Zero Trust Security Model을 통한 망연계 보안성 고도화 방안

i-oneNet

i-oneNet DD

i-oneNet DX

NGS

CamPASS

MoBiCa

i-Spector

ViSiCa

2022. 04. 21

연구개발본부장/전무 손동식 Ph.D.

HUNESION

Contents

HUNESION

Unknown Attack Spectrums

"이제는 모두가 인지한다. 알려지지 않은 방대한 공격 벡터"

Advanced Persistent Threats

Zeroday 형태의 공격은 10번의 시도중 9번은 성공할 정도로 탐지가 거의 불가능

Social Media Protection(SNS)

전자메일은 여전히 중요한 공격벡터이며 소셜 미디어를 통한 Scam은 70%이상이 수동으로 공유

Insider Threats

민감한 정보에 액세스 할 수 있는 관리자와 같은 권한이 부여된 사용자는 가장 큰 내부 위협요소

Mobile Security & Protection

모바일 장치의 사용이 증가함에 따라, 스팸, Scam 및 위협 등이 이러한 장치에 맞게 조정될 것이며, Bootkit와 같은 Mobile Malware는 더욱 제거하기 어려워 질것임

IOT (Internet of Things)

사물간 인터넷에 사용되는 허브, 스위치, 라우터들은 인터넷 연결과 저장 및 처리가 가능하며 네트워크를 공격하기 위한 수단으로 사용됨.

Critical Infrastructure

가장 중요한 추세로는 악성코드를 사용하여 감시 제어 데이터 수집 시스템(SCADA) 및 홈리스 관리 정보 시스템(HMIS,Wallpad) 등을 감염시켜 민감정보 및 데이터를 탈취하는 공격 등이 있음.

망연계와 침해 사례

"'망연계' 란 '망분리' 환경에서 분리된 망과 망사이, 연계 환경을 구축하는 네트워크 연계기술"

