

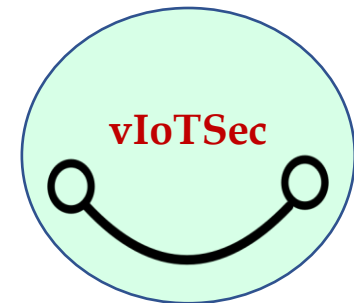
vIoTSec Products

- Open Source 기반 Virtual IoT Security Platform 개발 계획서 -
(*Simplified version*)

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

Doc. Revision: 2.3

Copyright© 2020 Chunghan.Yi, All Rights Reserved.



Contents

- 1. IoT Security Market
- 2. Our Technology **vIoTSec = EndSec + more**
- 3. IoT End to End 보안 **EndSec**
- 4. IoT Security Gateway **SBox**
- 5. IoT RTOS
- 6. Our Vision

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



Smart Bus Tracking



Remote Monitoring for PLCs

1. IoT Security Market(2) - 시장 규모



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



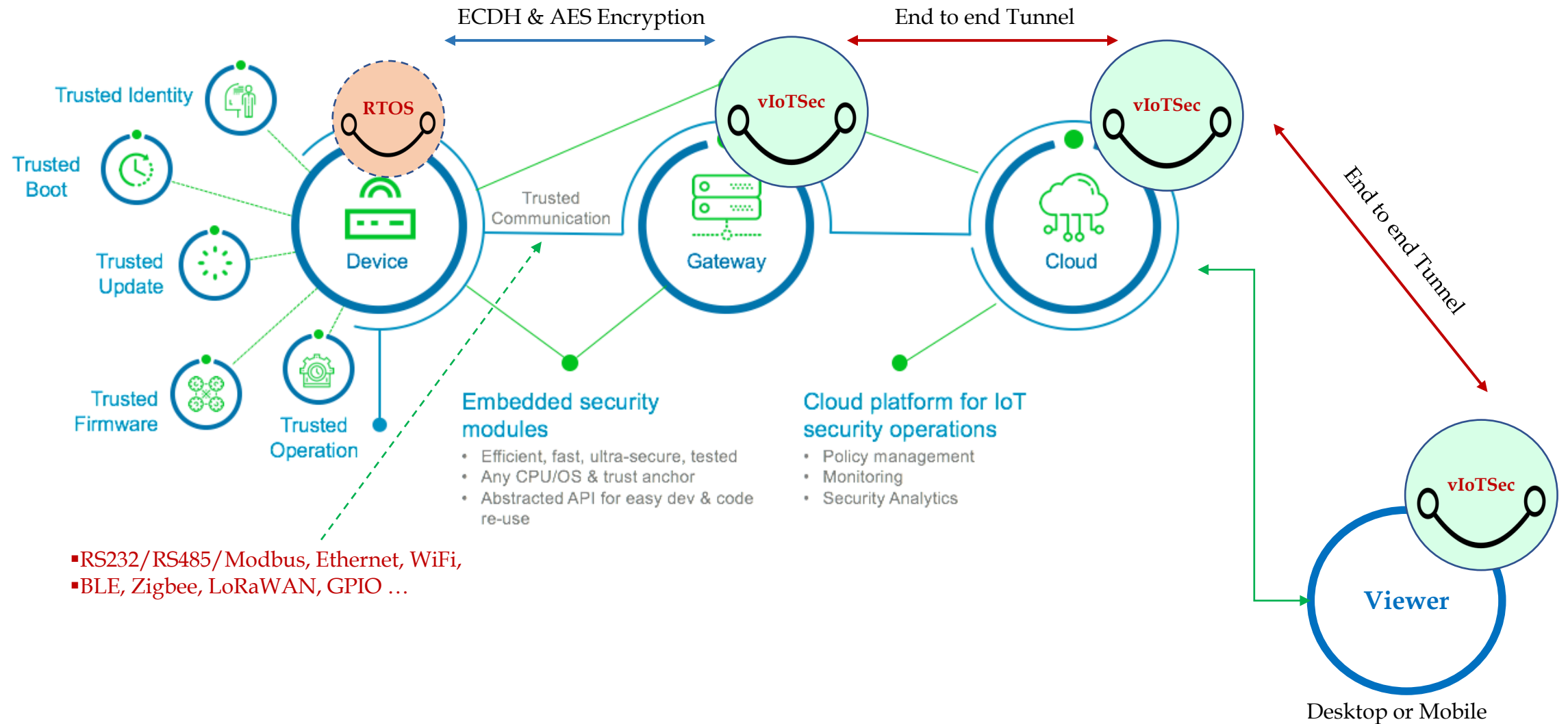
주: 1) 세계 시장은 2010~2019년까지, 한국 시장은 2013년~2020년까지 수치임

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

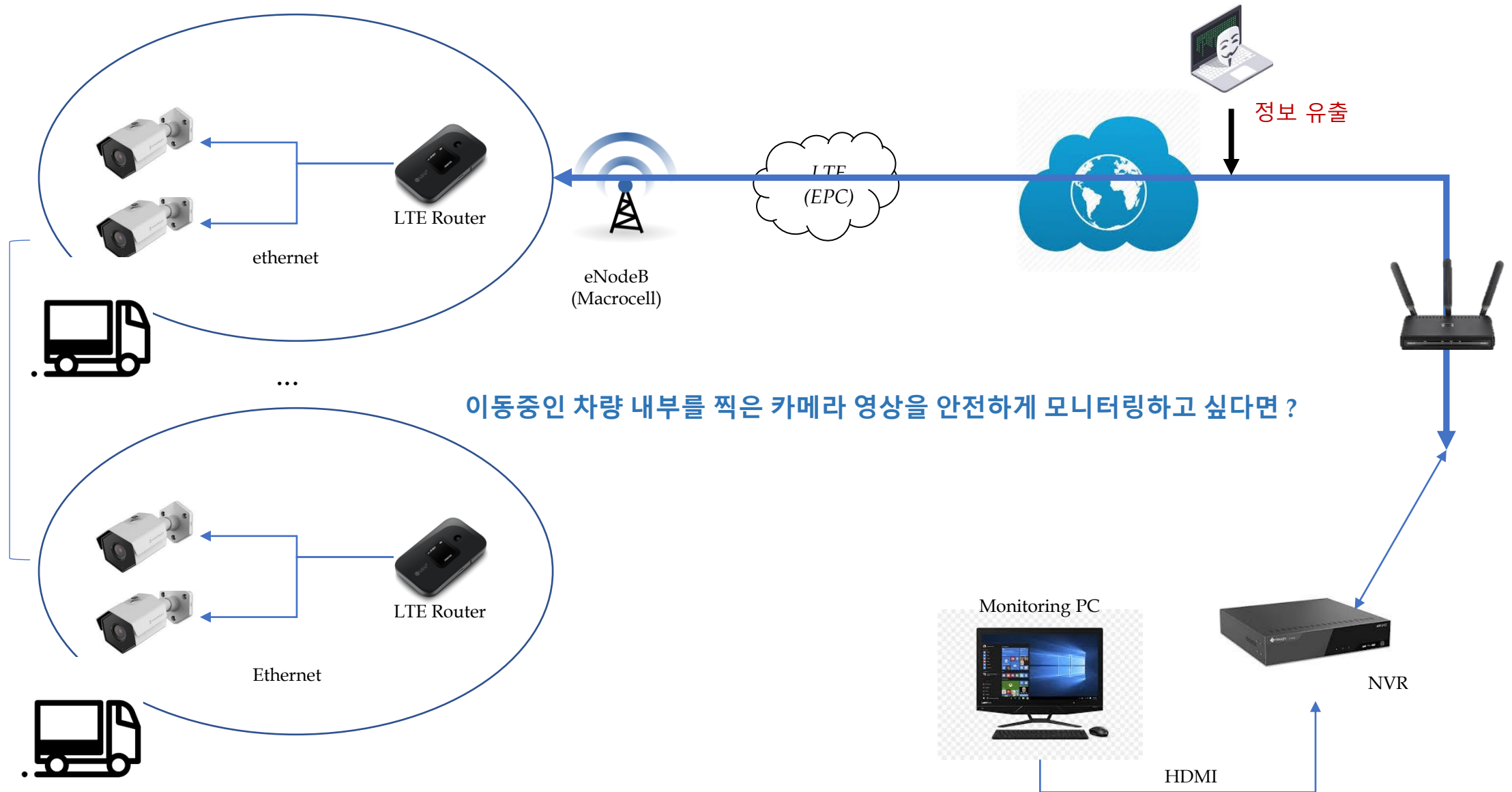
자료: Statista 2018, Machina Research(2014), 국회입법조사처(2017)을 참조하여 재구성

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

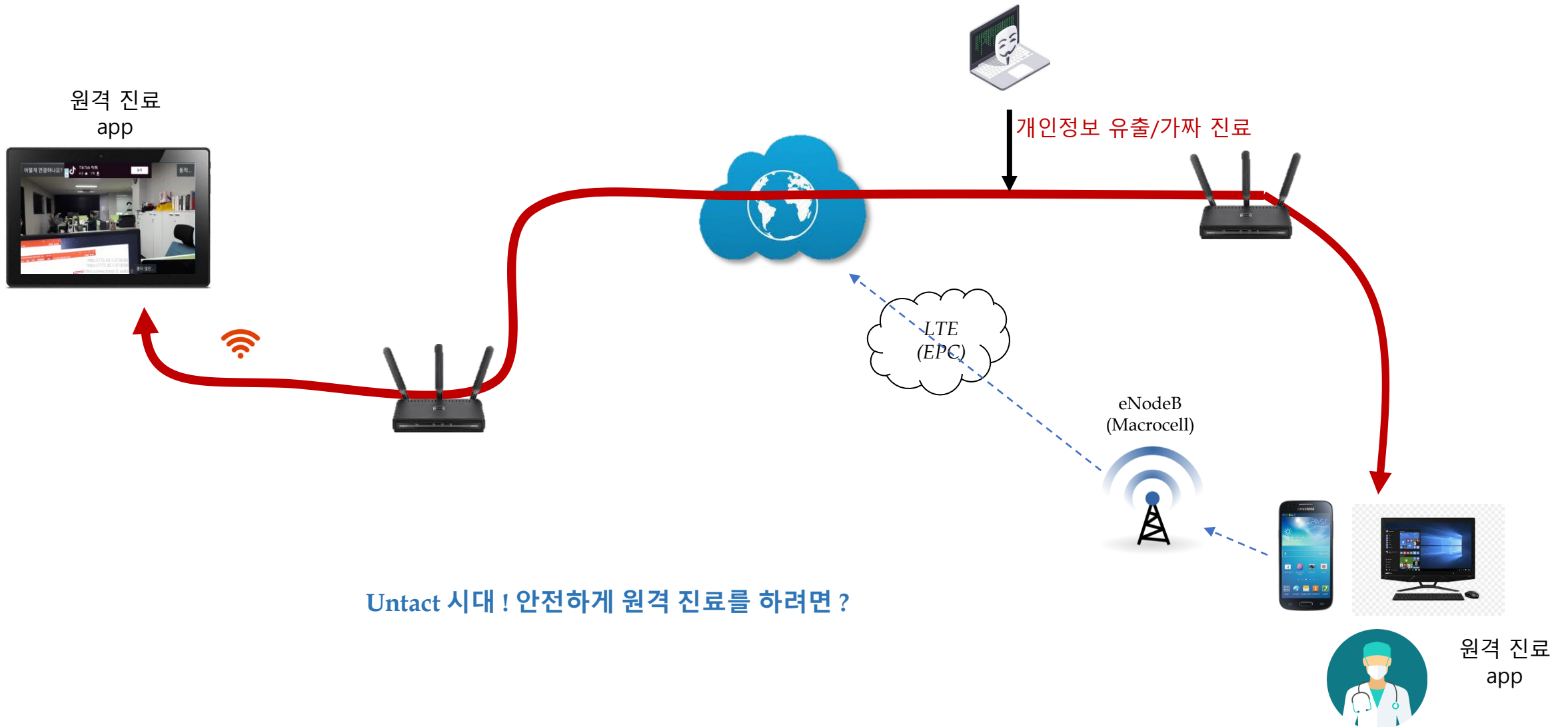
1. IoT Security Market(3) – IoT Security Area



