

vIoTSec Products

- Virtual IoT Security Platform 개발 계획서 -

Chunghan.Yi(chunghan.yi@gmail.com)

Doc. Revision: 1.2

Copyright© 2020 Chunghan.Yi, All Rights Reserved.



Contents

- 1. IoT Security Market
- 2. Our Technology **vIoTSec**
- 3. IoT End to End 보안 **EndSec**
- 4. 재택근무 VPN **OfficeSec**
- 5. POS 단말 보안 **POSSec**
- 6. IoT Security Gateway **SBox**
- 7. References

vIoTSec은 다양한 IoT 기기를 안전하게 연결해 주는 Virtual Security Platform 입니다.

1. IoT Security Market(1)



Video Surveillance



24/7 Real-Time Monitoring
In Mobile Hospitals



Smart Cold Chain



Smart Gas Metering



LoRaWAN-based Pig Farming



Office Temperature Monitoring
(LoRa)



Smart Bus Tracking(LoRa)



Remote Monitoring for PLCs

1. IoT Security Market(2) - 시장 규모



출처: <http://www.epnc.co.kr/news/articleView.html?idxno=79868>



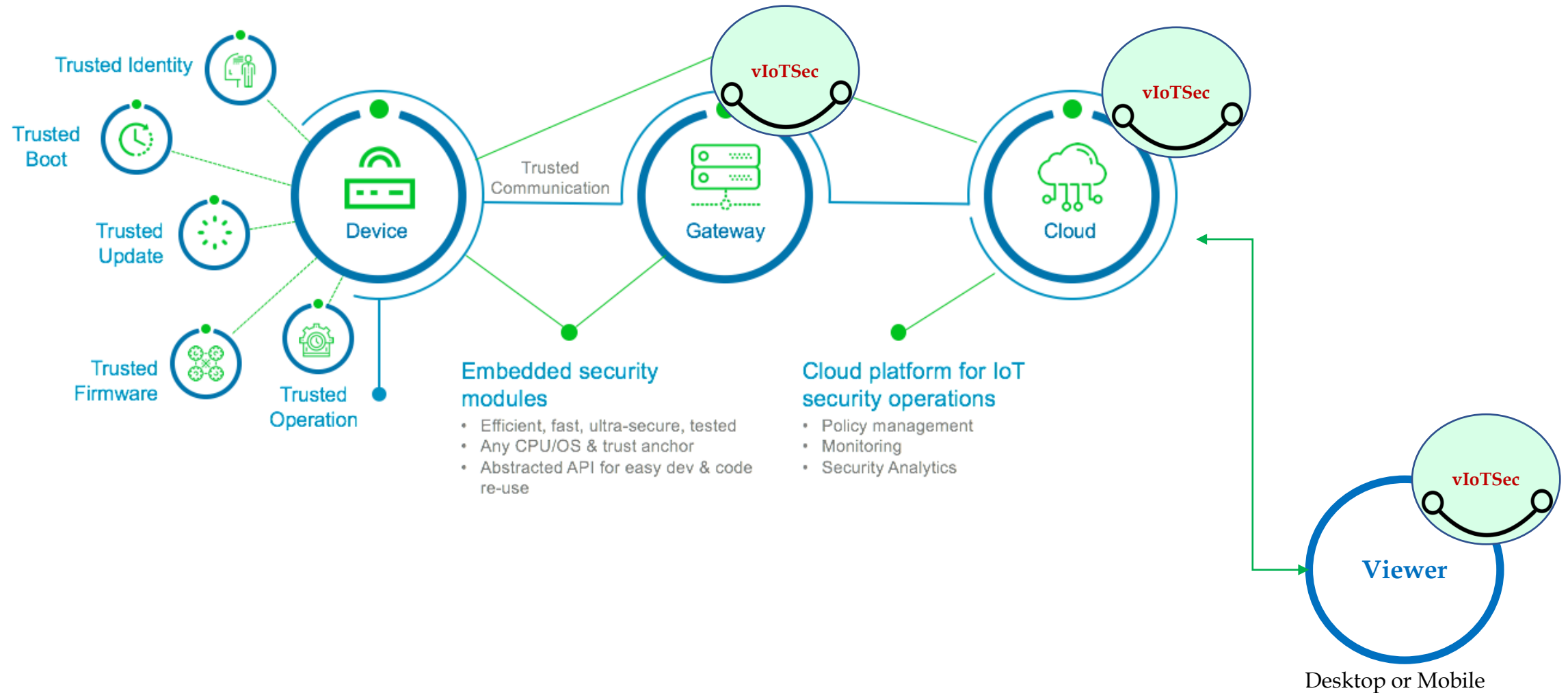
주: 1) 세계 시장은 2010~2019년까지, 한국 시장은 2013년~2020년까지 수치임

2) 분야별 매출액 추이에서 2016년은 잠정치이며, 2017년은 전망치임

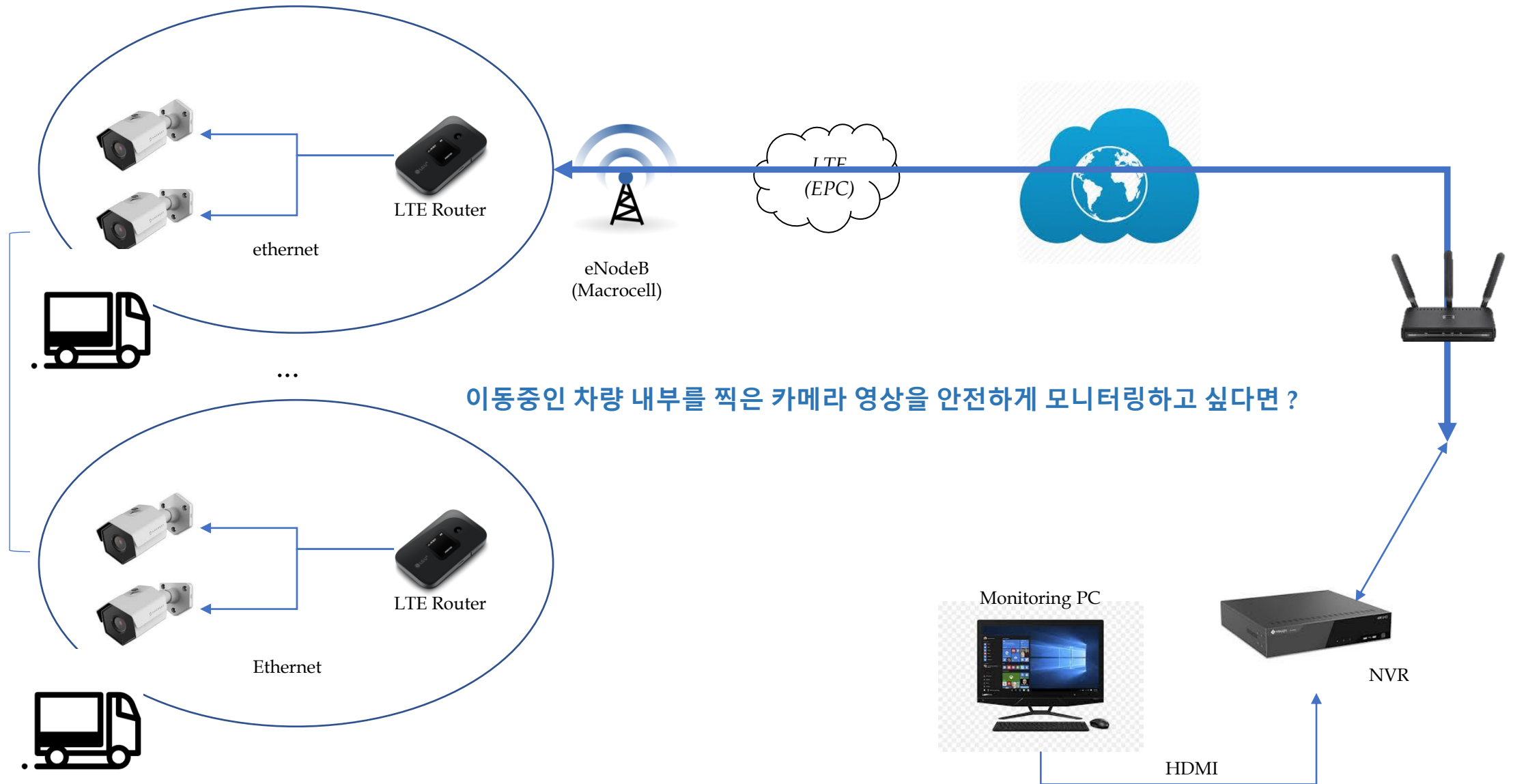
자료: Statista 2018, Machina Research(2014), 국회입법조사처(2017)을 참조하여 재구성

국내외 IoT 시장 전망 및 분야별 매출액 추이 / 자료제공=한국무역협회

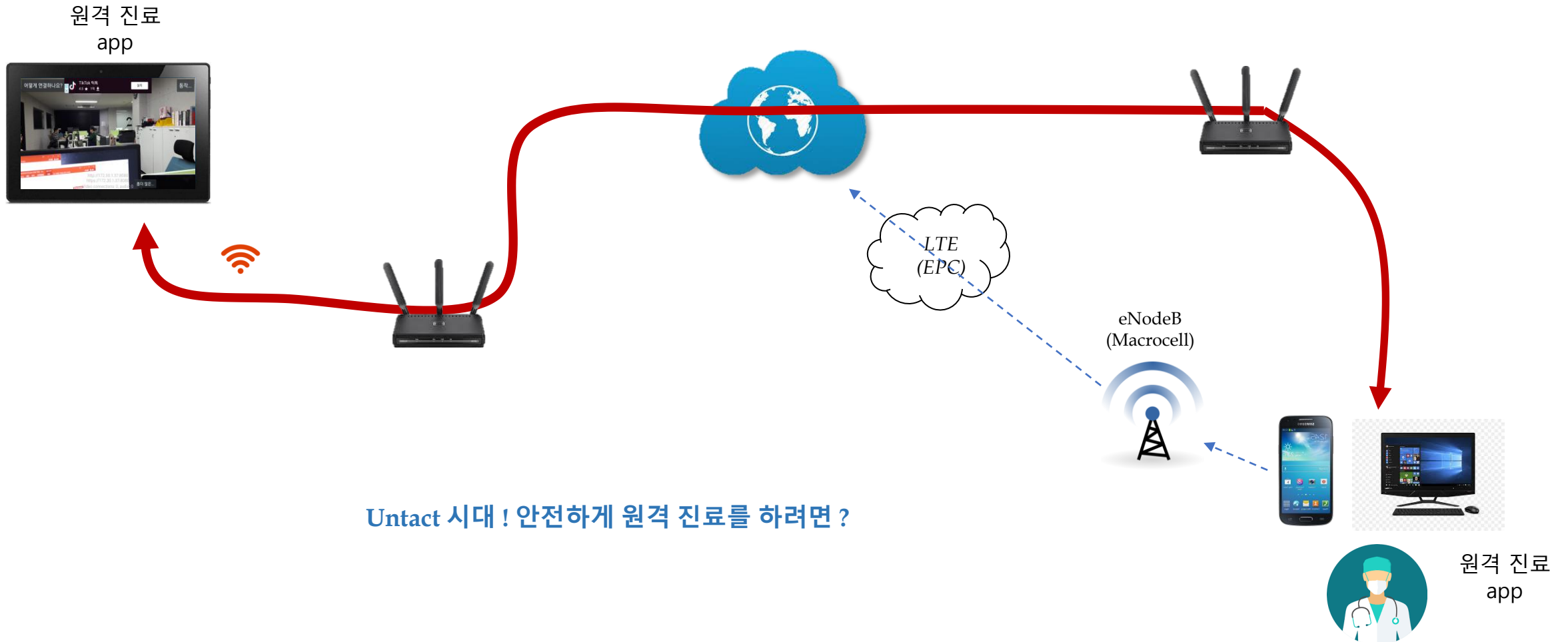
1. IoT Security Market(3) – IoT Security Area



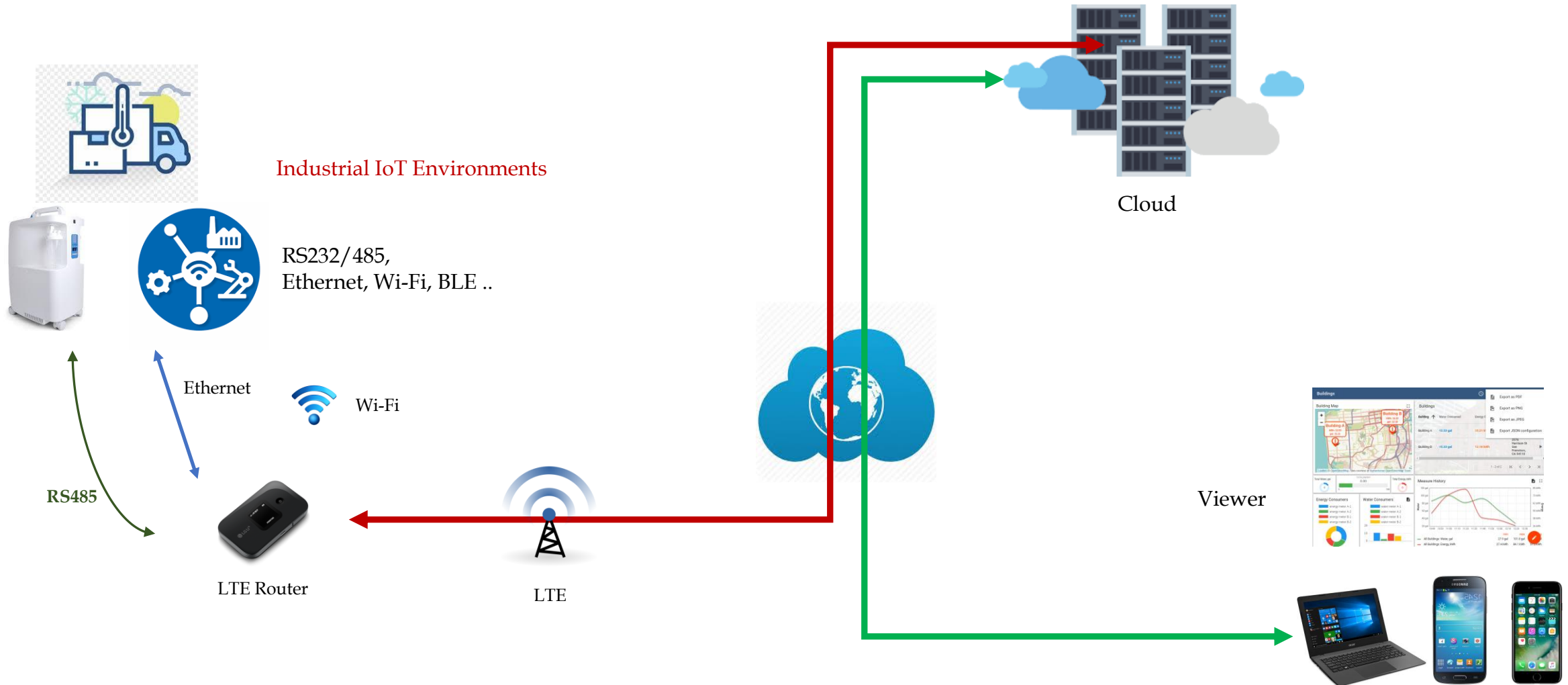
1. IoT Security Market(4) - Video Surveillance



1. IoT Security Market(5) - 원격 진료

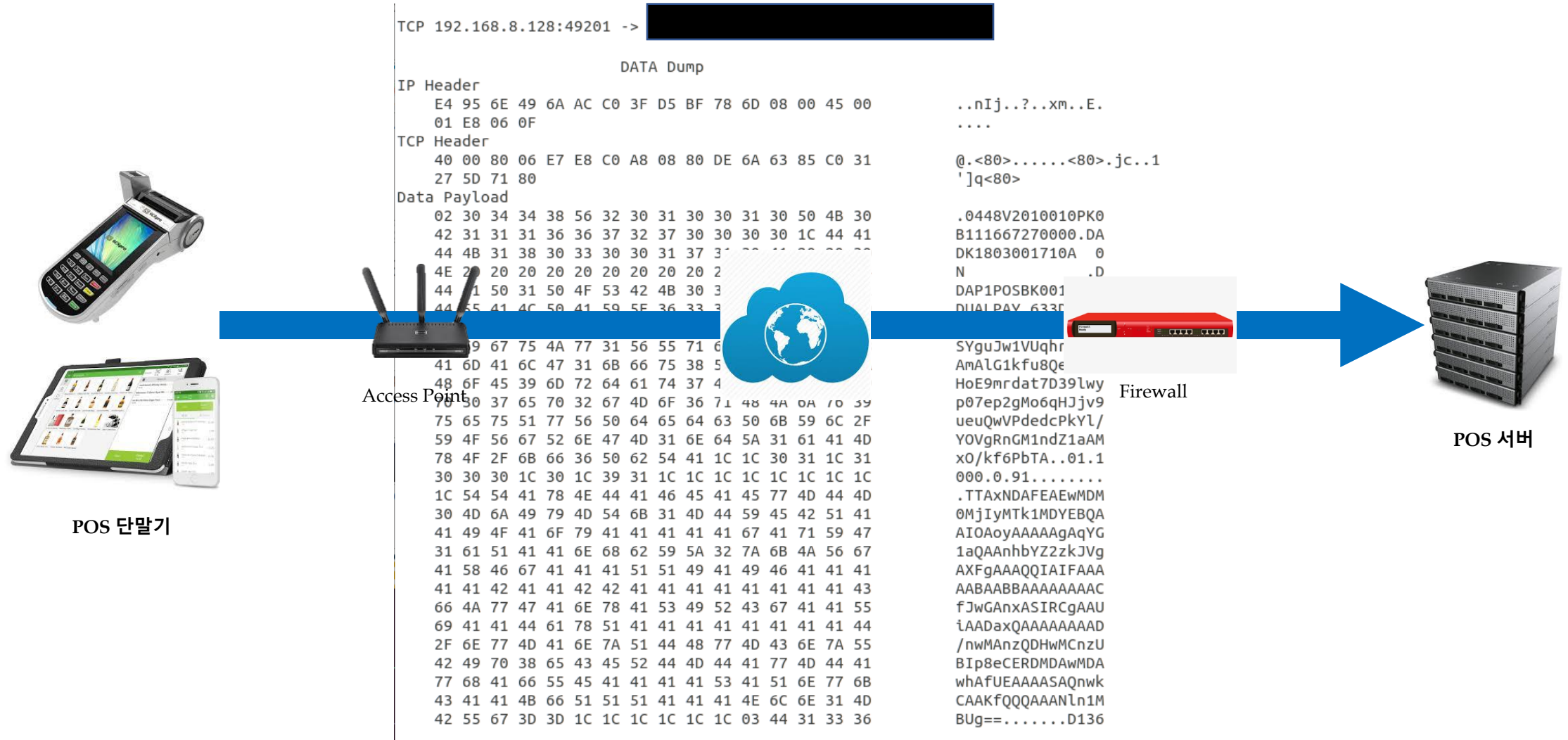


1. IoT Security Market(6) – 24/7 Real-Time Monitoring



IIoT 기기를 안전하게 감시 & 제어하려면 ?

