

vIoTSec Products

- Virtual IoT Security Platform 개발 계획서 -

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

Doc. Revision: 0.7

Copyright© 2020 Chunghan.Yi, All Rights Reserved.



Contents

- 1. IoT Security Market
- 2. IoT VPN **EndSec**
- 3. Peer to Peer VPN **P2PSec**
- 4. 재택근무 VPN **OfficeSec**
- 5. POS 단말 보안 **POSSec**
- 6. 유해 사이트 차단 **KidSec**
- 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>



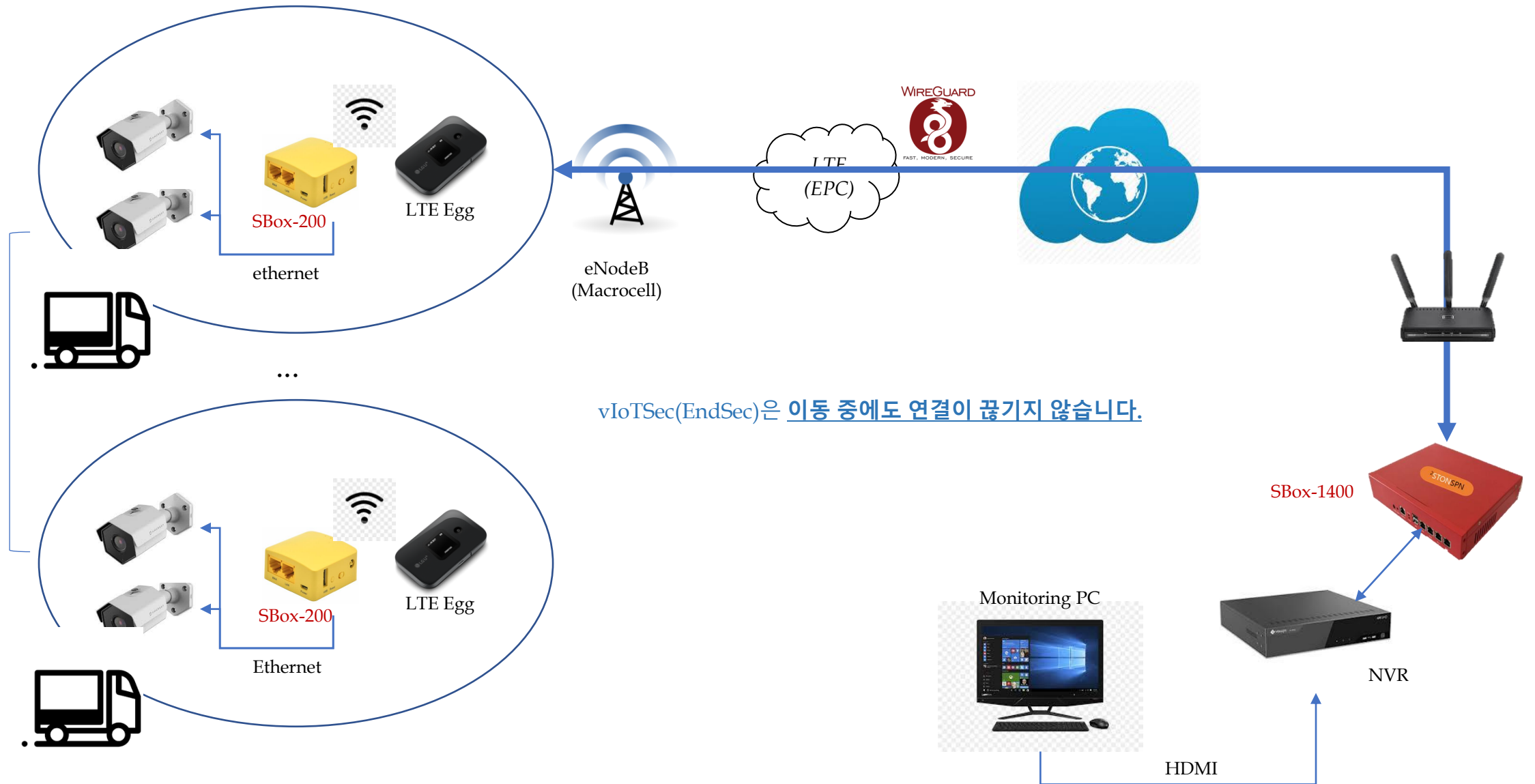
주: 1) 세계 시장은 2010~2019년까지, 한국 시장은 2013년~2020년까지 수치임

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

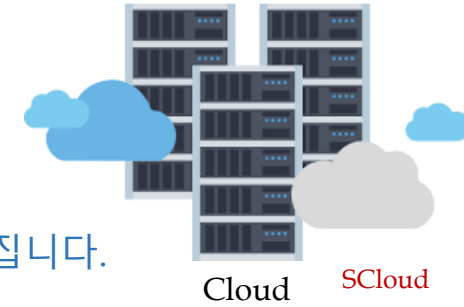
1. IoT Security Market(3) - Video Surveillance



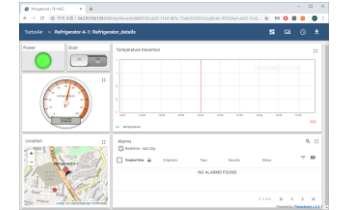
1. IoT Security Market(4) - 24/7 Real-Time Monitoring

vIoTSec(EndSec or P2PSec)을 이용하면 의료용 기기에 대한 안전한 원격 제어가 가능해집니다.

병원 공기살균기/산소발생기

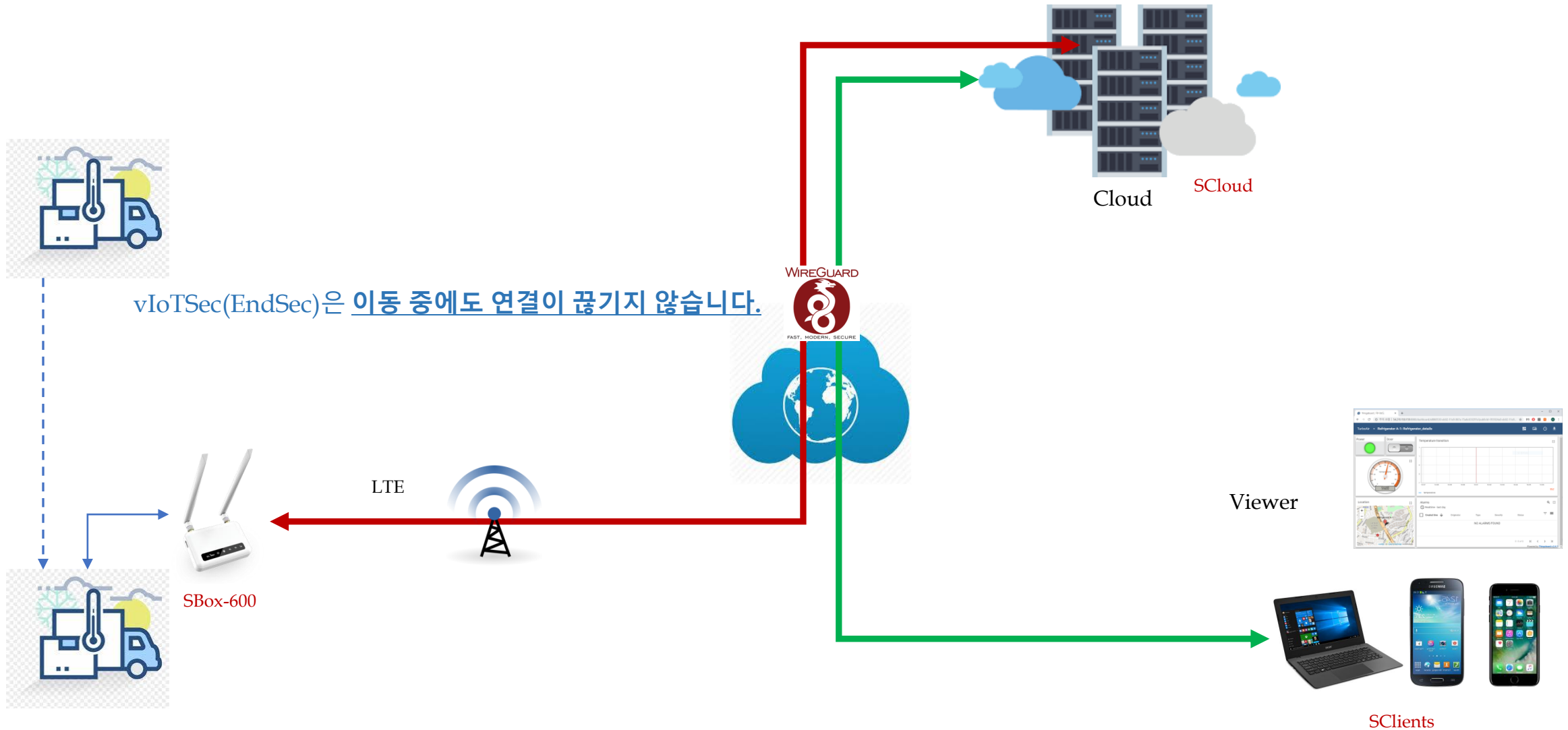


Viewer



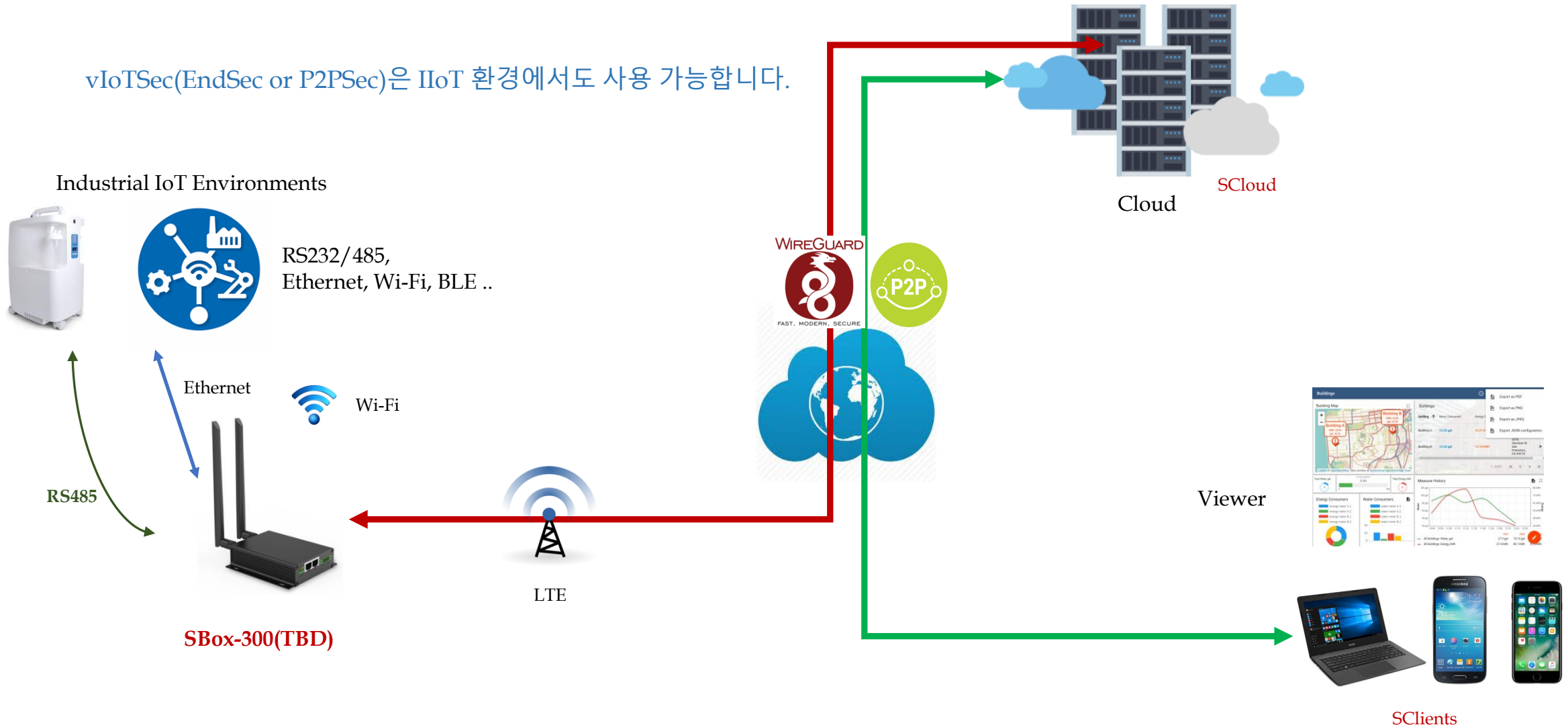
SClients

1. IoT Security Market(5) – ColdChain Security



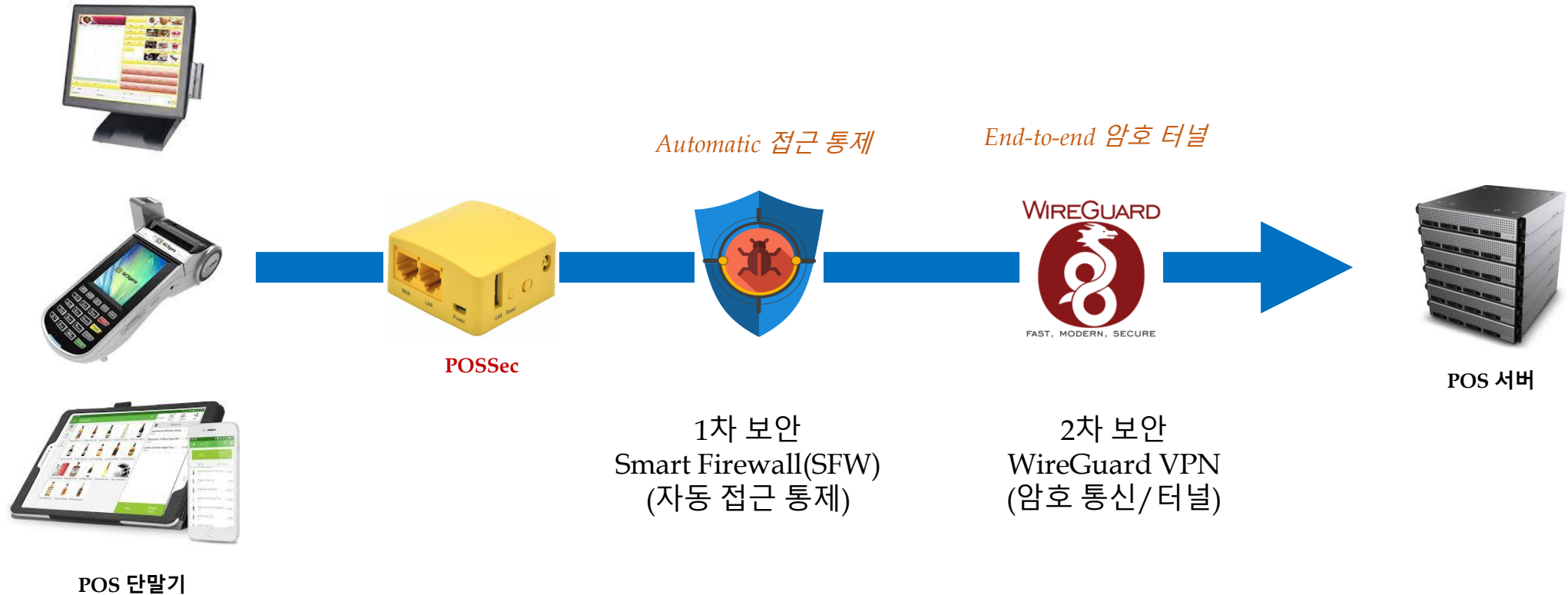
1. IoT Security Market(6) – Industrial IoT Security

vIoTSec(EndSec or P2PSec)은 IIoT 환경에서도 사용 가능합니다.



1. IoT Security Market(7) - POS(Point of Sale) 보안

POSSec은 악의적인 사용자 및 악성 코드로부터 POS 단말을 안전하게 보호해 줍니다.



참고: 2차 보안 기능인 WireGuard VPN을 사용하기 위해서는 POS 서버 앞단에 EndSec 장비가 설치되어 있어야 합니다.