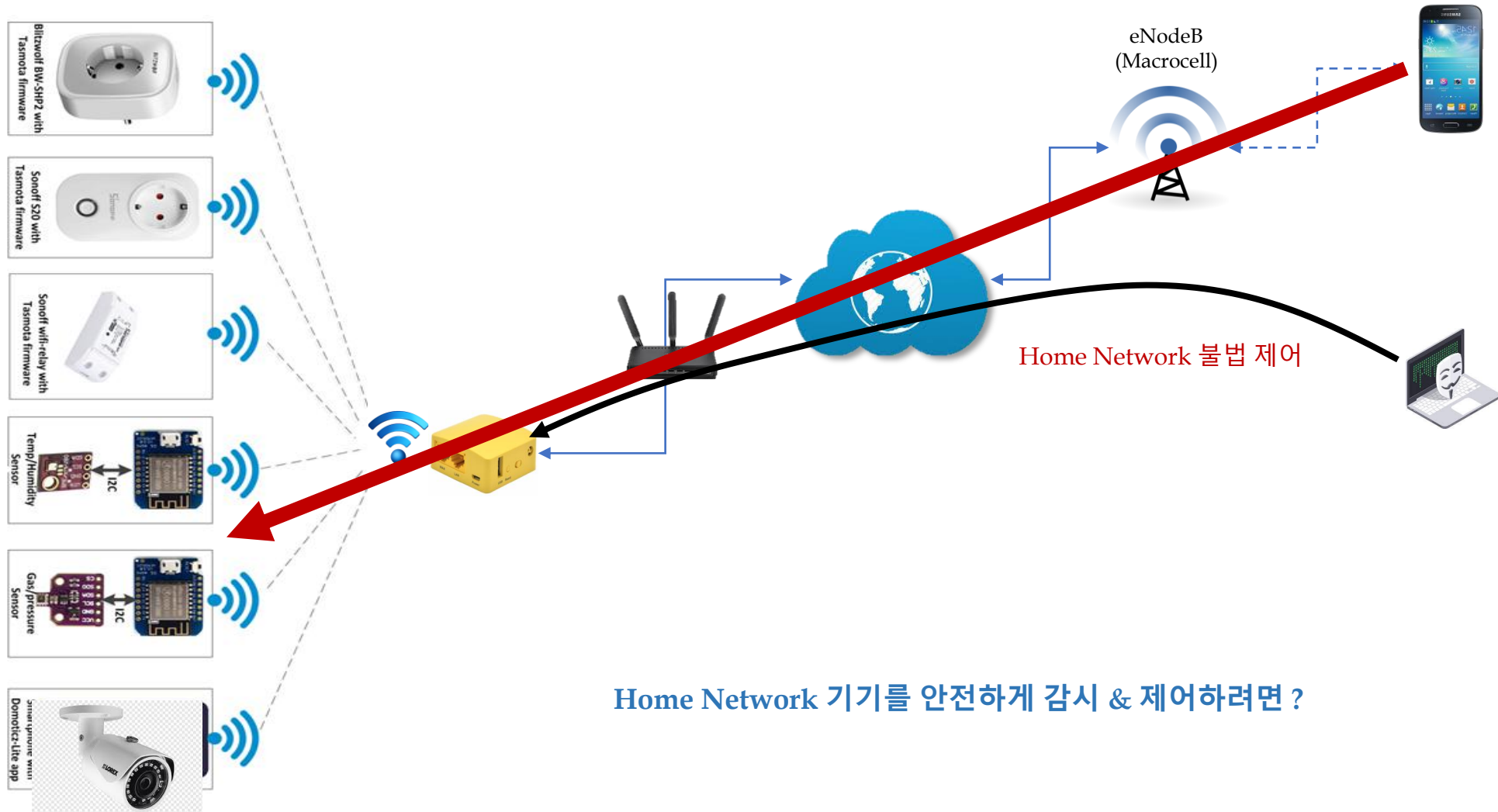
1. IoT Security Market(4) - Video Surveillance