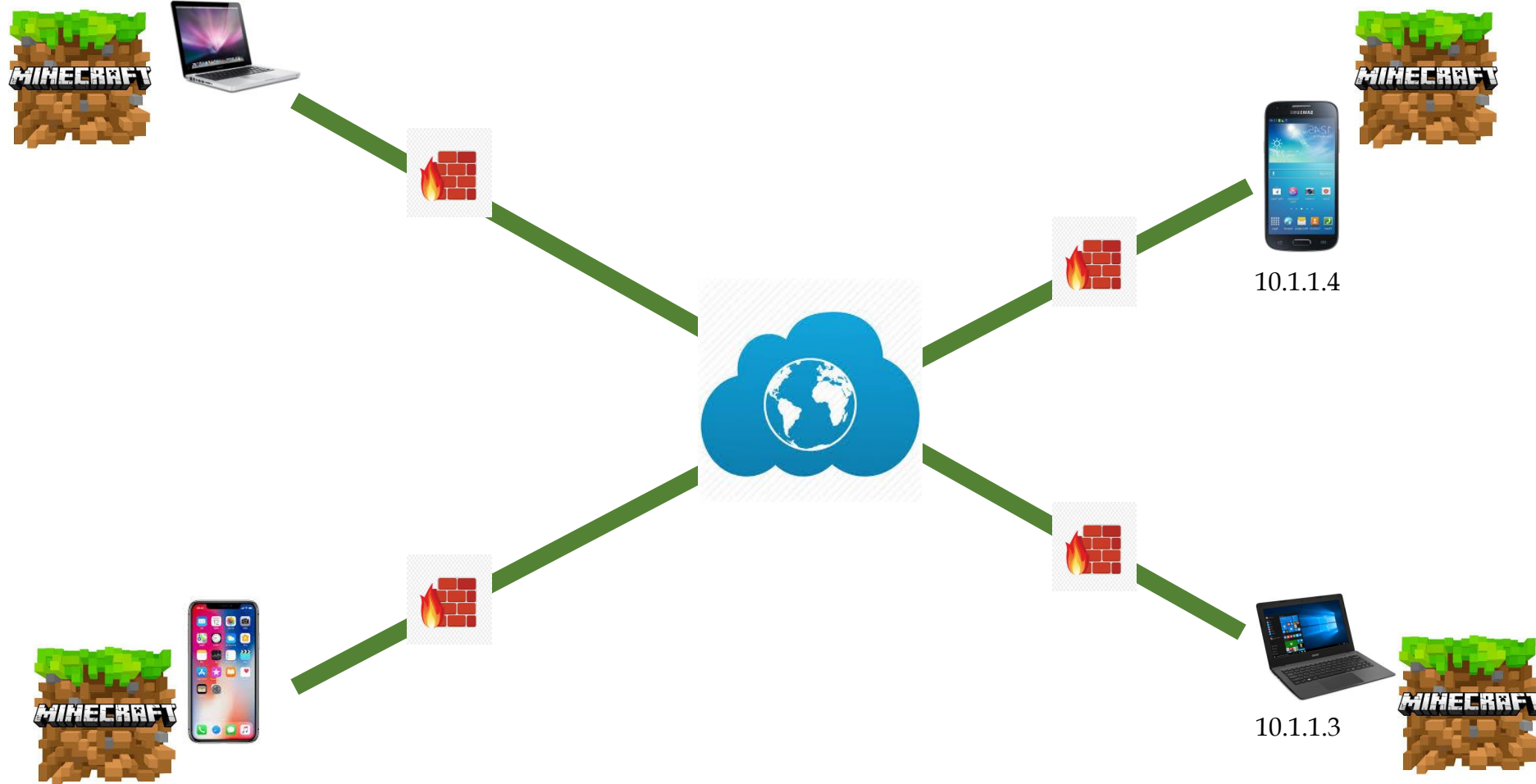
1. IoT Security Market(7) - POS 결제 데이터



POS 단말과 VAN사 서버 간의 결제 패킷을 안전하게 보호하고 싶다면 ?

1. IoT Security Market(8) – Online Gaming

방화벽/공유기 설정 변경 없이 P2P Game을 즐기고 싶다면 ?

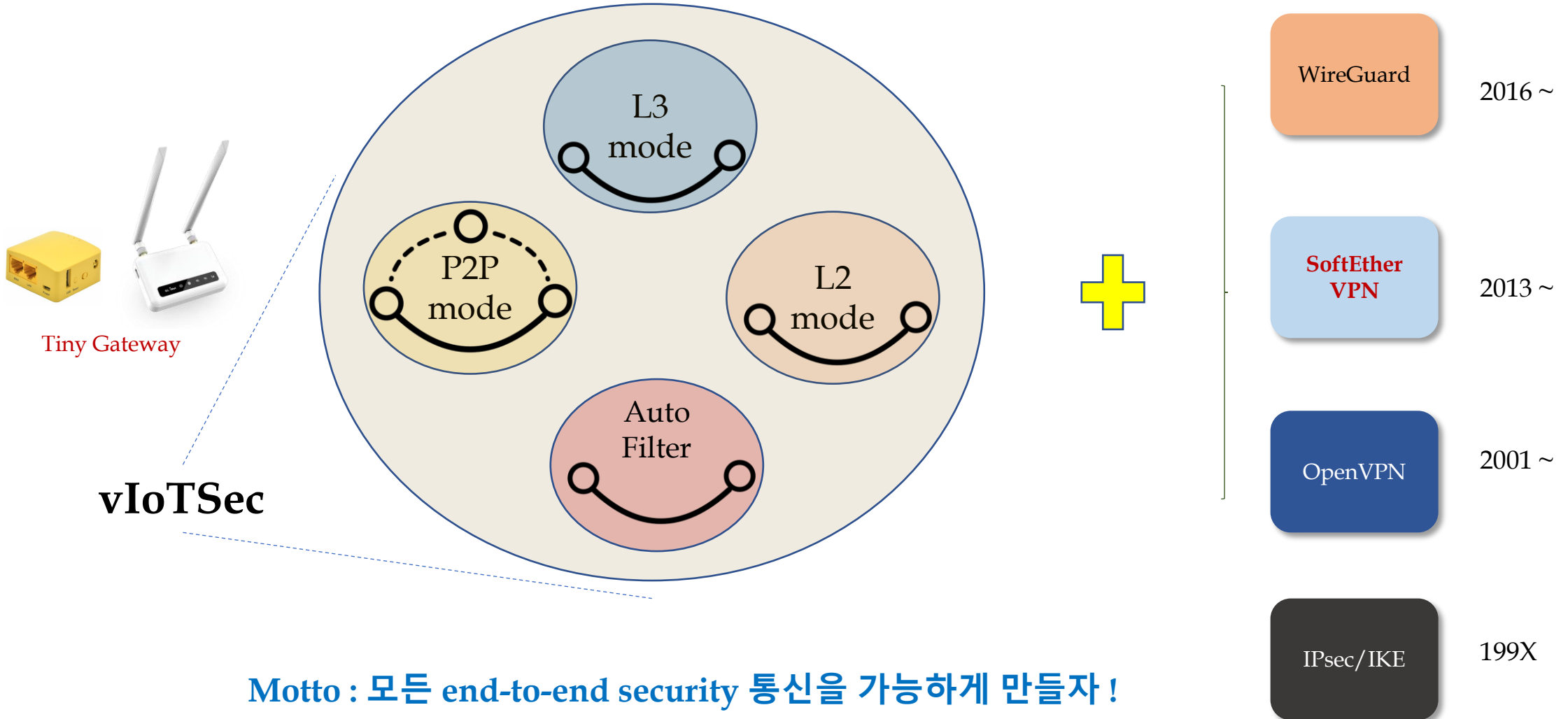


2. Our Technology vIoTSec(1)



vIoTSec provides you a secure network infrastructure.

2. Our Technology vIoTSec(2)



2. Our Technology vIoTSec(3)



Target1: Embedded Products(상용제품)

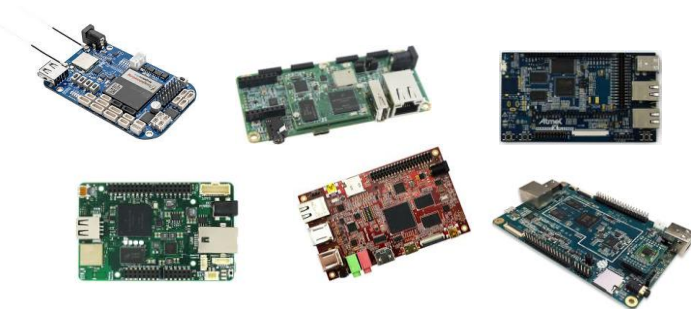


Tiny Security Gateway w/ vIoTSec Engine



Target2: Android/iOS/Windows/macOS

vIoTSec Applications



Target 3: Linux Embedded Boards

vIoTSec Engine(S/W)

2. Our Technology vIoTSec(4)

- 1. IoT End to End 보안 **EndSec**

- *IP Camera/CCTV 등의 영상을 안전하게 전송하고 싶다면 ...*
- *안전한 원격 진료를 제공받고 싶다면...*
- *산업 현장의 IoT 기기(RS485, Wi-Fi, Ethernet, BLE)를 안전하게 원격관리하고 싶다면 ...*
- *방화벽/공유기 설정 변경 없이 Game을 하거나, 회사 서버에 접속하고 싶다면 ...*

- 2. 재택근무 VPN **OfficeSec**

- *Untact 시대- 집에 있지만 마치 사무실망에 연결되어 있는 것처럼 하고 싶다면 ...*
- *L2 mode, SSL VPN, Very Fast & Stable*

- 3. POS 단말 보안 **POSSec**

- *POS 결제 단말을 해킹의 위협으로 부터 보호하고 싶다면 ...*
- *해킹 프로텍터, 저렴한 가격, 간편한 설치*

3. IoT End to End 보안 EndSec (Powered by WireGuard)



3. EndSec(1) – End to End Security(1)



안전한 데이터 전달은 기본 중의 기본(Encryption/Decryption, Mutual Authentication)



임의의 디바이스를 쉽고 안전하게 연결할 수 있어야 함(Easy Connectivity)



실시간 성능을 보장하기 위해 빠른 전송 속도(암호 통신)를 보장해야 함(High Speed)



이동 중에도 데이터(예: 영상 data) 전송에 끊김이 없어야 함(Mobility)

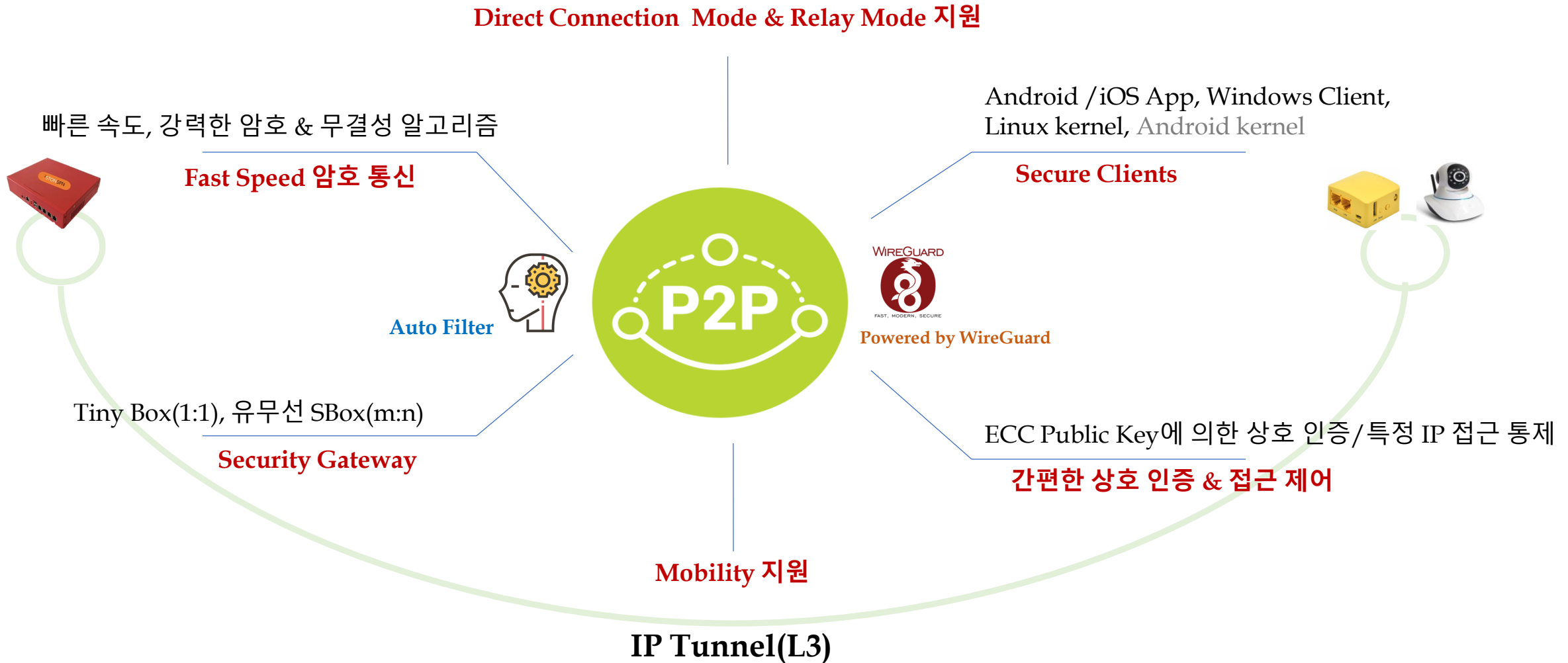


데이터 전송이 필요 없는 경우, 어떠한 패킷도 내 보내지 말아야 함(Stealth Mode)

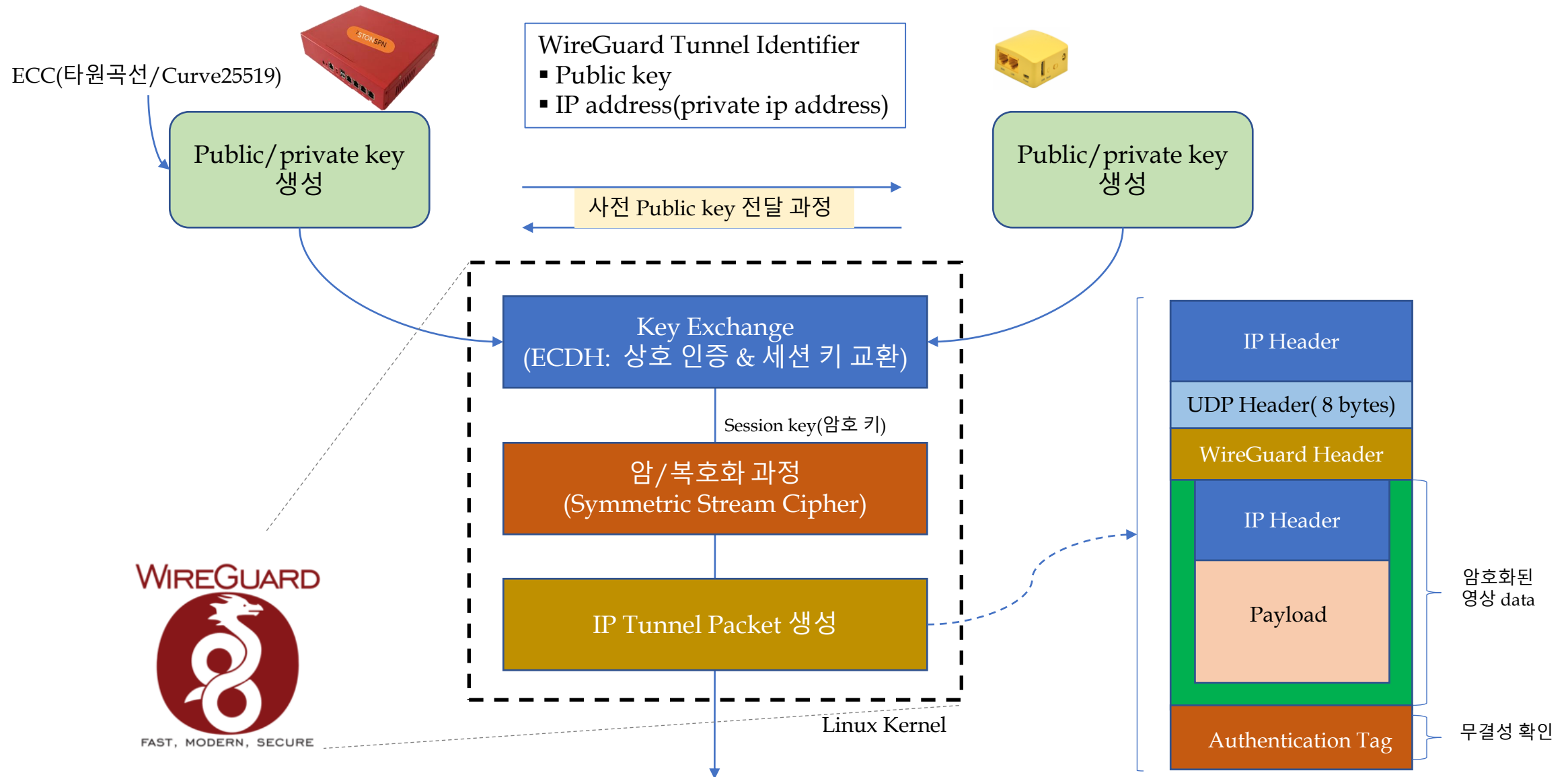


흐르는 트래픽을 분석하여 End node를 안전하게 보호할 수 있어야 함(Auto Filter)

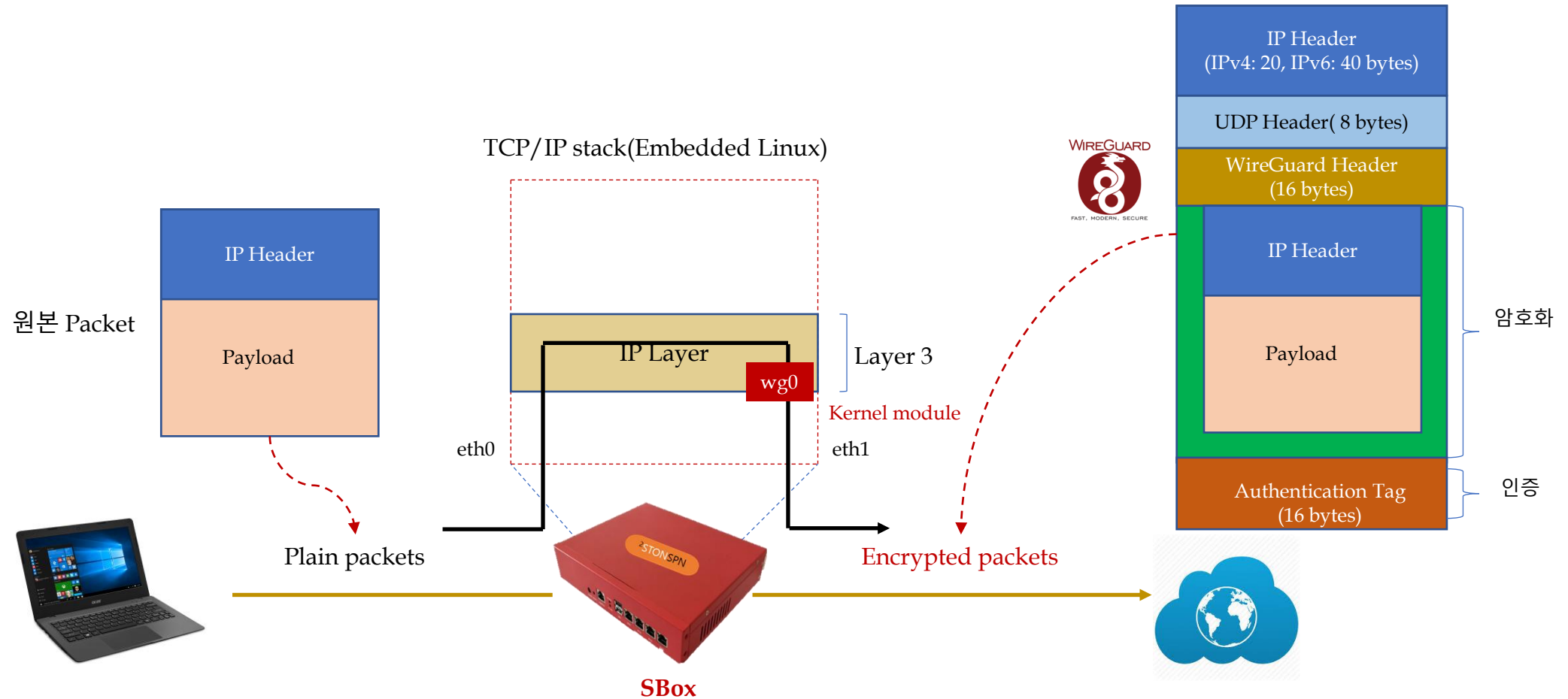
3. EndSec(1) – End to End Security(2)



