접속

기술의 발전에 따라 5G 서비스 개시로 인한 광대역 무선통신 및 수 Km 거리 연결이 가능한 Wi-Fi 장비들이 출시되어 실용화 되고 있기 때문에 향후, 산업용 Drone이나 Connected Car, Wi-Fi CCTV, Smart home 등의 다양한 IoT 기기 등은 개방된 인터넷을 통해 연결 될 것이며, 아주 작은 스마트 홈 시스템의 스위치 하나라도 해킹이나 악의적 행위로 인해 사용자의 안전에 위협을 가할 수 있기 때문에 모든 IoT기기들은 반드시 보안이 필요합니다.

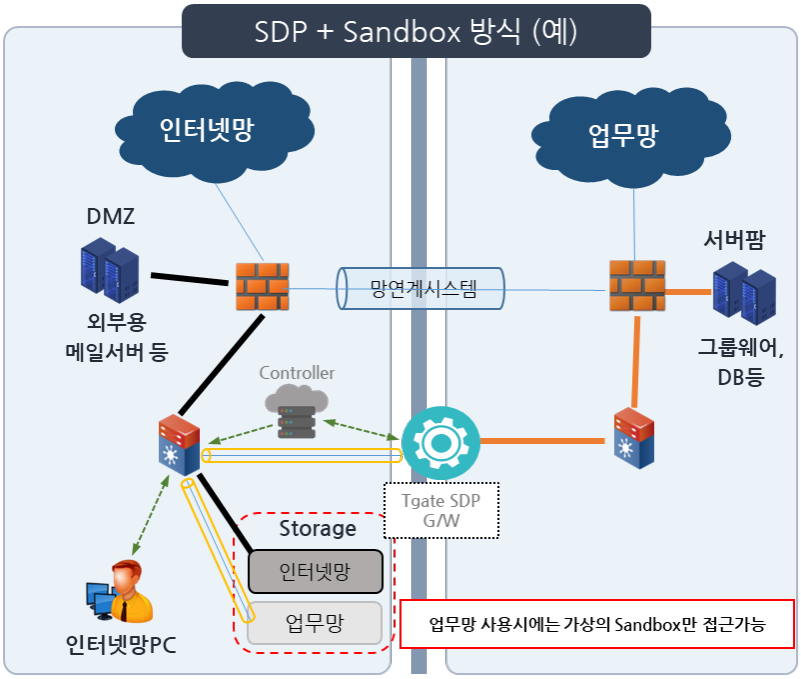
소프트웨어 정의 경계(SDP) 아키텍처는 일반적으로 업무에 사용되는 IT기기(PC, 노트북, 모바일, 태블릿 등)외에도 보안 연결이 필요한 **대부분의 모든 IoT기기에 적용이 가능**합니다.

재택근무 (VDI or SANDBOX)

COVID-19 사태와 같은 재난상황이 발생 시, 근무처 폐쇄 등의 상황이거나, 외부사용자나 업무자유도가 높은 환경의 고객사의 경우, SDP와 VDI 또는 Sandbox 등을 이용하면, 내부 서버 보안과 외부 자료 유출방지가 가능한 재택근무 환경을 구성하실 수 있습니다.



[그림12] SDP + VDI방식

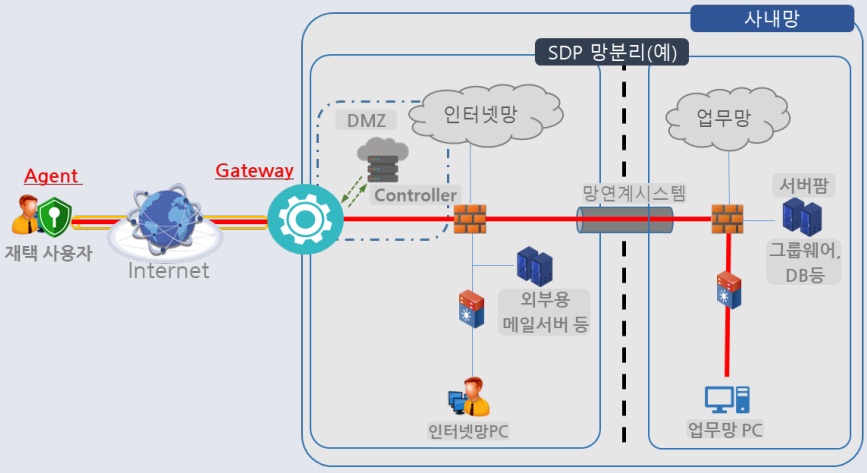


[그림13] SDP + Sandbox방식

재택근무 (원격제어)