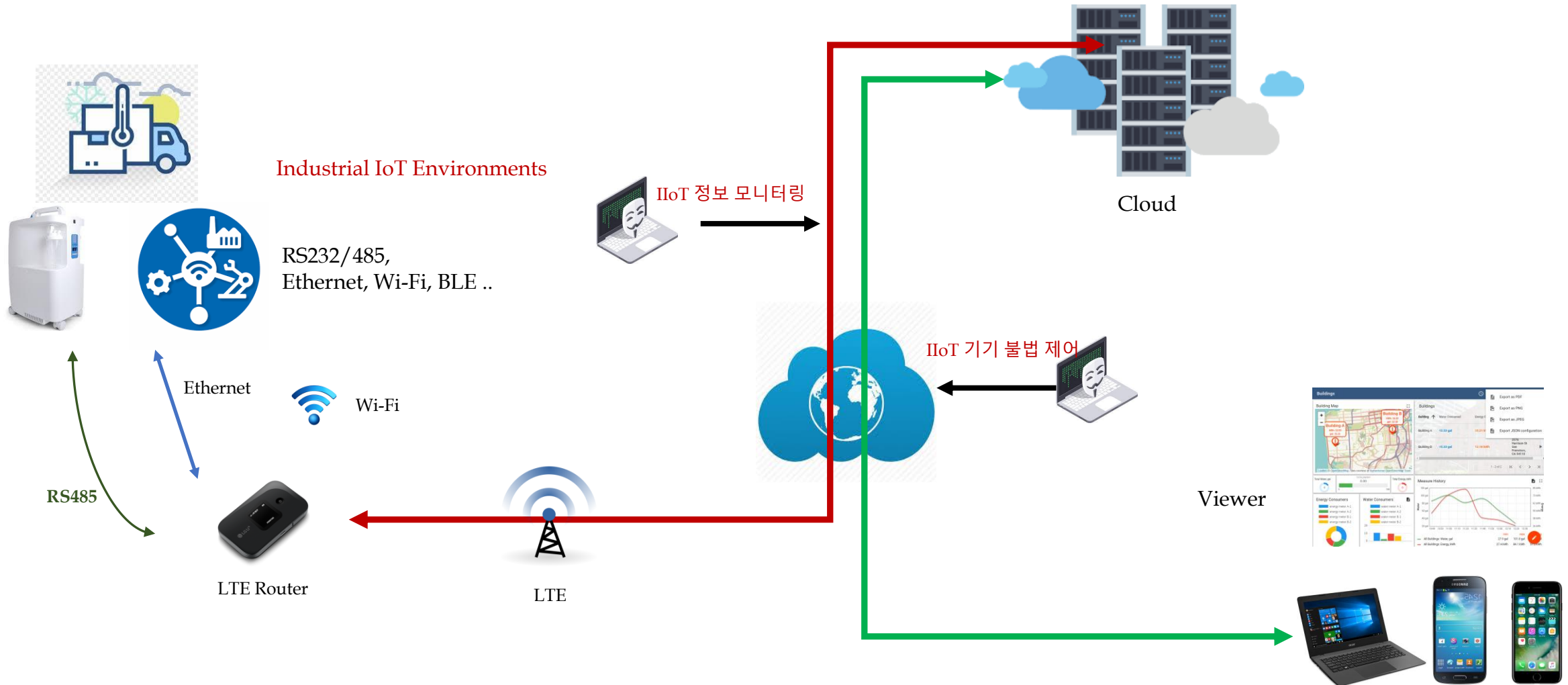
1. IoT Security Market(5) - 원격 진료



1. IoT Security Market(6) – Smart Home Network

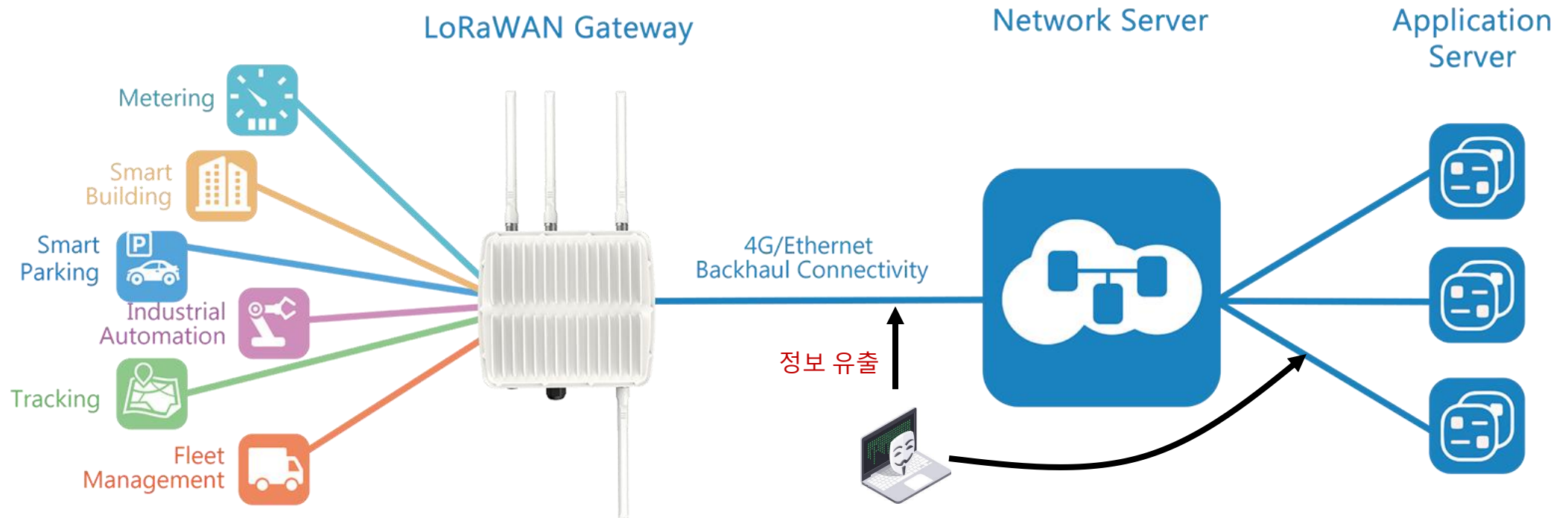


1. IoT Security Market(7) – 24/7 Real-Time Monitoring



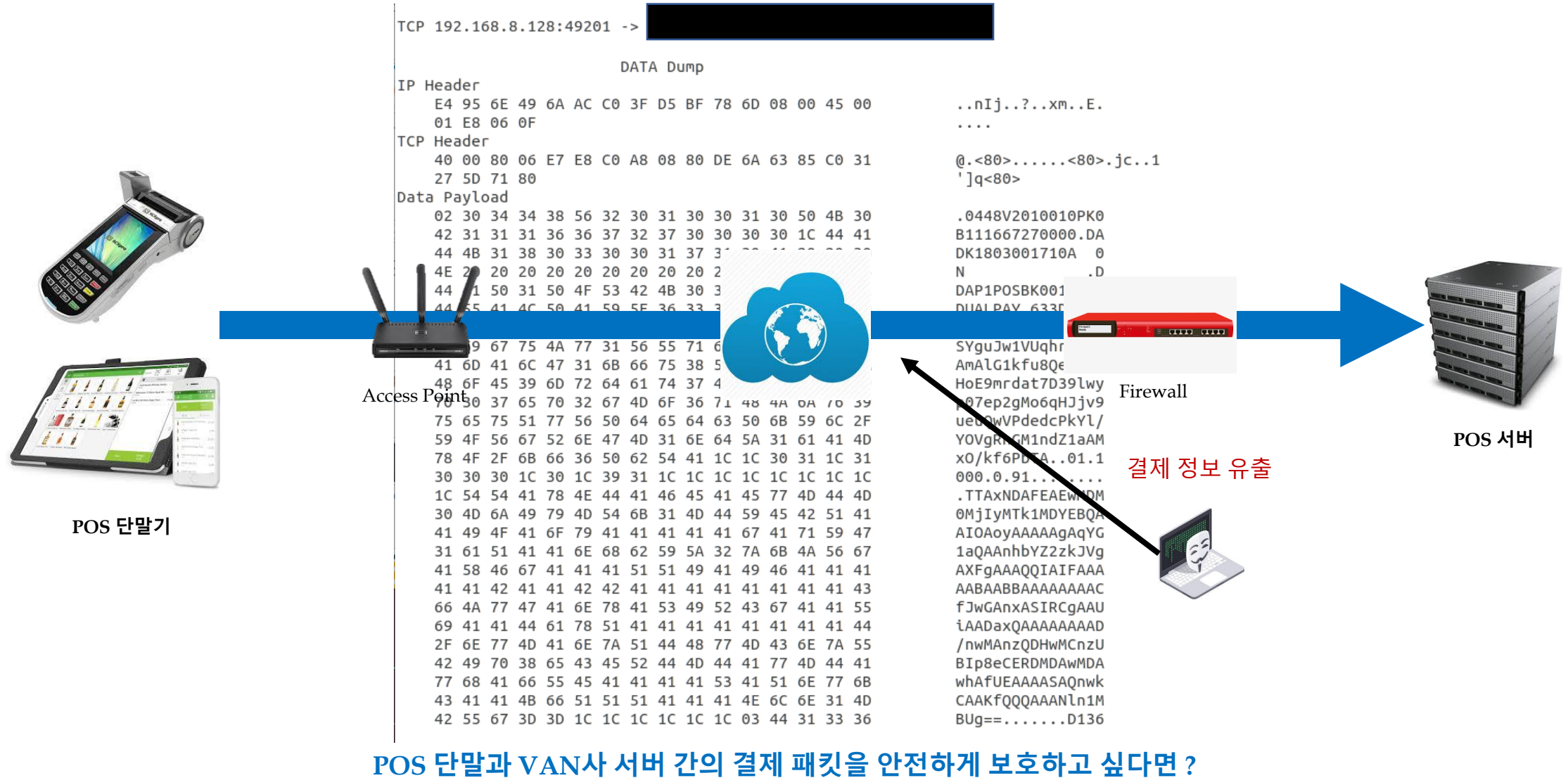
IIoT 기기를 안전하게 감시 & 제어하려면 ?

1. IoT Security Market(8) – LoRaWAN



LoRaWAN Gateway 뒷 단의 데이터를 안전하게 보호하려면 ...

1. IoT Security Market(9) - POS 결제 데이터

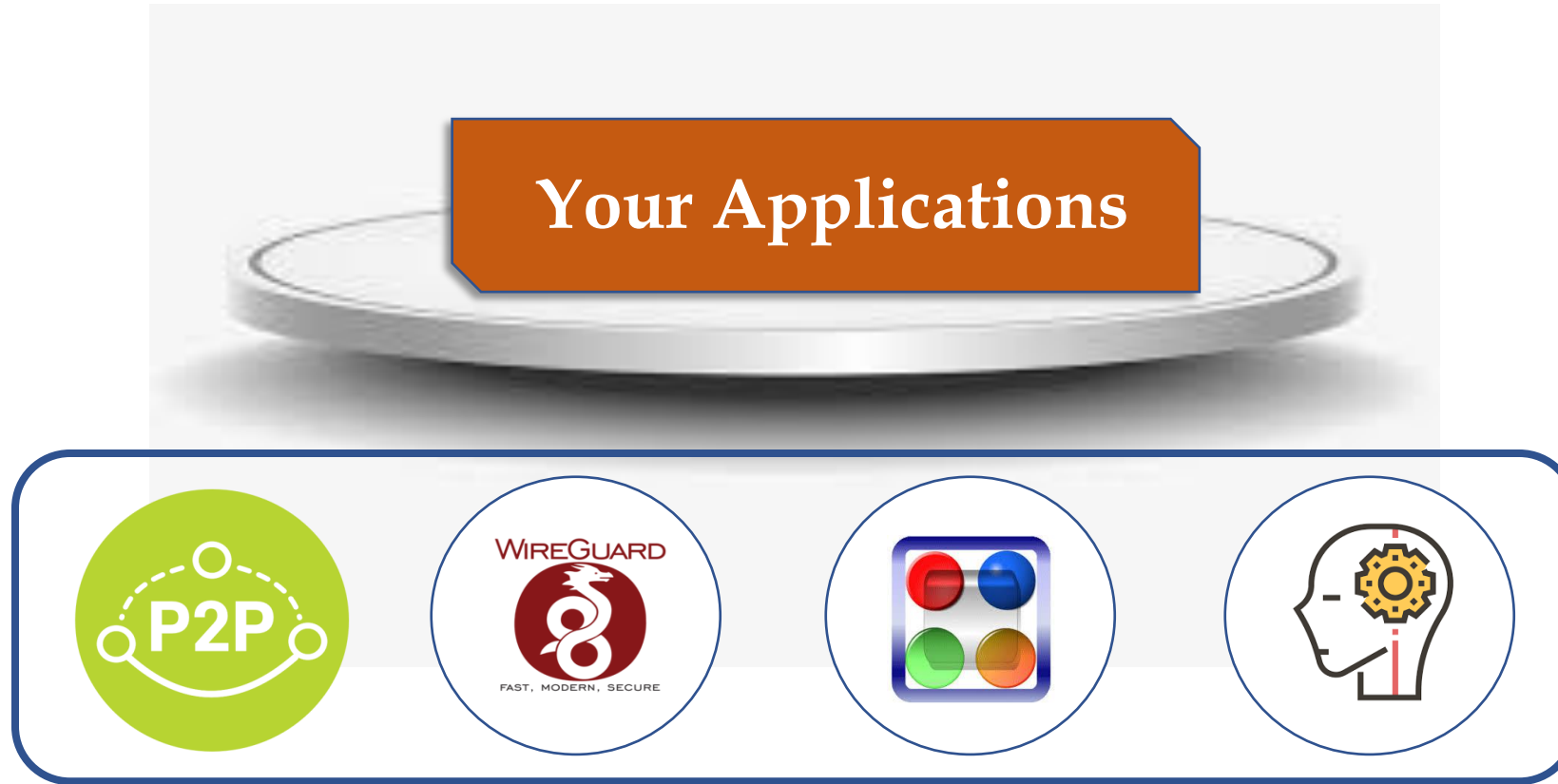


1. IoT Security Market(10) – Online Shopping



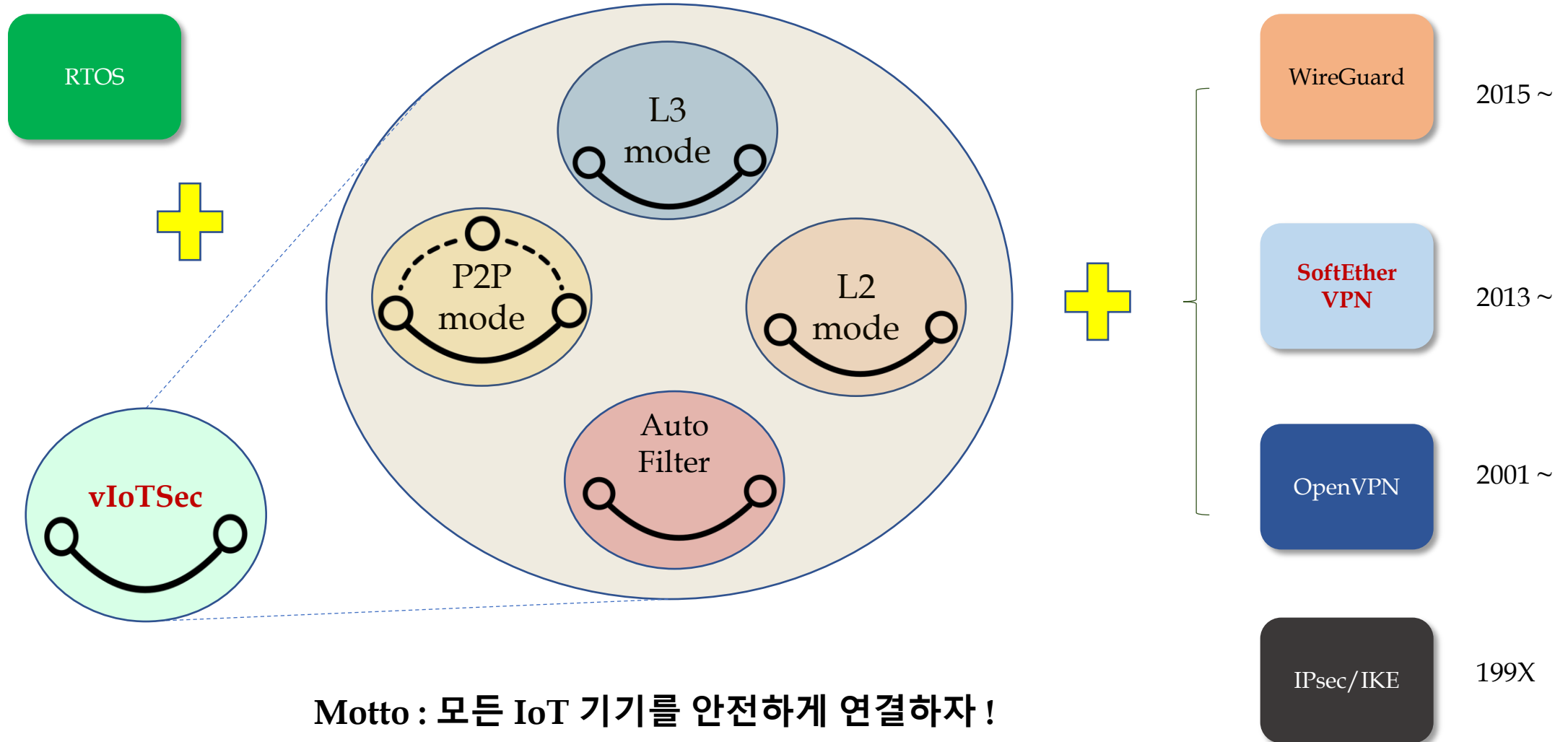
Online shopping을 안전하게 하려면 ?