3. EndSec(2) – WireGuard Tunnel(1)



3. EndSec(2) – WireGuard Tunnel(2)

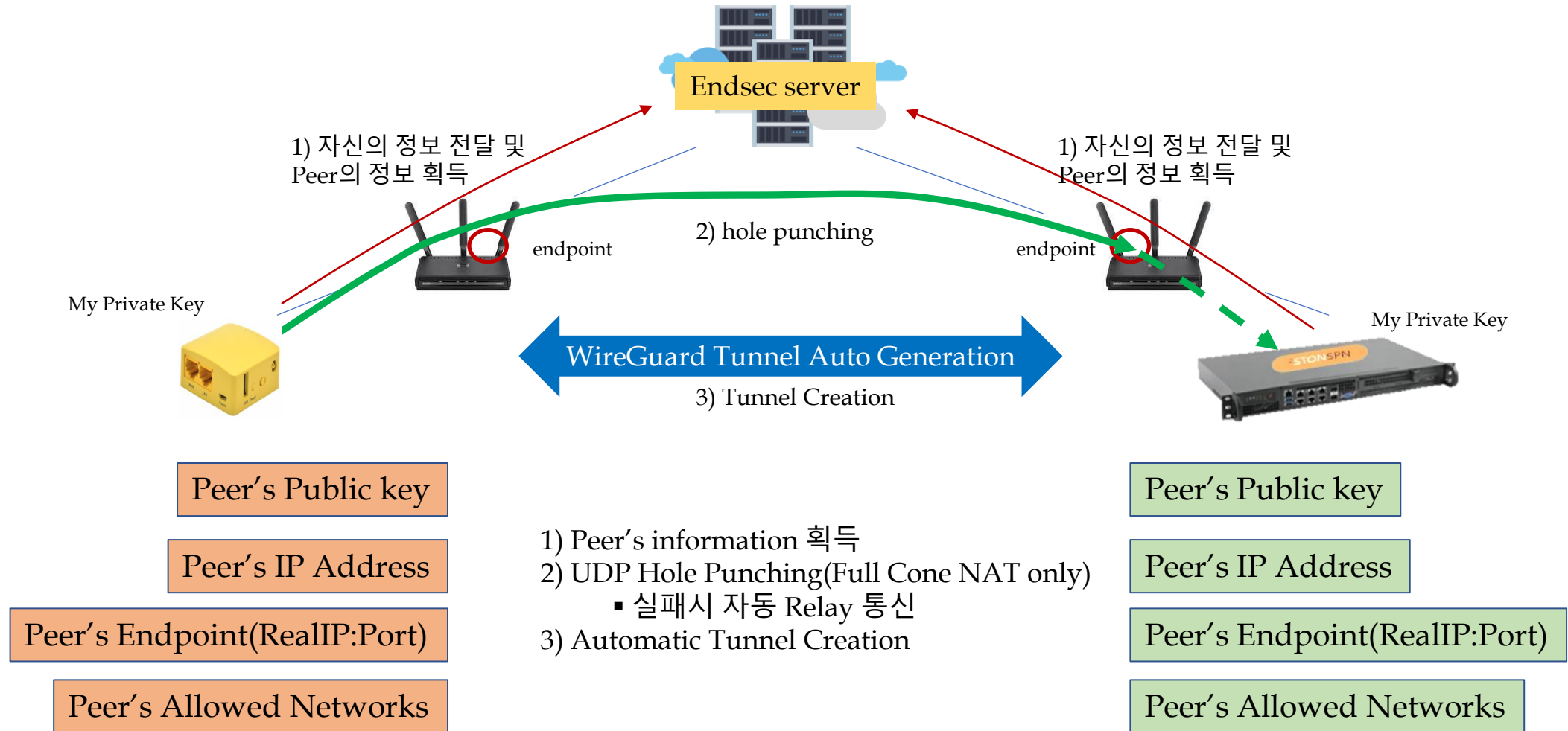


3. EndSec(2) – WireGuard Tunnel(3)

보안 알고리즘	상세 내용
Key 교환 방식 및 상호 인증	NoiseIK handshake 방식(Noise IKpsk2) <ul style="list-style-type: none">▪ ECDH(Diffie-Hellman) 기반▪ Curve25519 Public key(32 byte)를 교환 후, 이를 통해 안전하게 shared secret 생성<ul style="list-style-type: none">▪ Static/Ephemeral public key(2개) 이용▪ Key 교환 시 아래 기능 보장<ul style="list-style-type: none">▪ 키 침해 신분 위장 방지 기능, replay attack 방지 기능▪ Perfect forward secrecy 보장, Identity 감춤 기능 제공, DoS 공격 완화 기능(Cookie) Hash 알고리즘 <ul style="list-style-type: none">▪ BLAKE2s – fast secure hashing 알고리즘▪ SHA series 보다 빠름. 즉 MD5 수준임.
암호 알고리즘	ChaCha20 – 256 bit stream cipher(20 round cipher Salsa20 기반) <ul style="list-style-type: none">▪ Stream cipher는 일반적인 block cipher(예: AES-256-CBC)에 비해 속도가 빠름▪ key(32 bytes)는 대칭키를 사용(즉, 암호화 용 키와 복호화 용 키 동일)▪ Video/Audio 등 stream 암호화에 적합
무결성(Integrity) 검사 알고리즘	Poly1305 - message authentication code 알고리즘(16 byte output 생성)

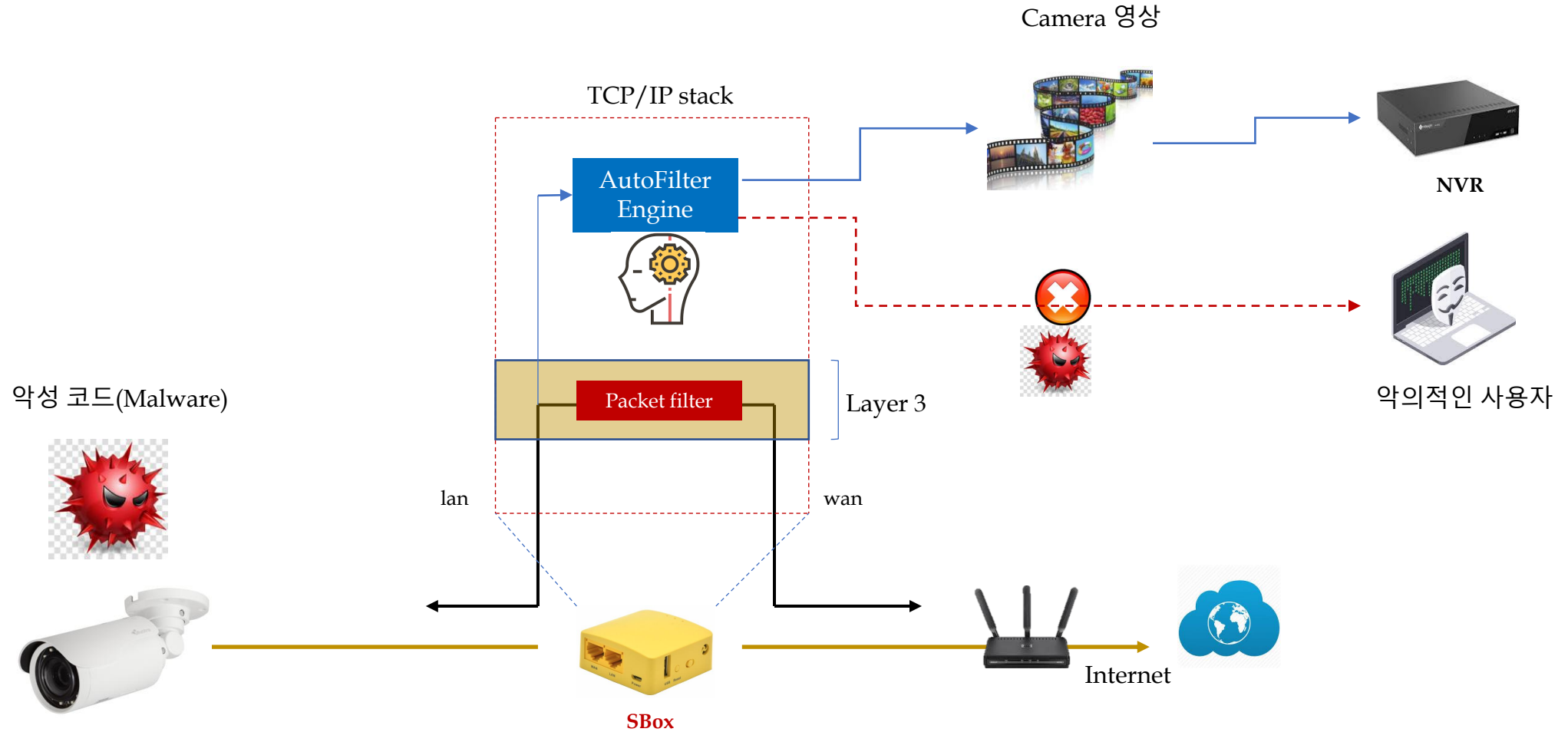
(*) 최대한 안전하면서도 빠른 알고리즘을 선택하므로써 전체적으로 network 성능을 끌어 올리도록 함.

3. EndSec(3) – Auto Connection



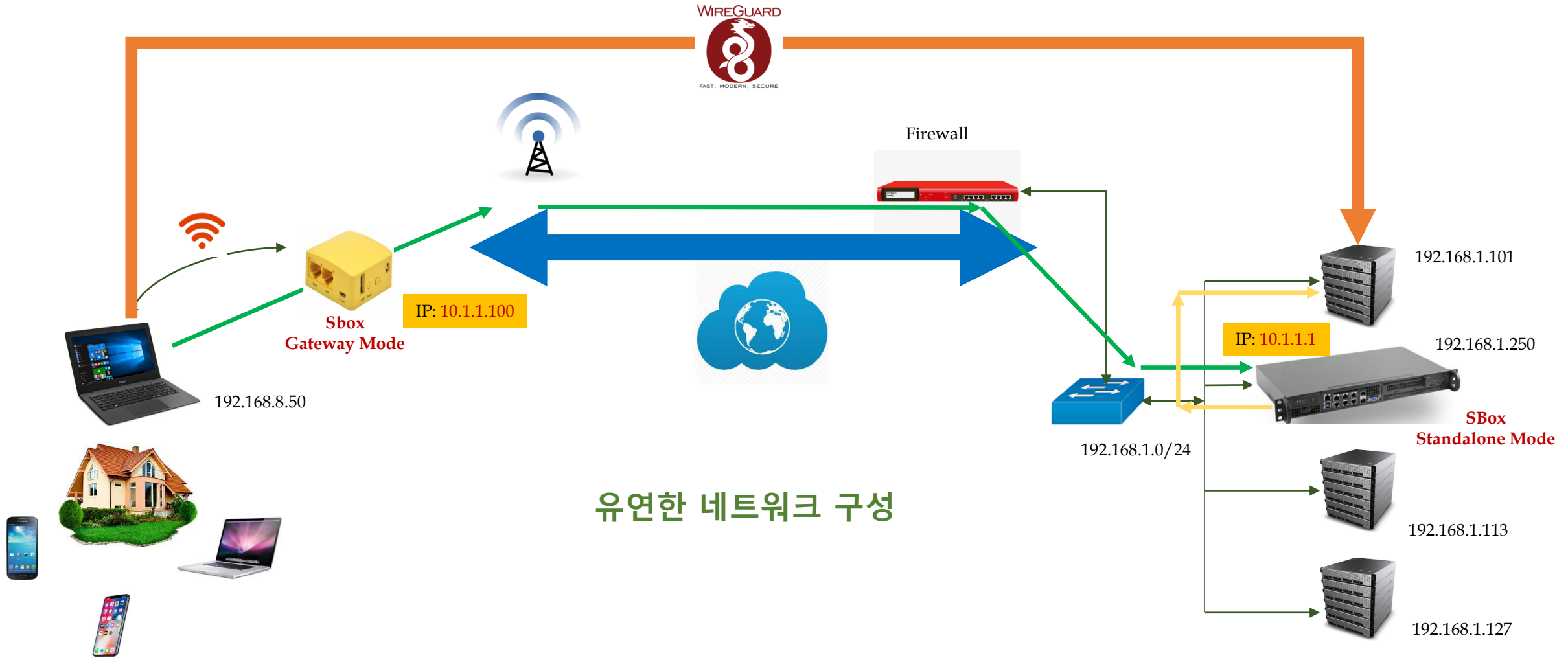
EndSec Auto Connection 기능을 사용하면 EndSec 기기간 연결이 한층 수월해 질 수 있습니다.

3. EndSec(4) - Auto Filter



Auto Filter는 허가된 Traffic(자동 감지)을 제외한 모든 패킷을 자동으로 차단하여 잠재적인 보안 위협을 막아 줍니다.

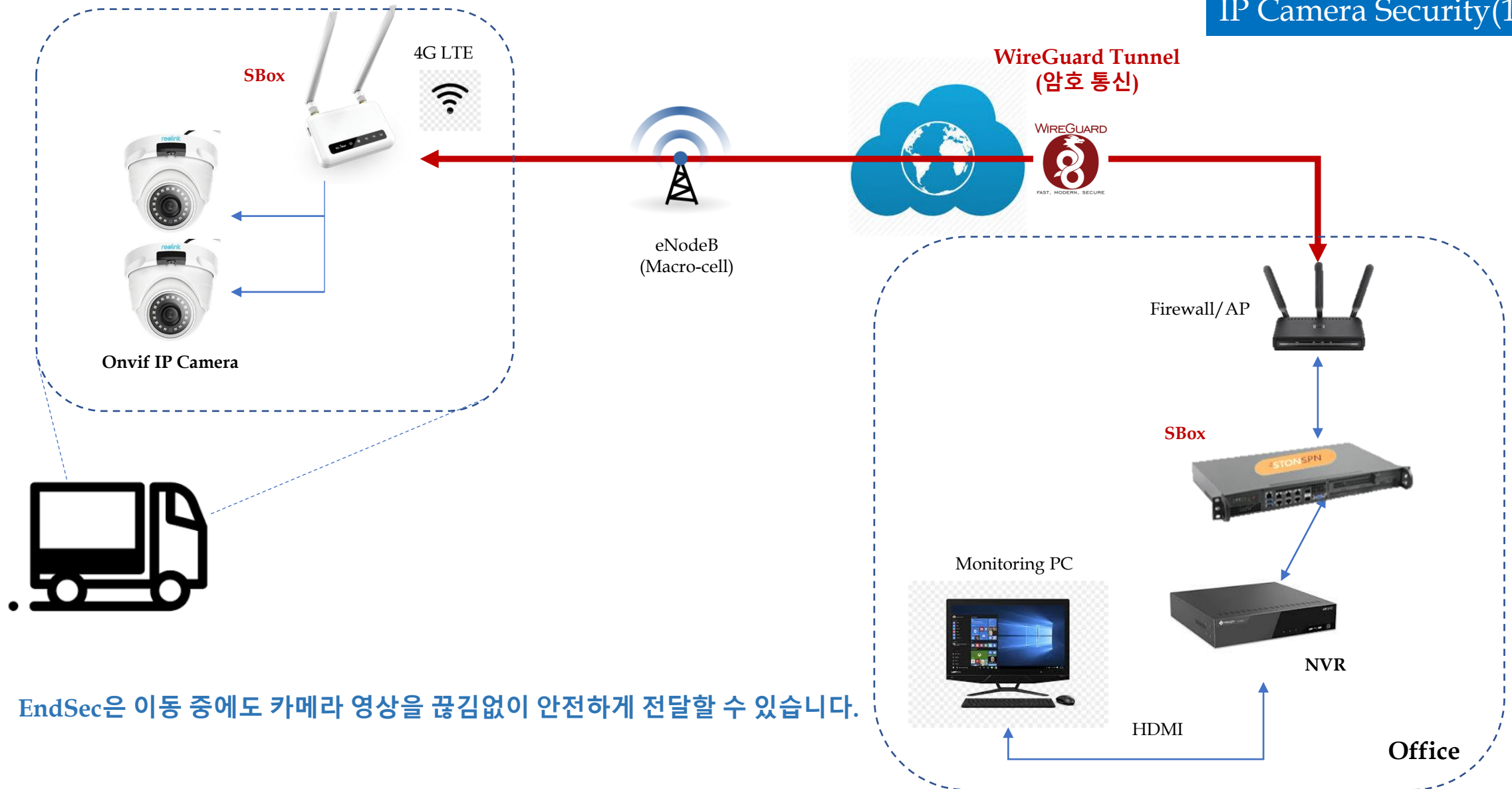
3. EndSec(5) – Gateway Mode vs Standalone Mode



EndSec Standalone Mode를 이용하시면 기존 네트워크 구성을 전혀 변경하실 필요가 없습니다.

3. EndSec(6) – Use Cases(1-1)

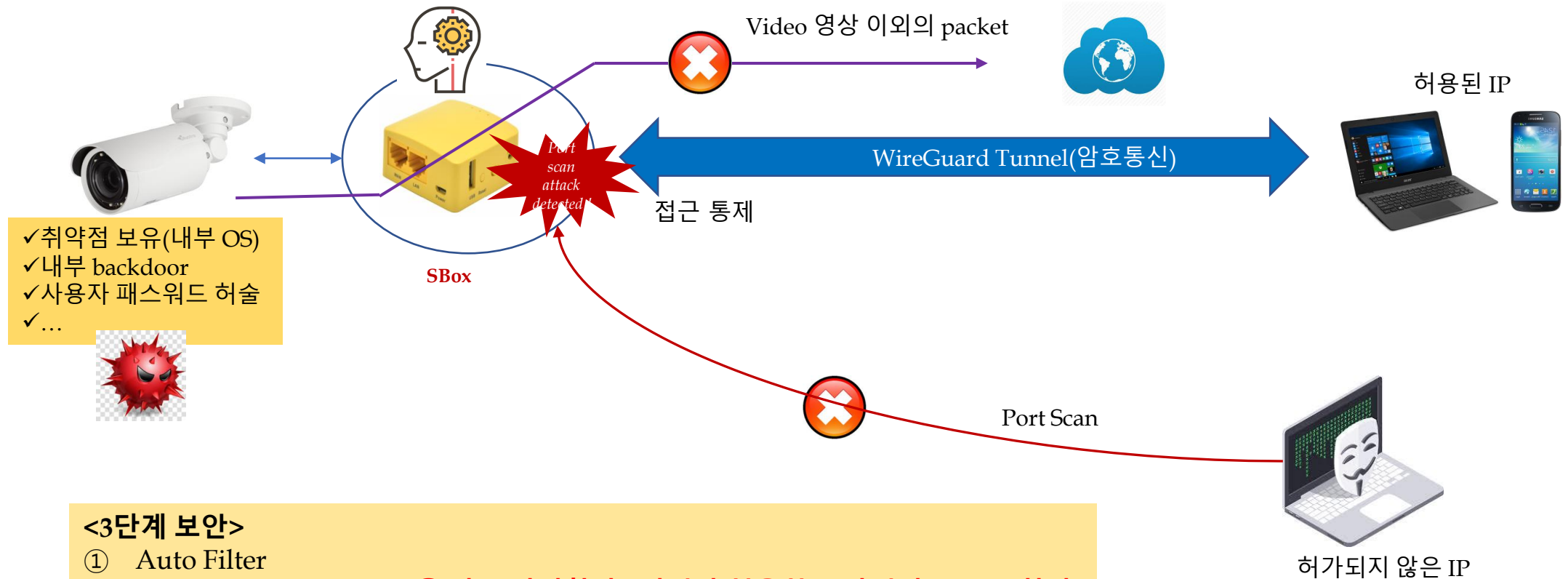
IP Camera Security(1)



3. EndSec(6) - Use Cases(1-2)

IP Camera Security(2)

허용된 IP 및 Tunnel 설정을 통과해야만 IP Camera에 접근할 수 있습니다.