1. IoT Security Market(8) – Our Technology(1)



Target1: Embedded Products(상용제품)



Tiny Gateway w/ IoTSec Engine



Target2: Android/iOS/Windows/macOS

IoTSec Applications



Target 3: Linux Embedded Boards

IoTSec Engine(S/W)

1. IoT Security Market(8) – Our Technology(2)



vIoTSec Technology

1. IoT Security Market(8) – Our Technology(3)

- 1. IoT VPN **EndSec**

- *IP Camera/CCTV 등의 영상을 안전하게 전송하여 보고 싶다면 ...*
- *달리는 기차 위에서도 회사망에 접속해 업무를 보고 싶다면 ...*
- *산업 현장의 IoT 기기(RS485, Wi-Fi, Ethernet, BLE)를 안전하게 원격관리하고 싶다면 ...*

- 2. Peer to Peer VPN **P2PSec**

- *방화벽/공유기 설정 변경 없이 Game을 하거나, 회사 서버에 접속하고 싶다면 ...*

- 3. 재택근무 VPN **OfficeSec**

- *Untact 시대 - 집에 있지만 마치 사무실망에 연결되어 있는 것처럼 하고 싶다면 ...*

- 4. POS 단말 보안 **POSSec**

- *POS 결제 단말을 해킹의 위협으로 부터 보호하고 싶다면 ...*

- 5. 유해 사이트 차단 **KidSec**

- *각종 유해한 인터넷 사이트로 부터 우리 아이를 안전하게 보호하고 싶다면 ...*

2. IoT VPN **EndSec** (Powered by WireGuard)



2. EndSec(1) – End to End Security



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



임의의 디바이스를 쉽고 안전하게 연결하고 보호할 수 있어야 함(Easy Connectivity)



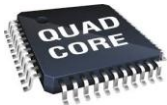
실시간 성능을 보장하기 위해 빠른 전송 속도를 보장해야 함(High Speed)



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

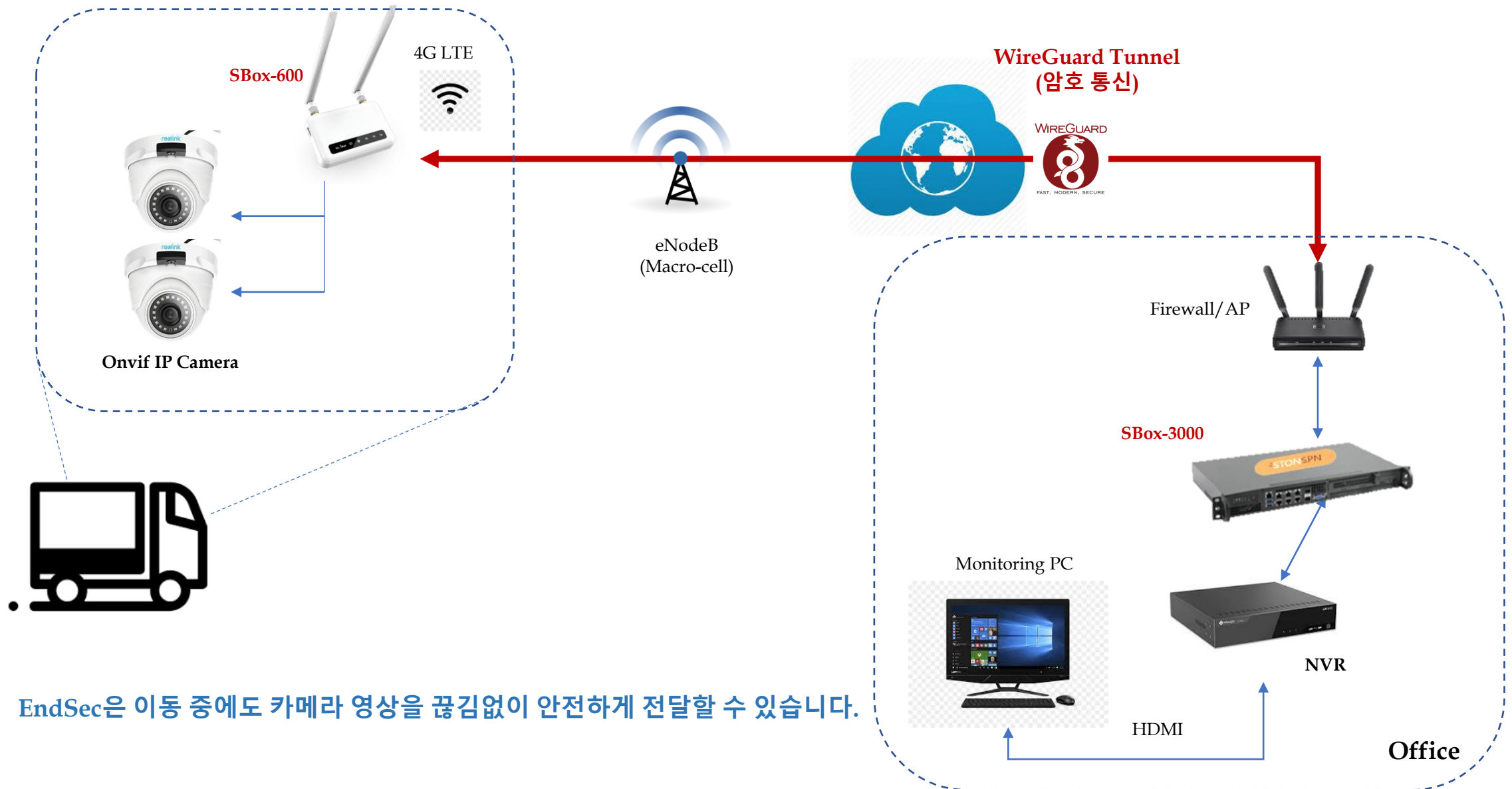


데이터 전송이 필요 없는 경우, 어떠한 패킷도 내 보내지 말아야 함(Stealth Mode)

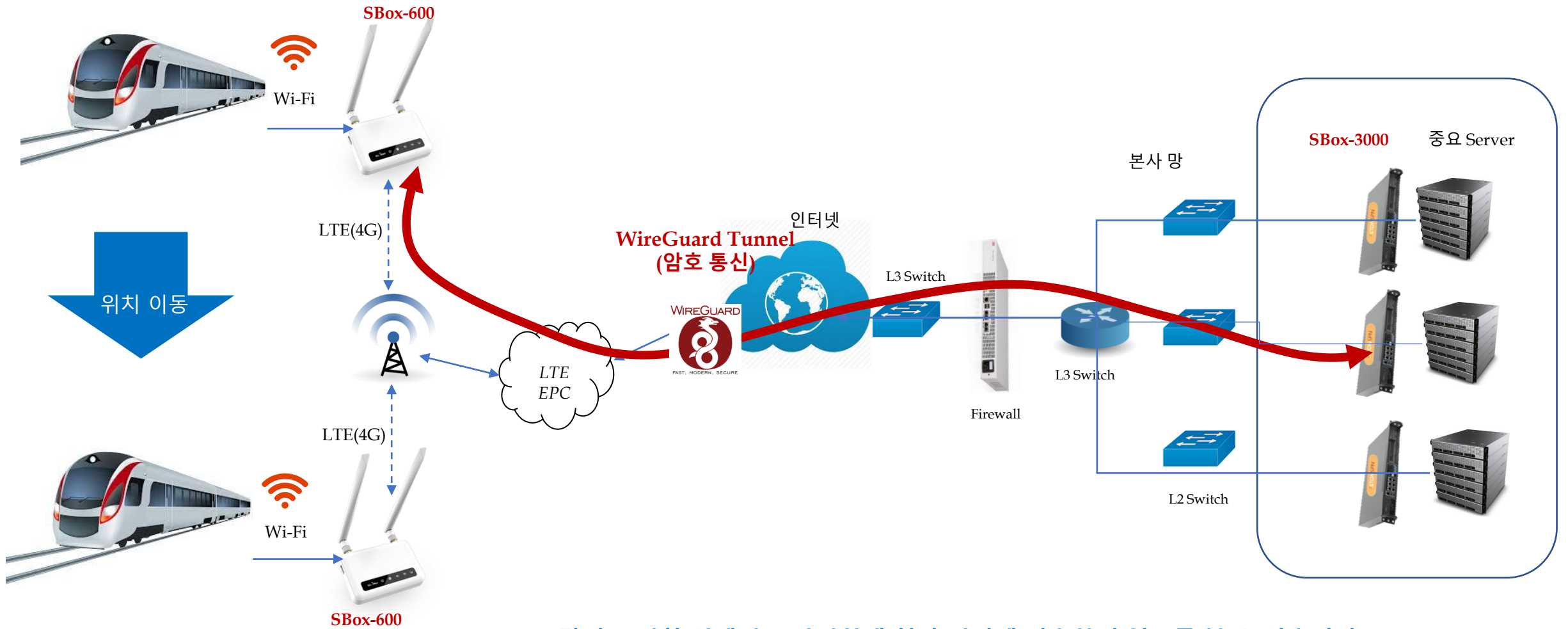


CPU 사용에 있어 최적화되어 있어야 함(CPU Optimization)

2. EndSec(2) – IP Camera Security

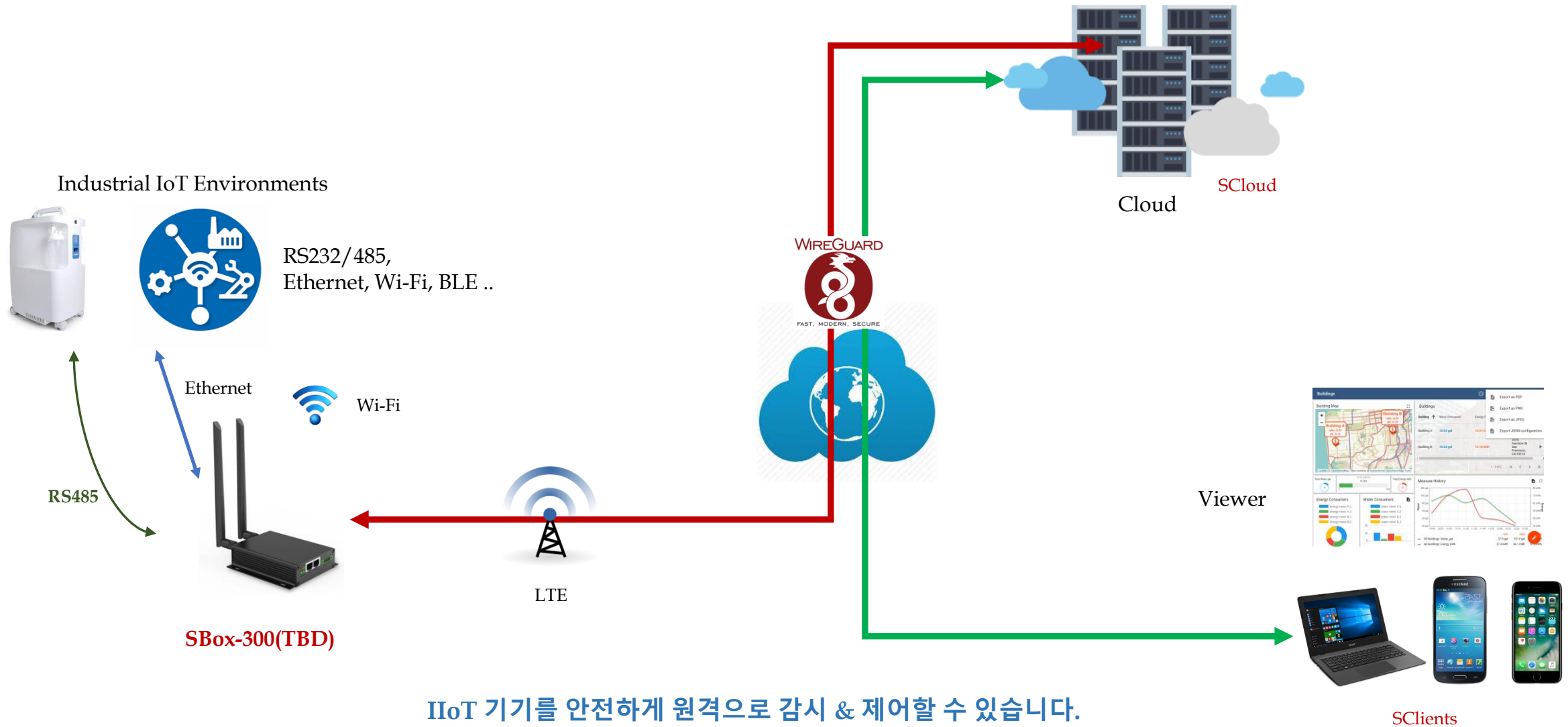


2. EndSec(3) - LTE Security



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

2. EndSec(4) – Industrial IoT Security



2. EndSec(5) - POS 결제 보안

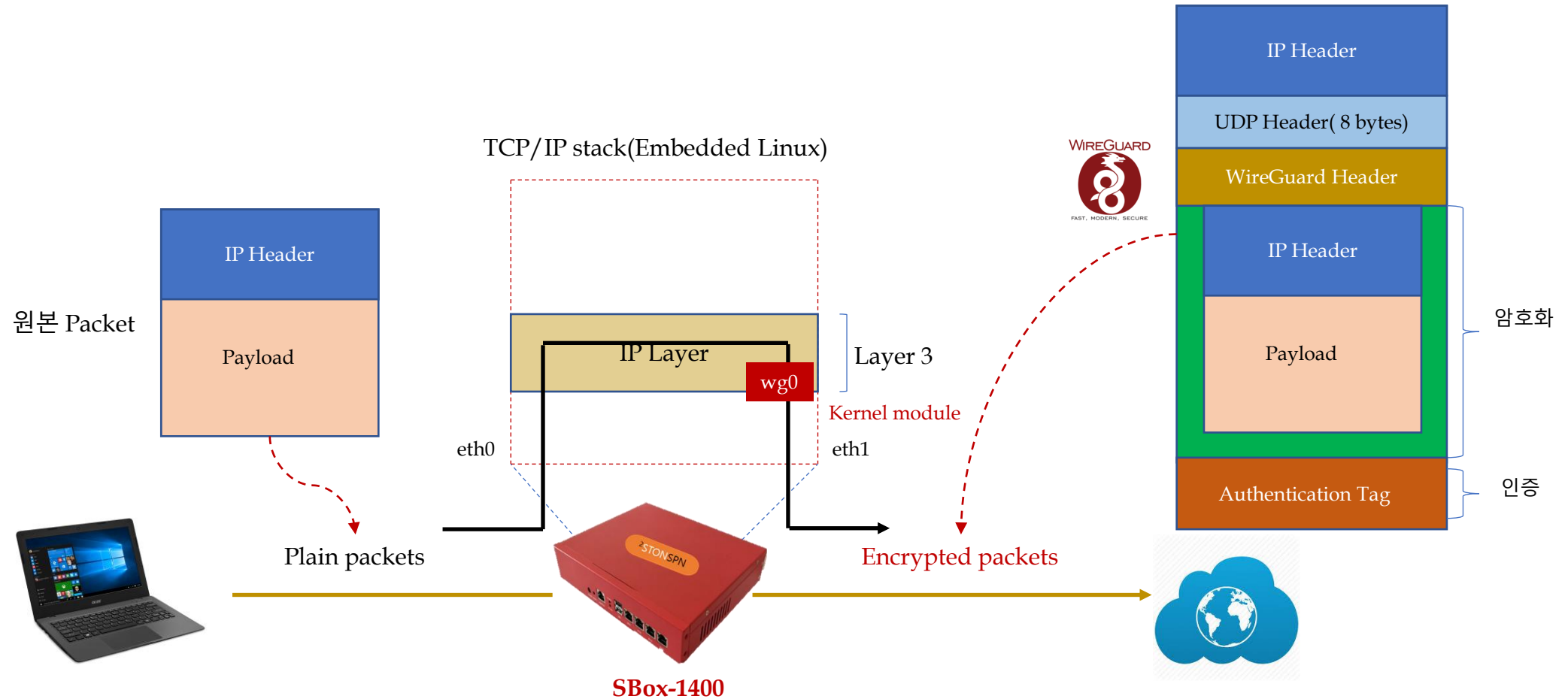
단말 Library 변경 필요

서버 IP 변경 필요



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

2. EndSec(6) – WireGuard(L3) Tunnel(1)



2. EndSec(6) – WireGuard(L3) Tunnel(2)

| 보안 알고리즘 | 상세 내용 |
|-------------------------|--|
| Key 교환 방식 및 상호 인증 | <p>NoiseIK handshake 방식, Curve25519(타원곡선 알고리즘)</p> <ul style="list-style-type: none">▪ ECDH(Diffie-Hellman)의 변형된 형태(NoiseIK handshake 방식)▪ Public key(32 byte)를 교환한 후, 이를 통해 안전하게 shared secret를 생성하는 방식▪ 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 <p>Hash 알고리즘</p> <ul style="list-style-type: none">▪ BLAKE2s - fast secure hashing 알고리즘▪ SHA series 보다 빠름. 즉 MD5 수준임. |
| 암호 알고리즘 | <p>ChaCha20 - 256 bit stream cipher(20 round cipher Salsa20 기반)</p> <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 | <p>Poly1305 - message authentication code 알고리즘(16 byte output 생성)</p> |

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

2. EndSec(7) - 소형 SBox(Access Point)

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

SBox-200(W/Y)



SBox
(유무선 Access Point 방식)