2. Our Technology vIoTSec(1)

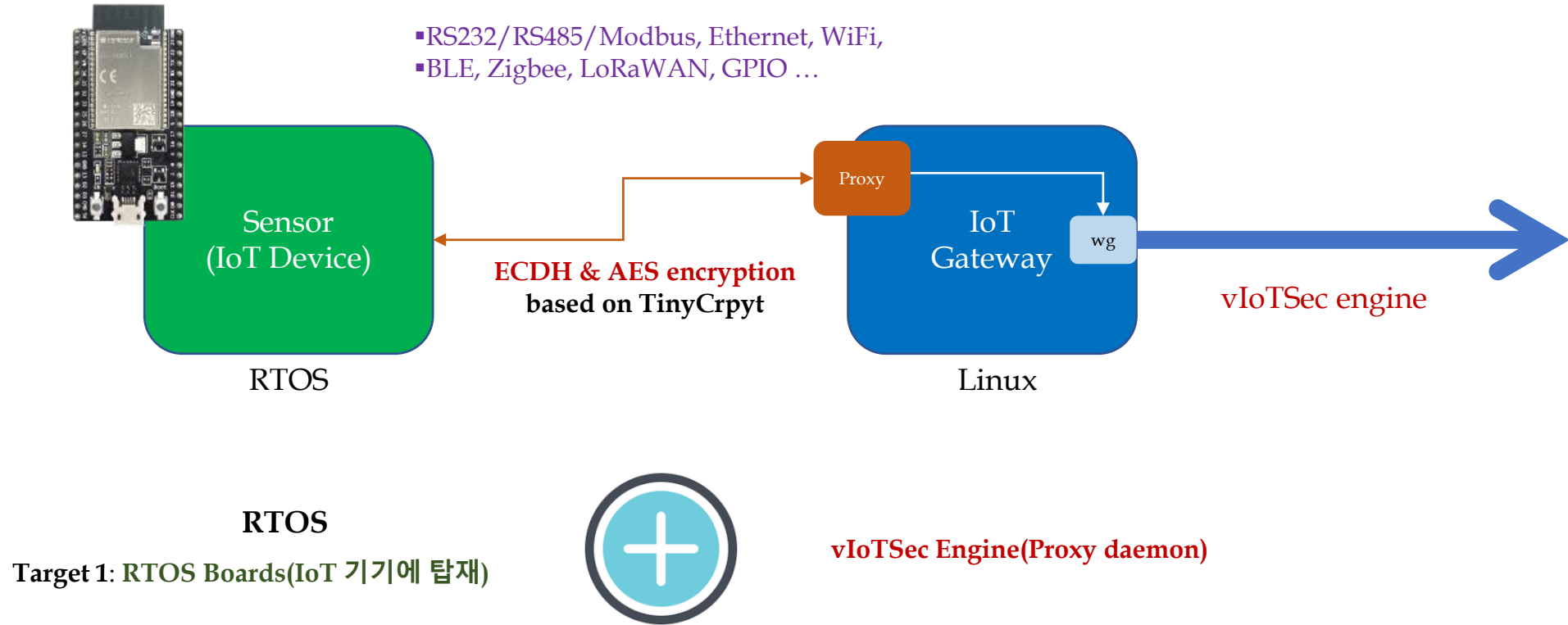


vIoTSec provides you a secure network infrastructure.

2. Our Technology vIoTSec(2)



2. Our Technology vIoTSec(3-1)



2. Our Technology vIoTSec(3-2)



Target 2: Linux Embedded Boards(IoT 기기에 탑재)



vIoTSec Engine(S/W)
(Kernel module 형태로 탑재)



Target 3: Embedded Products(상용제품)



Tiny Security Gateway w/ vIoTSec Engine
(Gateway 형태로 앞단에 설치)



Target 4: Android/iOS/Windows/macOS



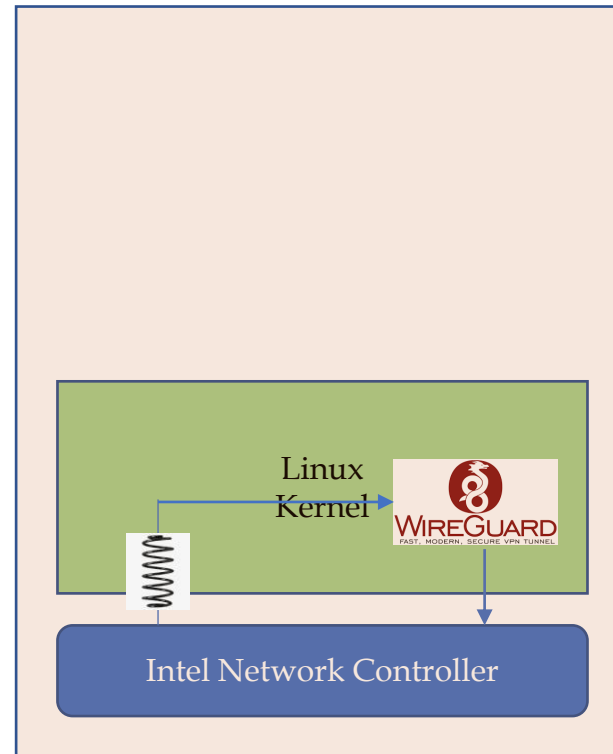
vIoTSec Applications
(App 형태로 설치)

2. Our Technology vIoTSec(3-3)

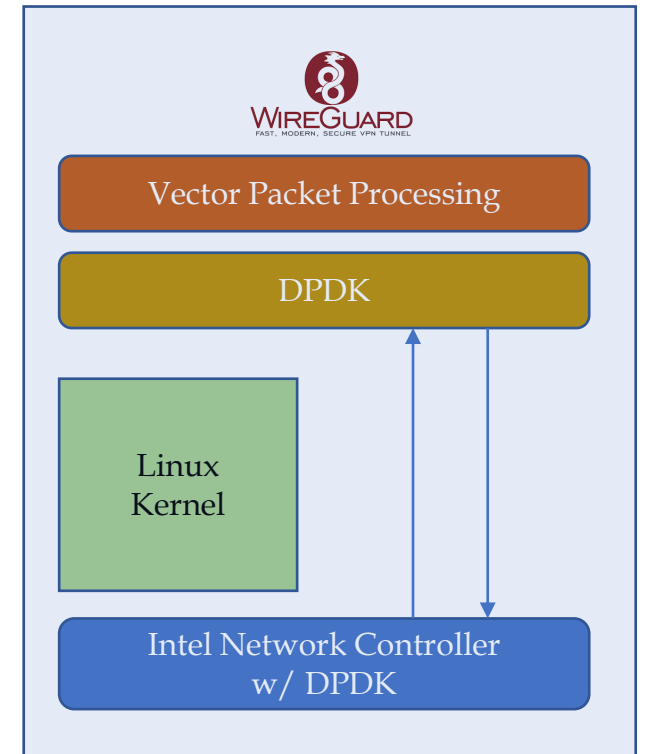


Target 5: Cloud Server

Very Fast Security Gateway



High Performance Security Gateway



vIoTSec Engine(S/W)
(Kernel module 형태로 탑재)

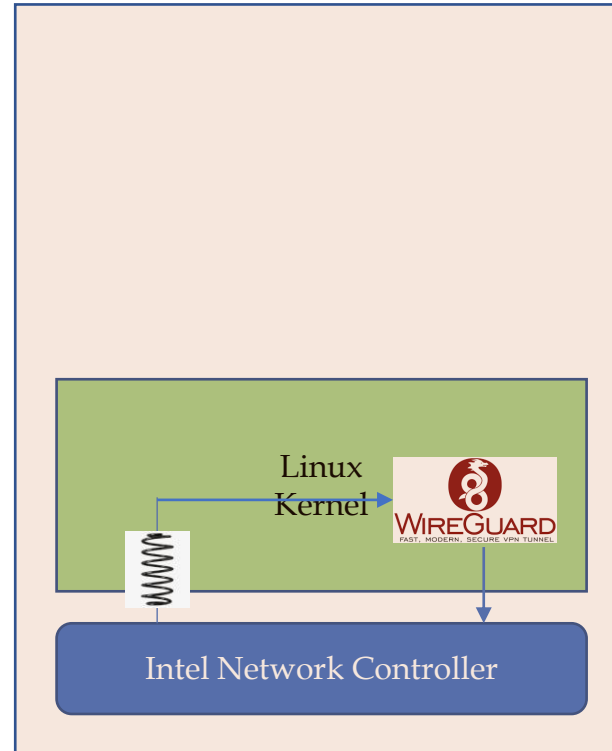
2. Our Technology vIoTSec(3-4)



Target 6: Network



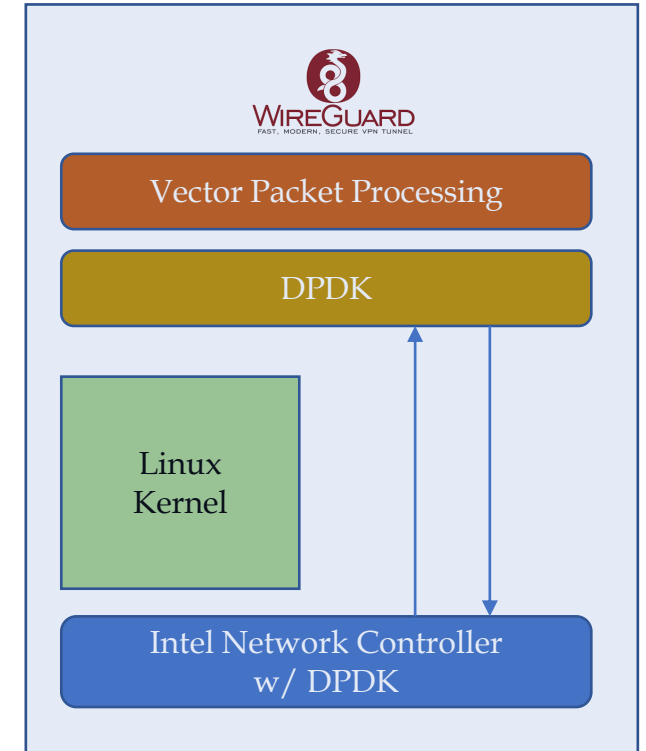
Very Fast Security Gateway



Security Gateway w/ vIoTSec Engine
(Gateway 형태로 네트워크 앞단에 설치)



High Performance Security Gateway



2. Our Technology vIoTSec(4)

- (기존) 경쟁 기술

- SSL VPN(예: OpenVPN) : 소형 SSL Gateway + 중앙의 대형 SSL Gateway로 구성(소형 ⇔ 대형/중앙 Gateway, end-to-end 연결에 적합하지 않음)
- SSL/TLS Protocol : end-to-end 연결에 적합하나, 주로 Web 기반 통신시 활용(다른 app으로 확장이 여유치 않음).
- 자체 app 보안(Android, iOS app 별 자체 통신 보안)

- 경쟁 기술 대비 장점

- 유연한 구성

- ✓ 임의의 End-to-End Node 연결에 적합, 이동중인 End node도 연결 가능, LTE to LTE 연결도 가능
 - ✓ Cloud에 탑재 가능, Android/iOS mobile 기기에 탑재 가능
 - ✓ 중앙의 Gateway or Server(Standalone) 구성 가능
 - ✓ 모든 IPv4/IPv6 network에 적용 가능(SSL/TLS 사용의 경우와 비교시)

- IoT 기기 보안에 최적화

- ✓ Tiny Gateway(저가) 제공, Embedded Board에 탑재 가능(응용성 높음)
 - ✓ 산업용 IoT기기와의 연결 가능 - RS232/RS485, Wi-Fi, BLE, Ethernet ...
 - ✓ Auto Filter를 이용하여 IoT 기기로의 자동 접근 제한

- 빠른 성능 및 우수한 보안성

- ✓ SSL VPN과는 구조적인 면에서 차이가 남(Kernel에서 모든 처리가 이루어져 빠른 속도 가능).
 - ✓ 최신의 암호 기술 사용 & 간결하고 안전한 키 교환 기법 도입

2. Our Technology vIoTSec(5)

- **보유 기술(Our Technology)**

- ✓ 1) Embedded 보드에 EndSec을 탑재하고, 임의의 IoT 기기와 연결(예: RS485)하는 기술
- ✓ 2) Tiny Gateway(OpenWrt Router, Gl.iNet)를 최적화하는 기술
- ✓ 3) Android, iOS, Windows 등에서 동작하는 EndSec app을 만드는 기술
- ✓ 4) 서버(Cloud)에 EndSec을 올리고 최적화하는 기술
- ✓ 5) Intel CPU 기반의 고성능 Security Gateway 제품을 만드는 기술
- ✓ 6) RTOS(Zephyr, mbedOS, FreeRTOS) 기술 및 암호 통신 기술

3. IoT End to End 보안 EndSec (Powered by WireGuard) : From IoT Gateway to Server



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)