그러나, 망분리를 통해 강화된 네트워크 보안환경에 사용자가 개입하여 자료를 전송하는 기술이다 보니, 사용자로 위장하여 외부의 해커 침투 발생

2010년 6월 Stuxnet

USB를 통해 원전 제어시설을 감염시켜 이란 부셰르 원전과 나탄즈 우라늄 농축시설의 가동을 멈춤

약1천개 이상의 원심분리기가 파괴됨

2014년 12월 한수원

악성코드가 포함된 한글파일의 E-mail전파를 통해 실행유도

업무망, 인터넷망 하드디스크 파괴 및 원전도면 등 데이터 유출

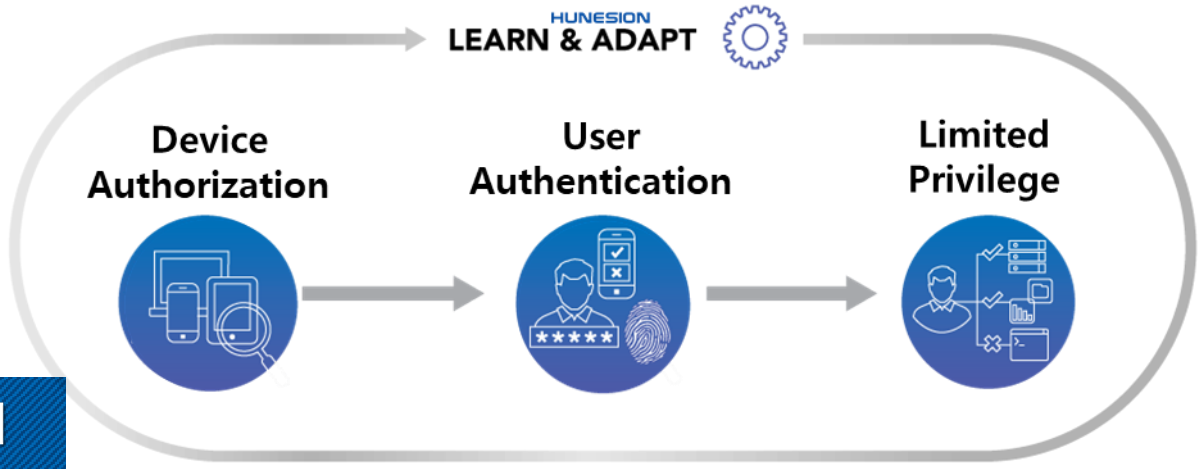
2016년 12월 국방부

북한의 해킹공격으로 인한 군사비밀을 포함한 일부 군사정보가 유출, 3200여대 악성코드 감염

Zero Trust Security Model

"제로 트러스트는 조직의 네트워크 아키텍처 보안에 대해 신뢰할 수 없다는 개념에서 출발하는 전략적 보안 접근 방식"