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



2. EndSec(8) - 중형 SBox & SClients

SBox-1400

SBox-3000

WebUI

CLI

SBox
중형 Security Gateway

WireGuard
FAST, MODERN, SECURE

SiOS

SAndroid

SWindows

SClient S/W

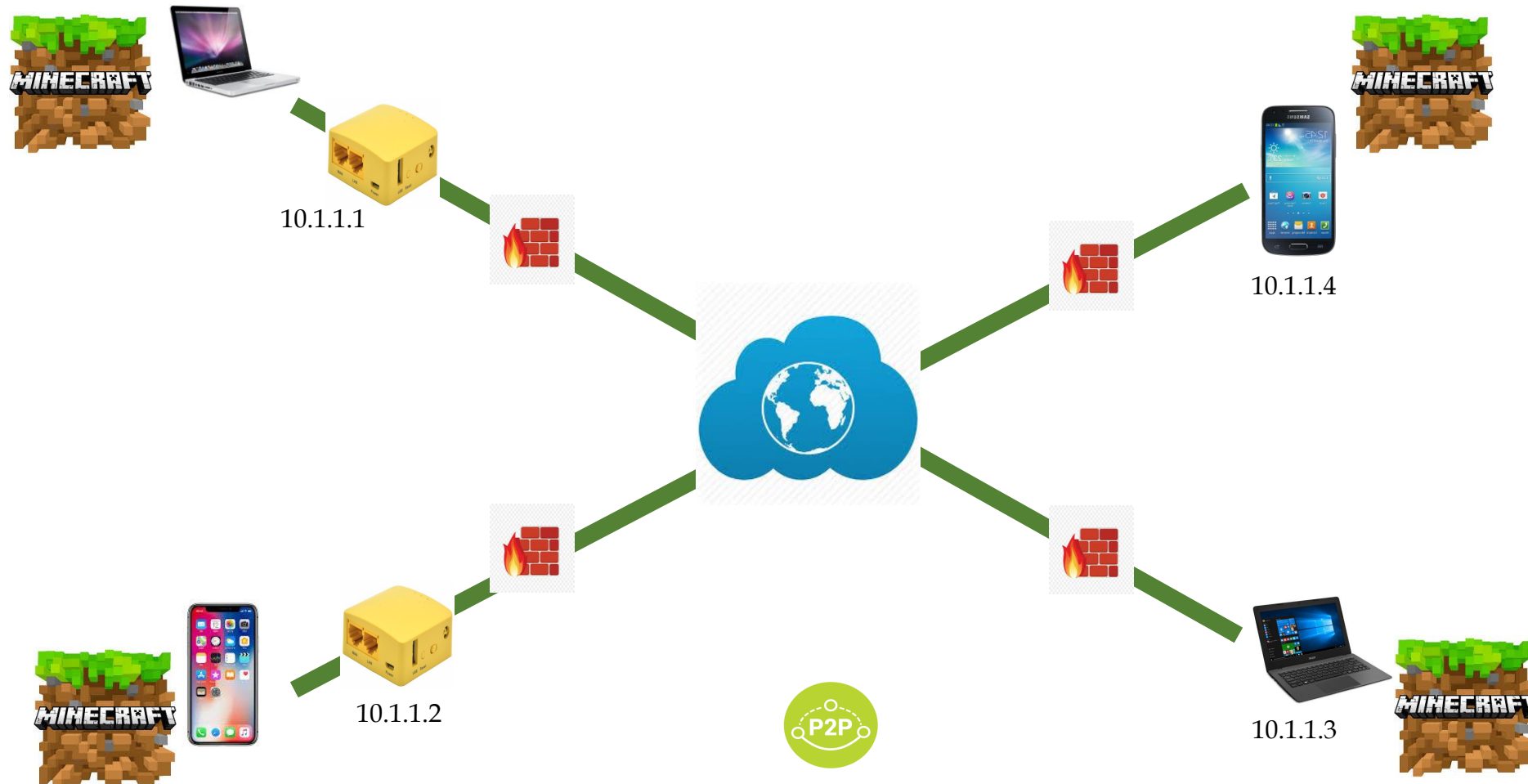
The diagram illustrates the components and interfaces of the EndSec(8) medium SBox and SClients. On the left, two hardware units are shown: the SBox-1400 (red) and the SBox-3000 (black). The SBox-3000 is labeled as a '중형 Security Gateway' (Medium Security Gateway). In the center, the WebUI interface is displayed, showing the 'SPN' section with 'L3 SPN' and 'Local Info' tabs. Below the WebUI, the CLI interface is shown with a list of commands and their descriptions. To the right, three client interfaces are shown: SiOS (iOS), SAndroid (Android), and SWindows (Windows). The SWindows interface shows a '2StonSPN - OnvifIPCam' window with a 'Reconnect' button and a 'Show Logs' button. The SAndroid interface shows a '2StonSPN' window with a 'START' button. The SiOS interface shows a 'SPN Tunnels' window with a 'Demo_Cam' button. The WireGuard logo is also present, indicating its use in the system.

3. Peer to Peer VPN **P2P**Sec



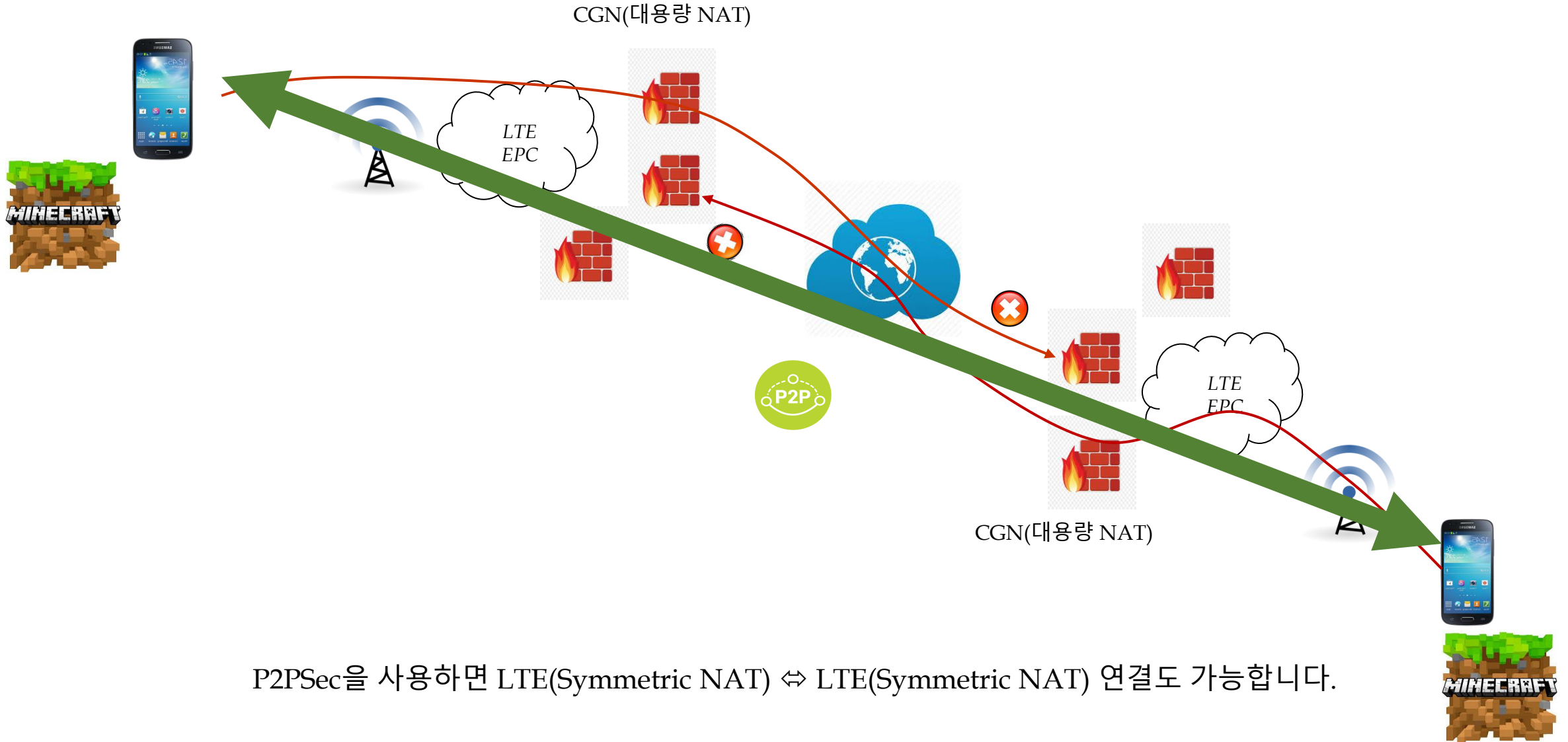
3. P2PSec(1) – Peer to Peer VPN(1)

P2PSec을 사용하면 방화벽/공유기 설정 변경 없이 Game이 가능합니다.

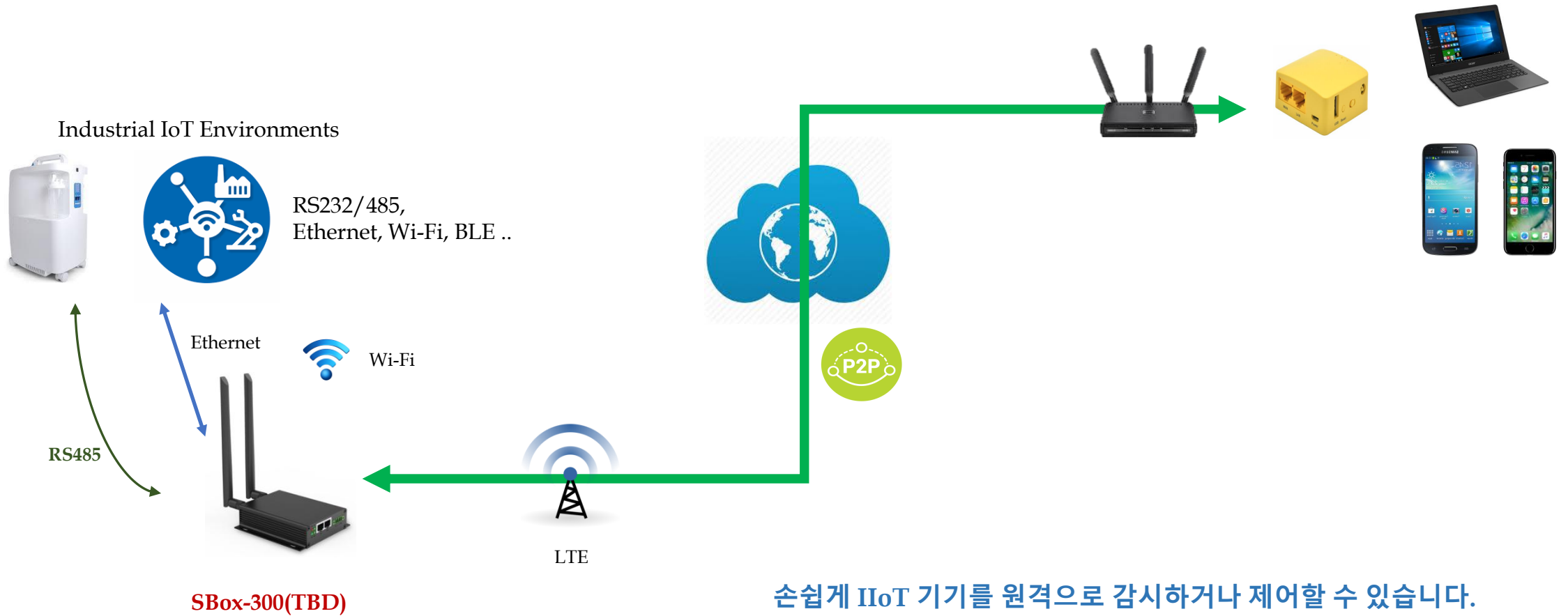


Securely Connect Any Device, Anywhere !

3. P2PSec(1) – Peer to Peer VPN(2)



3. P2PSec(1) – Peer to Peer VPN(3)

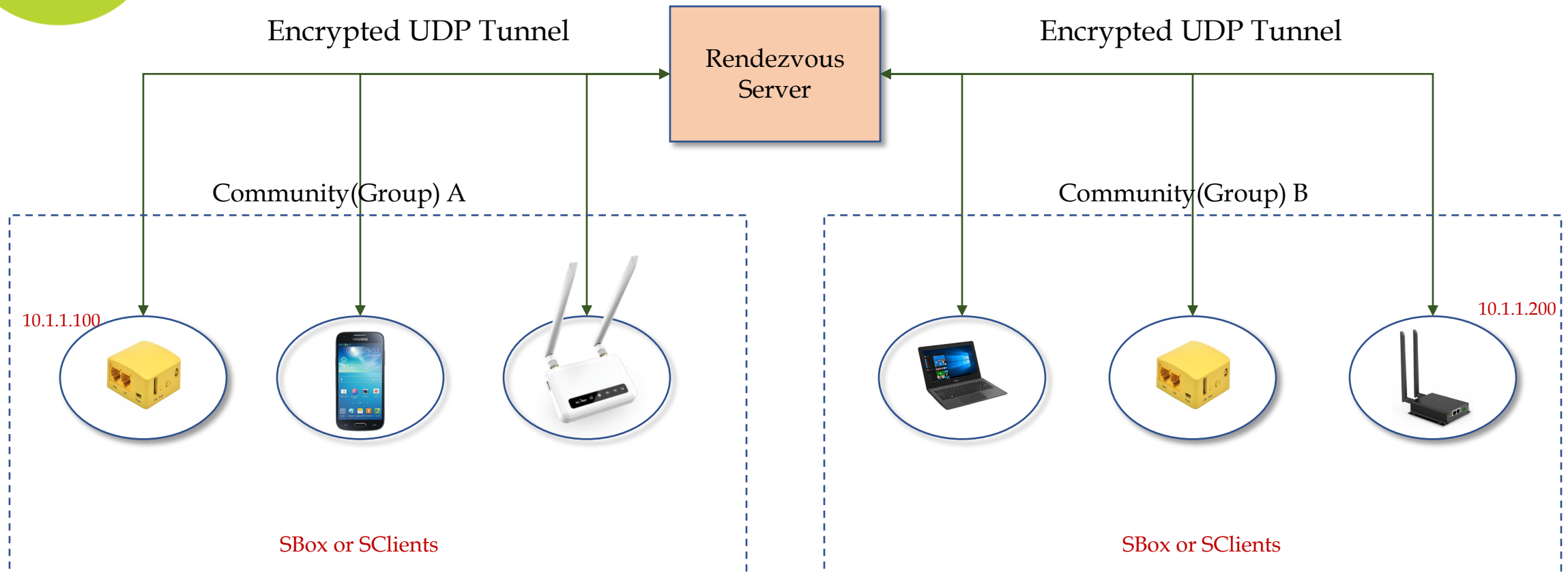


3. P2PSec(2) – Architecture(1)



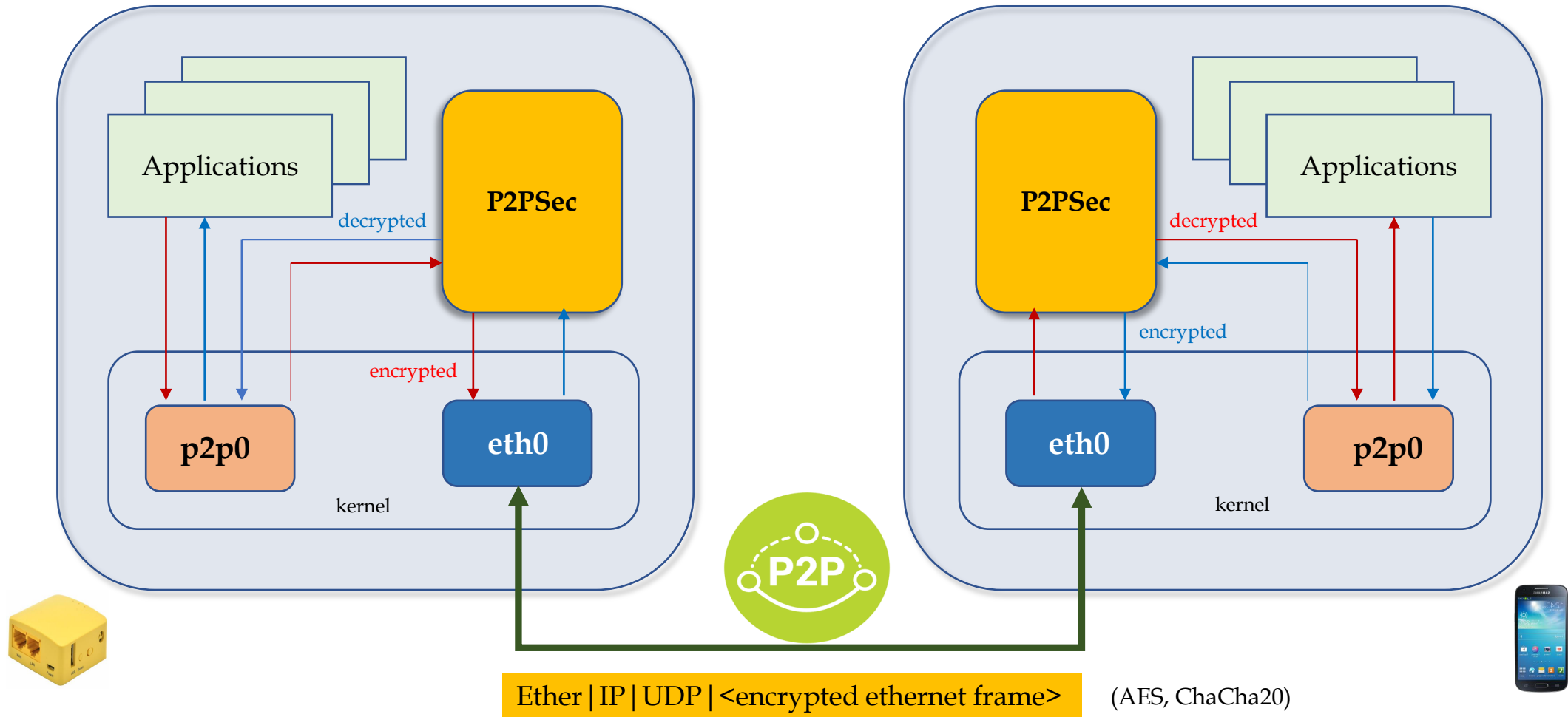
P2PSec은 복수개의 Peer(SBox or SClients)와 Rendezvous Server(중앙 서버)로 이루어져 있습니다.