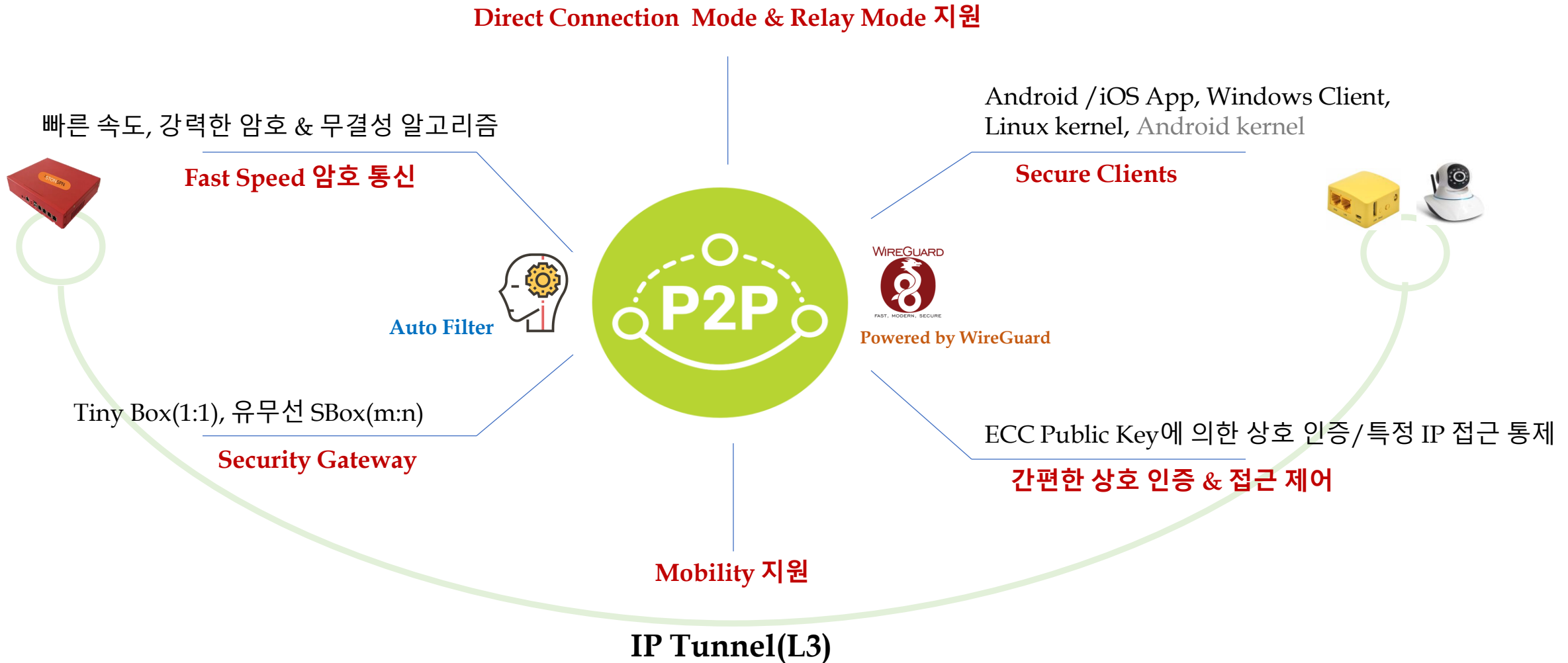


데이터 전송이 필요 없는 경우, 어떠한 패킷도 내 보내지 말아야 함(Stealth Mode)

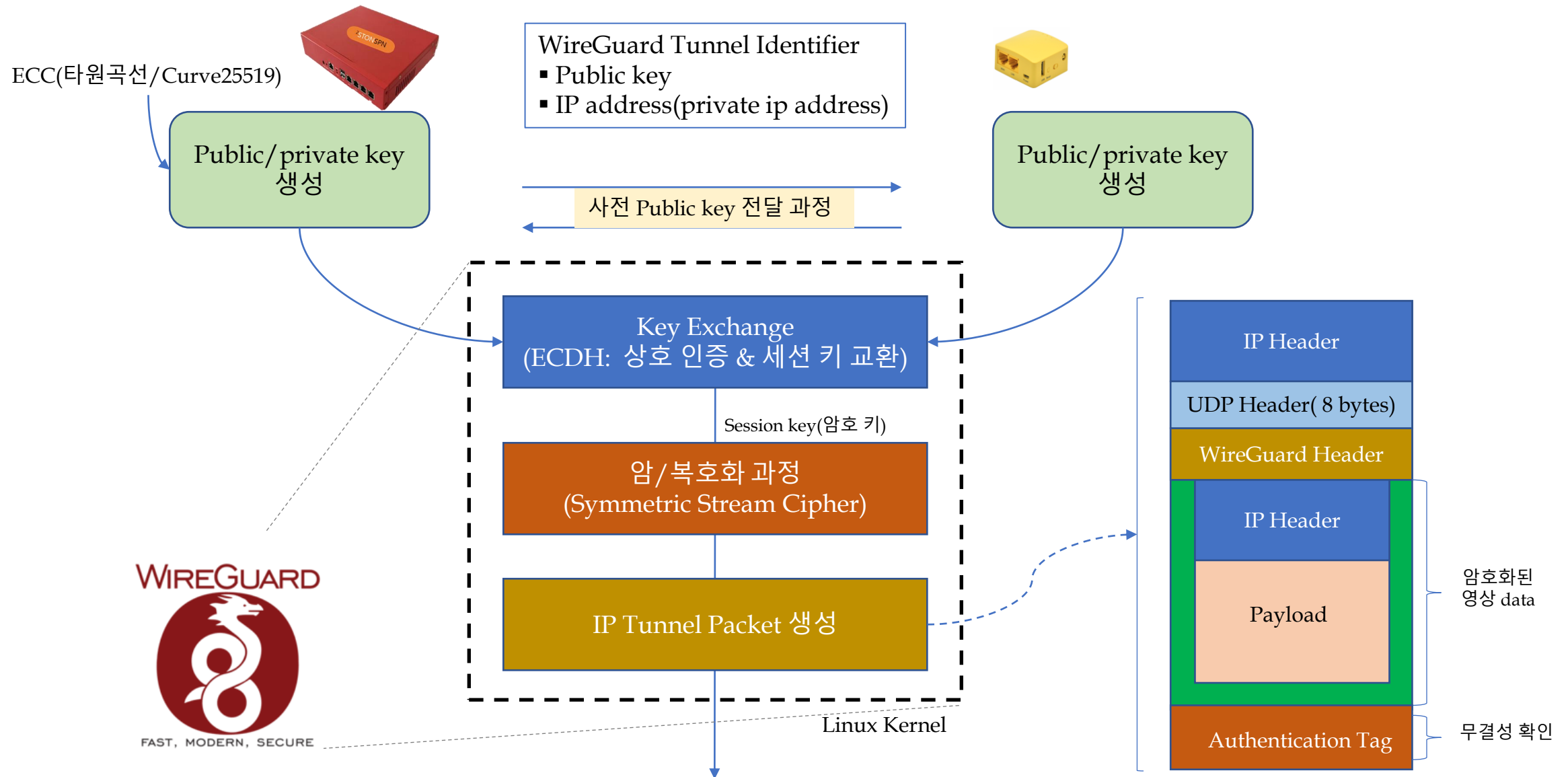


흐르는 트래픽을 분석하여 End node를 안전하게 보호할 수 있어야 함(Auto Filter)

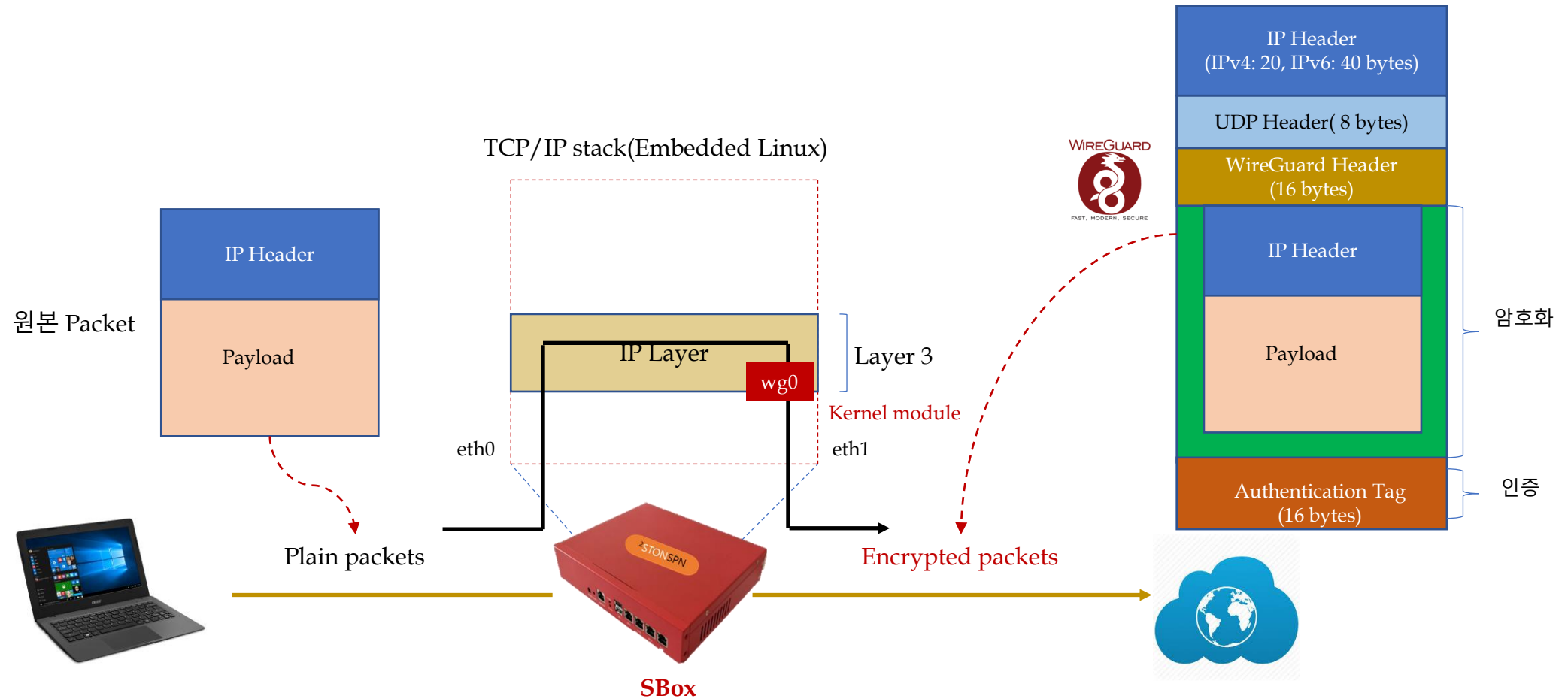
3. EndSec(1) – End to End Security(2)