VDI나 Sandbox가 없거나 구성이 어려운 고객사의 경우 원격제어 프로그램을 이용하여 업무망에 위치한 본인의 PC를 원격으로 접속하여 재택근무를 수행할 수 도 있습니다.

단, 이 경우에는 본인의 PC가 항상 켜져 있거나, 또는 내부에서 누군가가 전원을 켜줘야 하는 문제를 내포하고 있습니다. 그래도 COVID-19와 같은 긴급한 재난상황일 경우에는 충분히 활용 가치가 높은 운영 환경입니다.



- 업무망 개인 PC만 접속 가능
- 원격제어 PC에서 파일 업/다운로드 안 됨
- 업무망 개인 PC에서 업무망 서버 접속

[그림14] SDP + 원격제어

✓ 원격제어를 이용한 재택근무 환경 구성 장점

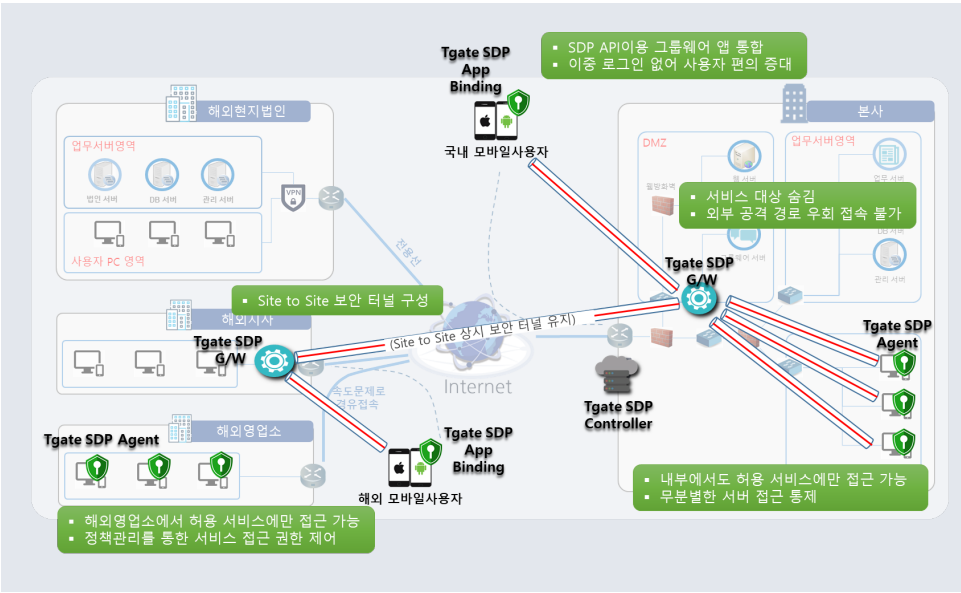
1. 기존의 망 분리 체계를 그대로 유지한 상태에서 구성 가능
2. VPN 환경보다 높은 수준의 보안을 제공
3. 구축과 운영이 간단하고 쉬움
4. 향후 증설이 매우 용이
5. 콜센터에도 유사 구축 가능함

- 재택근무(VDI or SANDBOX)
- 재택근무(원격제어)
- **외부 사용자 보안 접속**
- ATM/POS 단말 보안 접속
- 전용 API를 이용한 App-binding

외부 사용자 보안 접속

소프트웨어 정의 경계(SDP)는 그룹웨어 등의 외부 애플리케이션에 통합할 수 있는 API(Application Interface)를 제공합니다. 고객은 그룹웨어 앱과 API연결하여 별도 VPN 접속 없이 보안 접속 통신을 지원할 수 있습니다. 이렇게 되면, 비용절감과 동시에 사용자의 앱 접근성을 높여 편의성이 증가하게 되고, 사용자가 접근하는 서버를 숨기고, 프록시 서버가 필요 없게 되어 보안 취약점 발생을 방지할 수 있습니다.