- P2PSec Tunnel을 이용할 경우, 더 이상 Firewall에서 Port Forwarding 설정을 해 줄 필요가 없습니다.



3. P2PSec(2) – Architecture(2)

P2PSec은 Tap device를 사용하여 암호 통신을 하는 방식입니다. 따라서 기존 Application은 하나도 수정할 필요가 없습니다.



3. P2PSec(3) - 소형 SBox(Access Point) and SClients



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

SBox-200(W/Y)



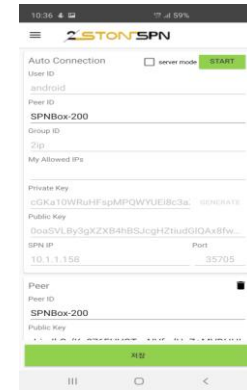
SBox-300

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



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

SBox-600



SAndroid

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

- 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 빅배치 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 더는면 시가침다"

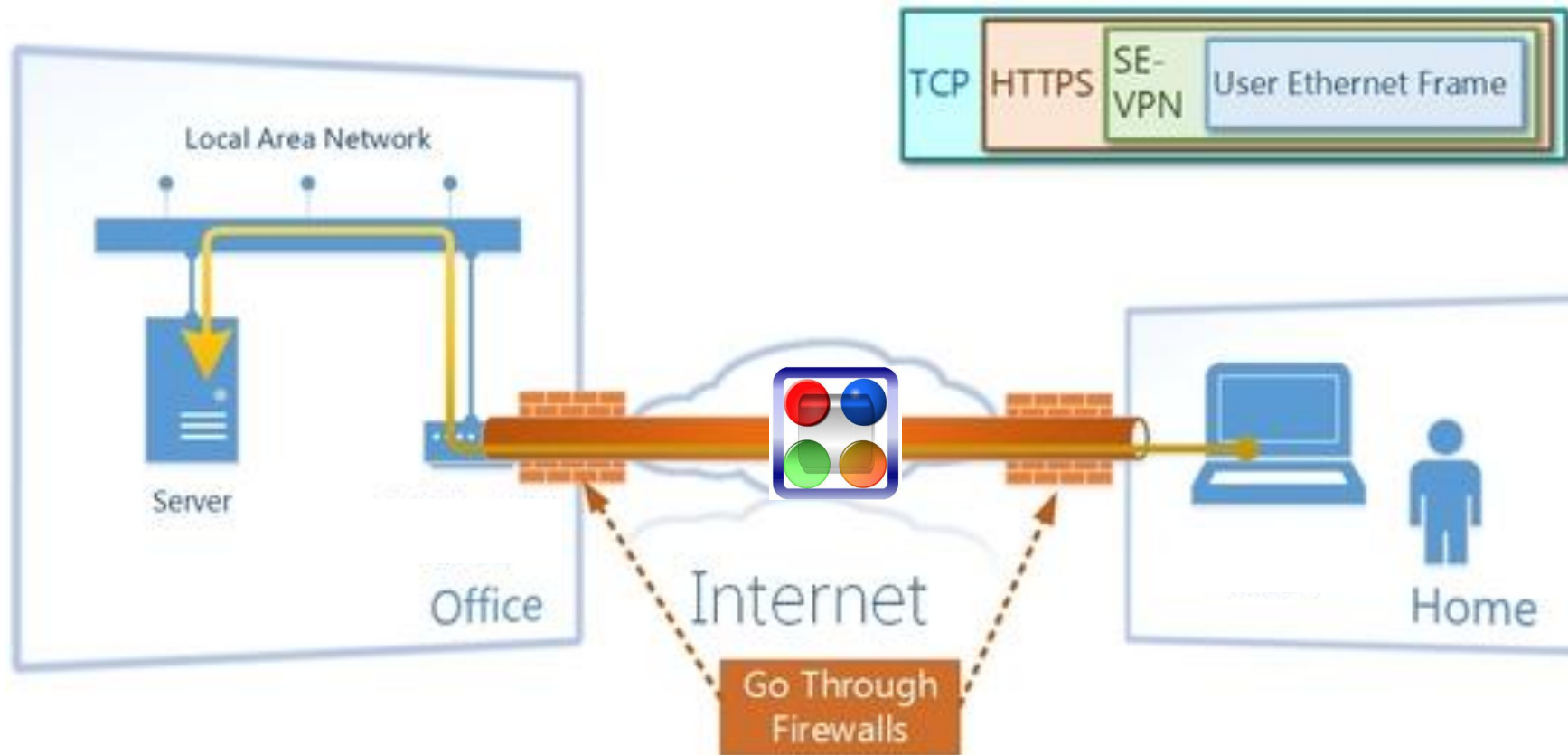
4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(2)

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)

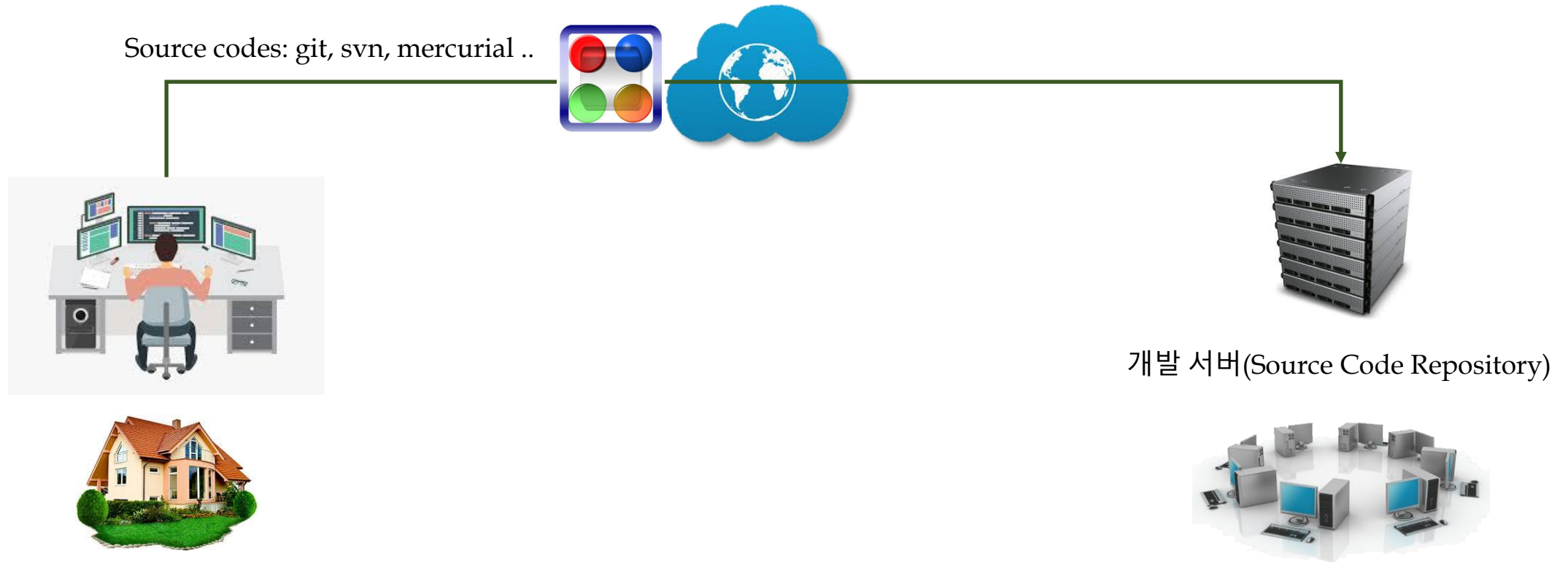


OfficeSec은 아주 긴 LAN 케이블을 회사 망에 연결한 것과 동일한 효과를 만들어 줍니다.

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

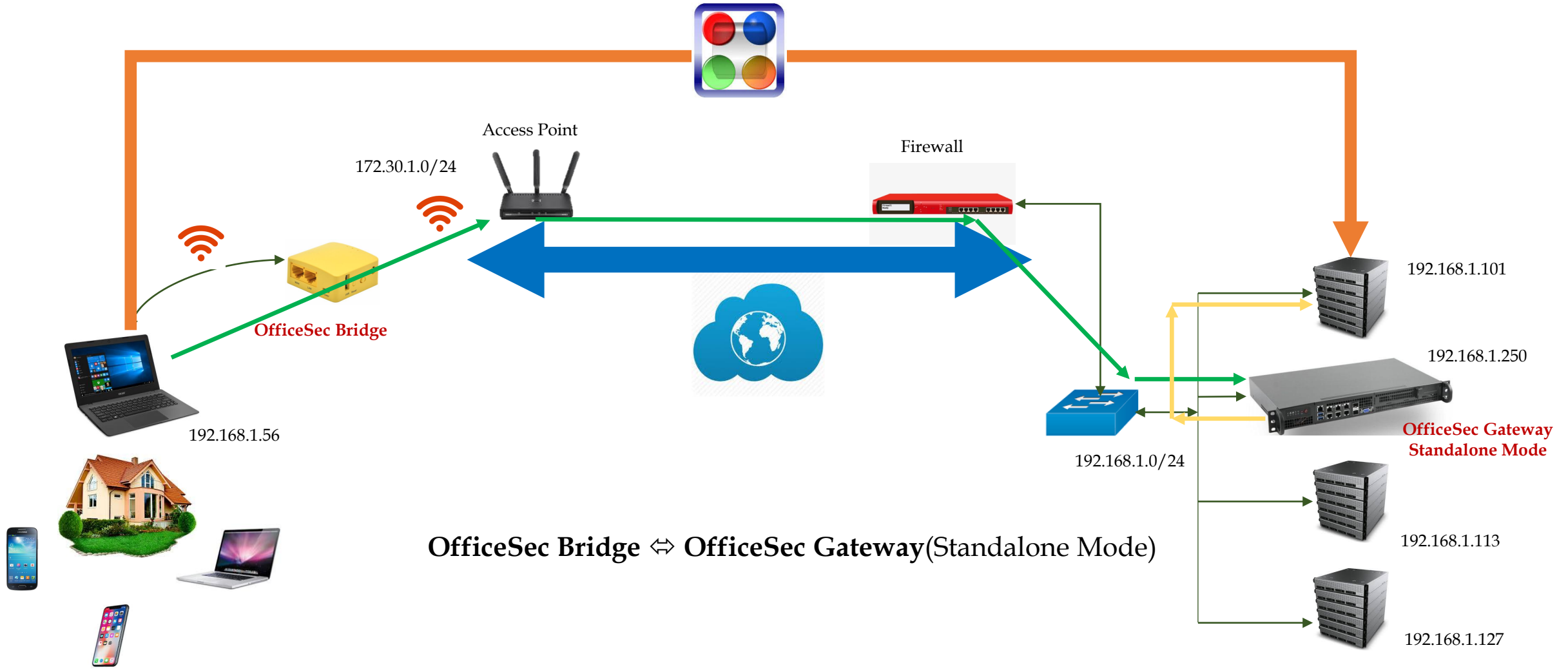


4. OfficeSec(1) - CORONA19 확산과 재택근무 확대(5)



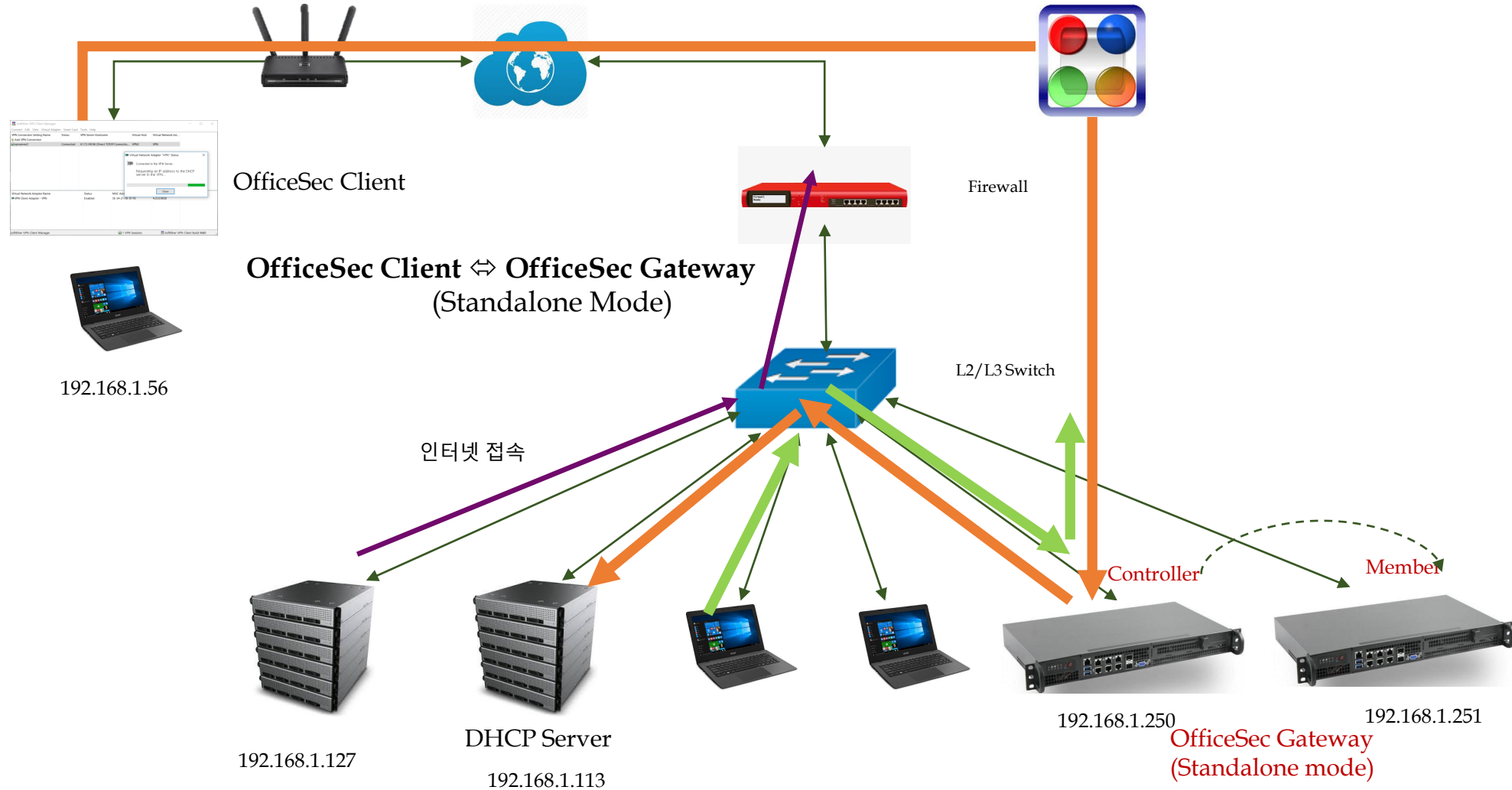
개발자에게 가장 필요한 것은 자신이 개발한 source code를 안전하게 서버에 올리는 일일 것입니다.