3. EndSec(2) – WireGuard Tunnel(1)



3. EndSec(2) – WireGuard Tunnel(2)

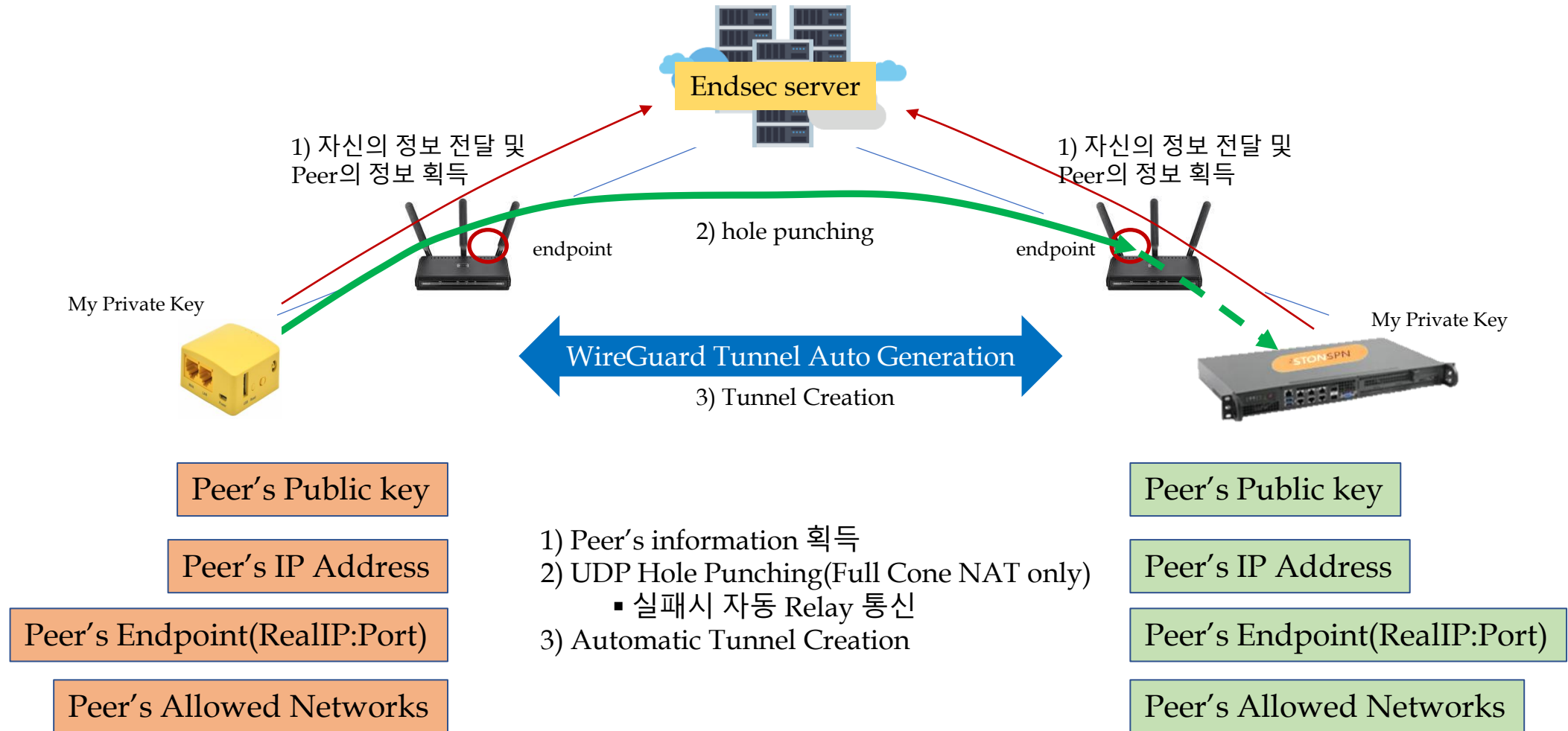


3. EndSec(2) – WireGuard Tunnel(3)

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)

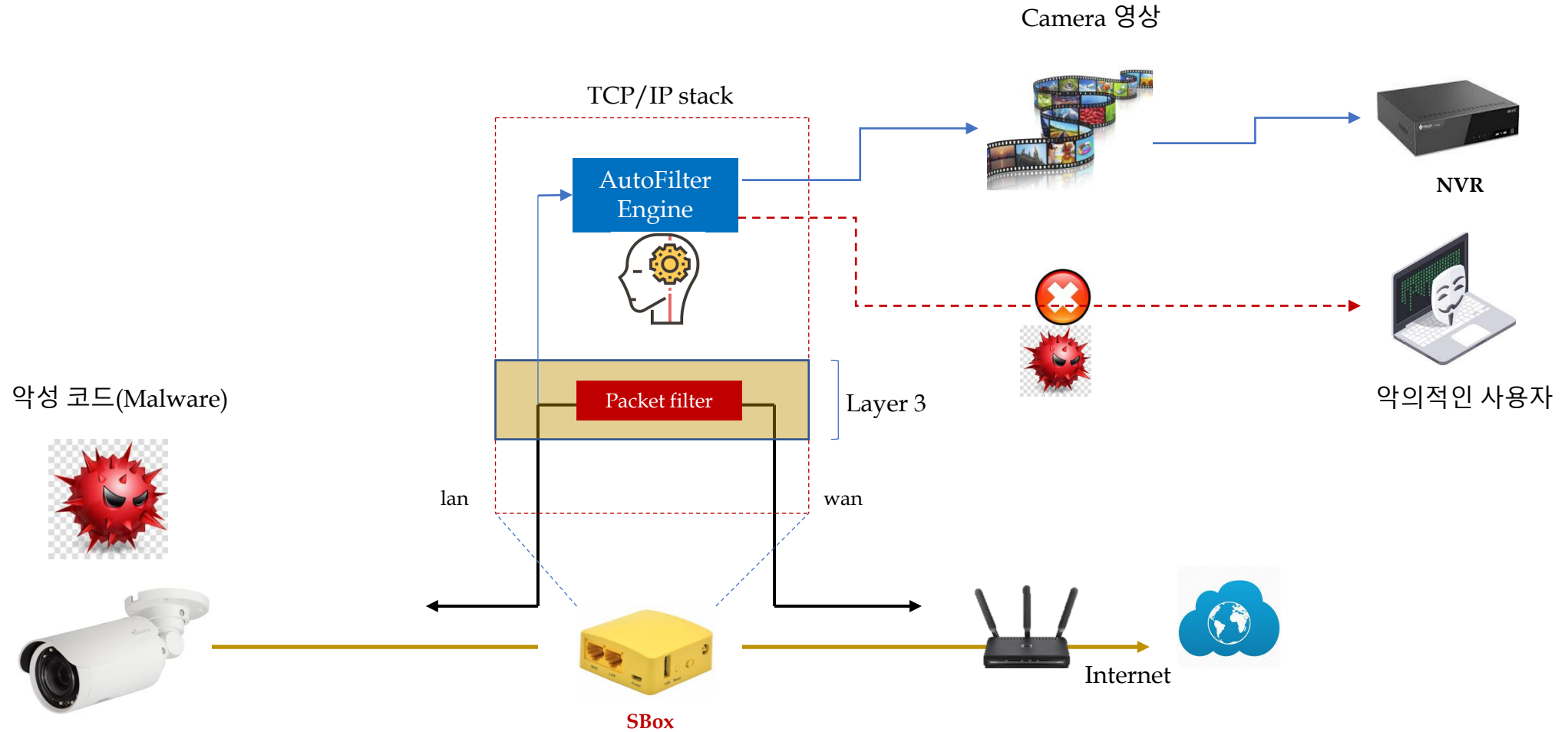
(*) 최대한 안전하면서도 빠른 알고리즘을 선택하므로써 전체적으로 network 성능을 끌어 올리도록 함.

3. EndSec(3) – Auto Connection



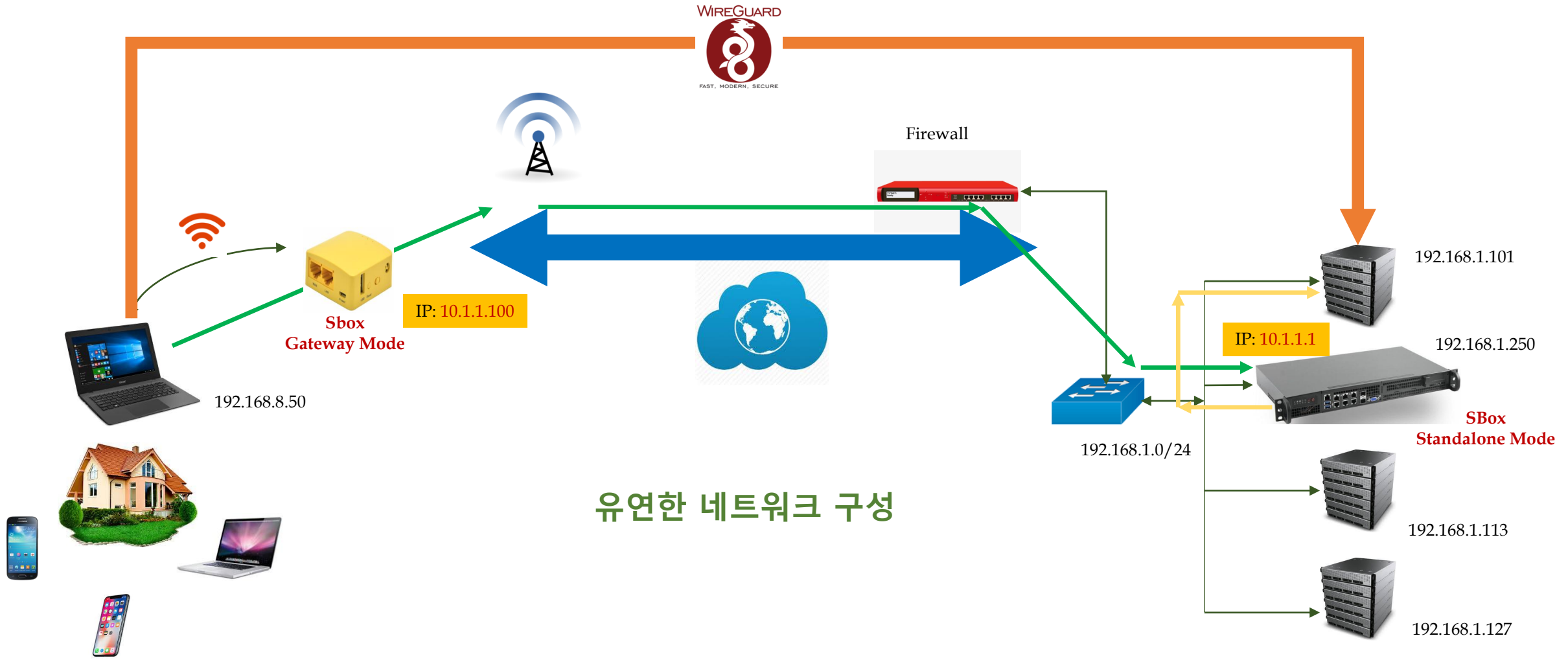
EndSec Auto Connection 기능을 사용하면 EndSec 기기간 연결이 한층 수월해 질 수 있습니다.