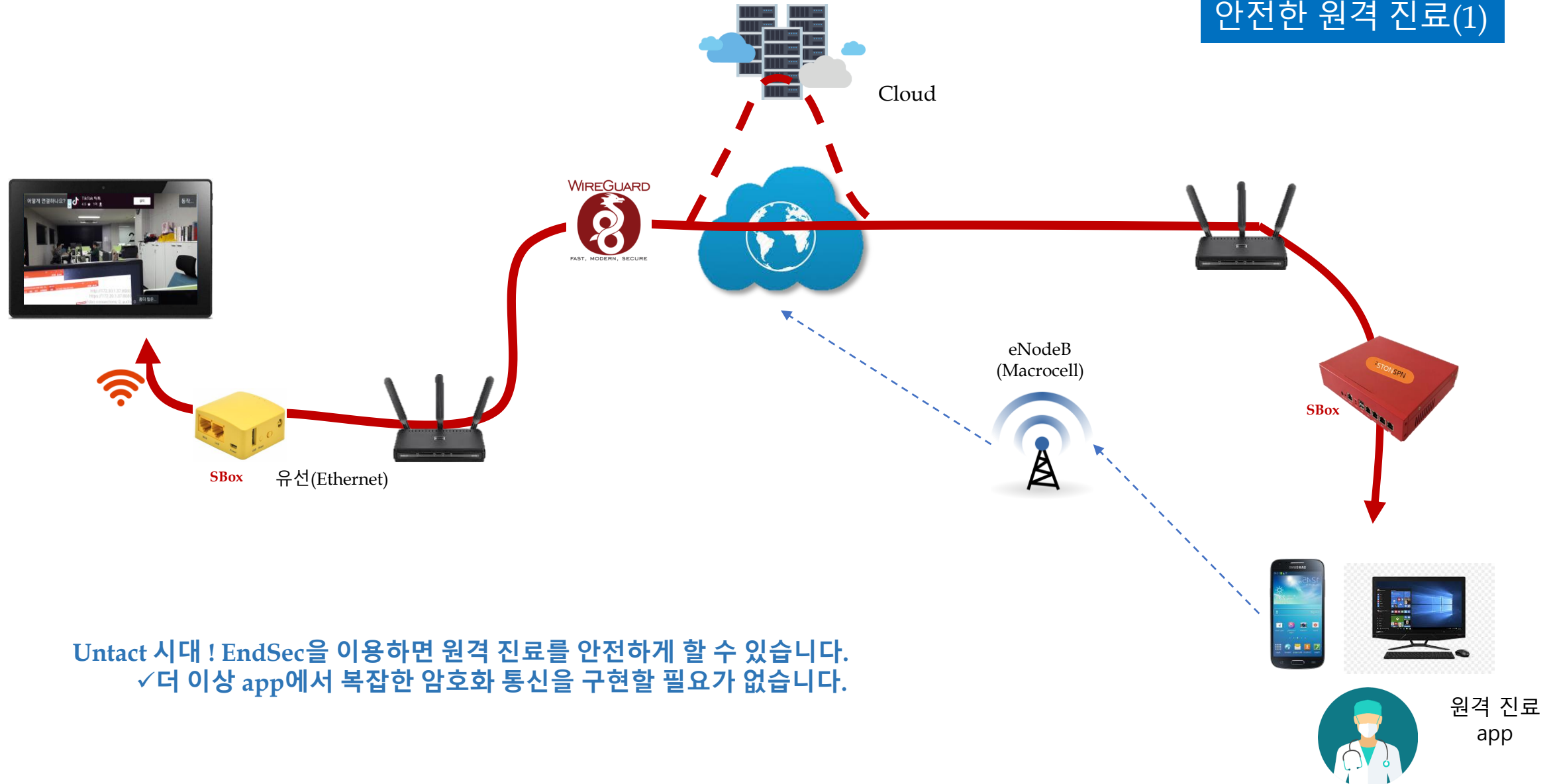


<3단계 보안>

- ① Auto Filter
 - ✓ IP camera packet을 자동 감지한 후, 이것만 허용하고 나머지는 모두 차단
- ② 접근 통제
 - ✓ 허용된 IP만 접근 가능
- ③ 암호호 통제 - WireGuard Tunnel 확립이 가능한 경우만 허용
 - ✓ 두가지 조건을 모두 만족해야만 IP Camera에 접근할 수 있음.

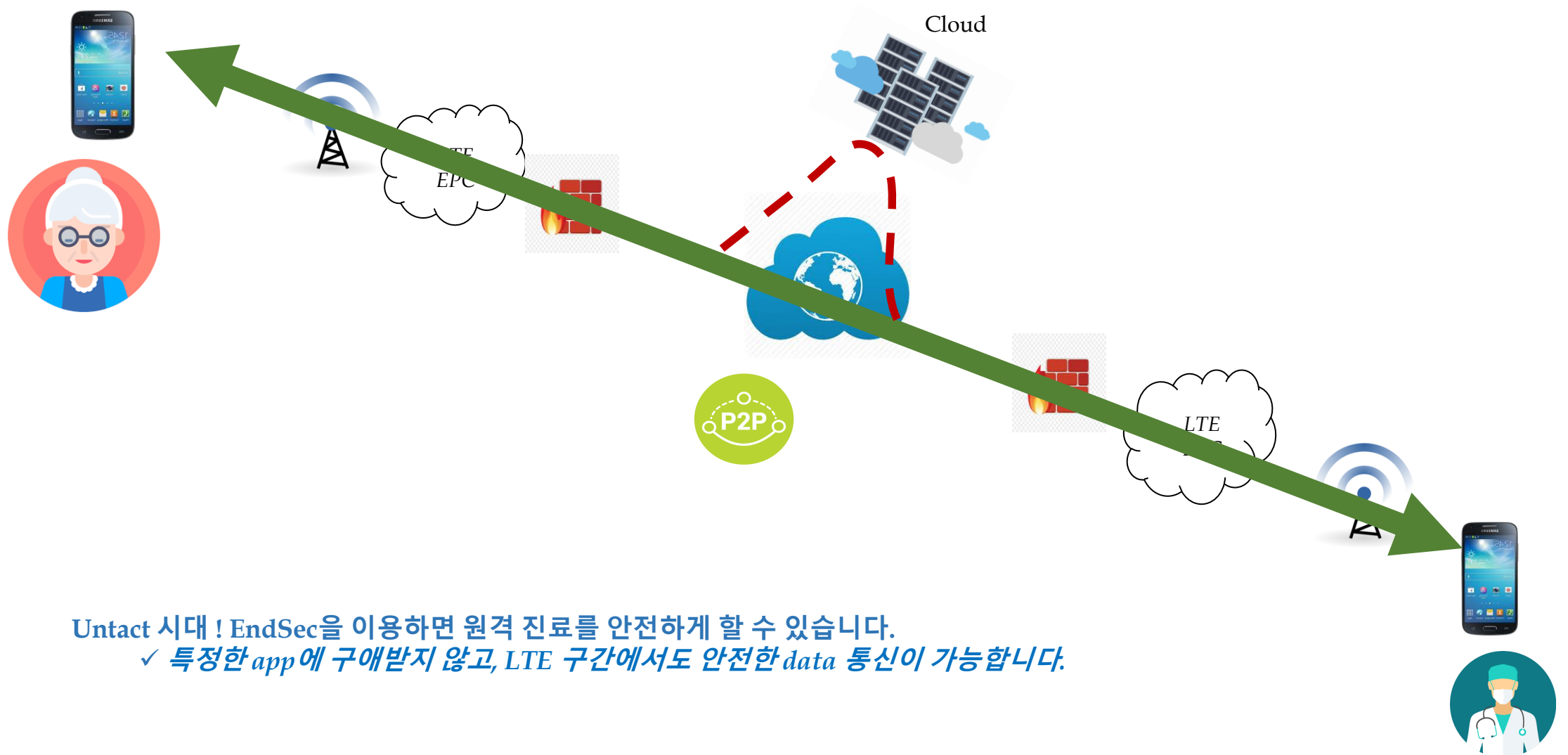
3. EndSec(6) - Use Cases(2-1)

안전한 원격 진료(1)



3. EndSec(6) – Use Cases(2-2)

안전한 원격 진료(2)

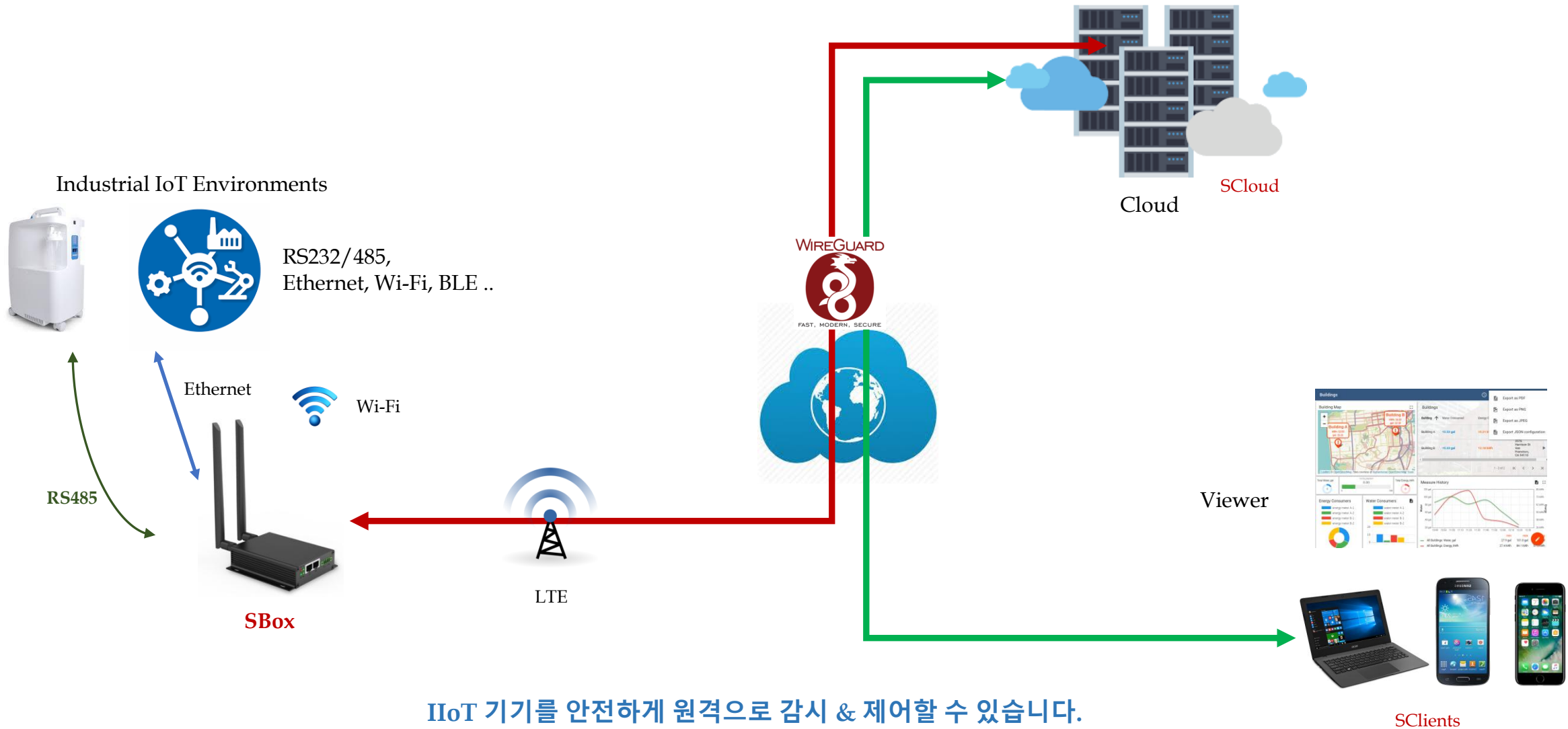


Untact 시대 ! EndSec을 이용하면 원격 진료를 안전하게 할 수 있습니다.

✓ 특정한 app에 구매받지 않고, LTE 구간에서도 안전한 data 통신이 가능합니다.

3. EndSec(6) – Use Cases(3)

Industrial IoT 보안



3. EndSec(6) – Use Cases(4)

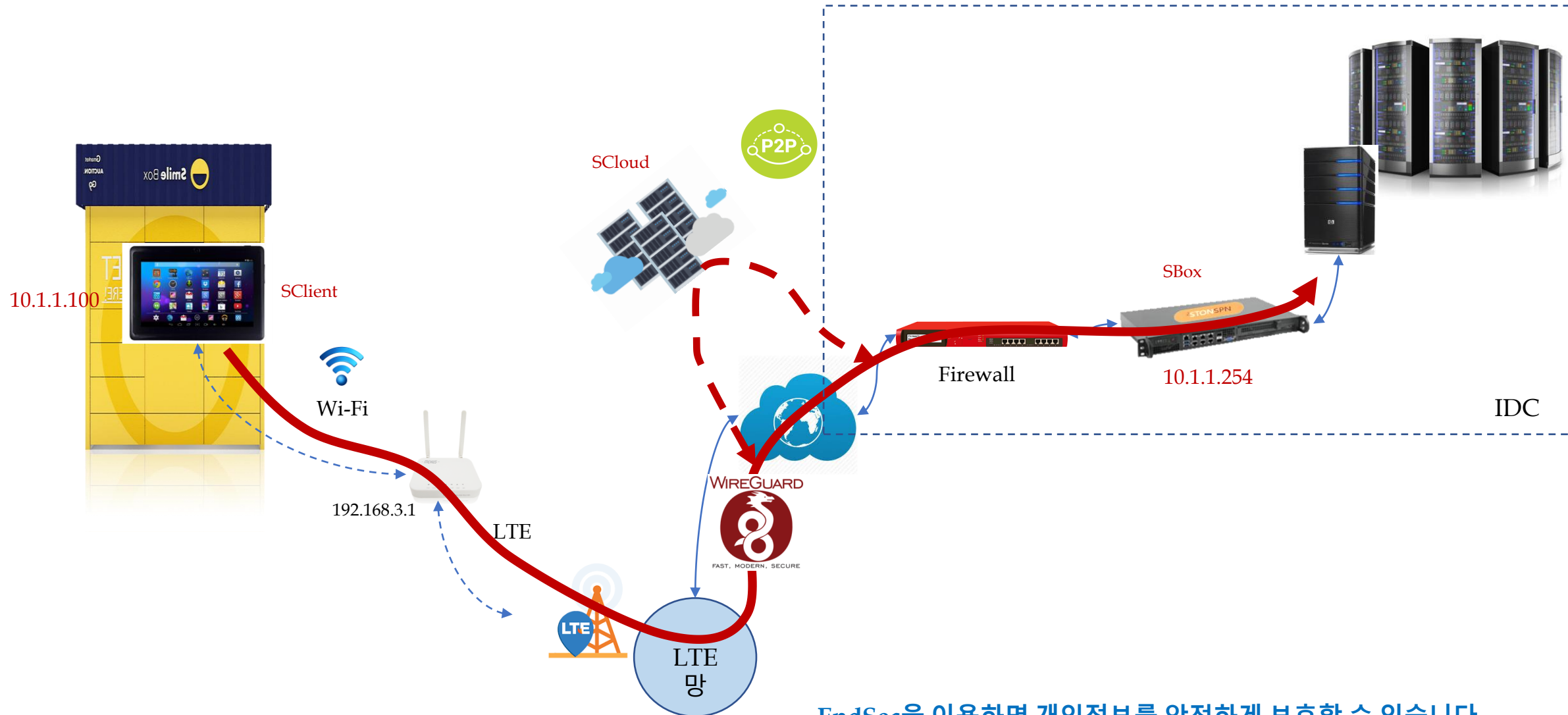
POS 결제 보안



EndSec을 이용하면 POS 단말과 VAN사 서버 간의 결제 패킷을 통째로 암호화할 수 있습니다.

3. EndSec(6) – Use Cases(5)

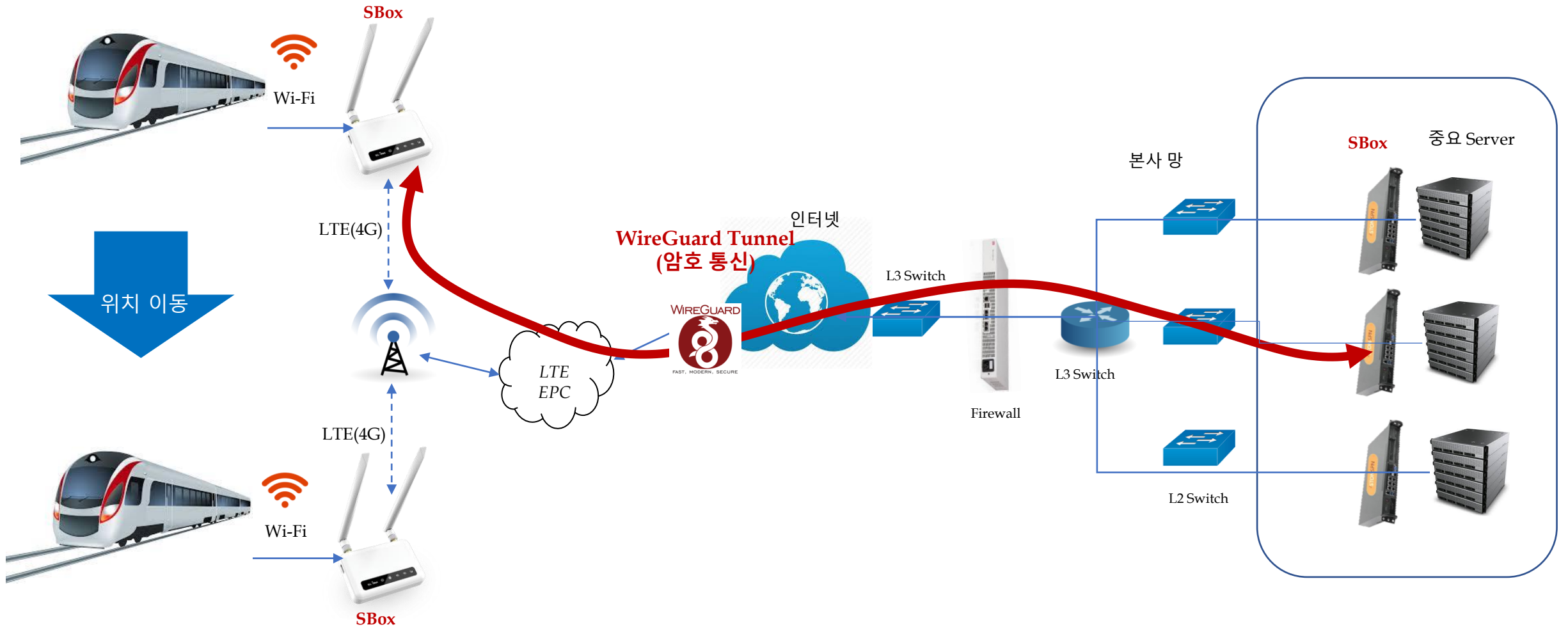
무인택배함 보안



EndSec을 이용하면 개인정보를 안전하게 보호할 수 있습니다.