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



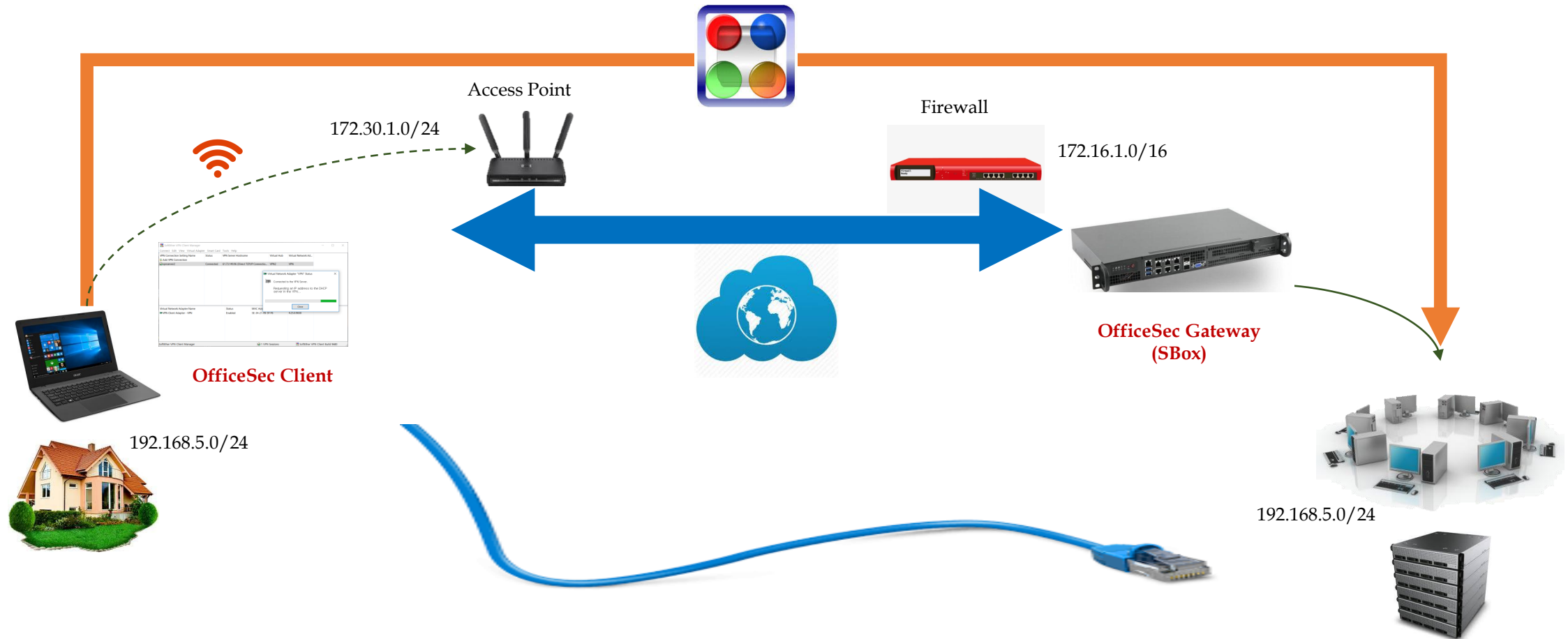
OfficeSec Gateway Standalone mode를 이용하시면 사무실 망 구성을 전혀 변경하실 필요가 없습니다.

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



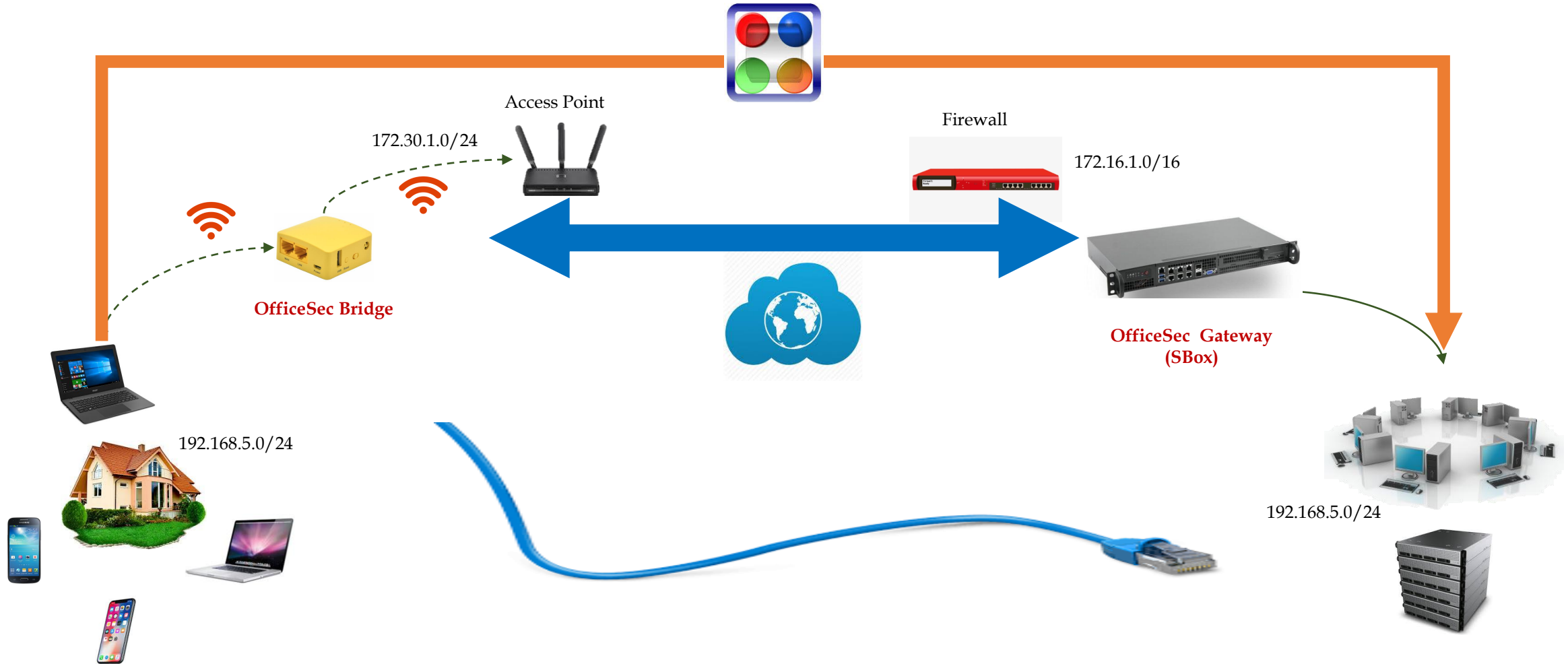
OfficeSec Gateway Standalone mode를 이용하시면 사무실 망 구성을 전혀 변경하실 필요가 없습니다.

4. OfficeSec(3) - Client & Gateway 구성



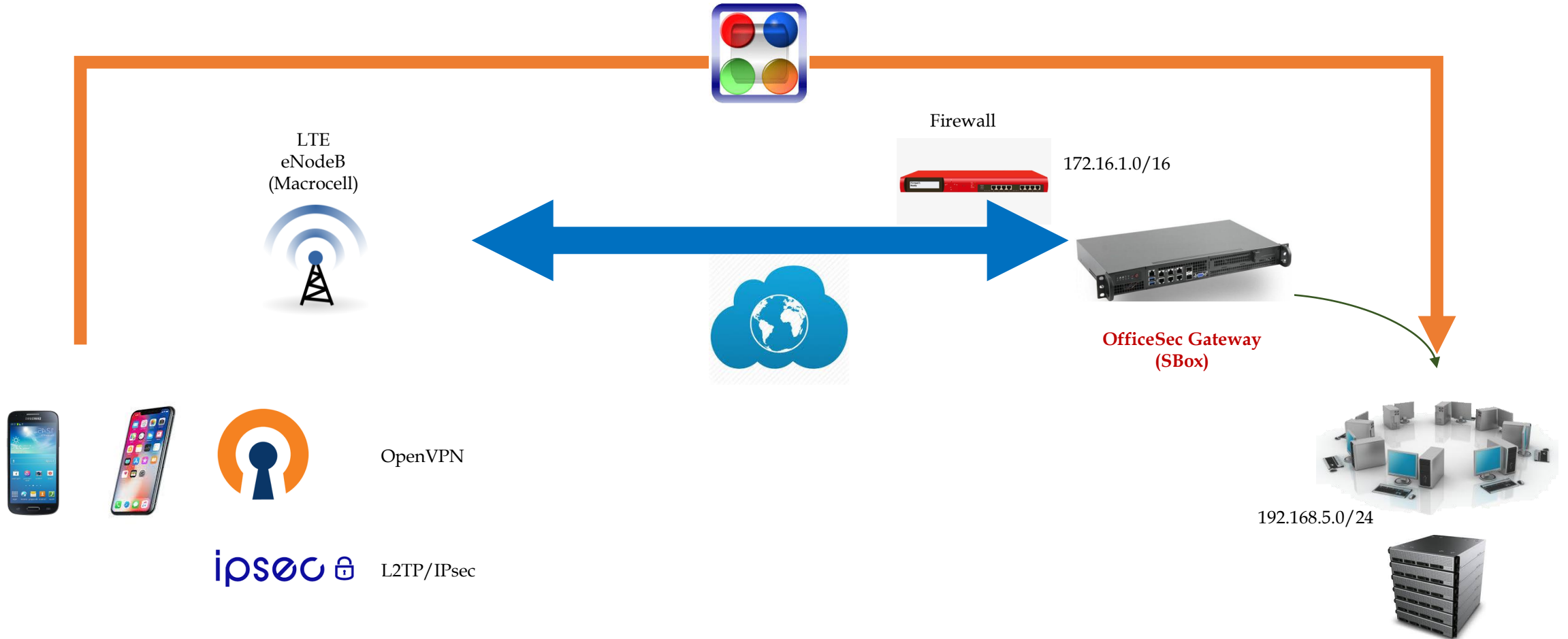
OfficeSec은 아주 긴 LAN 케이블을 회사 망에 연결한 것과 동일한 효과를 만들어 줍니다.

4. OfficeSec(4) - Bridge & Gateway 구성



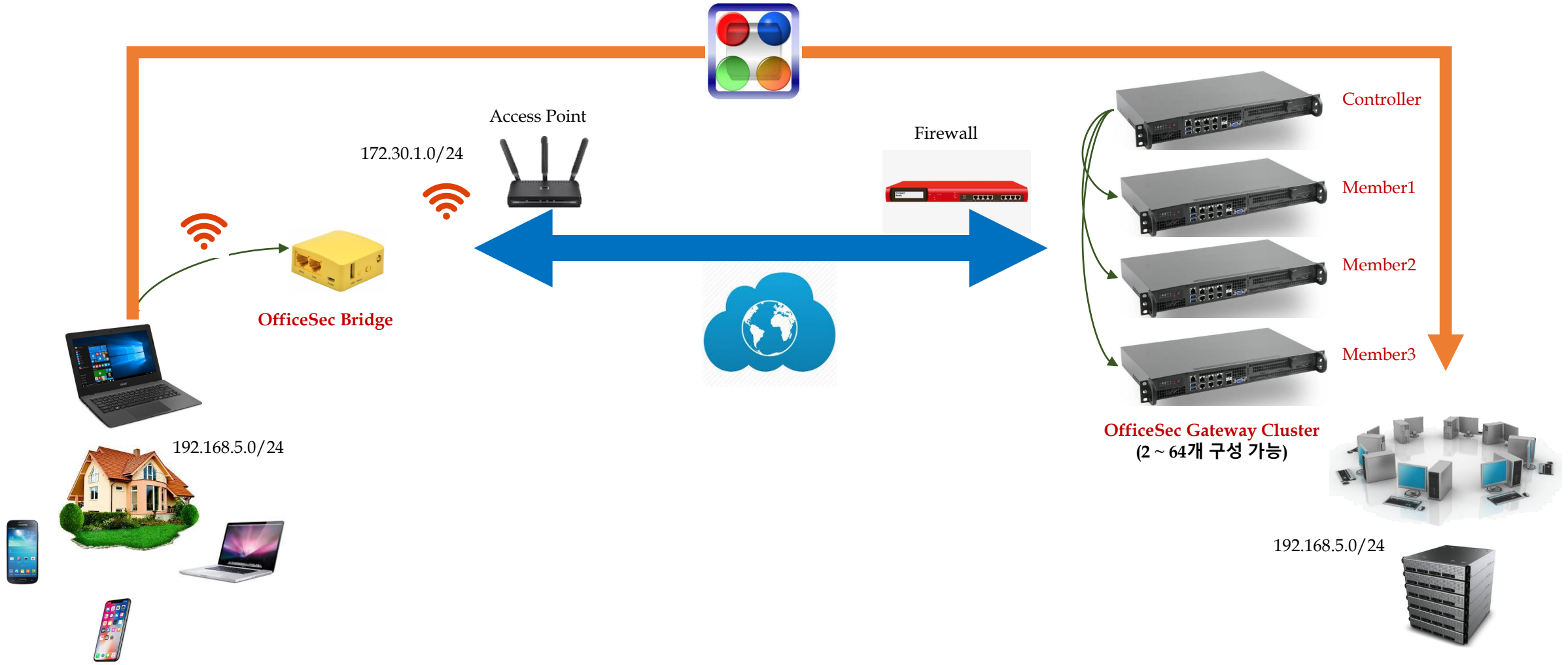
OfficeSec Bridge를 이용하면 3~4개의 네트워크 장치(Notebook, Smart Phone ..)를 동시에 사용할 수 있습니다.

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



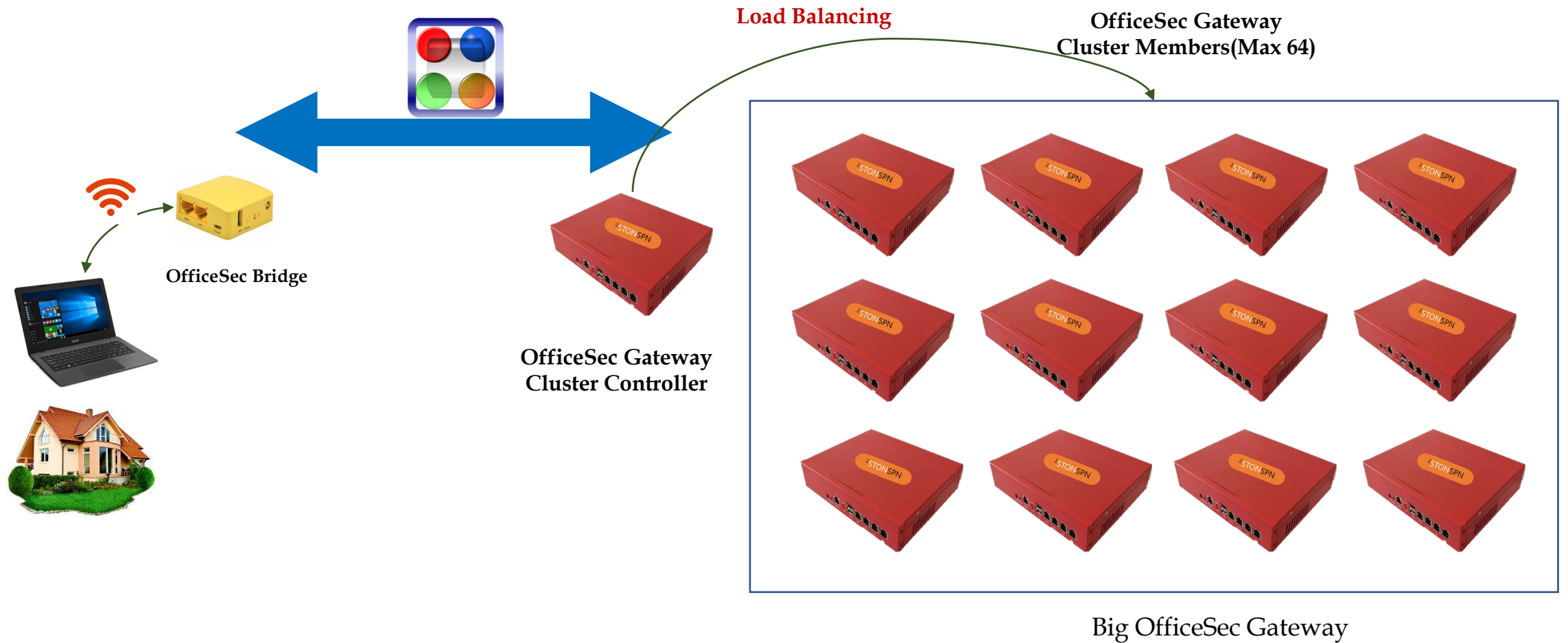
OpenVPN or L2TP/IPsec app을 이용하면 Smart Phone에서 LTE 망을 통해 사내 망에 접근할 수 있습니다.