3. EndSec(4) - Auto Filter



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

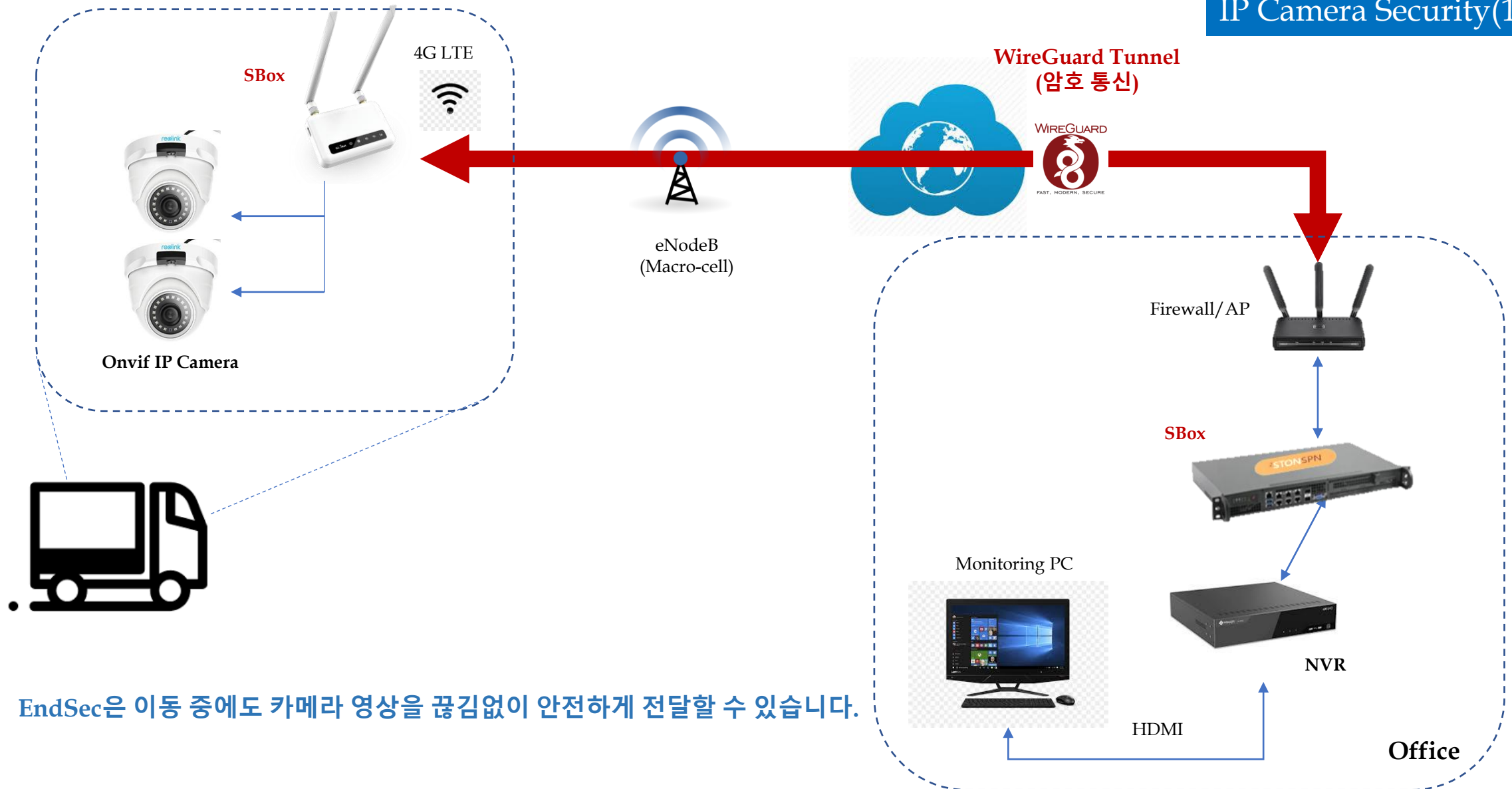
3. EndSec(5) – Gateway Mode vs Standalone Mode



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

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

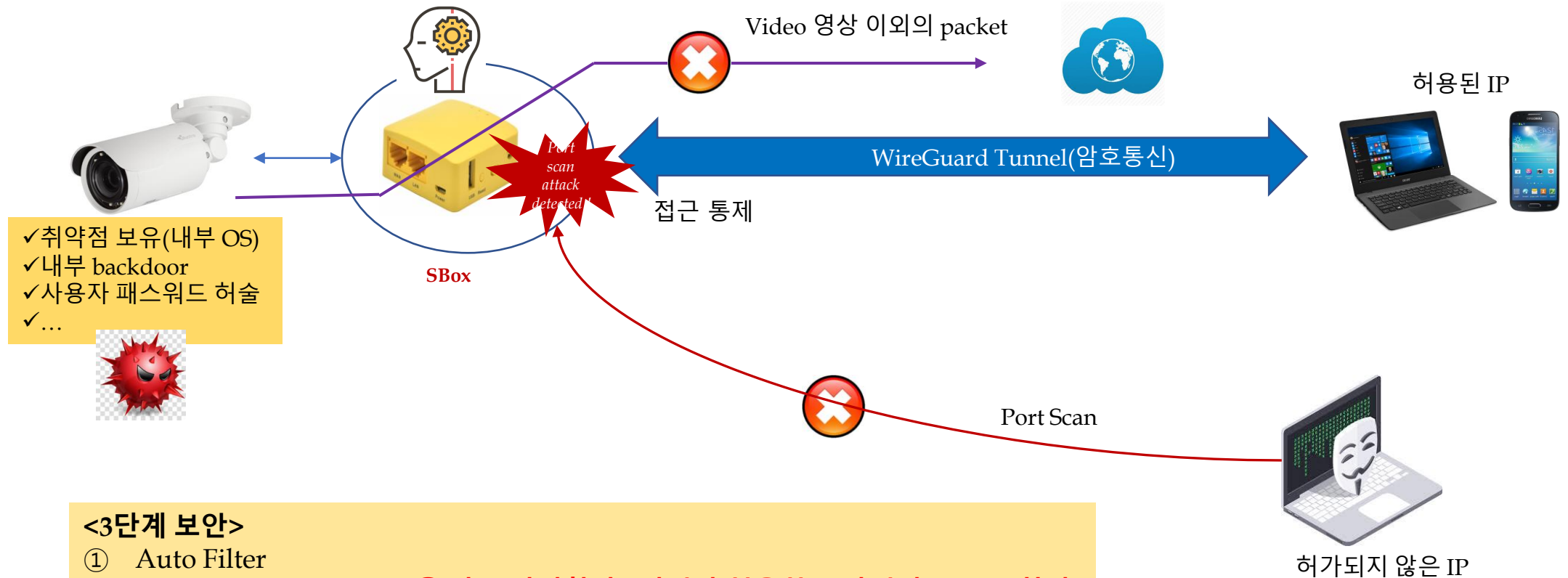
IP Camera Security(1)



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

IP Camera Security(2)

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

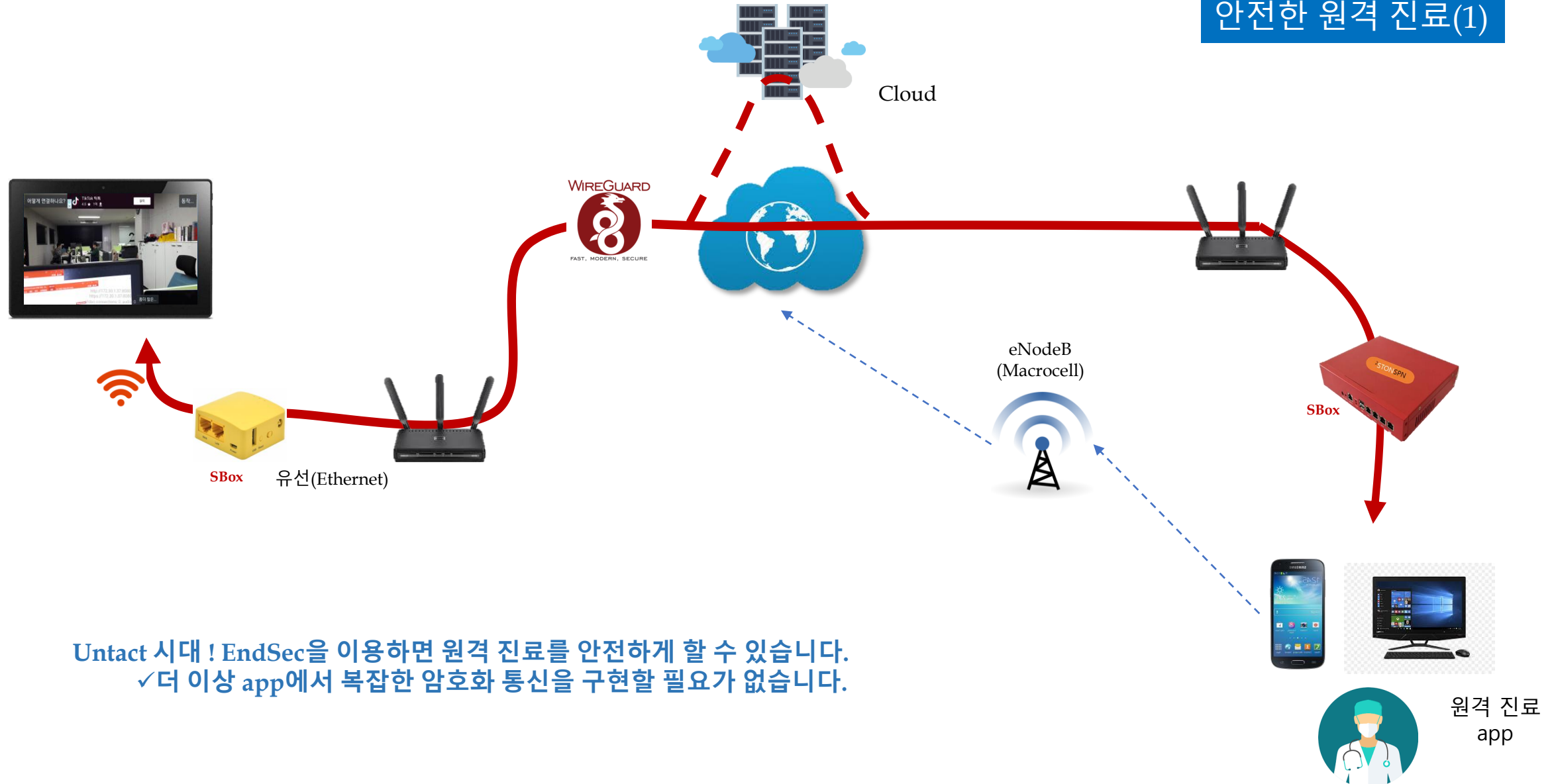


<3단계 보안>

- 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.

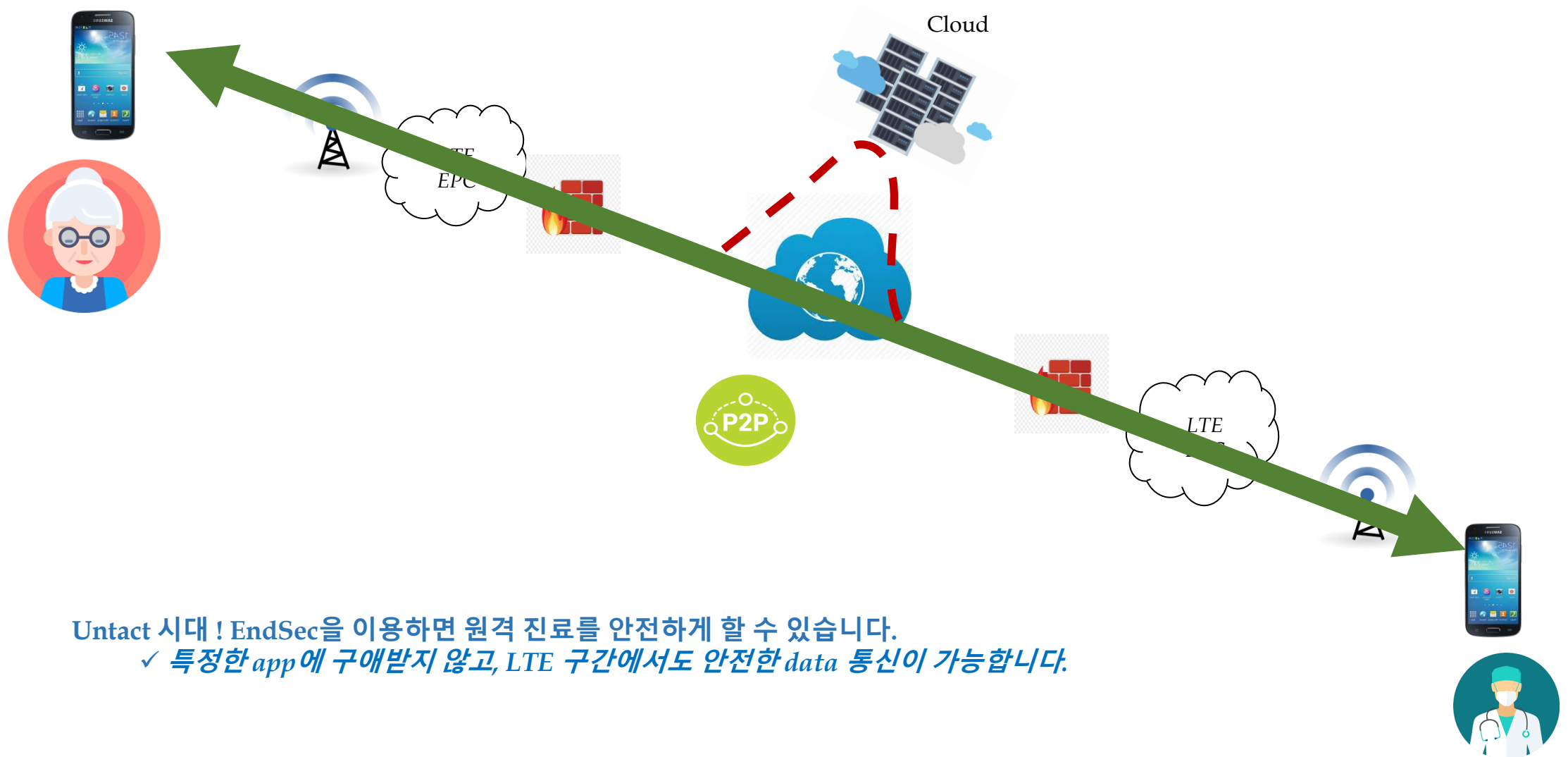
3. EndSec(6) - Use Cases(2-1)