신뢰할 수 없는 내부 객체, 직접적인 보안관리, 다중 신분확인, 모든 액세스 시도의 신뢰성 검증 을 통해 복잡해지는 네트워크 보안환경을 해소



Zero trust Network 3단계

Zero trust 접근방식

전통적인 보안 접근 방식은 회사 네트워크 내부의 모든 요소를 신뢰할 수 있다고 가정 함. 그러나 망연계, 재택 및 이동성, IoT, 클라우드, 협업 증가로 인해 이러한 가정은 더 이상 맞지 않는 것이 현실임. 제로 트러스트 모델에서는 모든 리소스를 외부 리소스로 간주하고 신뢰 여부를 지속적으로 확인한 후 필요한 액세스 권한만 부여.
출처를 불문하고 모든 액세스 요청에 대해 신뢰 설정
애플리케이션과 네트워크 전반에 걸친 액세스 보안
신뢰를 확장하여 분산형 네트워크에서 클라우드 등 다양한 엔터프라이즈 환경 지원

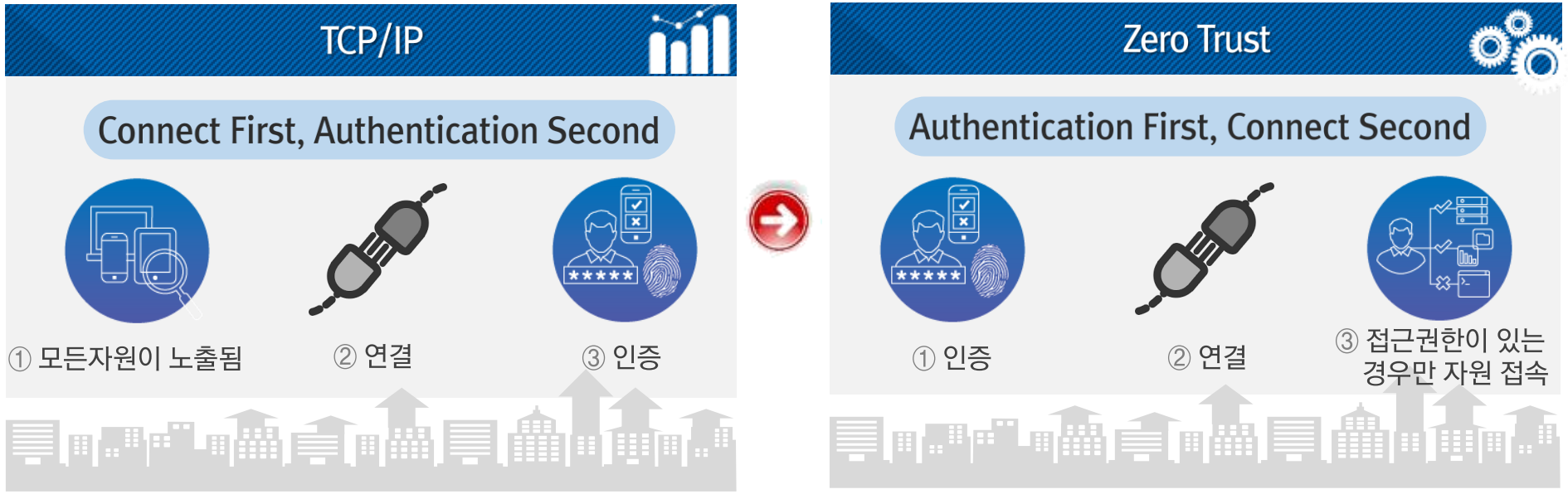
SDP(Software Define Perimeter)