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



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

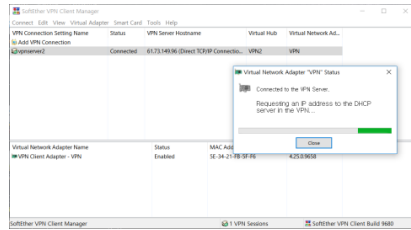
4. OfficeSec(6) - Bridge & Cluster 구성(2)



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]



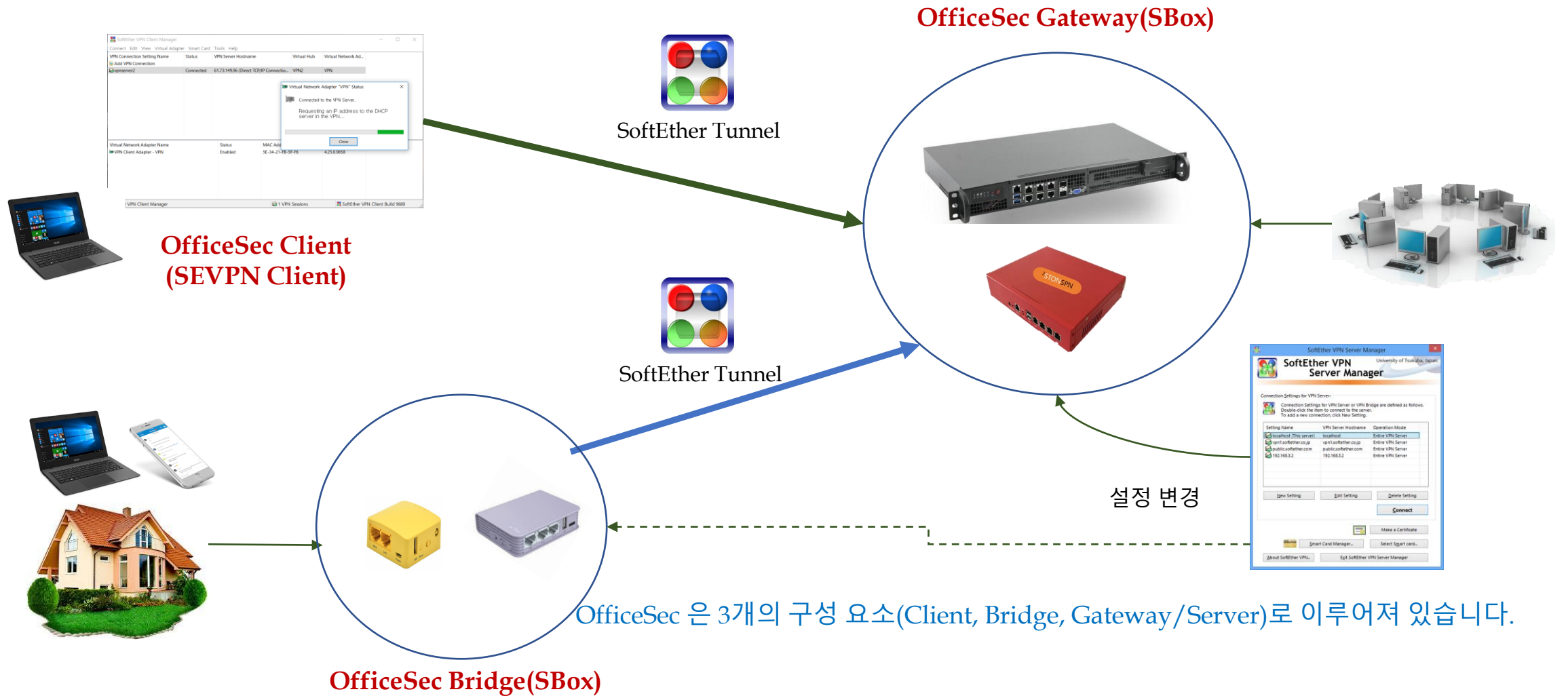
Tunnel 20~30개 처리



OfficeSec Gateway
(a.k.a SBox)

Tunnel 5~10개 처리

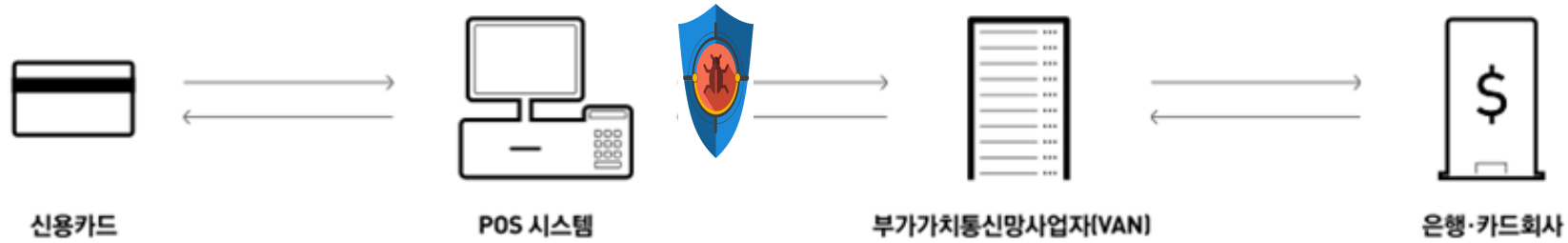
4. OfficeSec(7) - 제품 구성(2)



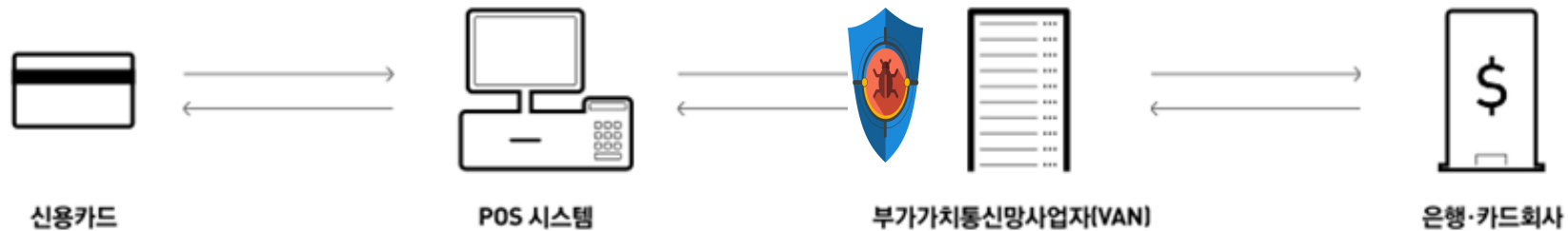
5. POS 단말 보안 **POSSec**



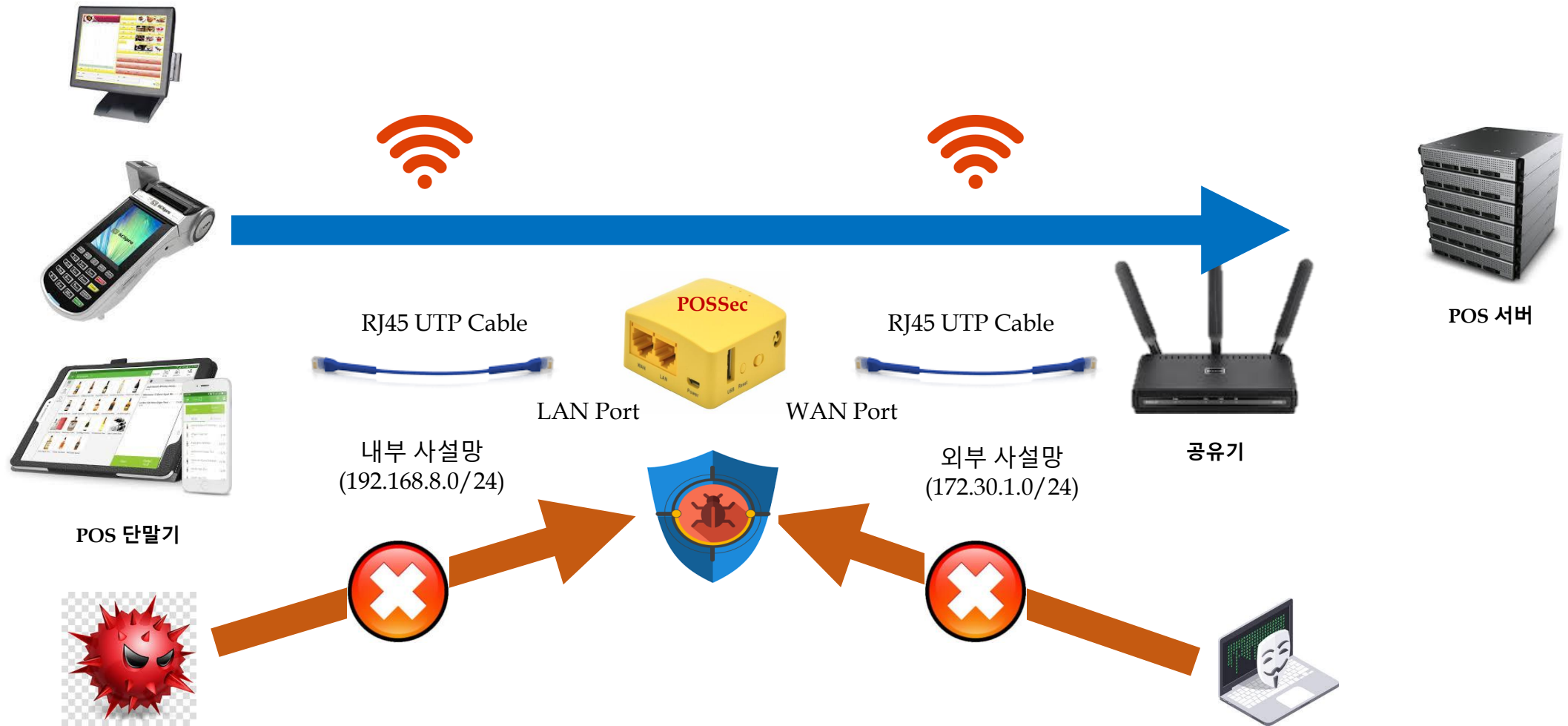
5. POSec(1)



- 1) 다양한 OS 지원, 급변하는 신종 공격, 백신 설치가 불가능한 환경 → Network 차단 방식의 필요성 !
- 2) POS 서버(목적지 주소 & Port)로 향하는 트래픽을 제외한 모든 Route를 차단/통제 해야 함.
→ 악성 코드 유입 및 확산 원천 봉쇄
- 3) 이 모든 것은 자동으로 이루어져야 함.



5. POSSec(2) - 네트워크 구성

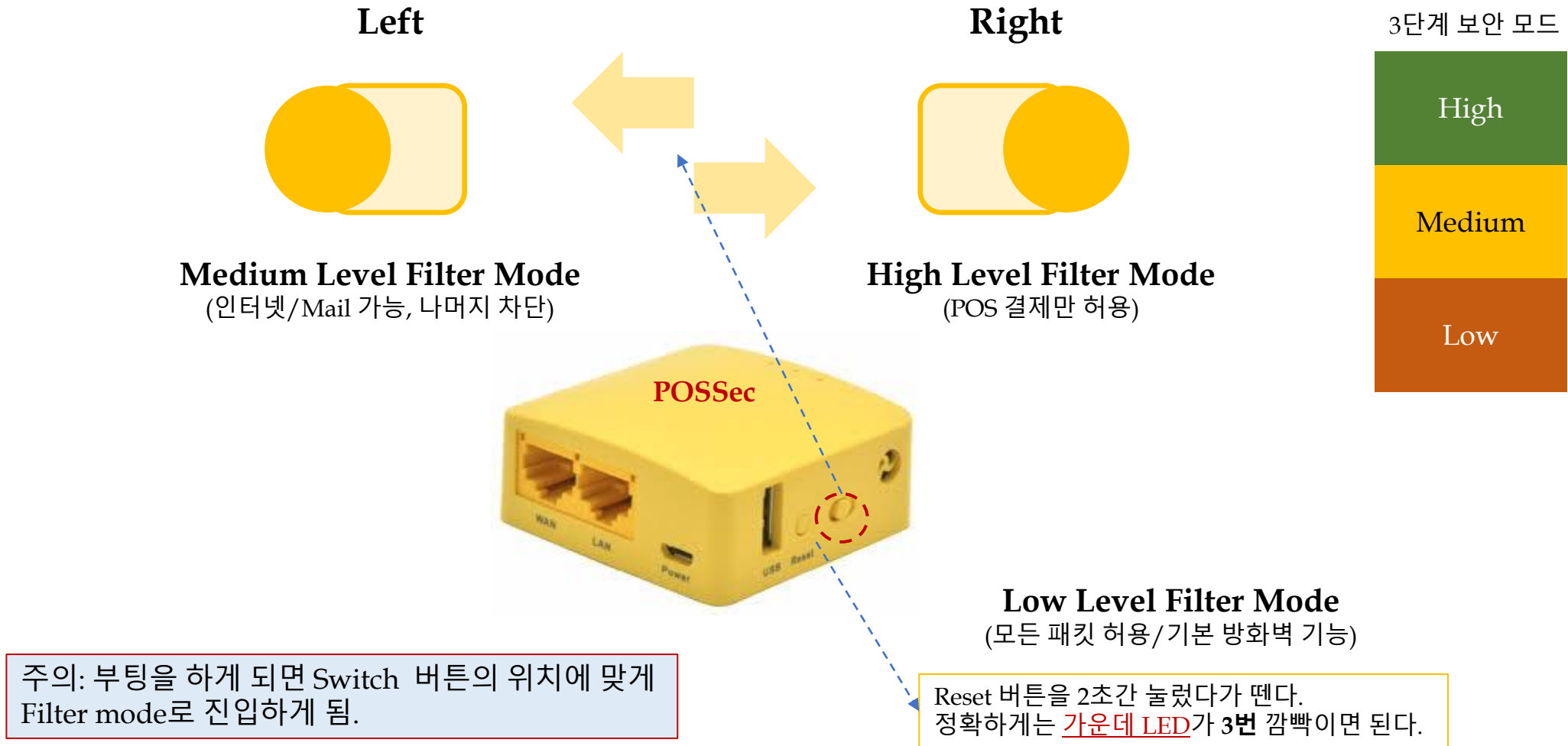


5. POSec(3) - 개통 절차

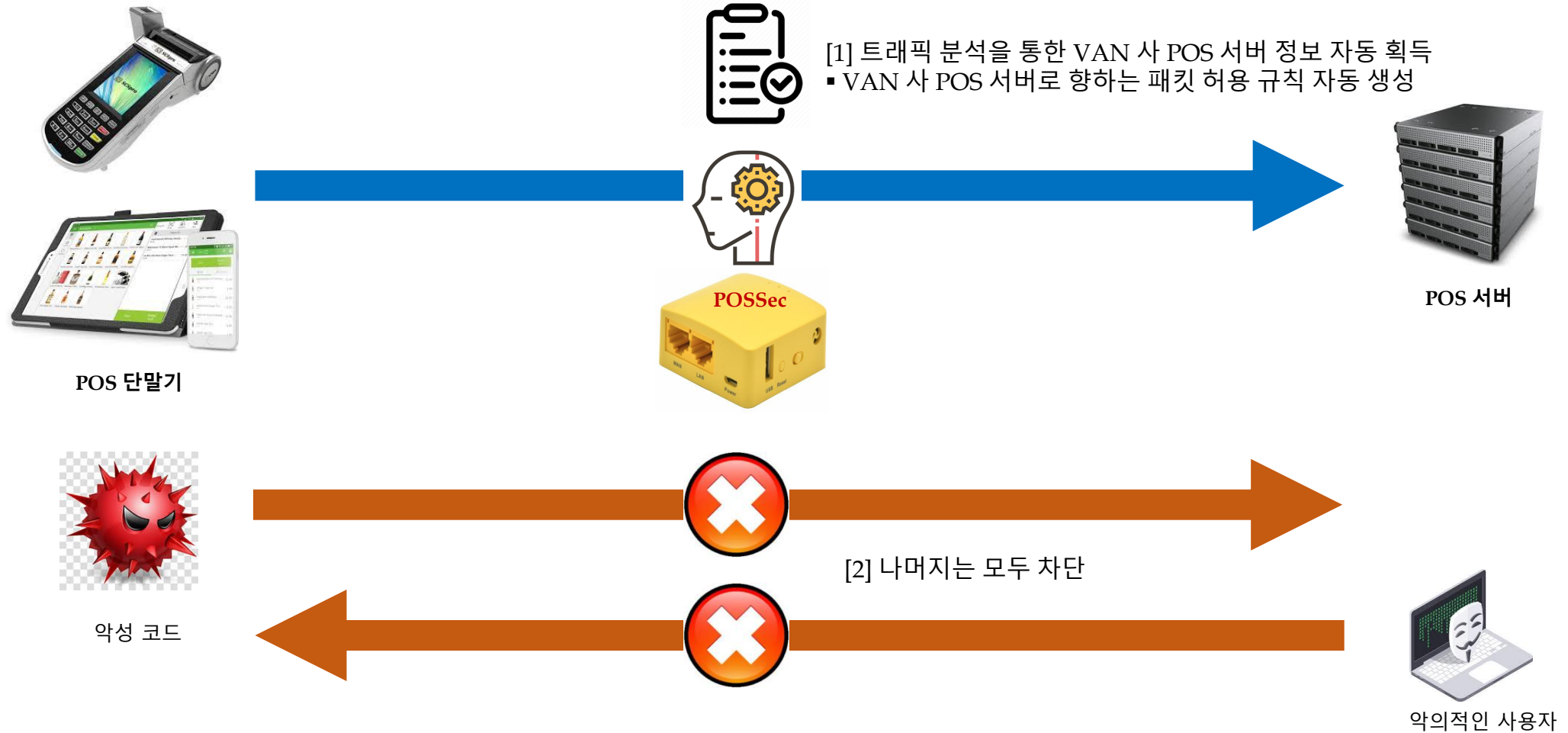


1. POSec에 LAN Cable을 연결하고 전원을 넣는다.
2. POS 단말기의 전원을 켜다(혹은 재 부팅한다). 주의: POS-GUARD가 켜져 있는 상태에서 POS 단말이 켜져야 IP 획득에 문제가 없다.
3. 개통: **30분 이내에 테스트 결제를 한 차례 진행한다.** 참고: 이 시간 동안에 외부 접속(예: 정산, 발주 관련)이 필요한 부분이 있다면 최대한 연결 시험을 해 본다.
4. POSec은 자동으로 서버 연결 정보를 확보한 후, **POS 서버로의 연결을 제외한 내/외부로 부터의 모든 공격을 차단한다.**
5. 이후 안심하고 POS 단말기를 사용하여 결제를 진행한다. **30분이면 충분합니다.**