또한, 본사 내부사용자도 SDP 에이전트를 통해 허용 서비스에만 접근할 수 있도록 권한을 제어하여, 무분별한 업무 서비스 접근을 방지 할 수 있습니다. 해외 지사의 경우, 인터넷 회선 속도 문제를 고려하여 속도가 우수한 인근 지역의 지사를 통해 본사와 통신할 수 있도록 Site-to-Site 보안 터널 연결을 상시 유지할 수 있도록 구성이 가능하며, 외부 사용자 단말 분실 시 에도 장비 인증을 취소함으로써 빠른 권한 회수가 가능합니다.

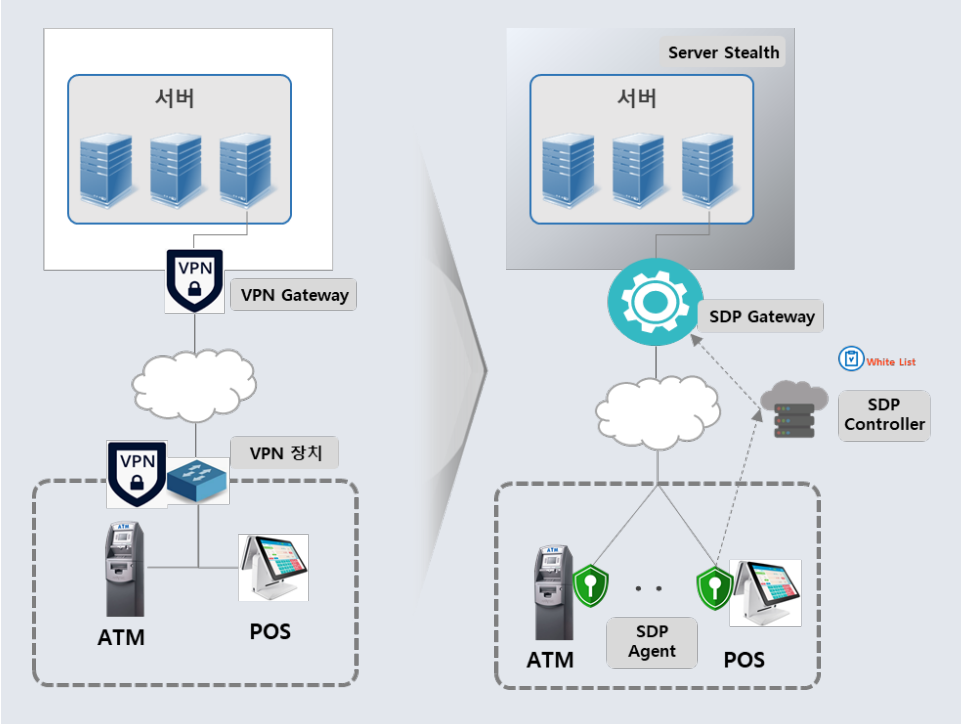


[그림15] API를 이용한 그룹웨어App 통합 구성

ATM/POS 등 외부 단말 보안 접속

현금인출기(ATM)나 판매관리시스템(POS)등에도 네트워크 통신보안을 위해 VPN 을 이용하는 경우가 많습니다. 이를 위해 영업점 신설 및 이동 시마다 VPN 장치 구매와 설치, 유지보수 비용 등 관리포인트나 비용이 증가하게 됩니다.

소프트웨어 정의 경계(SDP)를 이용하면 ATM기나 POS단말에 SDP Agent를 탑재하거나 전용 애플리케이션에 API를 연동하여 쉽고 빠르게 설치운영이 가능해질 뿐 아니라, 점포 이동 시에도 손쉽게 대응이 가능합니다.