3. EndSec(6) - Use Cases(6)

LTE 이동 데이터 보안

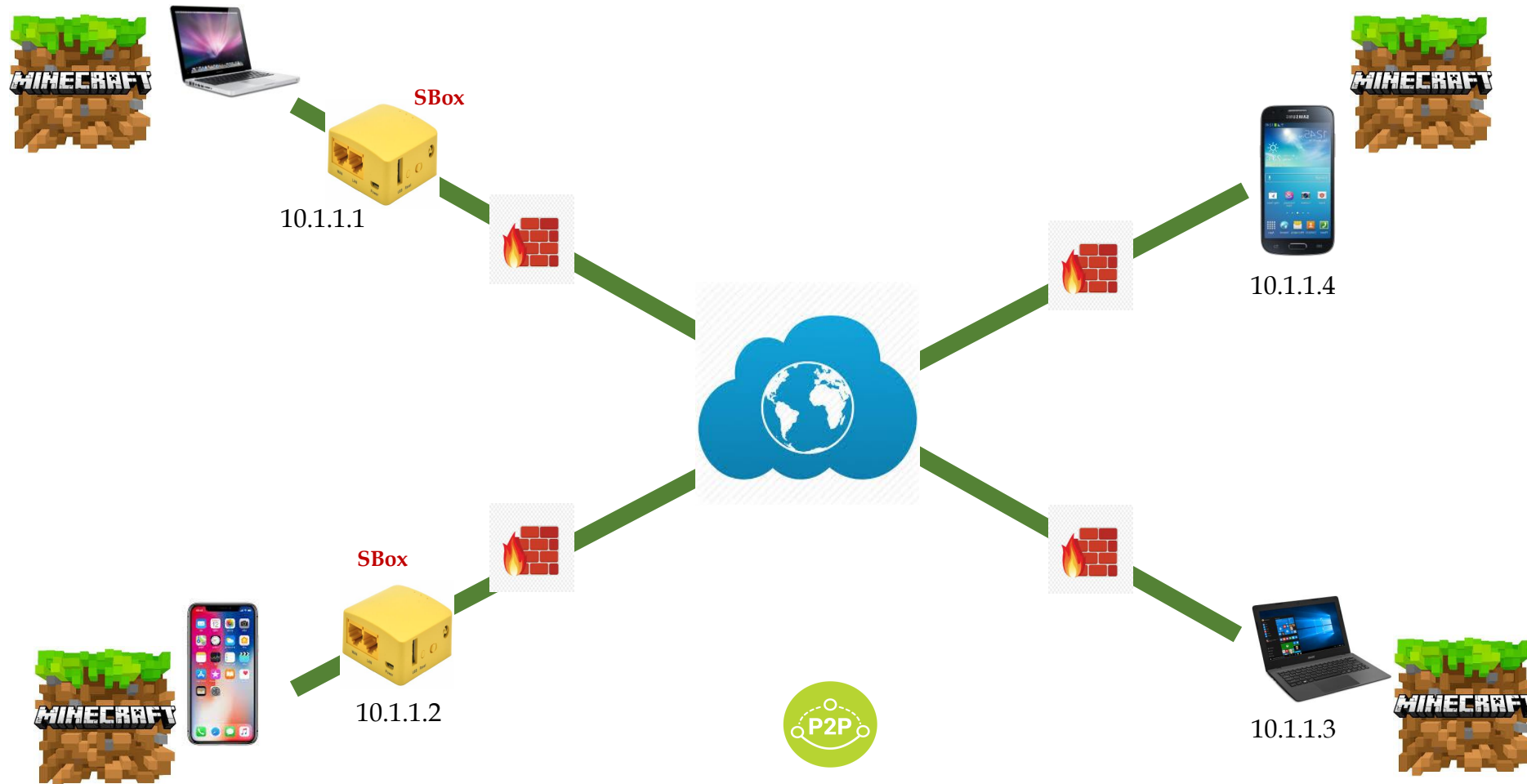


달리는 기차 위에서도 안전하게 회사 서버에 접속하여 업무를 볼 수 있습니다.

3. EndSec(6) – Use Cases(7)

Online Gaming

EndSec을 사용하면 방화벽/공유기 설정 변경 없이 P2P Game이 가능합니다.



Securely Connect Any Device, Anywhere !

3. EndSec(7) – Products Line-Up(1)

Wi-Fi, Ethernet(2 ports)
IP Camera, POS 단독 보호

SBox-200



SBox
(유무선 Access Point 방식)



소형 SBox(Access Point)



Dual Wi-Fi, LTE 지원 AP 용
3 LAN(2 LAN, 1 WAN) ethernet ports

SBox-600

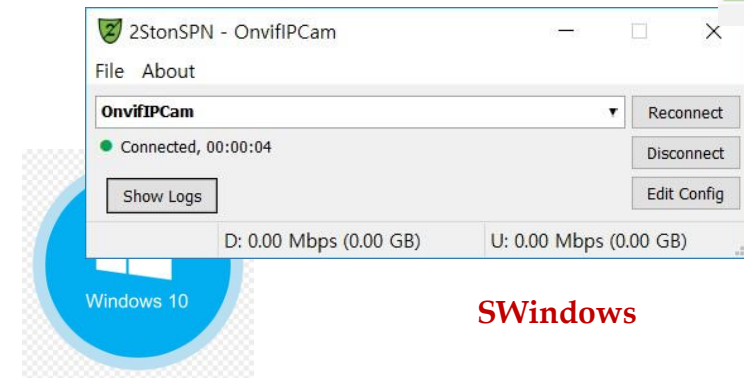
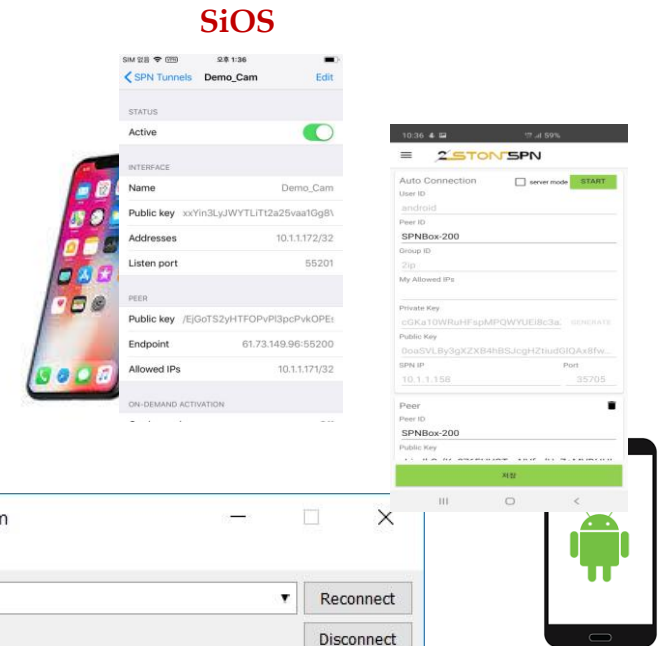
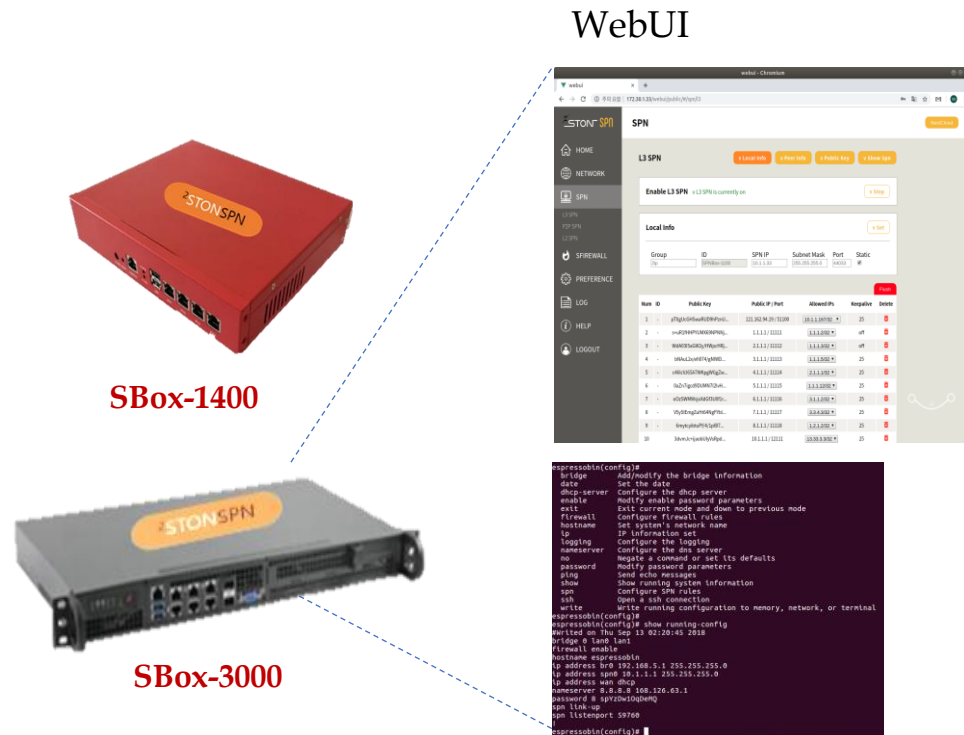


Wi-Fi, LTE 지원 AP 용
2 LAN(1 LAN, 1 WAN) ethernet ports
1 RS 485

SBox-300 (TBD)

3. EndSec(7) – Products Line-Up(2)

중형 SBox & SClients



SAndroid

SWindows

SBox
중형 Security Gateway

SClient S/W

4. 재택근무 VPN OfficeSec (Powered by SoftEther VPN)



4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(1)

예고없던 재택·원격근무 '시험대에 올랐다' - Chromium

news.bizwatch.co.kr/article/mobile/2020/02/28/0011

비즈니스 with BUSINESSwatch

최신뉴스 ▶ '코로나 때문에'...D-2개월 초조한 상하계 유예 단자들 위치뉴스 ▶ 비트코인 반감기 다가오자 난무하는 설정설

예고없던 재택·원격근무 '시험대에 올랐다'

이유미 기자 youme@bizwatch.co.kr
2020.02.28(금) 14:51

기업들 '코로나19' 방지 위해 재택근무 확대
갑작스런 재택근무 조치에 준비 미흡한 곳도 있어



관련 뉴스

- 코로나19가 불러온 머쓱한 호황
- 게임업계 뒤흔친 코로나19 'PC방·e스포츠 타격'
- 마·중전쟁 속 코로나19, 위기일까 기회일까

많이 본 뉴스 more

- SK, 하이닉스 실적 칼바람에 '우르르'
- 성수동 원룸, 공짜로 살아본 이야기 (feat...)
- 롯데쇼핑 구조조정의 후폭풍
- 두산중공업, 못지 못할 호실적
- 선생님 개인 전화번호 노출걱정 해결한 '...

/사진=이명근 기자 qwe123@

대기업 재택근무 확산...은행권도 시작 - 중앙일보 - Chromium

news.joins.com/article/23716484

중앙일보 경제

대기업 재택근무 확산...은행권도 시작


신종 코로나바이러스 감염증(코로나19) 확산에 따라 재택근무를 실시하는 기업이 늘고 있다. 금융당국이 금융회사의 본점·영업점 모든 직원의 재택근무가 가능하다는 지침을 내놓으면서 은행권에도 재택근무가 시작됐다.

SK그룹 이어 LG상사·CJ ENM도 씨타·신한·국민은행도 부분 도입

클라우드(인터넷에 접속해 어디서든 데이터를 주고받는 시스템)와 가상사설망(VPN)·스마트 워킹 시스템 같은 업무 환경이 확산하면서 가능해진 일이다.

하지만 이 같은 환경이 구축되지 않은 중소기업은 재택근무 전환이 어려워 고민이 크다.

SK그룹 계열사와 정보통신기술(ICT) 기업들이 재택근무로 전환한 데 이어 대기업 종합상사도 재택근무 대열에 합류했다. LG그룹 계열 종합상사인 LG상사는 26일 “코로나19 우려가 커지는 가운데 추가 확산 방지와 임직원 안전을 위해 전면 재택근무를 실시하기로 했다”고 밝혔다. LG상사는 27일부터 내달 4일까지 최소한의 필수 인력을 제외하고 전면 재택근무에 들어간다. 업무는 클라우드 PC 시스템을



추천기사

- "정봉주 당은 친문 위성정당 정의당, 토사구팽 심정 어떤가"
- "신천지 신도 42명 중우한서 들어왔다"
- "코로나 발원지 중국 아닐수도" 한달만에 말바꾼 중사서영웅, 왜
- '장당 1500원' 마스크 풀린다 "전국 약국에 100만장 배송중"
- 확진자 3000명 넘었다 하루 813명 늘어 3150명
- 민주당, 전남 목포에 김원이 공천 박지원·윤소하와 빅데치 벌인다
- 文 '코로나 종식' 발언에 NYT "대가 큰 실수" 일침
- "코로나 걸리면 엄중 문책" 전직원에 문자 보낸 경남銀
- 코로나에 부러라 韓 떠난다 집 싸는 불법체류자 3배 급증
- 안철수 "한중 확진자 비율 동일 으면교정 더 늦으면 시가침다"

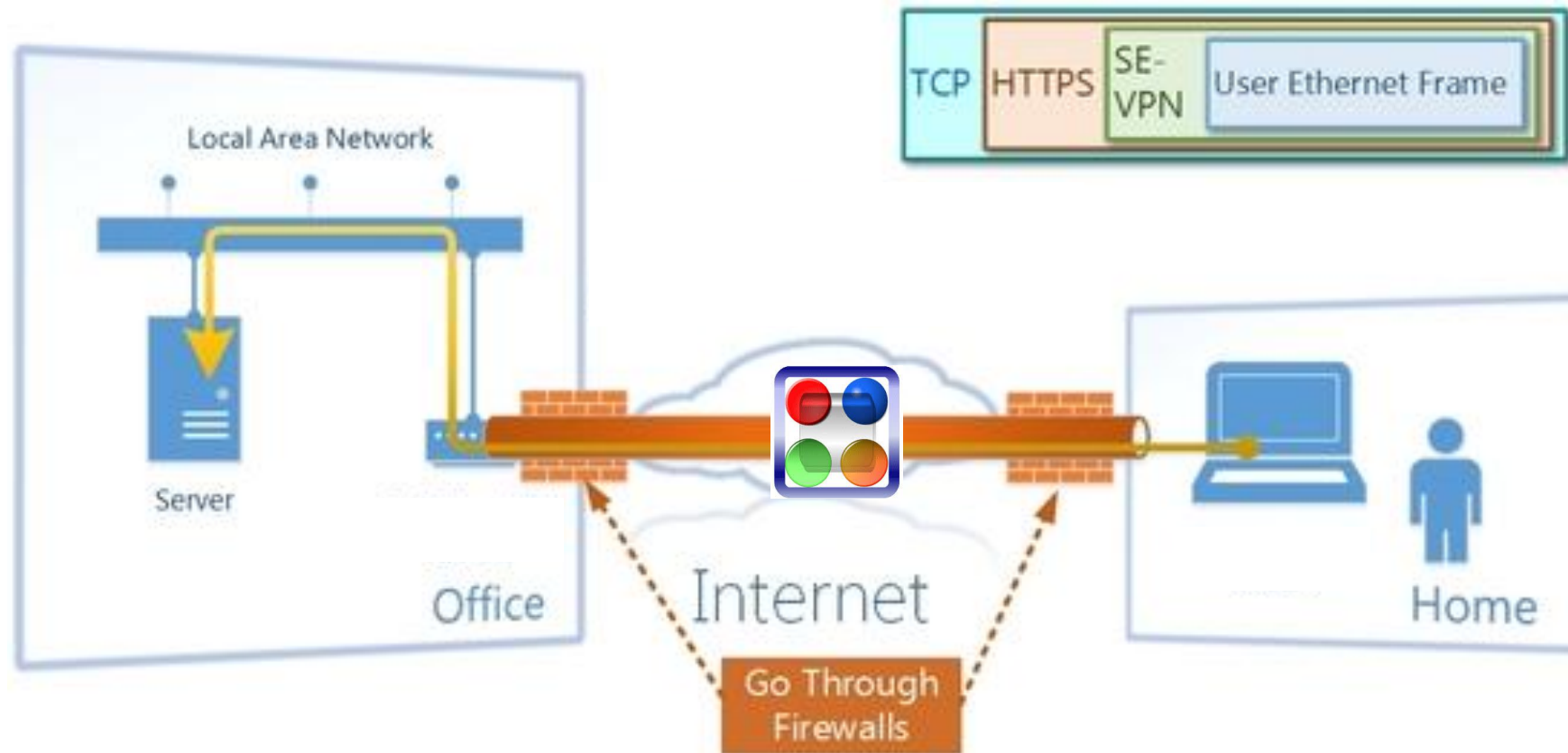
4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(2)

회사에서 아주 긴 랜선을 끌어다 집에 연결한 것처럼

집에 있으나, 마치 회사에 있는 것과 같은 동일한 네트워크 환경을 만들 수는 없을까?



4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(3)

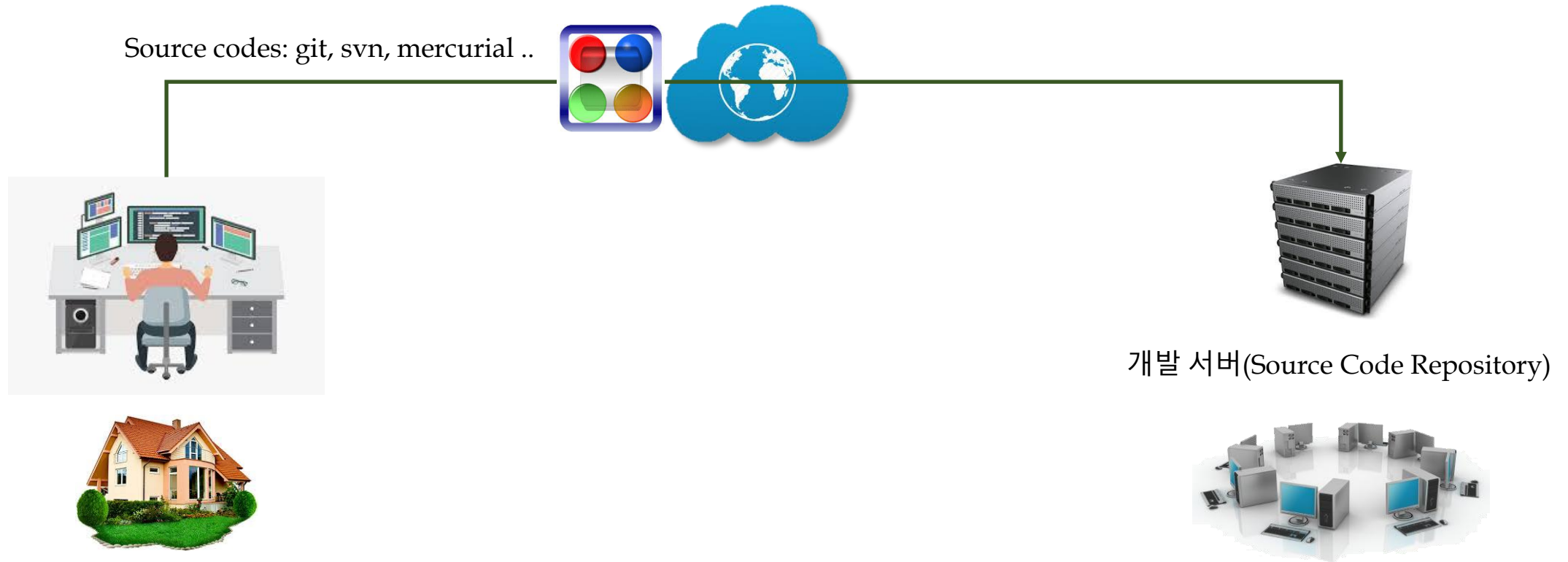


OfficeSec은 아주 긴 LAN 케이블을 회사 망에 연결한 것과 동일한 효과를 만들어 줍니다.