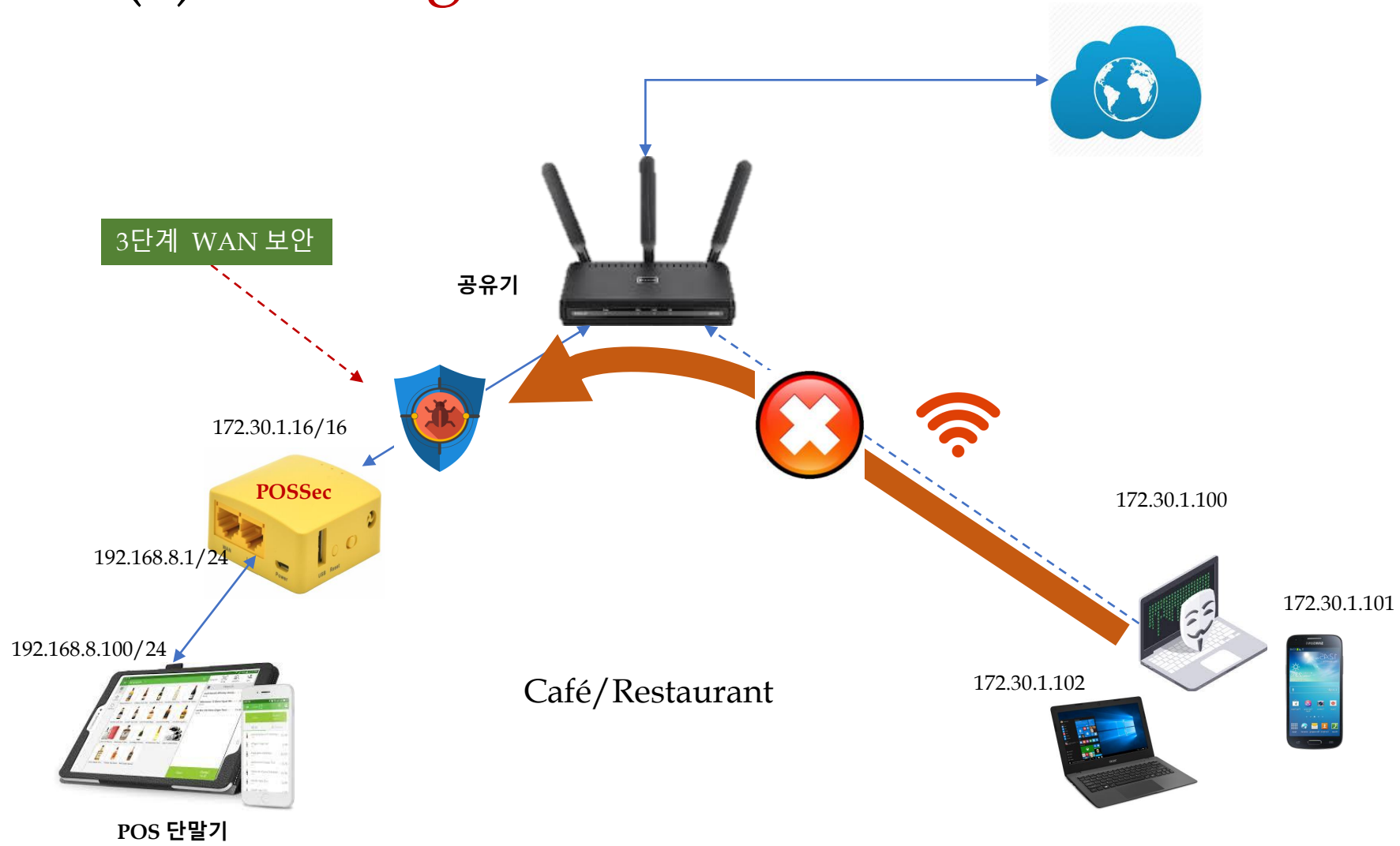
5. POSSec(4) - 3단계 보안 모드



5. POSSec(5) – Auto IP Filter

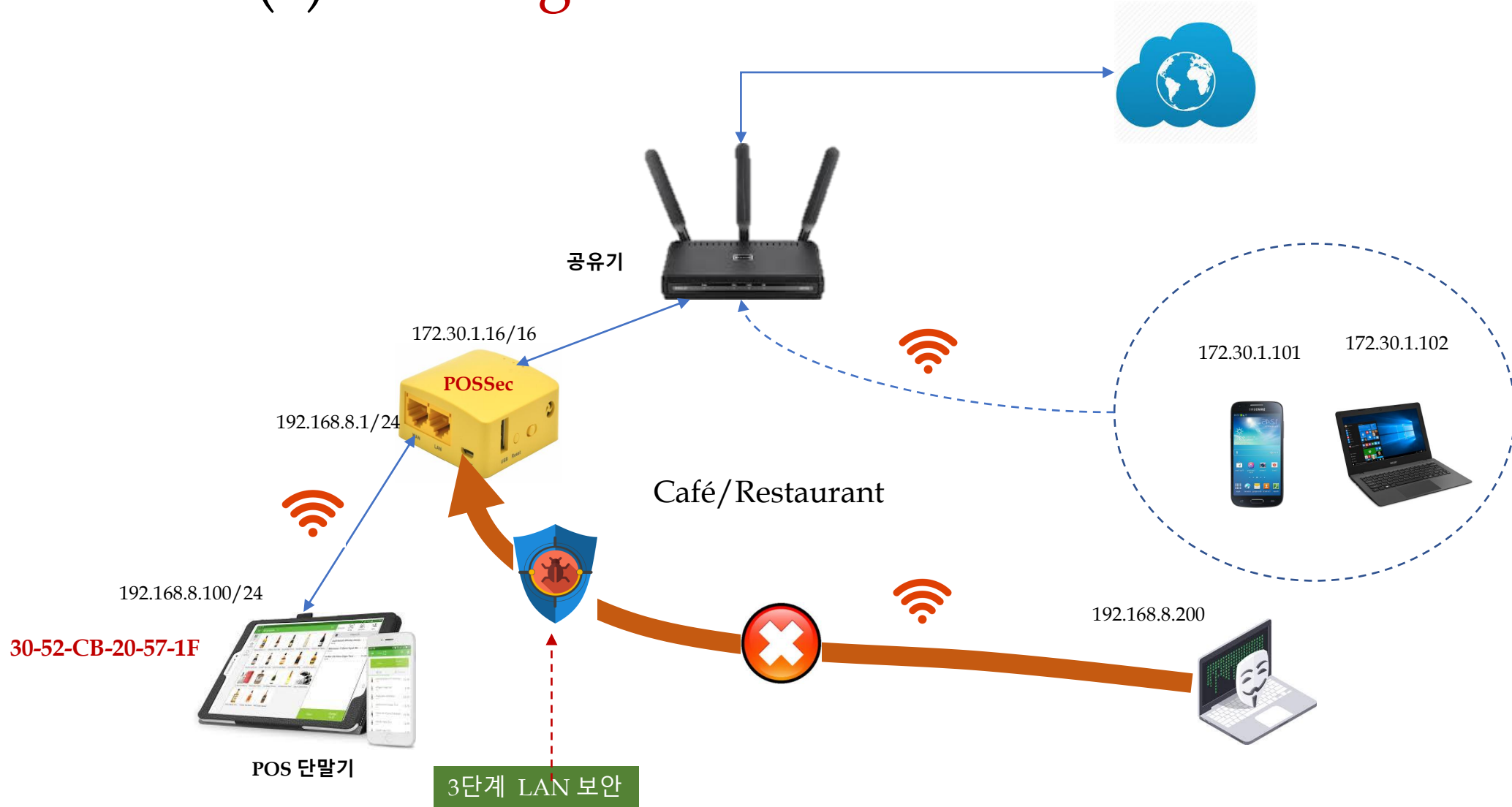


5. POSec(6) - Strong WAN 보안



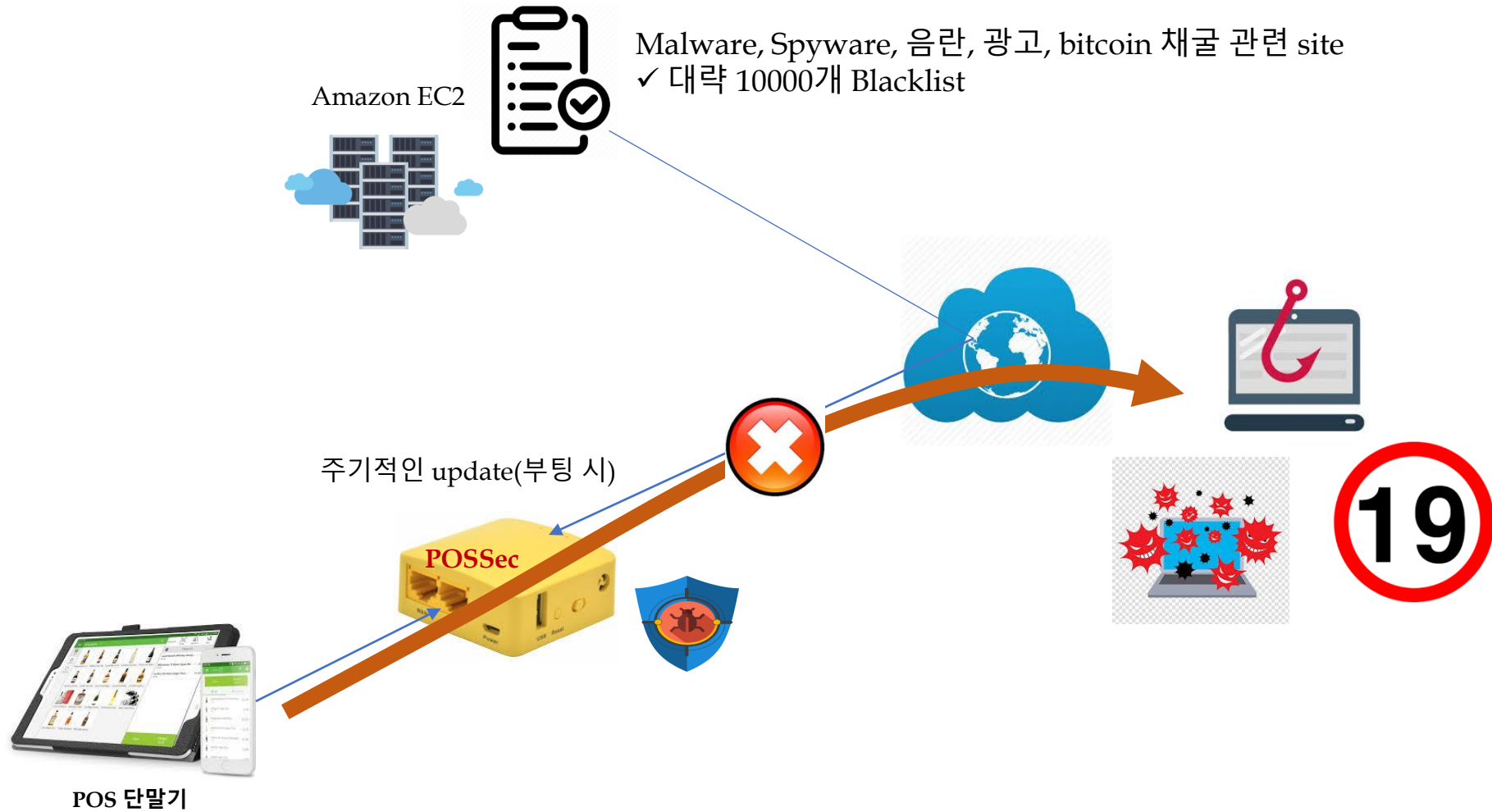
POSec은 공유기에 연결된 외부 공격자로 부터의 해킹 시도를 자동으로 차단(원천 봉쇄)합니다.

5. POSSec(7) - Strong LAN 보안



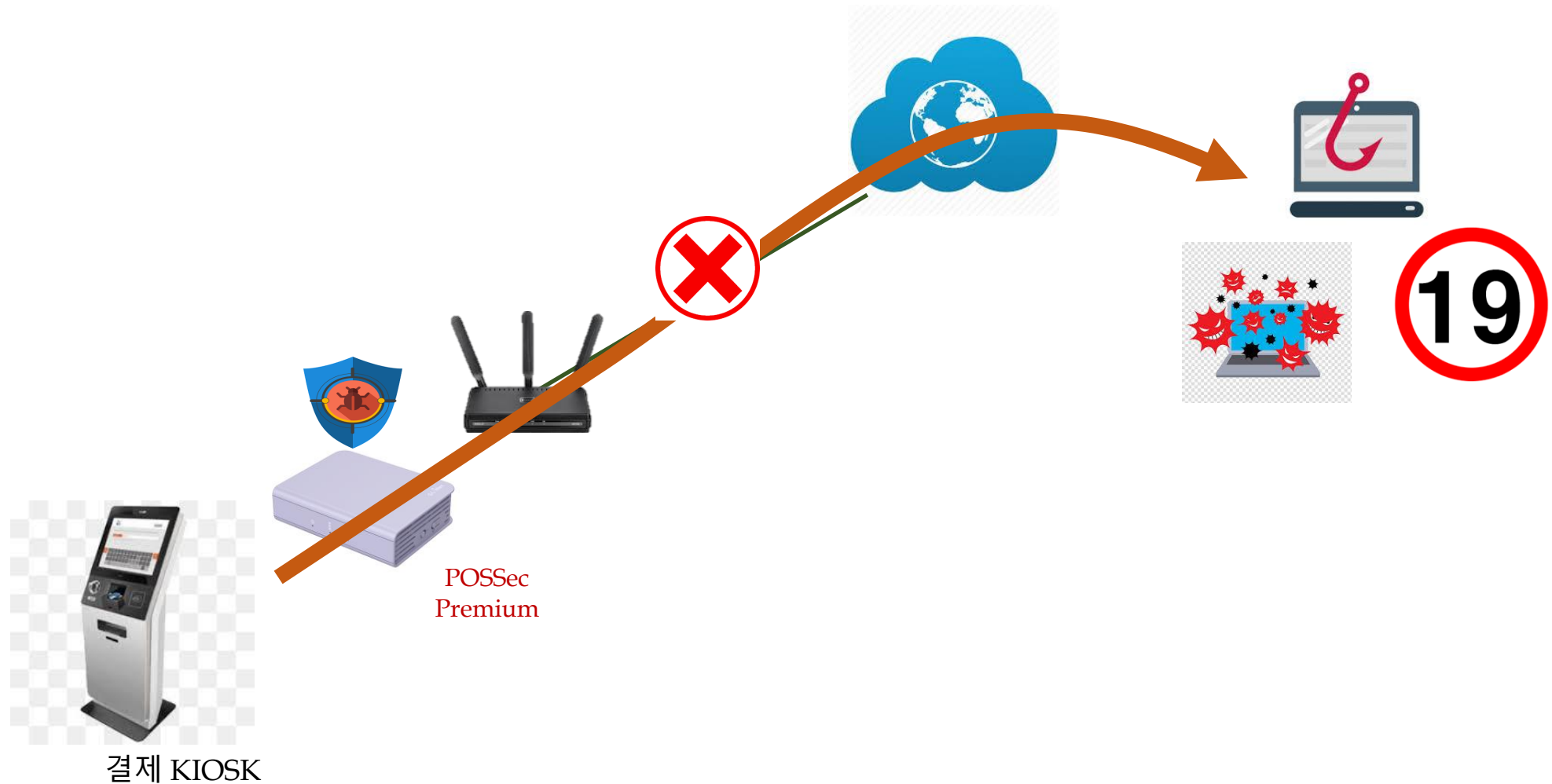
POSSec은 악의적인 사용자가 POSSec(LAN 포트)에 접속하려는 것으로 자동으로 차단합니다.