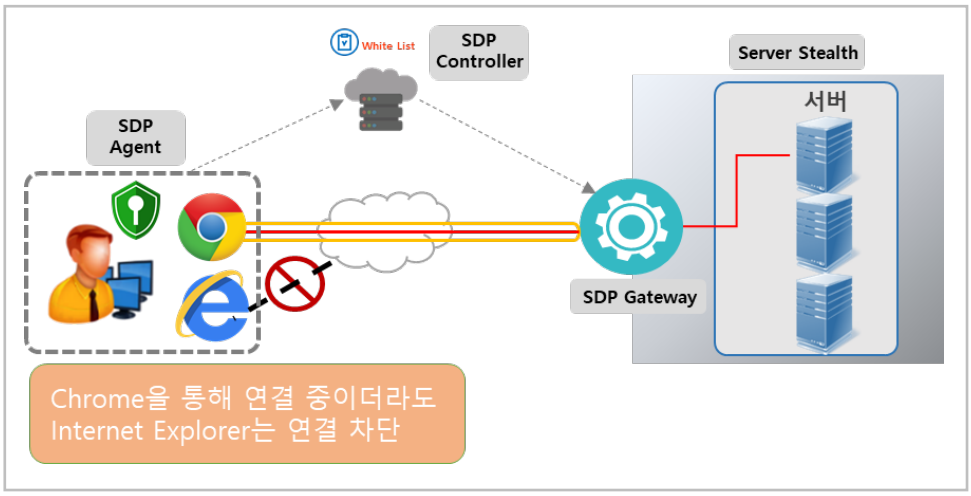


[그림16] SDP를 이용한 ATM / POS 단말 연결

전용 API를 이용한 App-binding

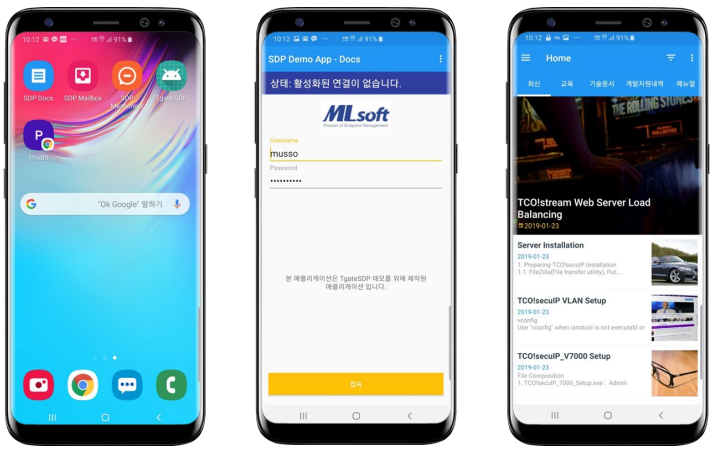
App-binding이란? 네트워크 접속 권한을 관리할 때 서버의 IP나 Port 외에도 접속이 가능한 App을 지정하여 허가된 App이 아니면 통신이 불가능하도록 제어하는 기술

소프트웨어 정의 경계(SDP)는 App-binding 기능을 제공하는데, PC Agent를 통해 지정된 소프트웨어를 사용해야만 서버에 접속할 수 있는 방법과 제공되는 표준 API를 이용하여 그룹웨어, 메신저, 이메일 등의 개별 앱을 개발 연동하여 접속을 제어하는 방법 2가지를 제공합니다.
App-Binding을 할 경우에는 허용되는 App을 이용하여 서버에 접속한 On-line 상태라도, 해당 App외에 다른 SW로는 접속이 불가능 합니다.



[그림17] App-binding 시 허용 App 연결 외 차단

아래 그림과 같이 사내 Document 시스템에 접근하기 위해 전용 앱에 API를 연동하여 사내 서버에 접근하는 시스템 구현도 가능합니다.