“ 소프트웨어 정의 경계(SDP)는 신원을 기반으로 리소스 액세스를 제어하는 보안 프레임워크로서 Connection Oriented Protocol의 취약점에 착안한 Zero Trust의 대표적인 기술임. ”

기존의 선접속 후인증(인가)의 구조에서 선인증(인가) 후접속의 형태로 접속대상의 DNS 정보나 IP 주소를 알 수 없는 블랙 코어로 동작하며, On-prem, Hybrid, Cloud 환경에서 ZTNA(Zero Trust Network Access)구현을 위한 완벽한 네트워크 보안을 제공

01 보호대상 은닉
02 상호 보안연결
03 Need to know
04 Dynamic Firewall
05 Application Control

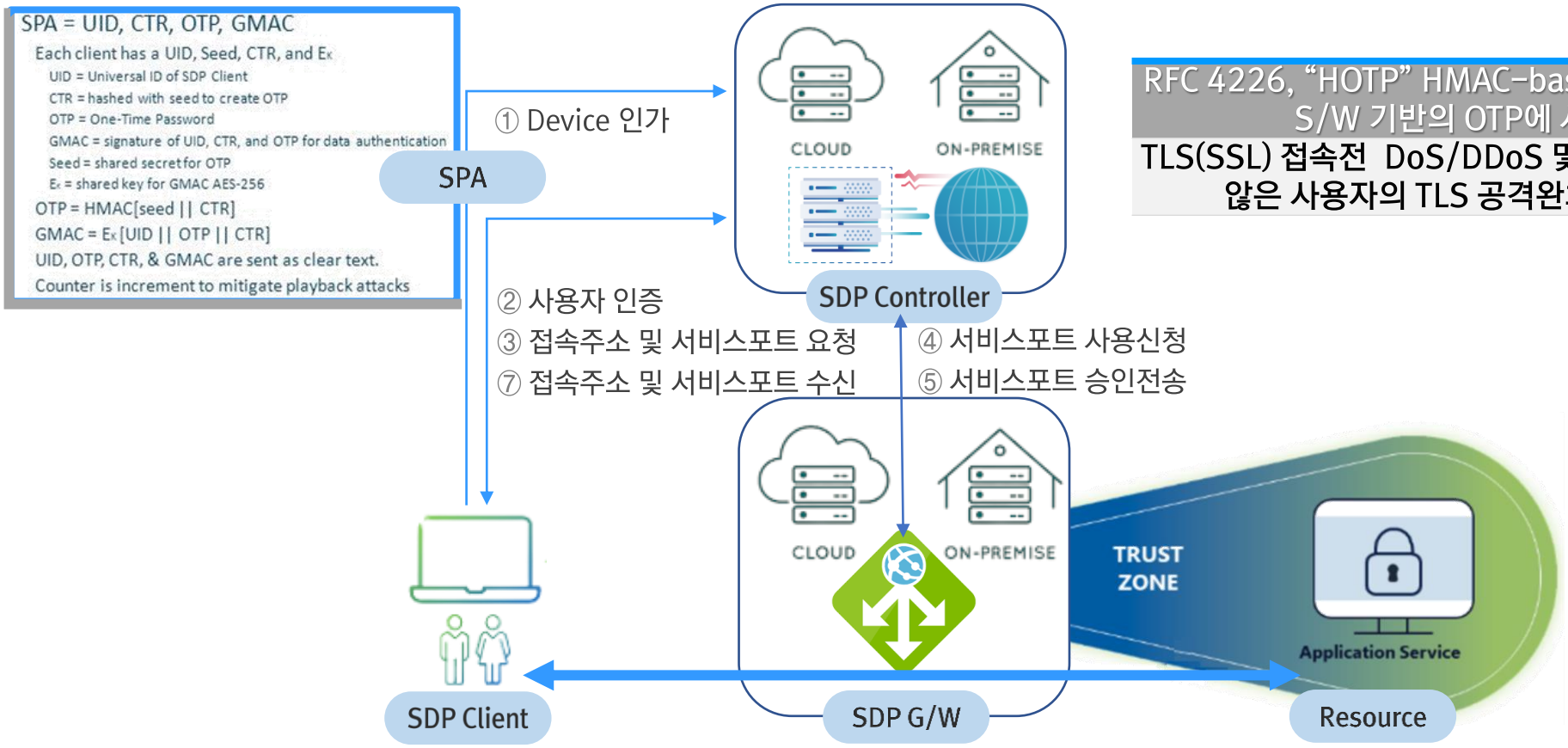
SDP 핵심 구성 요소



SDP/SPA

"Single Packet Authorization(SPA)은 통신을 위해 세션을 맺기 이전에 서로 연결하려는 종단(end to end) 간의 상호 신뢰 세션을 맺기 위한 방법으로 단일패킷을 통한 권한 인가에 사용"

1) IP 노출 2) port 노출 3)측면이동 허용 등에 대한 위험 요소를 제거



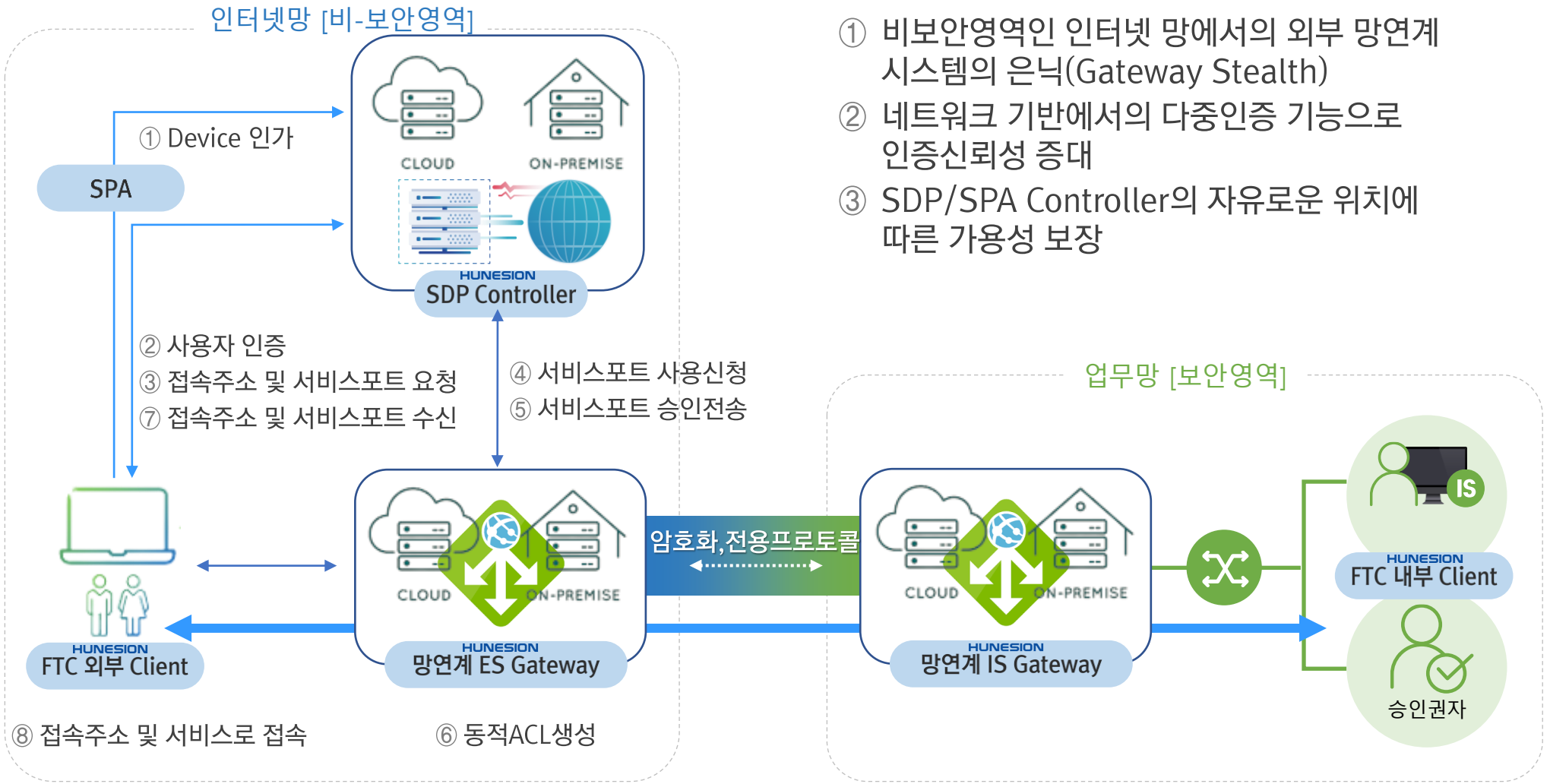
RFC 4226, "HOTP" HMAC-based OTP, H/W S/W 기반의 OTP에 사용