4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(4)

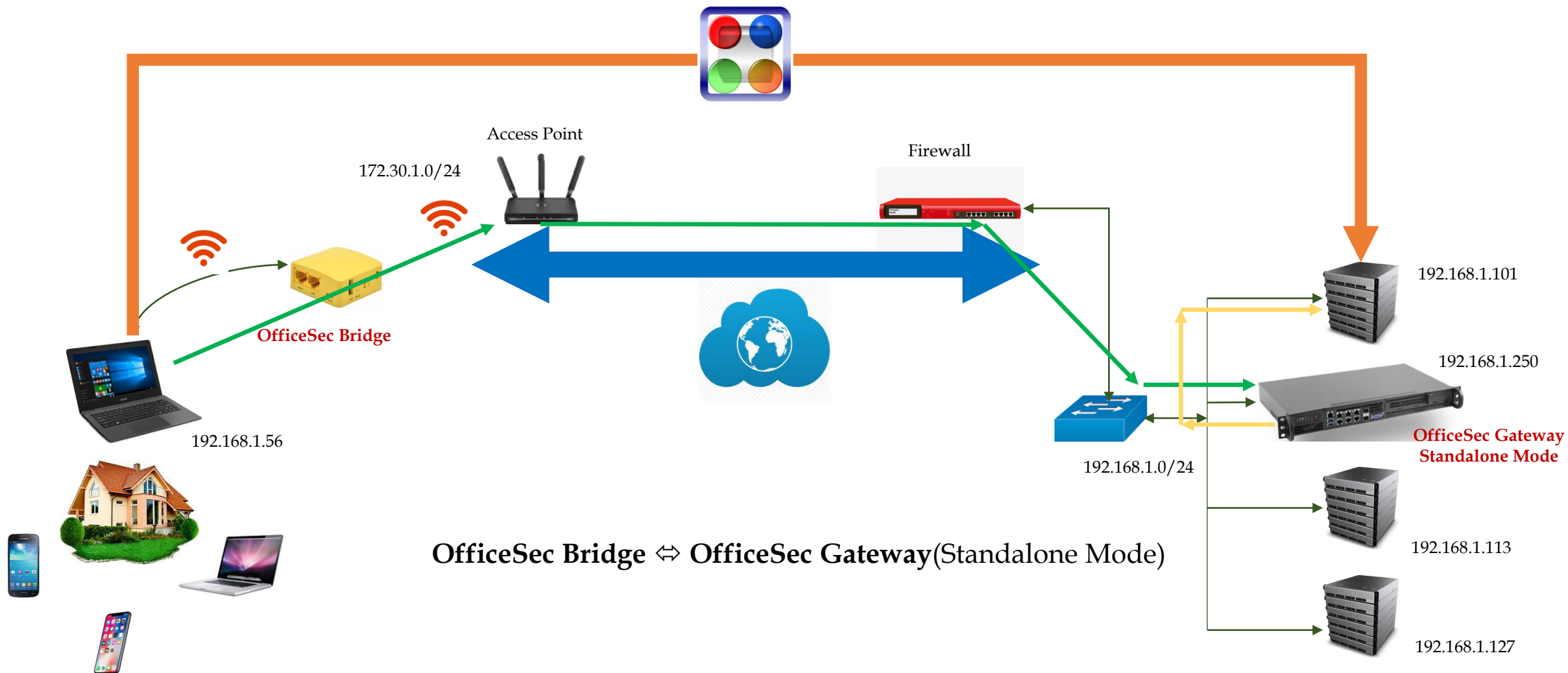


4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(5)



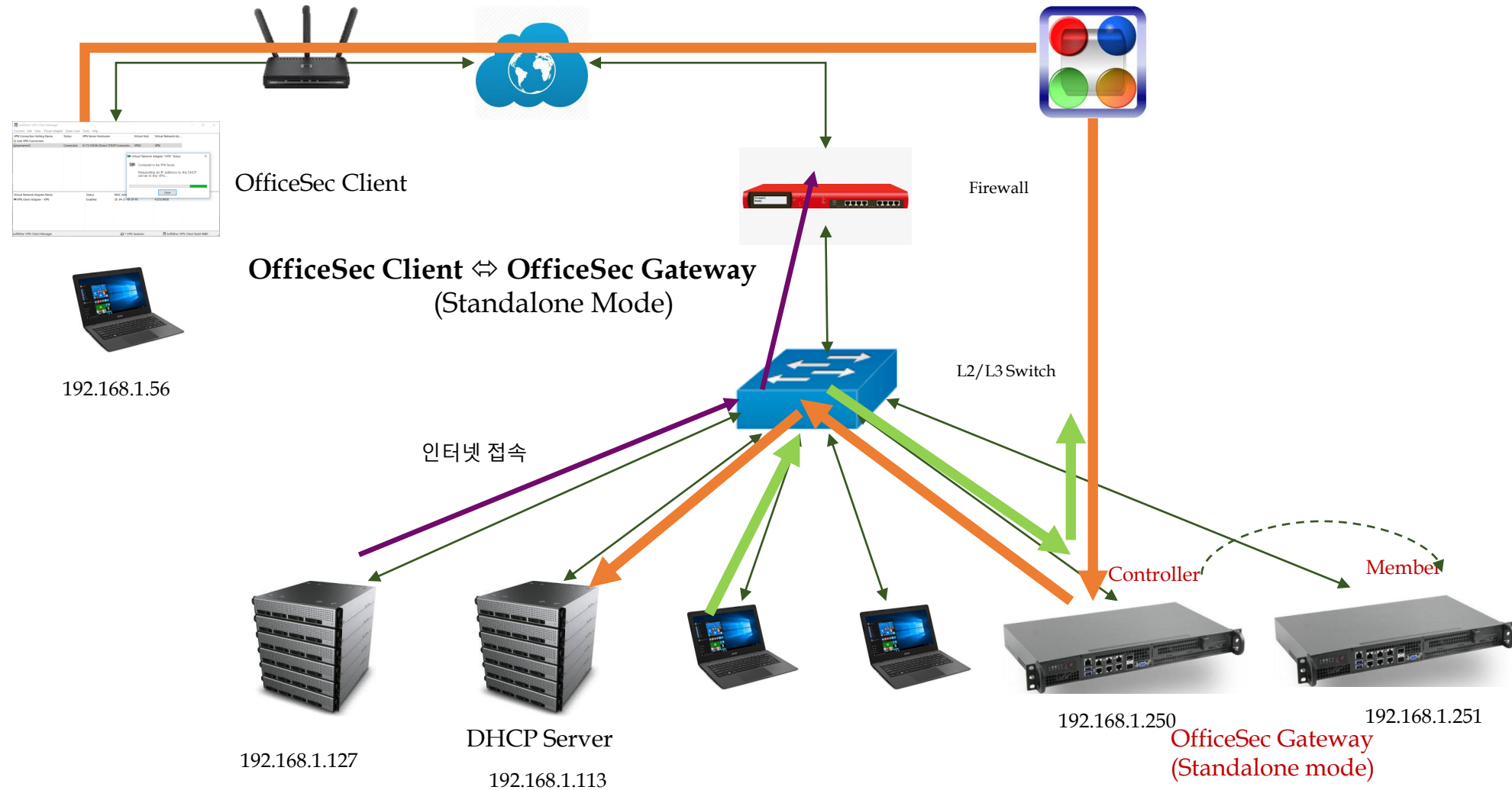
개발자에게 가장 필요한 것은 자신이 개발한 source code를 안전하게 서버에 올리는 일일 것입니다.

4. OfficeSec(2) - Standalone Mode 구성(1)



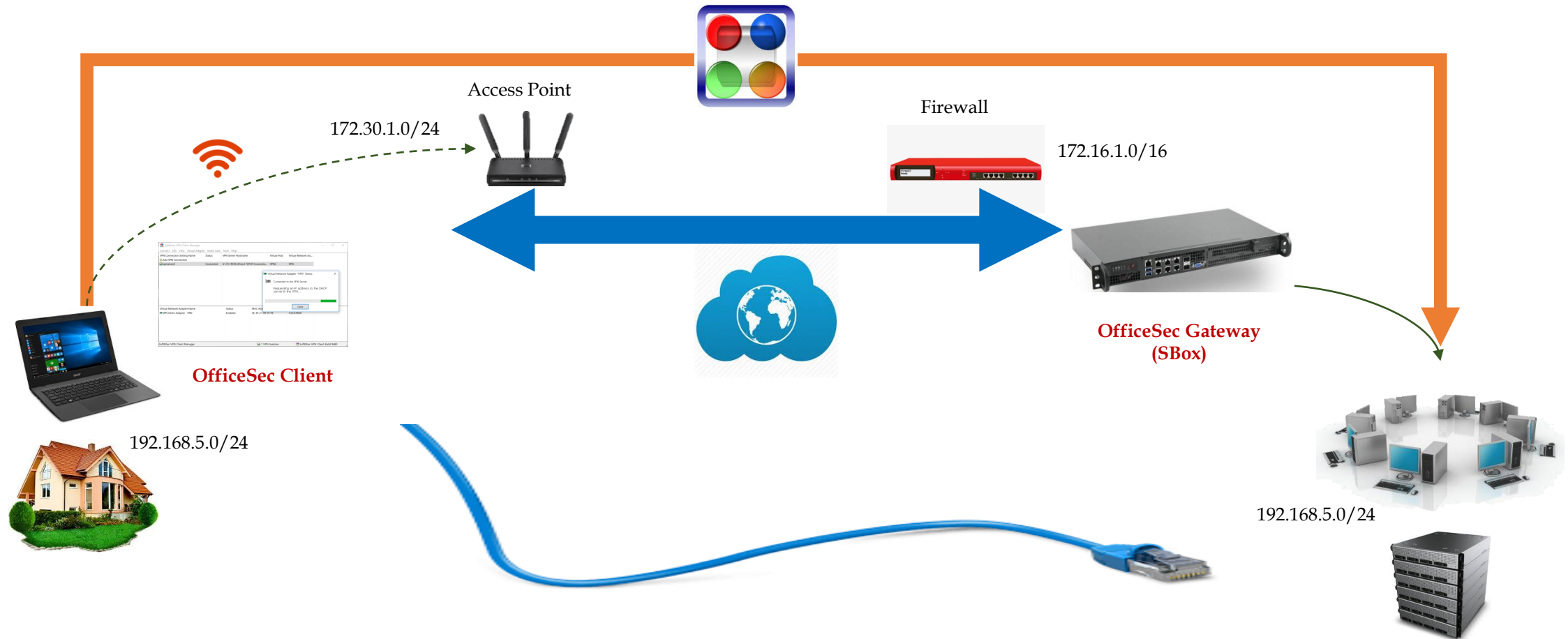
OfficeSec Gateway Standalone mode를 이용하시면 사무실 망 구성을 전혀 변경하실 필요가 없습니다.

4. OfficeSec(2) - Standalone Mode 구성(2)



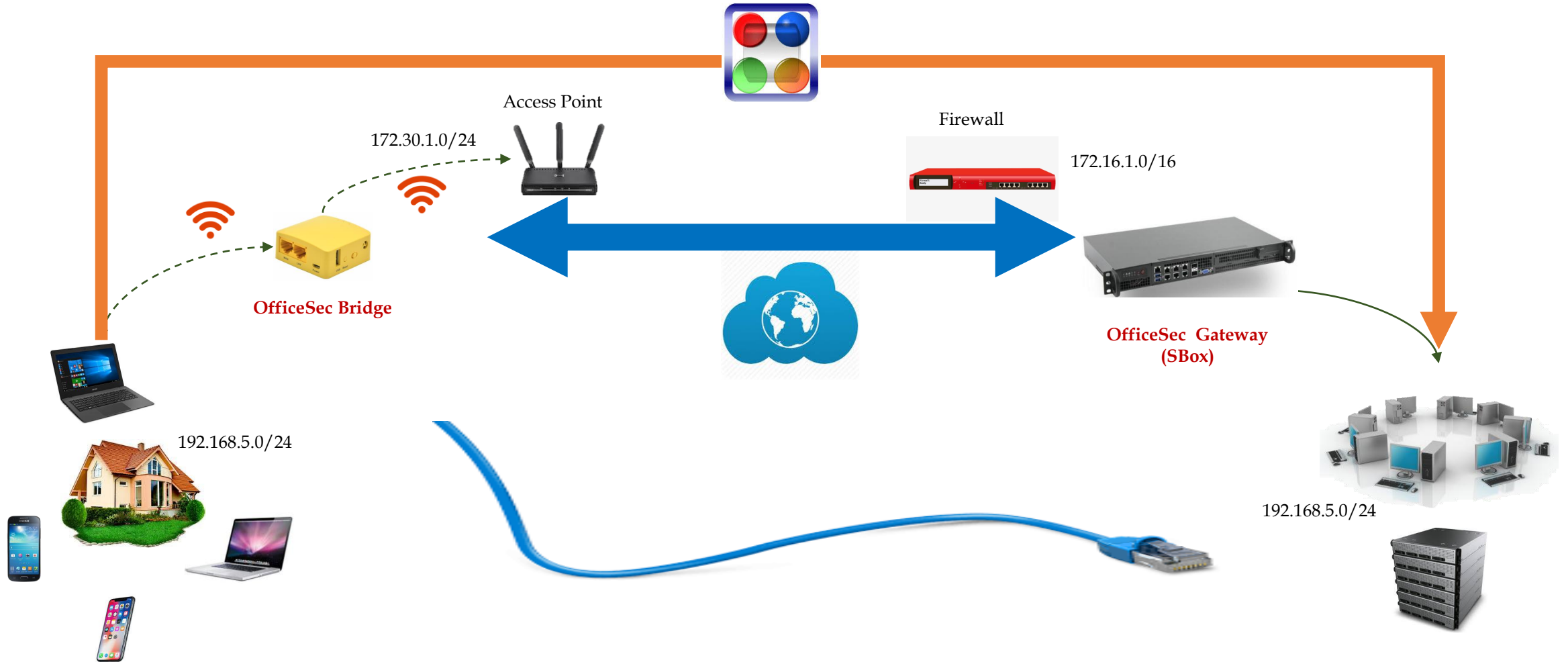
OfficeSec Gateway Standalone mode를 이용하시면 사무실 망 구성을 전혀 변경하실 필요가 없습니다.

4. OfficeSec(3) - Client & Gateway 구성



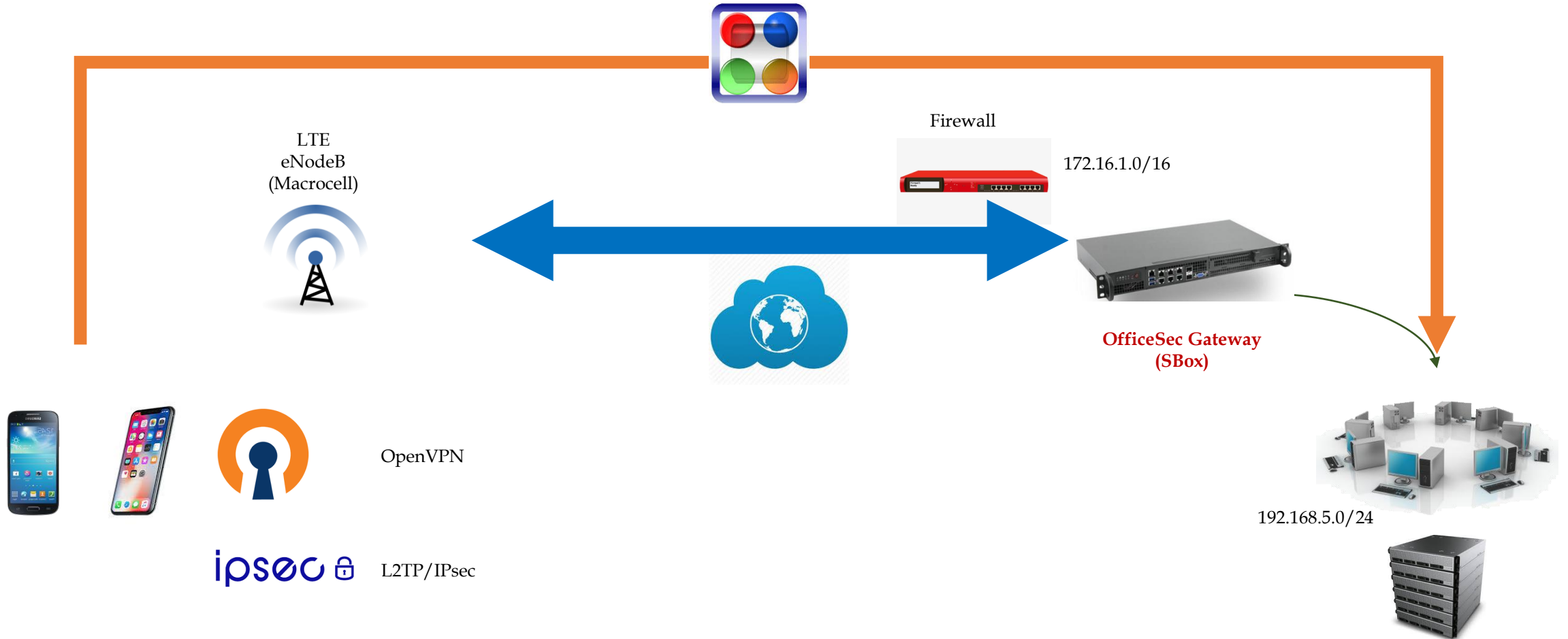
OfficeSec은 아주 긴 LAN 케이블을 회사 망에 연결한 것과 동일한 효과를 만들어 줍니다.

4. OfficeSec(4) - Bridge & Gateway 구성



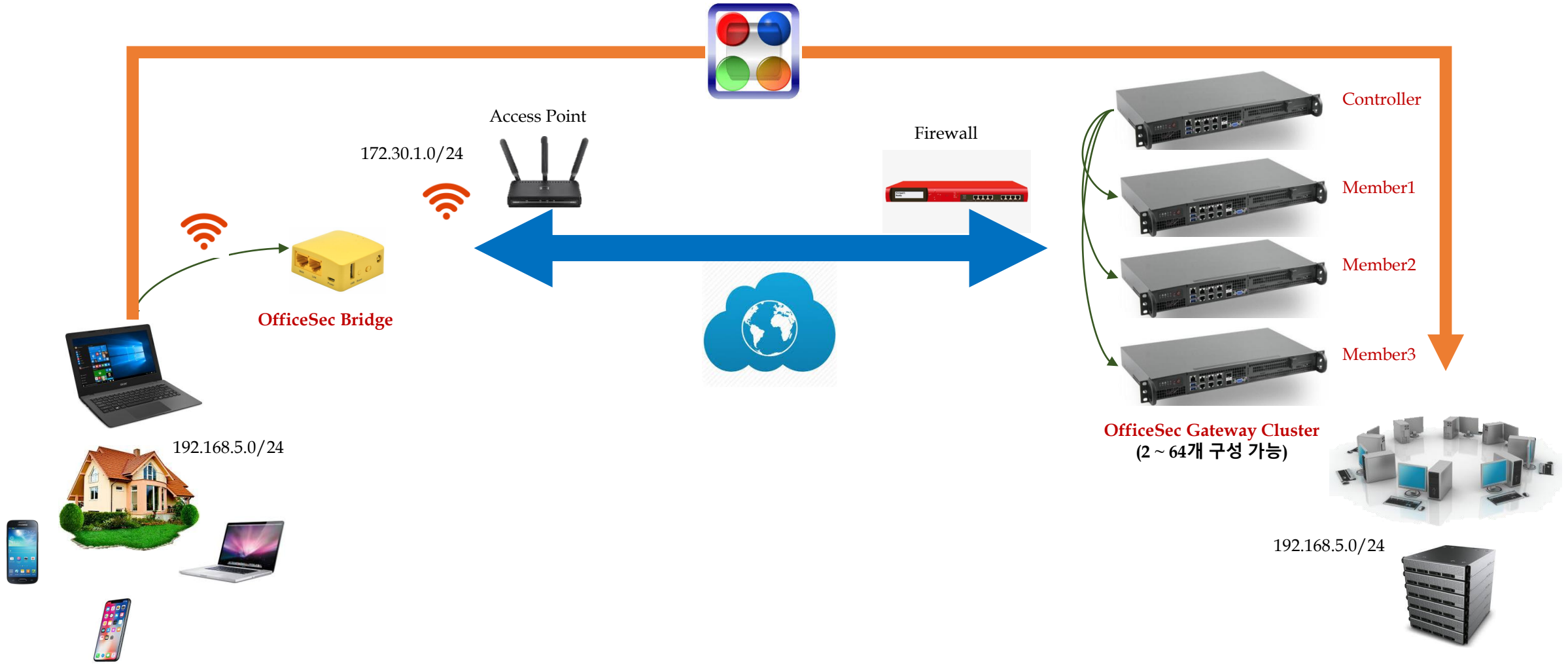
OfficeSec Bridge를 이용하면 3~4개의 네트워크 장치(Notebook, Smart Phone ..)를 동시에 사용할 수 있습니다.