[그림18] 전용 API를 이용하여 개발된 App

정성적 효과

비즈니스 모델의 변화에 따른 민첩한 Application Centric으로의 변화

민첩성 (Agility)

- Location, Hardware, Service-Provider 등 네트워크와 보안환경에 대한 제약조건이 적어, 사업모델 변경 시 신속한 업무중심의 응용프로그램 환경 구성 가능
- SDP는 지리적으로 분산된 여러 엔드포인트, 데이터 센터 및 가상 사설 클라우드를 연결하는 등의 유연성 제공

보안성 강화

- **서버 스텔스(Server Stealth)**
  대상 네트워크 정보를 외부에 노출하지 않음
- **SPA(Single Packet Authorization)**
  최소한의 인증 과정으로 인해 DDoS 공격 방지
- **Dynamic Firewall**
  화이트리스트 기반의 사전에 허용된 대상에
- **IPsec Tunnel**
  IPsec을 이용한 강력한 보안 터널 연결
- **App Binding**
  지정된 Application만 서비스 연결 가능

정량적 효과

불특정 다수 보안 : 비용증가 VS 지정대상 보안 : 비용절감, 시간절약

비용절감

- **구축 비용 절감**
  신규 구축 시 Branch용 VPN장비가 필요 없고, 기간 단축으로 구축 비용이 저렴
- **확장 비용 절감**
  사용자 및 서비스 추가 시에도 별도 SW나 HW필요 없이, Agent License 추가 만으로 확장 가능
- **관리 비용 절감**
  운영 시 네트워크 설정 변경(방화벽, 라우터 등)범위가 적으며, 관리작업을 위한 비용 절감 효과

시간절약

- **보안 정책 관리 단순**
  데이터센터 또는 가상 프라이빗 클라우드 내에서 액세스 권한을 부여 할 때 추가 구성 및 유지 관리 대상이 거의 없어, 보안 정책 관리가 단순하여 작업시간 단축
- **변경 관리 용이**
  SDP 이용하면 사용자와 이용 서비스를 연결하는 정책만으로 설정할 수 있어, 기존의 네트워크 환경 설정(방화벽, 스위치 등)에 걸리는 시간을 획기적으로 단축할 수 있음

마무리 하며

지금까지 알아본 바와 같이 소프트웨어 정의 경계(SDP)의 활용은 그 범위와 영역에 상관없이 무한한 가능성이 열려 있습니다. 기업에서는 비즈니스 컴퓨팅을 위해 장소와 경계에 무관하게 적용이 가능하며, 각종 IoT장비의 보안 통신을 가능하게 합니다. 전국 방방곡곡 설치되어 있는 현금인출기나 카드 결제 단말기, POS시스템 등 사용자와 밀접한 접점에 있는 무인 단말기에도 적용이 가능합니다. 또한, 민감한 고객정보를 다루는 보험설계사용 단말에도 적용이 가능하고, Wi-Fi를 이용하는 산업용 Drone이나 Connected-car 등의 통신에도 안전한 보안을 제공하며,
이 모든 것은 4차 산업혁명의 시대와 5G등의 점점 더 빨라지는 IcT 기술을 통해 발전하는 비즈니스의 환경변화를 뒷받침할 수 있는 중요한 기술이 될 것입니다.

저희 엠엘소프트는 2018년부터 ETRI로부터 기술이전을 받아 2019년 SDP 솔루션인 "Tgate SDP"를 출시하였고, 기존에 자사에서 서비스하던 Tgate NAC 제품과 Seamless하게 연동되도록 구성하였습니다. 2020년 전세계 팬데믹 현상인 COVID-19사태를 맞아 Tgate SDP 제품을 신속하게 서비스 하여, 긴급상황에서 고객의 비즈니스가 중단되지 않도록 최대한 지원하고 있습니다. 앞으로도 지난 25년과 같이 고객의 Needs를 적극 반영하여 고객과의 동반성장을 목표로 4차 산업혁명 시대의 Cloud 보안 전문회사로 거듭나도록 하겠습니다.

감사합니다.

since 1995 MLsoft
www.mlsoft.com
02-501-3221
sales_grp@mlsoft.com