TLS(SSL) 접속전 DoS/DDoS 및 기타 인가되지 않은 사용자의 TLS 공격완화에 사용

SDP/SPA for 망연계(망간자료전송)

"SDP/SPA 기반의 ZTNA를 통해 망연계시스템의 망간자료전송에 보안성을 강화하는 방법으로 사용"

망연계 외부 게이트웨이의 완벽한 Transparency 보장



① 비보안영역인 인터넷 망에서의 외부 망연계 시스템의 은닉(Gateway Stealth)

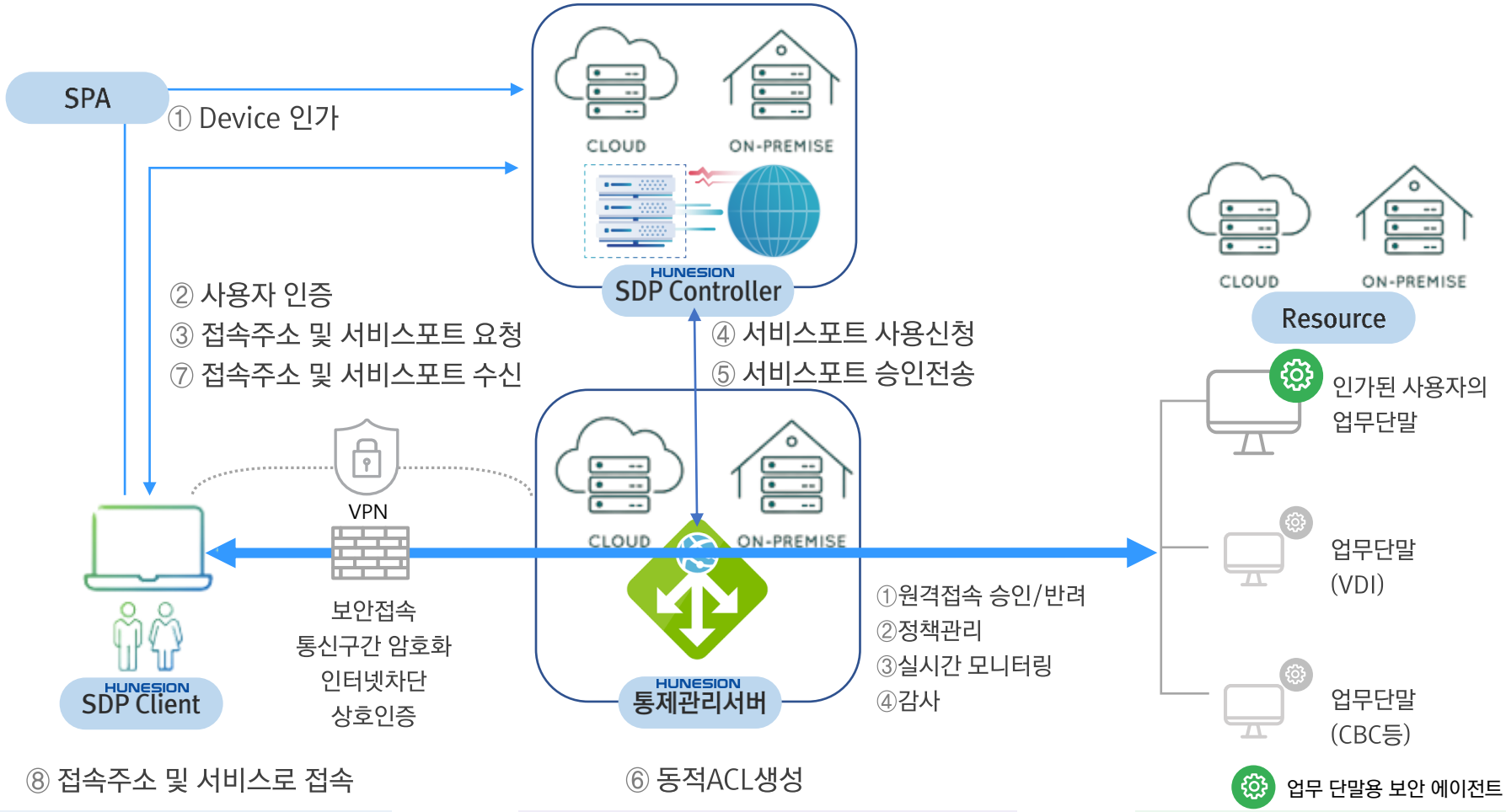
② 네트워크 기반에서의 다중인증 기능으로 인증신뢰성 증대

③ SDP/SPA Controller의 자유로운 위치에 따른 가용성 보장

SDP/SPA for 재택근무

"SDP/SPA 기반의 ZTNA를 통해 상대적으로 보안성이 취약한 Home network를 통한 내부 인프라 접속에 보안성을 강화하는 방법으로 확장 적용"

감염된 홈네트워크 PC의 Encryption 접속 및 공격등에 대한 위험 요소를 제거



원격접속 클라이언트	통제관리 서버	업무단말 보안 에이전트
재택 PC 사전 보안점검	정책설정	실시간 감시 및 자동설정

Zero Trust Security Model Advantage

Adv. 01
인프라 은닉

① 접속대상을 은닉하여 인가 및 인증된 시스템만 접속가능

② 동적정책으로 인한 인바운드 트래픽에 대한 묵시적거절 정책효과 (Default Deny)

③ 외부에 노출된 VPN서버의 은닉에도 효율적

④ 해커의 공격면 감소로 Service, Scanning, DDoS 공격방어 에도 효율적

Adv. 02
강력한 인증

① 사용자, 어플리케이션, 디바이스에 이르는 집중화된 보안인증 아키텍처

② NAC을 통한 접근제어가 불가능한 클라우드 환경에서도 디바이스, 사용자 통제 가능

Adv. 03
확장성

① 선인증 후접속을 통한 모든 Connection 기반 정보보안 시스템 및 서비스에 도입가능

② 기존 인증시스템에 확장 적용하여 Multi factors 인증 시스템으로 보안성 증대

③ On-prem, Cloud 등 환경에 자유로운 보안성 제공

감사합니다.

overdass@hunesion.com

HUNESION