4. OfficeSec(5) - Smart Phone & Gateway 구성(1)



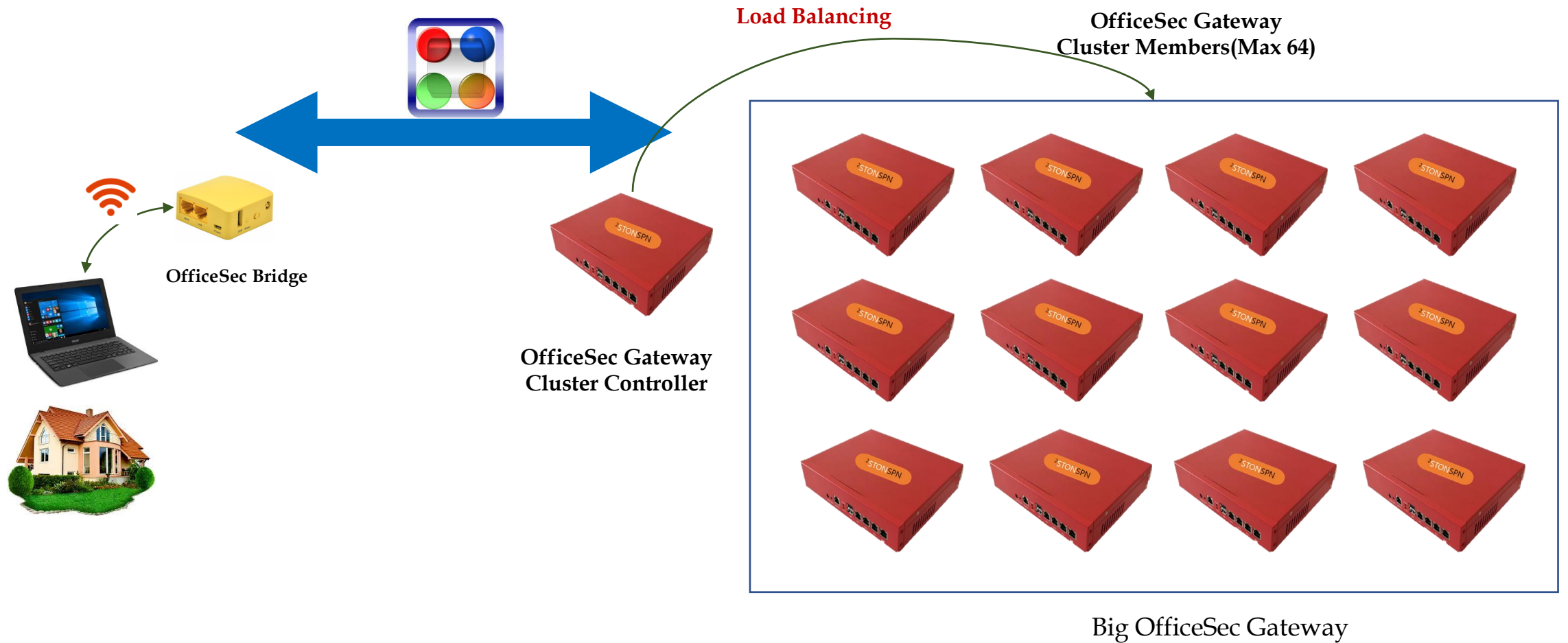
OpenVPN or L2TP/IPsec app을 이용하면 Smart Phone에서 LTE 망을 통해 사내 망에 접근할 수 있습니다.

4. OfficeSec(6) - Bridge & Cluster 구성(1)



OfficeSec Gateway Cluster는 저사양의 OfficeSec Gateway를 여러 개 연결하여 하나의 고성능 OfficeSec Gateway를 만들어 줍니다.

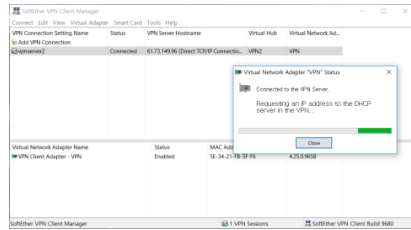
4. OfficeSec(6) - Bridge & Cluster 구성(2)



주의: Cluster를 구성하는 OfficeSec Gateway 중 반드시 하나에서만 DHCP Server를 구동시켜야 함.

4. OfficeSec(7) - 제품 구성(1)

Home 사용자용
(Client or Bridge)



OfficeSec Client
Client 1대 처리
Windows Only



OfficeSec Bridge
Client 2~4대 이상 처리
비 Windows도 가능
(유무선 기능 지원)



OfficeSec Bridge
Client 2~10대 이상 처리
비 Windows도 가능
(유선 Only)



사무실 설치용
(Gateway/Server)



Tunnel 50 ~ 100개 처리
[개발 중]



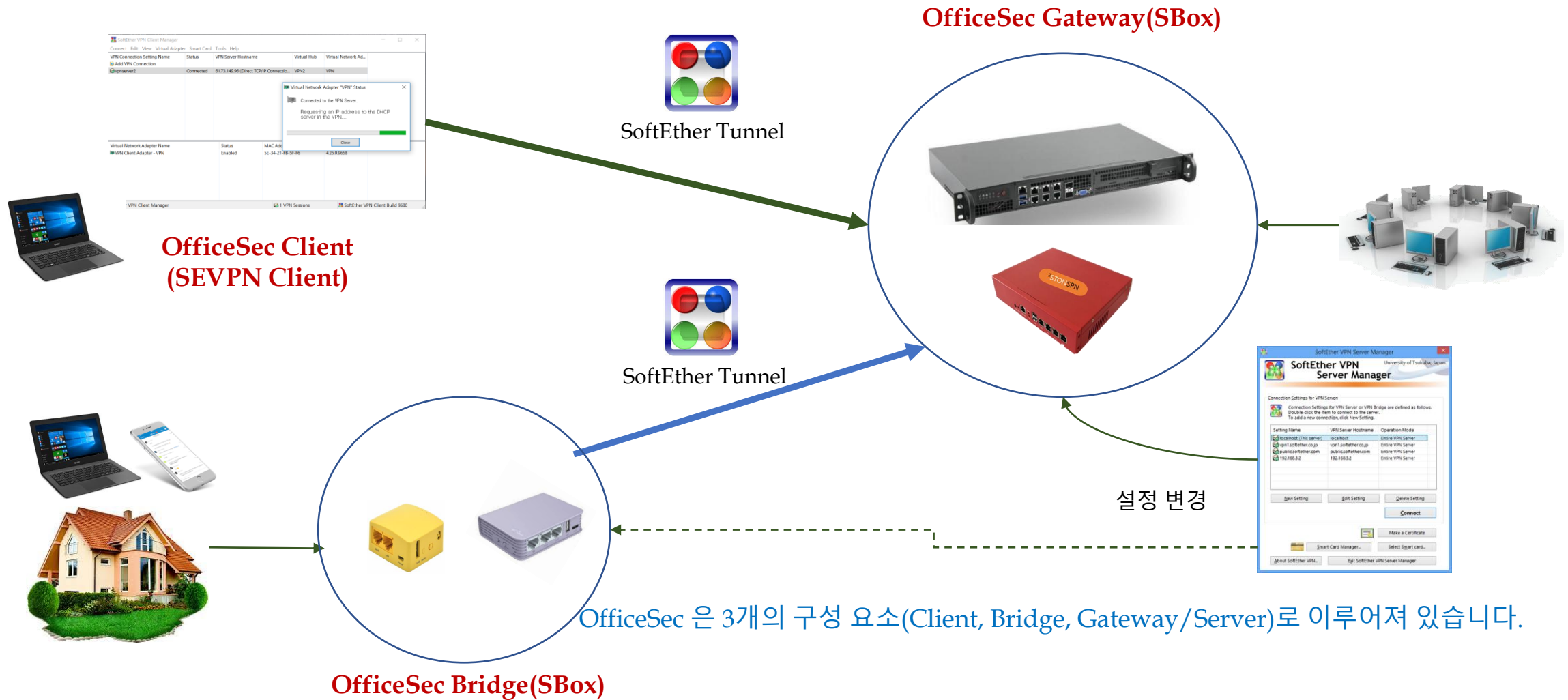
Tunnel 20~30개 처리



OfficeSec Gateway
(a.k.a SBox)

Tunnel 5~10개 처리

4. OfficeSec(7) - 제품 구성(2)



5. POS 단말 보안 **POSSec**

: POS 단말에 자물쇠를 채우자 ~



5. POSSec(1)



작지만 철저한 보안 

*POSSec은 해킹과 악성 코드에 무방비로 노출되어 있는
POS 단말기를 해킹으로 부터 안전하게 보호해 주는
소형 해킹 프로텍터입니다.*

5. POSSec(2) – POS 보안 위협



카드단말기 보안사고

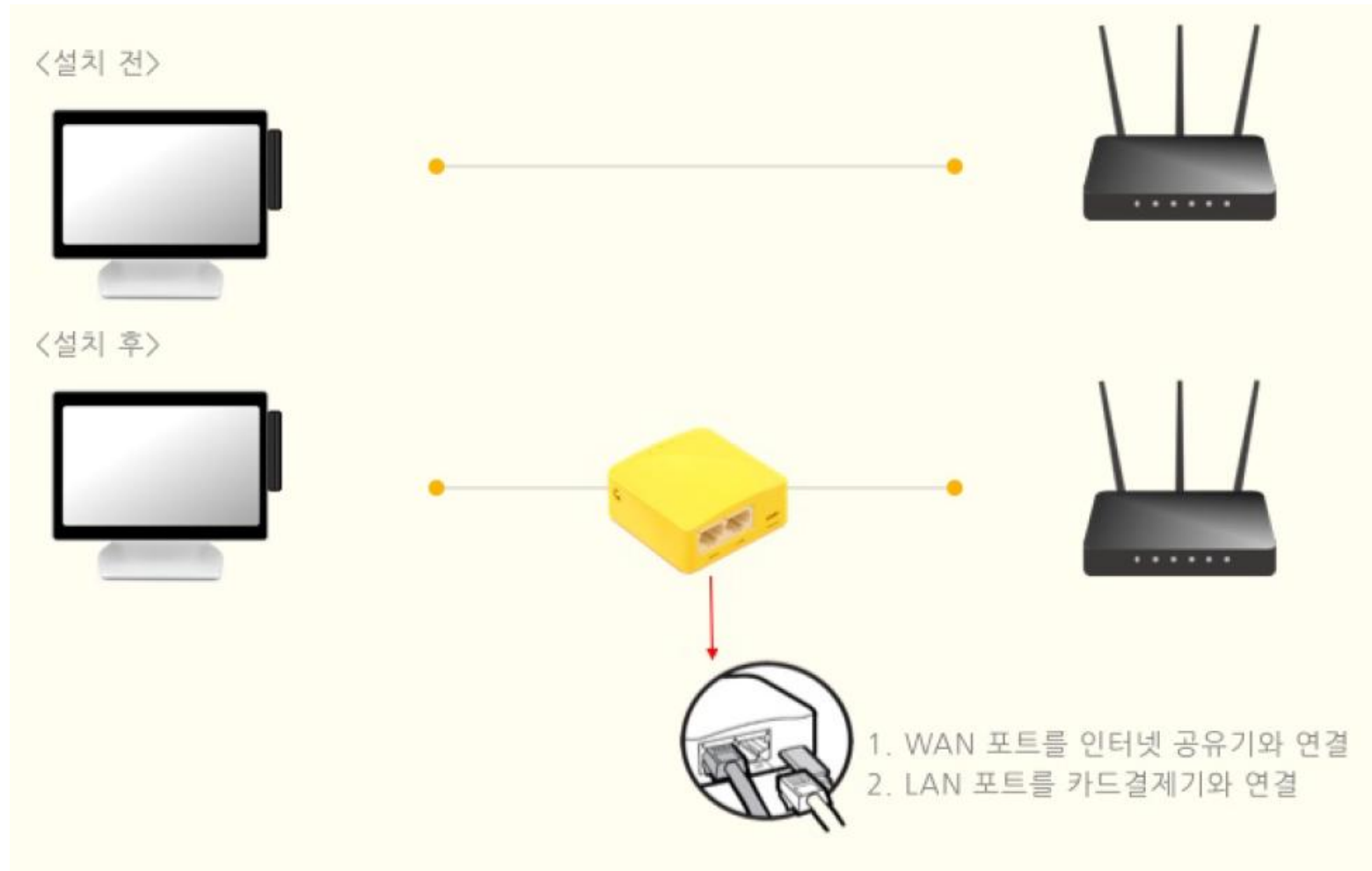
카드단말기(POS)는 다양한 위험 요소에 노출되어 있습니다.



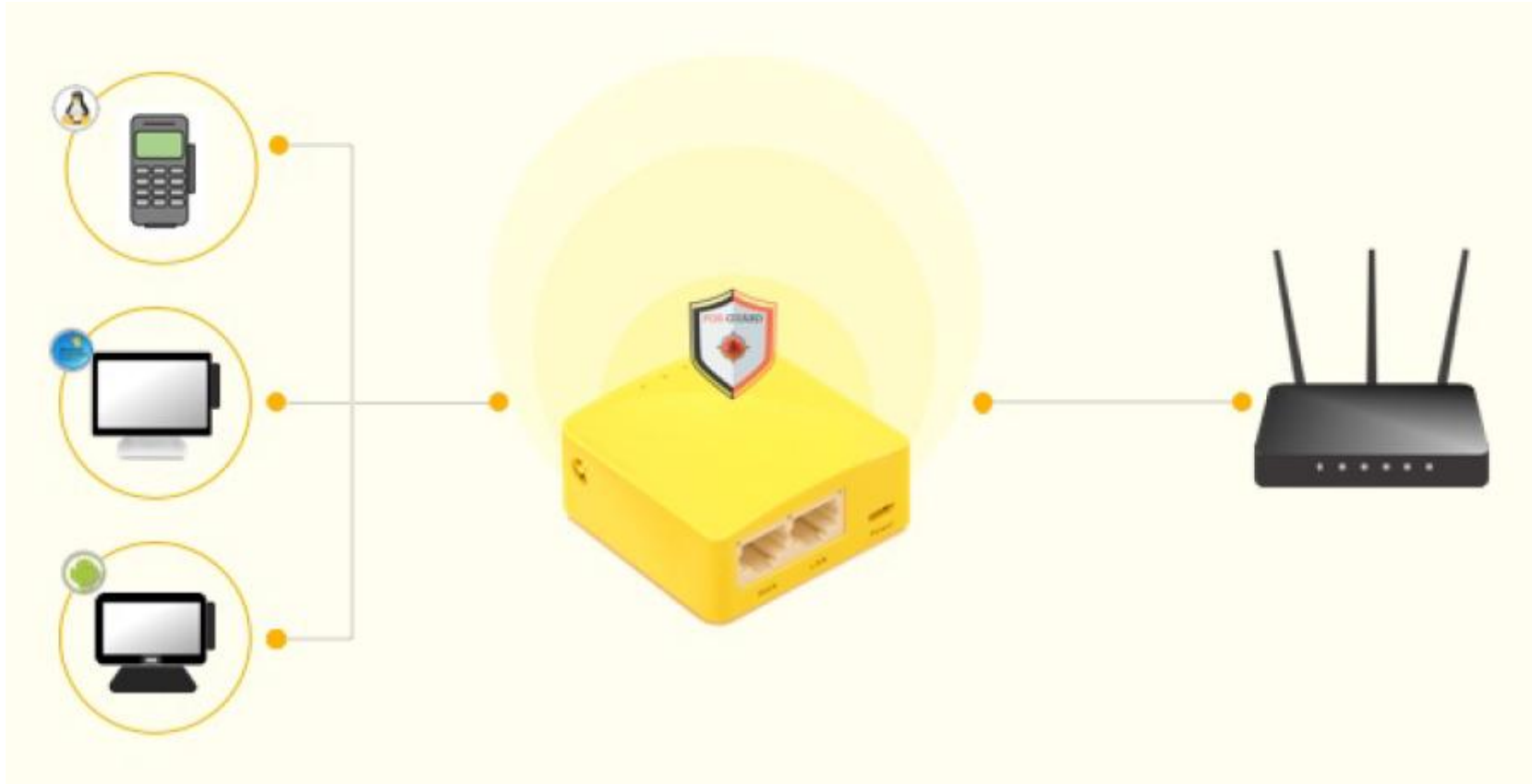
사례 1 결제기엔 19년 된 윈도우XP...사이버 보안 '구멍'
(2020.01.16 SBS 8 NEWS)

사례 2 카드결제기 무더기 해킹, 고객 개인정보 '줄줄'
(2018.07.13/뉴스투데이/MBC)

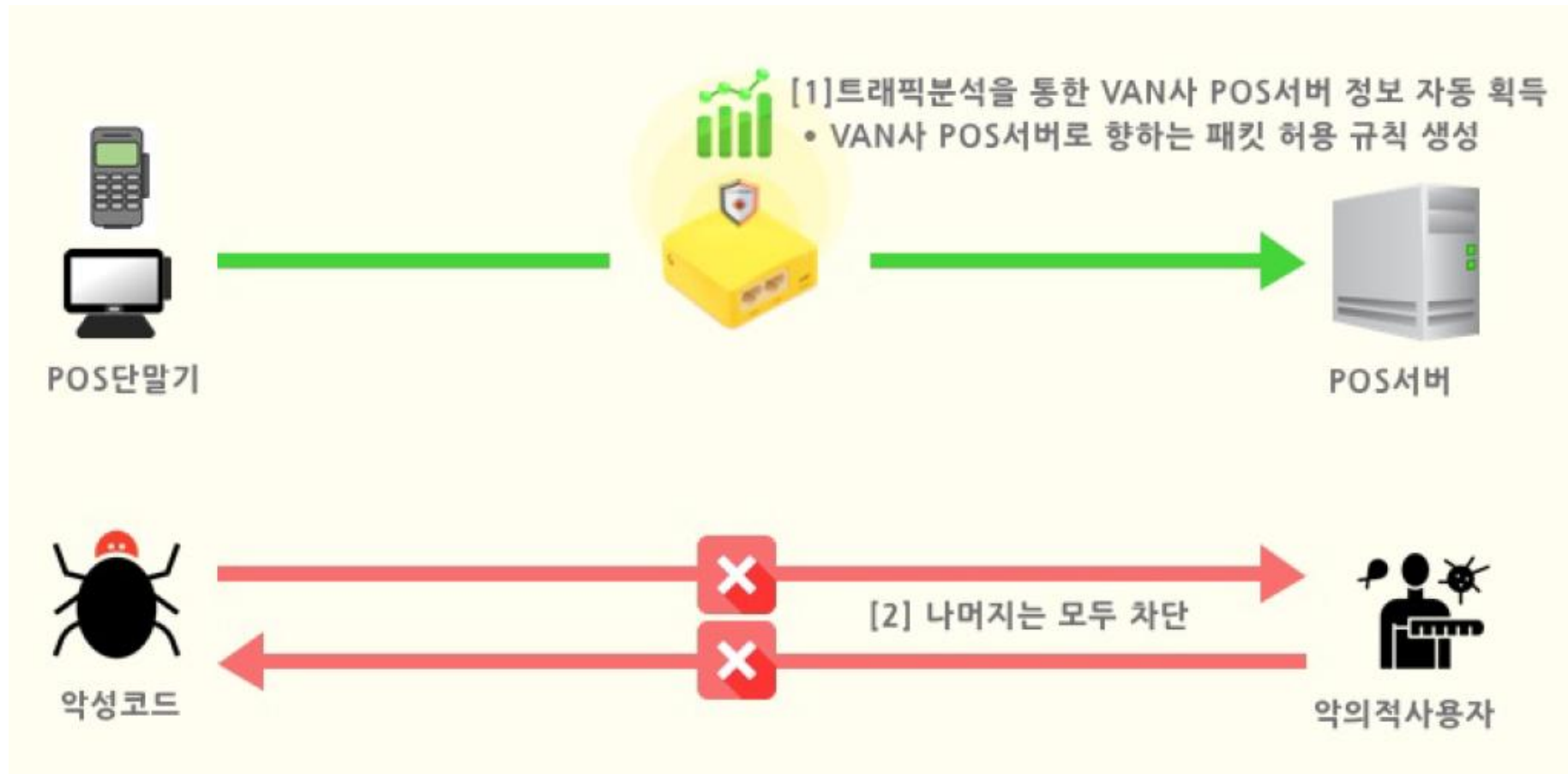
5. POSSec(3) - 간편한 설치(1)