5. POSSec(8) – DNS Filter(1)

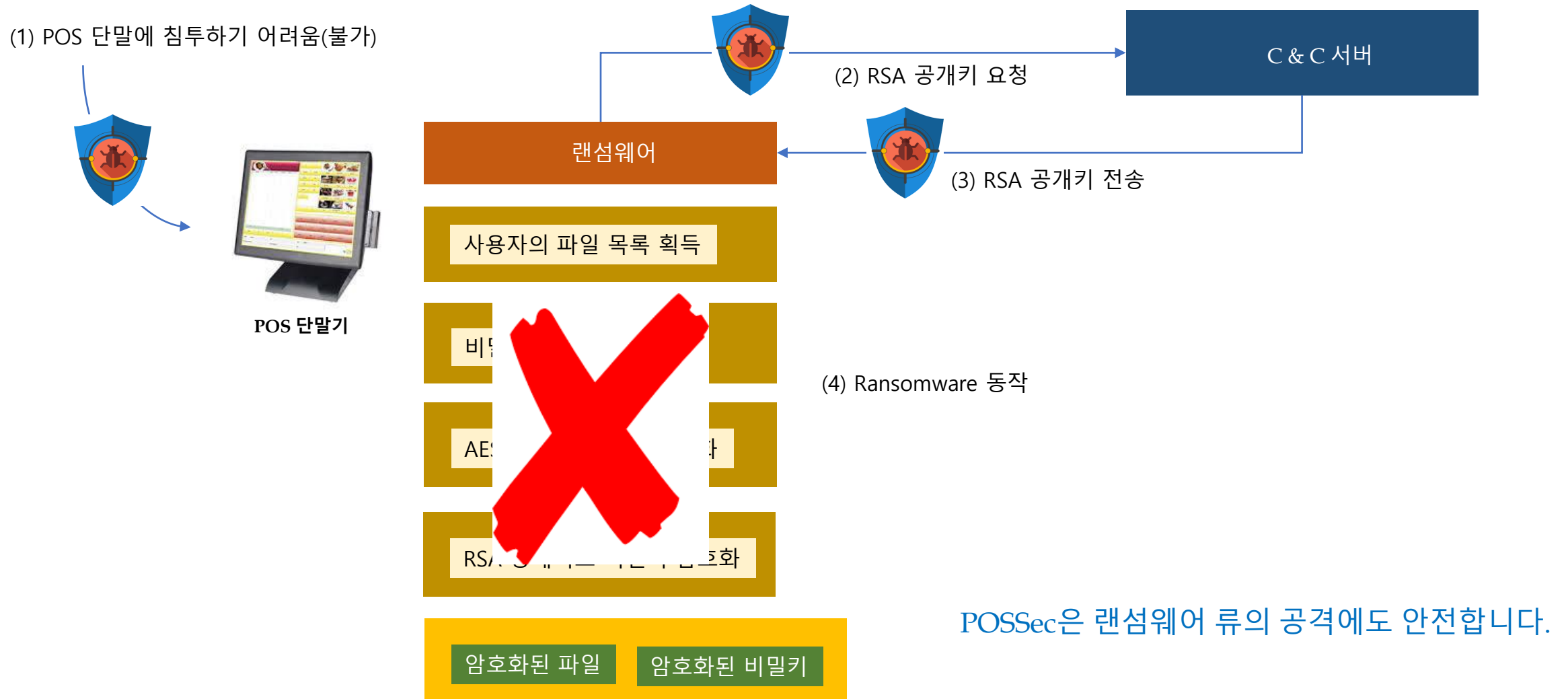


POSSec은 Malware, Spyware, Phishing, 광고, bitcoin 채굴, 음란 site 등을 자동으로 차단해 줍니다.

5. POSSec(8) – DNS Filter(2)



5. POSec(9) – Ransomware 차단



5. POSSec(10) – 지원 모델



POSSec Lite

일반 POS 단말용



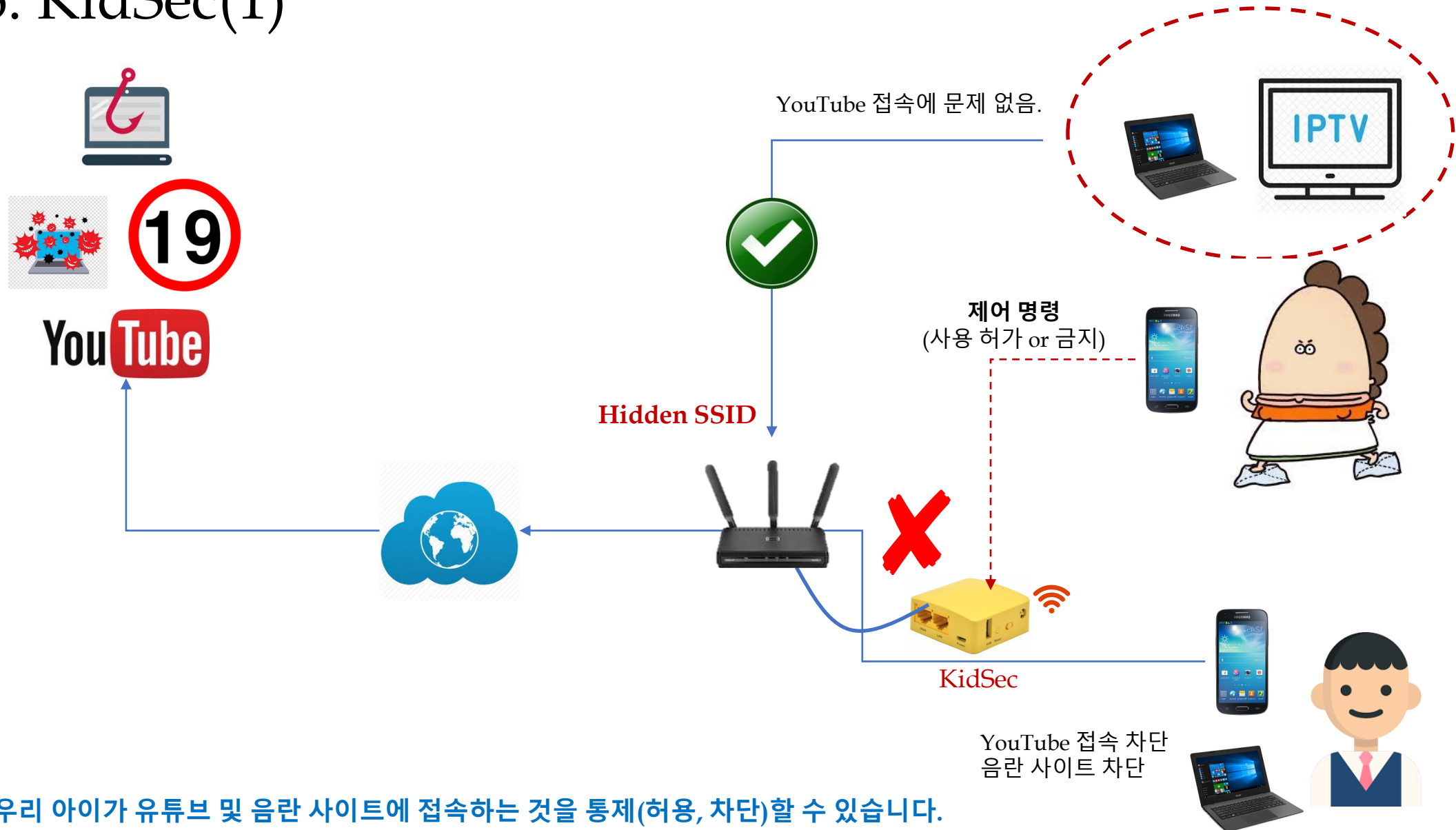
POSSec Premium

복수개의 POS 단말 or Kiosk 용

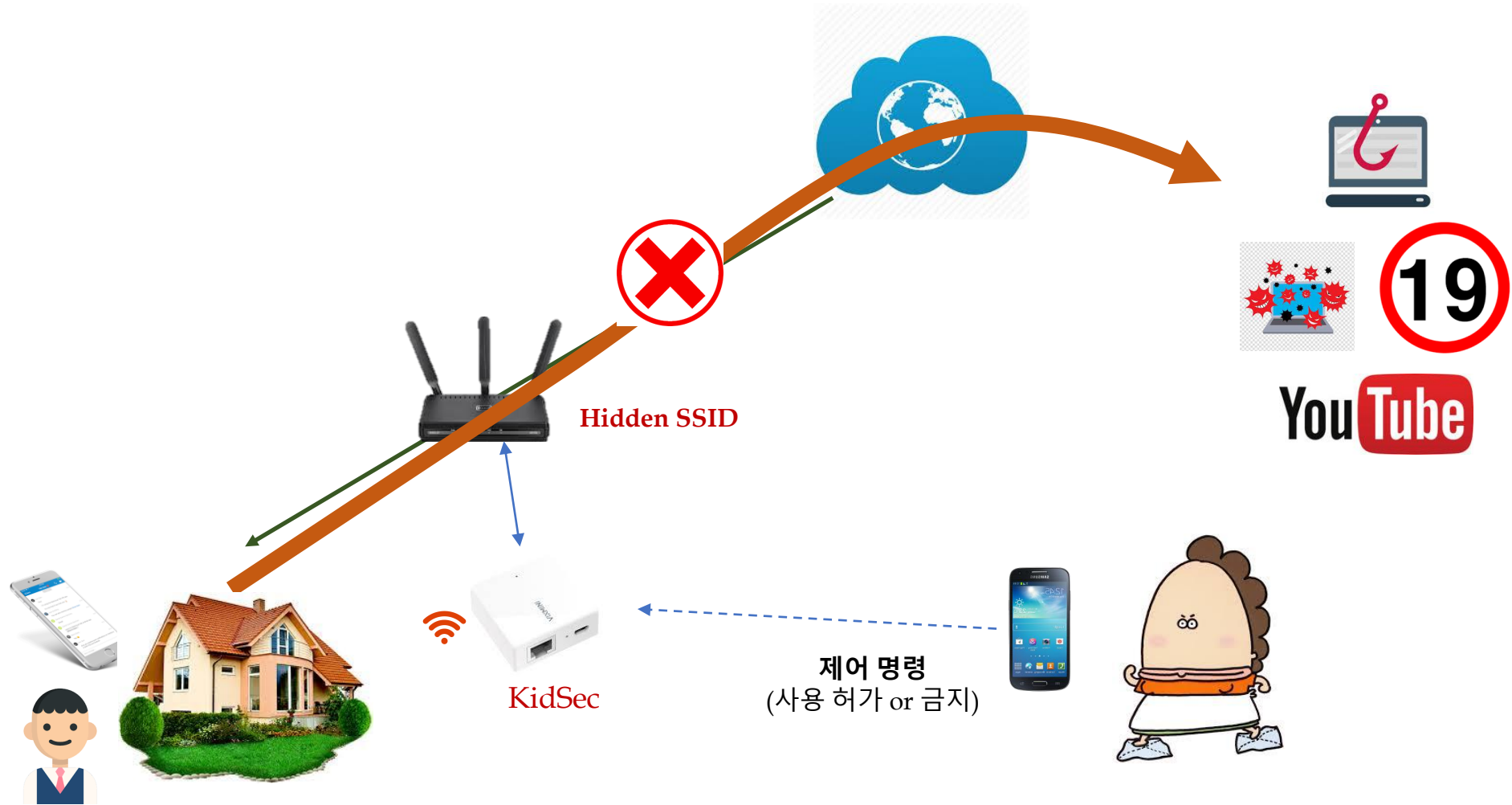
6. 유해 사이트 차단 **KidSec**



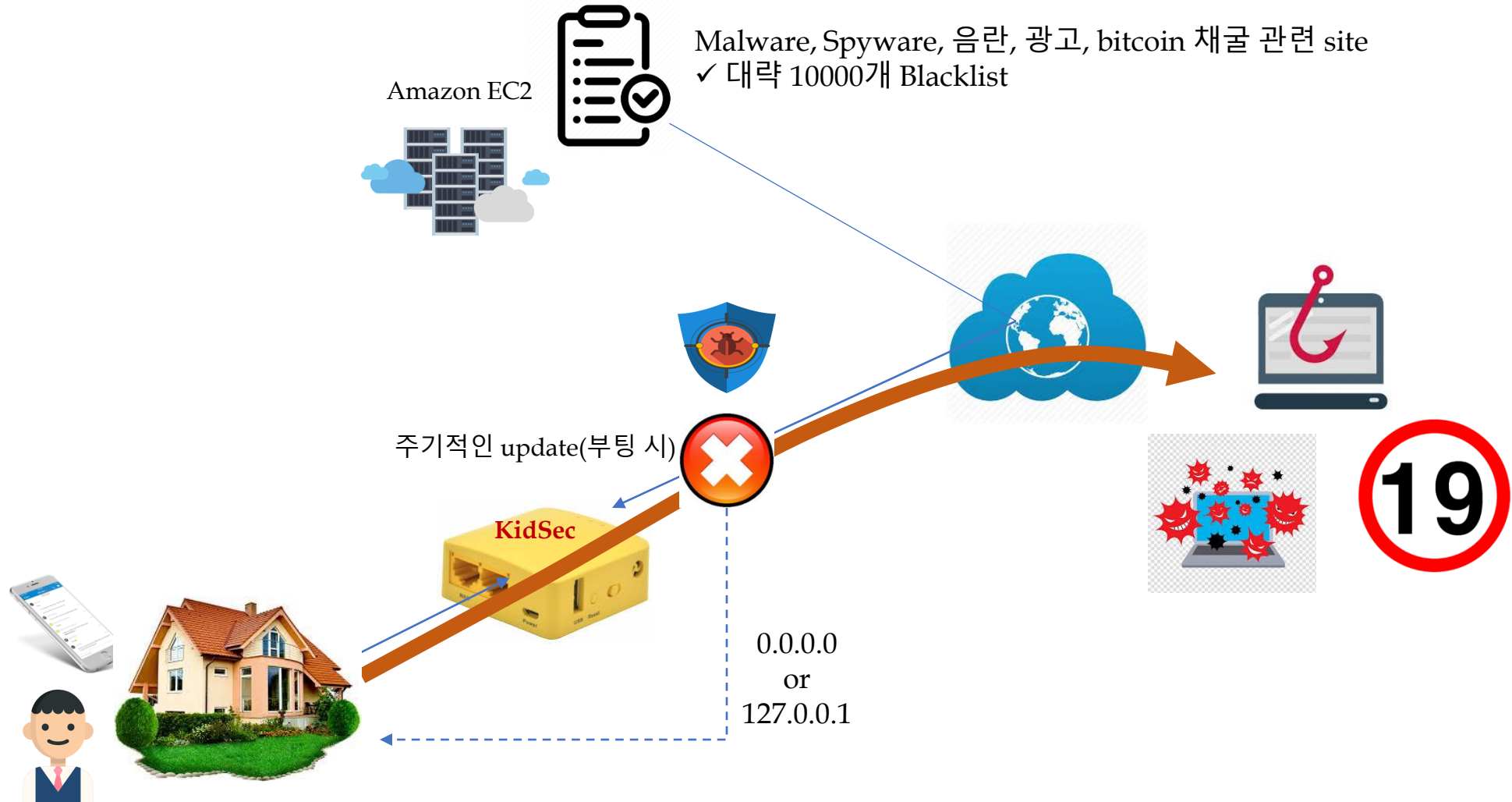
6. KidSec(1)



6. KidSec(2)



6. KidSec(3) - DNS Filter



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

6. KidSec(4) – Management Tool

KidSec Mini



무선 to 유선(Repeater) 가능
무선 2.4G 지원

KidSec Lite



무선 to 무선(Repeater) 가능
무선 2.4G 지원

KidSec Premium



무선 to 무선(Repeater) 가능
무선 2.4G/5G 지원



KidSec Control Web Page
(web based UI)

1. 인터넷 사용 시간 통제
2. Youtube 사용 차단/허용 제어
3. 음란, 도박, 유해 사이트 차단
4. 알림 기능(인터넷 사용)
5. 인터넷 사이트 목록 확인

19

Management Tool은 개발해야 함.

6. KidSec(5) – 참고 사항

- 1) 가격이 저렴하다(저렴해야 한다).
 - \$30 정도 선(단, premium model은 제외)
- 2) IPTime과 같이 자체 유해차단 기능이 있는 AP를 사용하면 되는데, 굳이 KidSec과 같은 추가 장치를 사용해야 하는 이유는 ?
 - Repeater 기능을 해준다. 즉, 인터넷 연결이 잘 안되던 아이의 공부방에서도 인터넷이 잘 터지게 만들어 준다.
 - 부모가 SmartPhone/Notebook을 통해 인터넷 사용을 세세히 통제할 수 있다(쉽고 편리하다).
 - 가정에서 사용하는 AP는 대부분 통신사에서 제공하는 것이고, 여기에는 이러한 기능이 없다.

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/>



Intel CPU를 사용하는 산업용 appliances

7. 참고 사항(2) - TODO

- 1) 최대한 쉽고 사용하기 편리하게 만들어야 한다.
 - *현재까지 만들어진 부분을 더욱더 같고 다듬어야 한다는 의미!*
 - *5개 모델(EndSec, P2PSec, OfficeSec, POSec, KidSec) 중 어떤 제품은 상용 제품 수준으로 개발되어 있고, 어떤 제품은 UI 등을 추가 개발해야 함.*
- 2) 다양한 환경에서의 시험을 진행해야 한다.
 - *(특히) POSec의 경우는 필드 시험을 진행해 보아야 한다.*
- 3) KidSec은 UI를 추가 개발해야 한다.
- 4) SBox는 전파인증을 획득해야 한다.
- 5) (향후) 고성능 SBox를 개발해야 한다.
- 6) (향후) 소형 SBox(Gl.iNet model)는 자체 생산할 수 있어야 한다.
- 7) (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