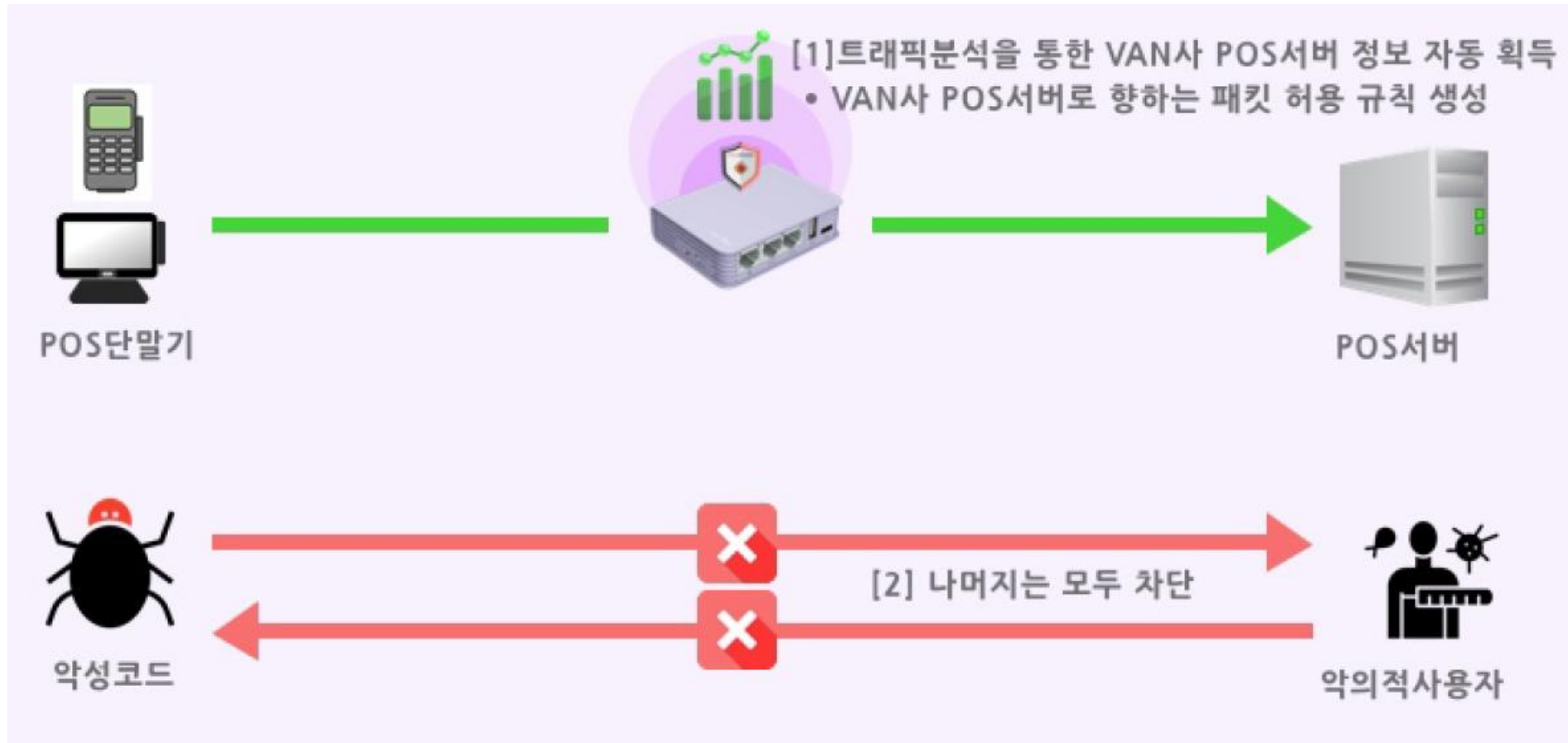
5. POSSec(3) - 간편한 설치(2)



5. POSSec(3) - 간편한 설치(3)



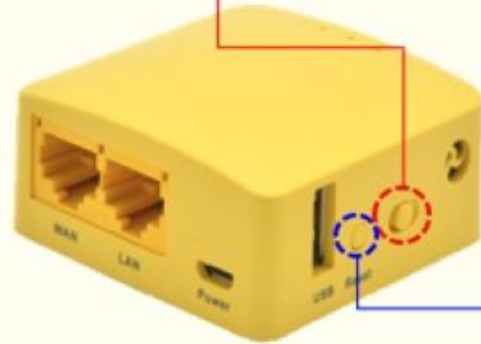
5. POSSec(3) - 간편한 설치(4)



5. POSSec(4) - 보안 모드

〈 3단계 보안 모드 〉

보안모드	보안수준	기타
상급 보안 모드 (High Security Mode)	카드 결제만 허용	광고 및 음란 사이트 차단 기능 제공
중급 보안 모드 (Medium Security Mode)	카드 결제 및 인터넷/e-mail허용	
하급 보안 모드 (Low Security Mode)	기본 방화벽을 제외한 모든 기능허용	



하급 보안 모드
(Low Security Mode)

"Reset" 버튼을 2초간(설정 LED 3회 점멸) 눌렀
다가 땡니다.

5. POSSec(5) - 개통 절차(1)



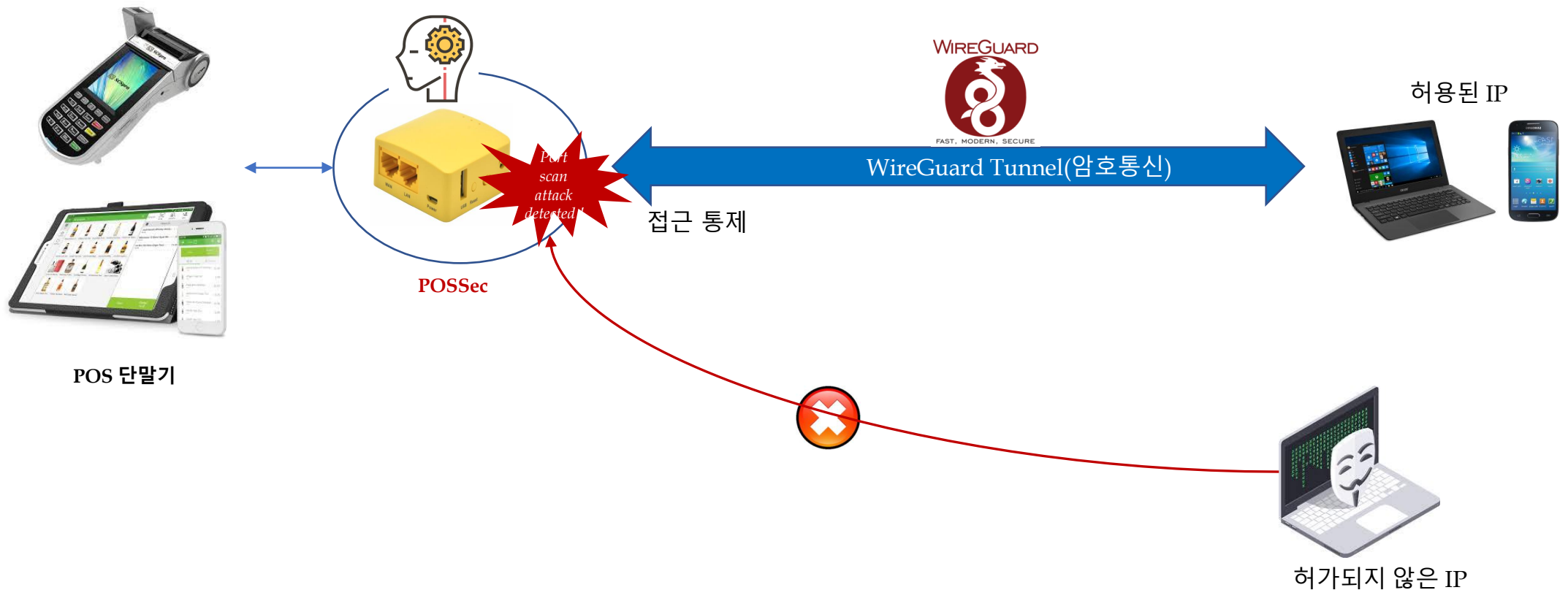
1. POSSec에 LAN Cable을 연결하고 전원을 넣는다.
2. POS 단말기의 전원을 켜다(혹은 재 부팅한다). 주의: POSSec이 켜져 있는 상태에서 POS 단말이 켜져야 IP 획득에 문제가 없다.
3. 개통: **1시간 이내에 테스트 결제를 한 차례 진행한다.** 참고: 이 시간 동안에 외부 접속(예: 정산, 발주 관련)이 필요한 부분이 있다면 최대한 연결 시험을 해 본다.
4. POSSec은 자동으로 서버 연결 정보를 확보한 후, **POS 서버로의 연결을 제외한 내/외부로 부터의 모든 공격을 차단한다.**
5. 이후 안심하고 POS 단말기를 사용하여 결제를 진행한다.

5. POSSec(5) – **개통 절차(2)**

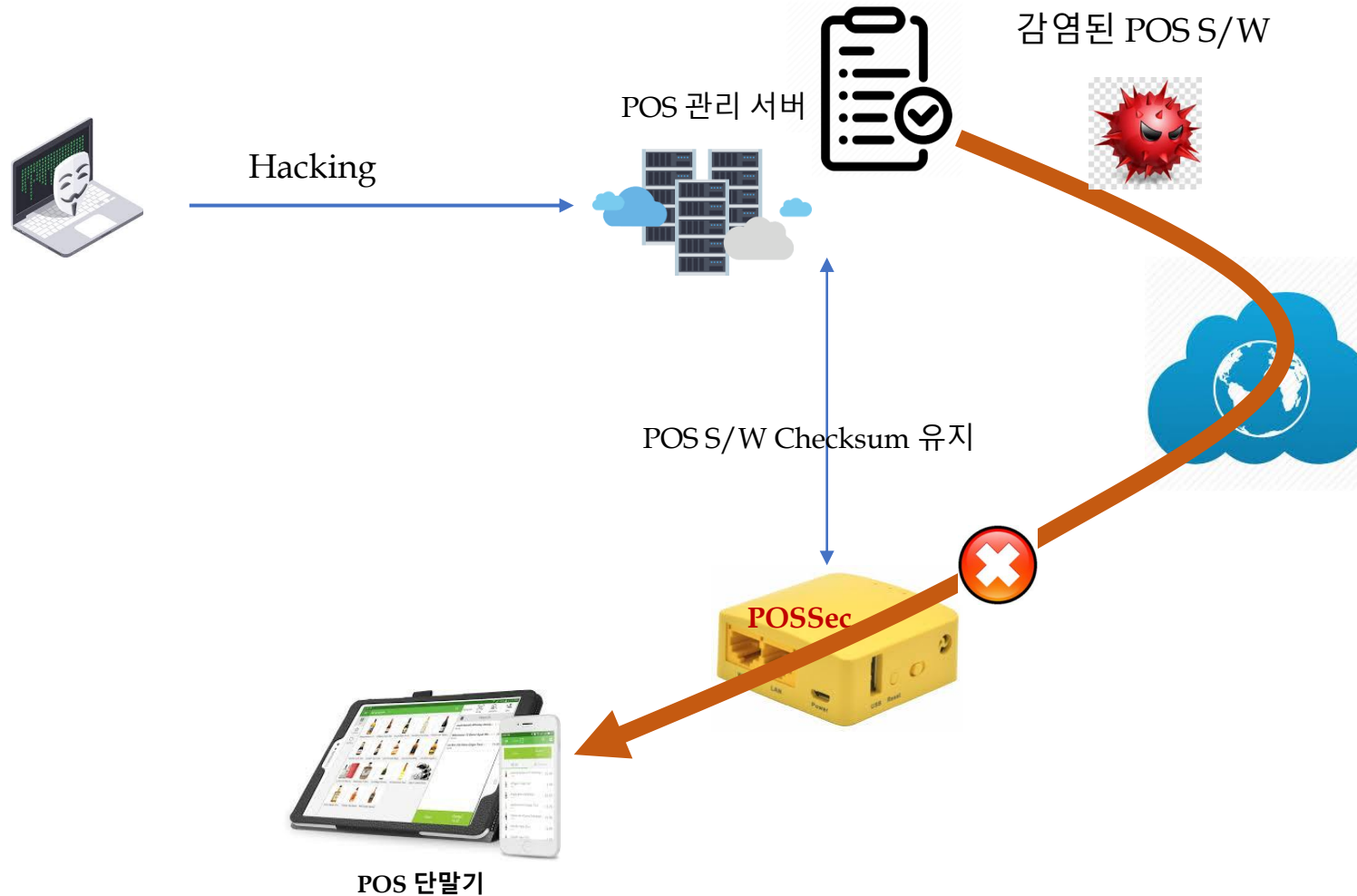
- 1) **기본 원칙:** VAN 사 서버로 전달되는 결제 packet을 자동 감지하고 이를 허용한다.
- 2) 개통 시간 동안에 외부 접속(예: 정산, 발주 관련)이 필요한 부분이 있다면 최대한 연결 시험을 해 본다.
- 3) 자주 사용하는 인터넷, SNS 등이 있다면 개통 단계(1시간 동안)에 접속을 시도해 둔다.
 - *접속 기록이 남아 있는 것(최대: 30개 site)에 한하여 자동으로 허용해 준다.*
- 4) **개통 시간이 지나면 앞서 자동으로 인식한 내용을 제외한 모든 트래픽이 자동으로 차단되게 된다.**
 - *만일, 이후(개통 시간이 지난 후) 특정한 서비스를 허용하고 싶다면, WebUI를 통해 추가로 허용 규칙을 생성해 준다.*
- 5) POS 관리 업체가 원격 관리를 하고자 한다면, EndSec Tunnel을 이용하도록 한다.
 - *지정된 사용자(관리자)만 접근 가능하도록 해 줌. POSSec(6) 페이지 참조*

5. POSSec(6) - 안전한 원격 관리

허용된 IP 및 Tunnel 설정을 통과해야만 POS 단말에 접근할 수 있습니다.



5. POSSec(7) - 안전한 S/W Upgrade

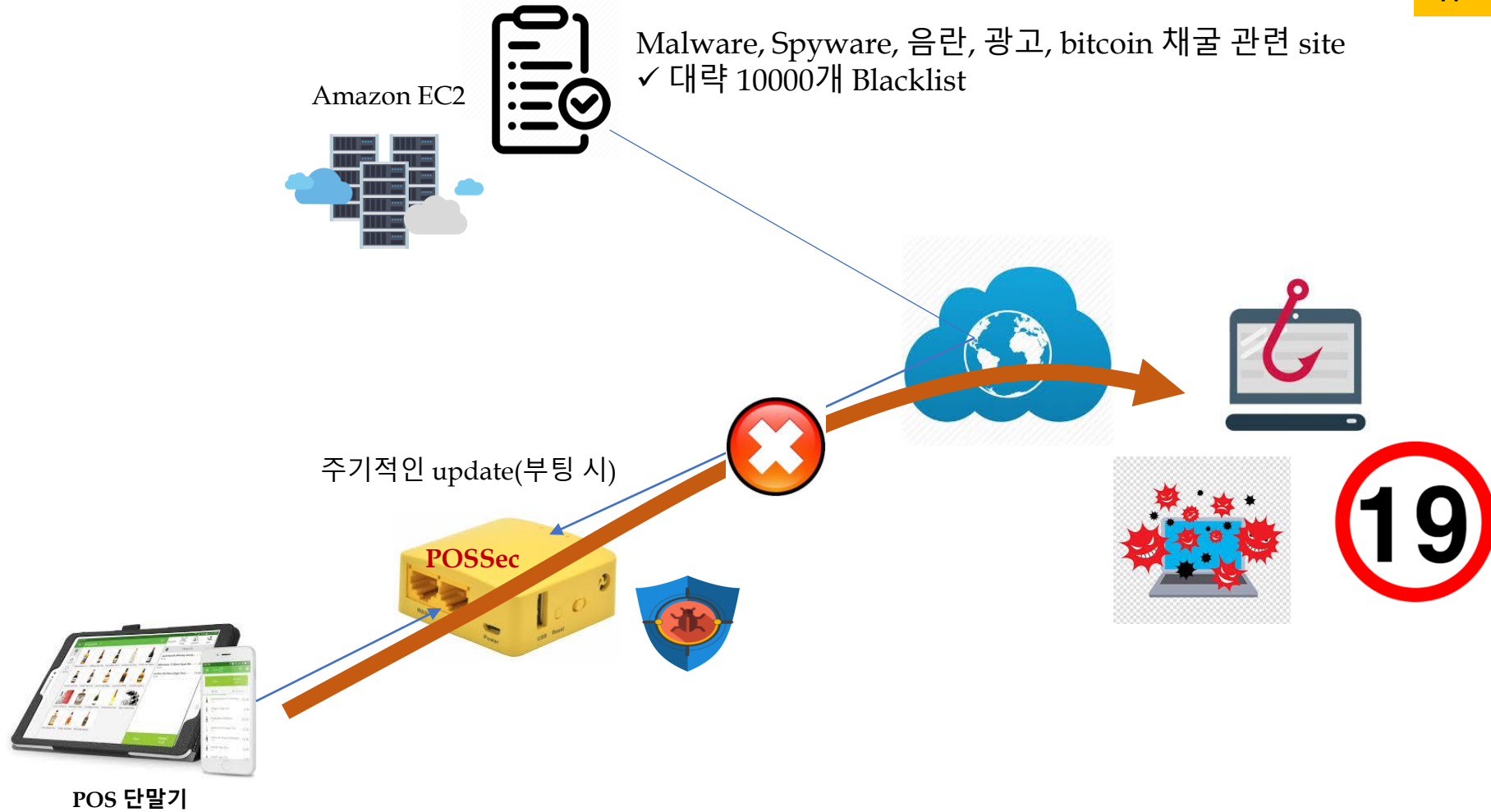


악의적인 사용자가 감염시킨 POS S/W는 POSSec에 의해 차단되어 설치되지 않습니다.

POS 관리 업체와 사전 조율 필요함.

5. POSSec(8) - 부가 기능(1)

유해 Site 차단



POSSec은 Malware, Spyware, Phishing, 광고, bitcoin 채굴, 음란 site 등을 자동으로 차단해 줍니다.

5. POSSec(8) – 부가 기능(2)



POSSec은 랜섬웨어 류의 공격에도 안전합니다.

5. POSSec(8) - 부가 기능(3)

암호통신(결제 데이터 보안)



POSSec과 EndSec을 결합하면 POS 단말 자체 보안(접근 통제)과 결제 패킷 보안(암호 통신)을 동시에 할 수 있습니다.

5. POSSec(9) - 지원 모델



POSSec Lite

POS 단말용



POSSec Premium

Kiosk 용

6. IoT Security Gateway **SBox**



6. SBox(1) – Board Level Gateway for Projects



SBox-G
(Based on GrapeBoard)



SBox-R
(Based on Raspberry Pi)

SBox-E
(Based on ESPRESSObin)



6. SBox(2) – Tiny Gateway



Gl.iNet Wireless Router + vIoTSec S/W

6. SBox(3) – Medium Gateway



Network Appliances powered by Intel CPU

7. 참고 사항(1)



<https://www.wireguard.com/>



<https://www.softether.org/>



GL.iNet h/w를 기반으로 한 제품(초소형 AP)임.
<https://www.gl-inet.com/>

7. 참고 사항(2) - TODO

- 1) 최대한 쉽고 사용하기 편리하게 만들어야 한다.
 - *현재까지 만들어진 부분을 더욱더 같고 다듬어야 한다는 의미!*
 - *3개 모델(EndSec, OfficeSec, POSSec) 중 어떤 제품은 상용 제품 수준으로 개발되어 있고, 어떤 제품은 UI 등을 추가 개발(보강)해야 함.*
- 2) 다양한 환경에서의 시험을 진행해야 한다.
 - *(특히) POSSec의 경우는 다양한 필드 시험을 진행해 보아야 함.*
- 3) SBox는 전파인증을 획득해야 한다.
- 4) (향후) 고성능 SBox를 개발해야 한다.
- 5) (향후) 소형 SBox(Gl.iNet model)는 자체 생산할 수 있어야 한다.
- 6) (향후) 개별 SBox 관리는 WebUI로 하지만, 전체 SBox를 관리할 수 있는 원격 관리 도구를 개발해야 한다.

We Secure the Internet of Things with vIoTSec !



Thank You