안전한 원격 진료(1)



3. EndSec(6) – Use Cases(2-2)

안전한 원격 진료(2)

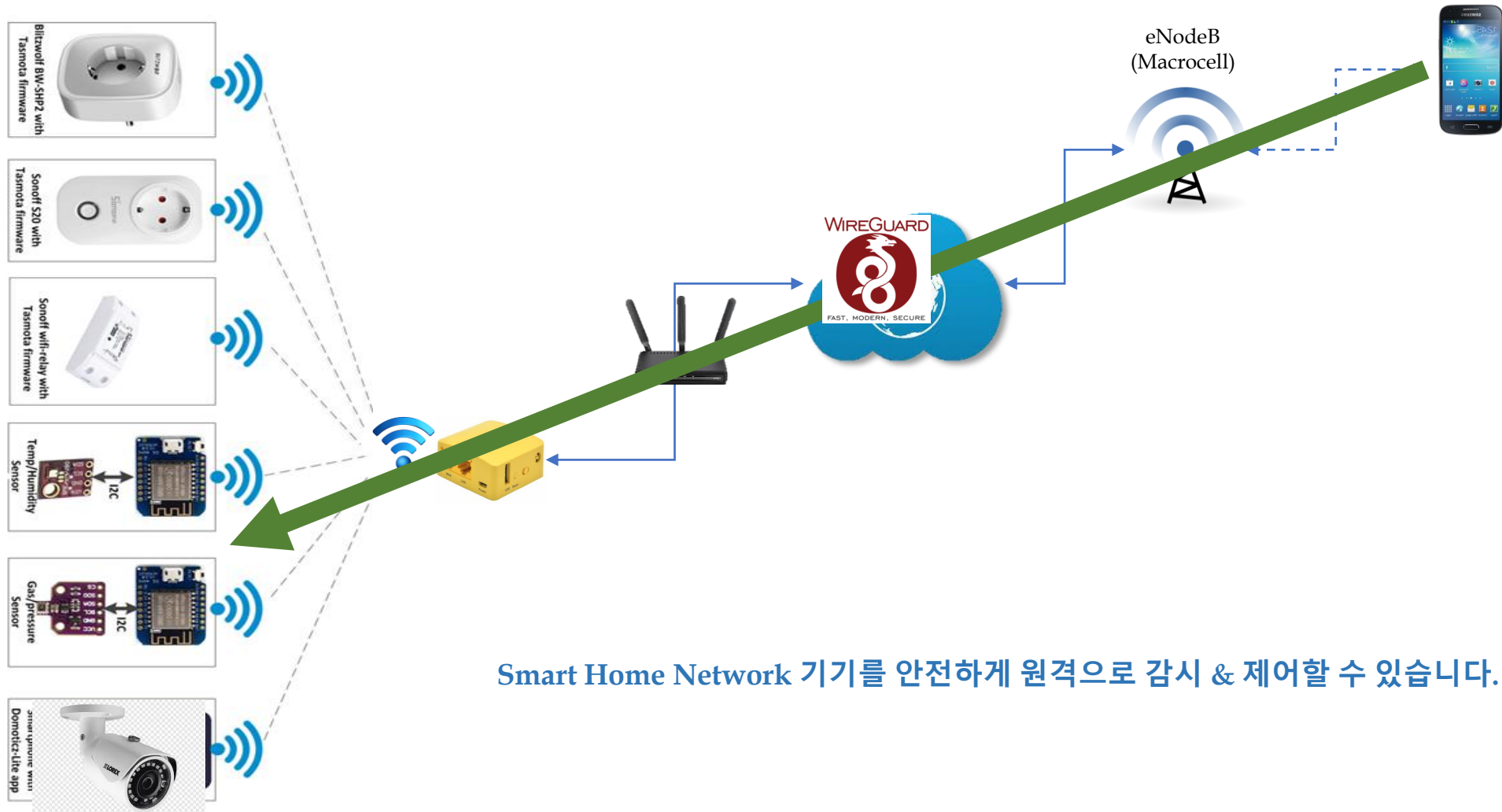


Untact 시대 ! EndSec을 이용하면 원격 진료를 안전하게 할 수 있습니다.

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

3. EndSec(6) – Use Cases(3)

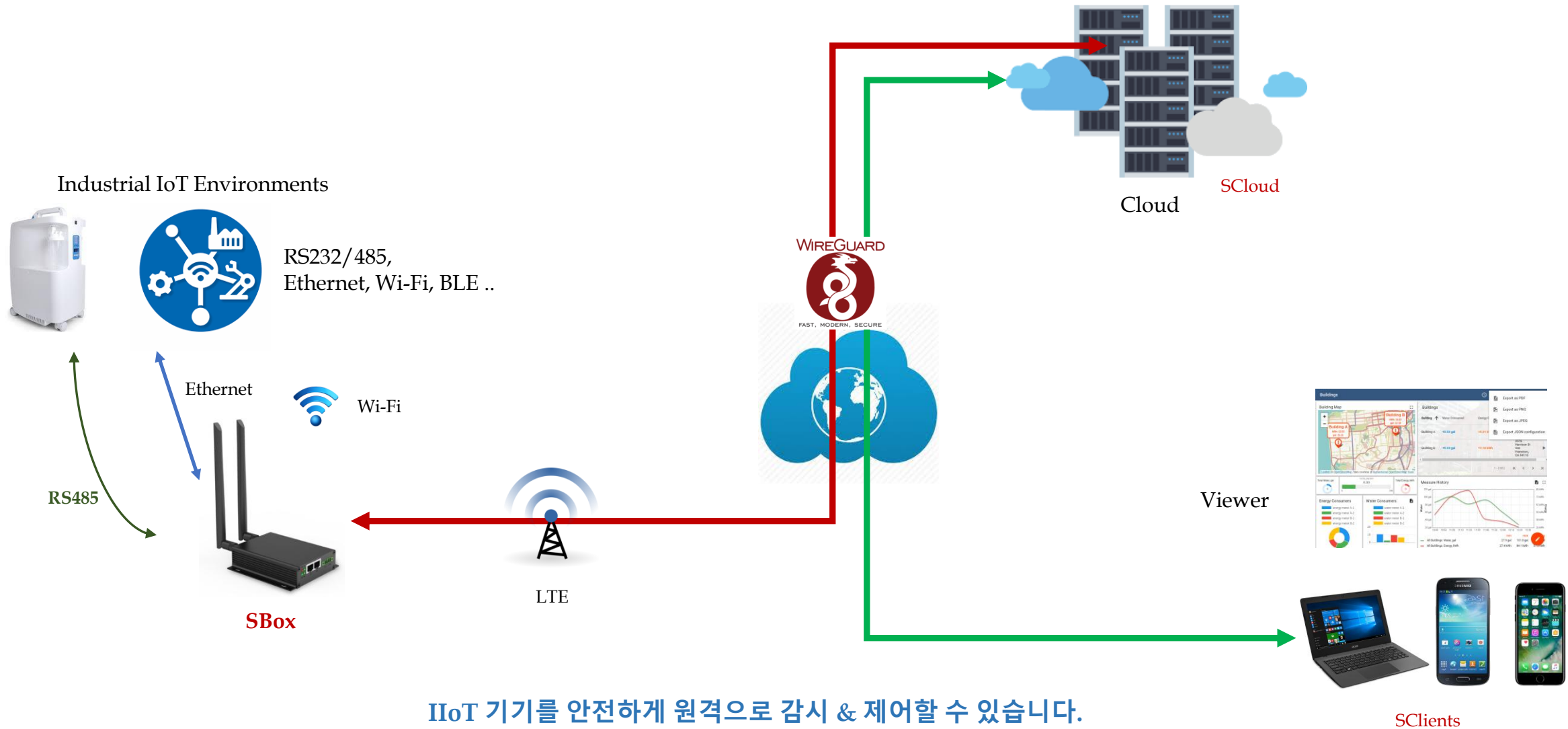
Smart Home Network 보안



Smart Home Network 기기를 안전하게 원격으로 감시 & 제어할 수 있습니다.

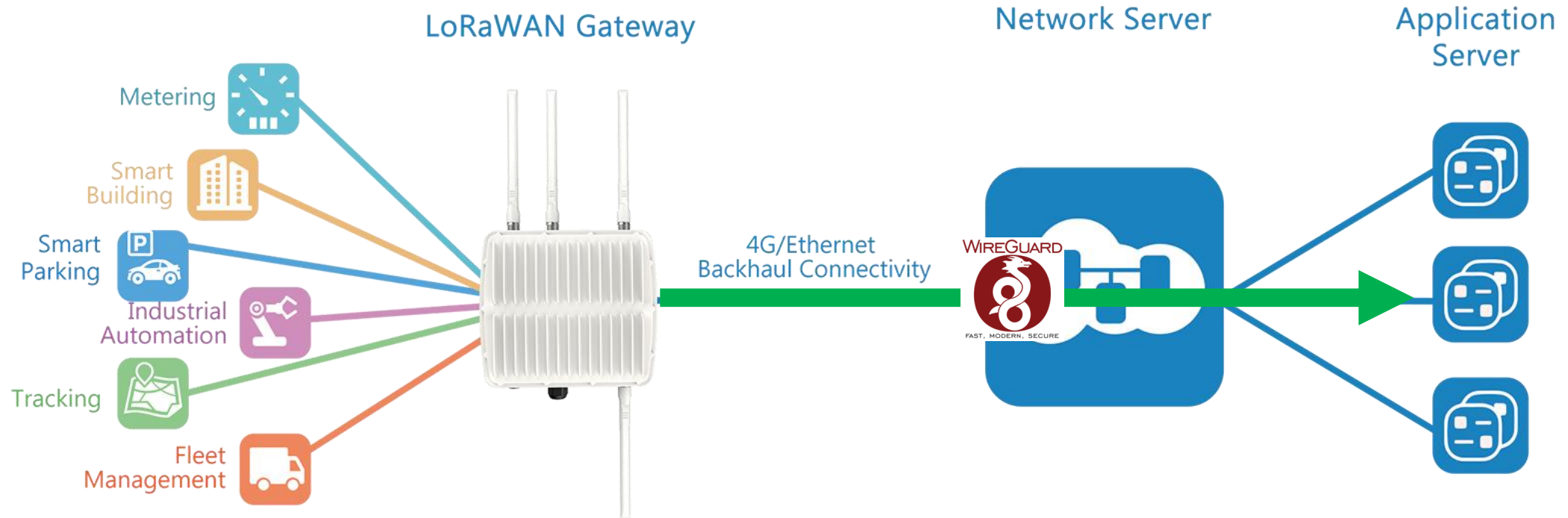
3. EndSec(6) – Use Cases(4)

Industrial IoT 보안



3. EndSec(6) – Use Cases(5)

LoRaWAN 보안



LoRaWAN Gateway 뒷 단의 데이터를 안전하게 보호할 수 있습니다.

3. EndSec(6) – Use Cases(6)

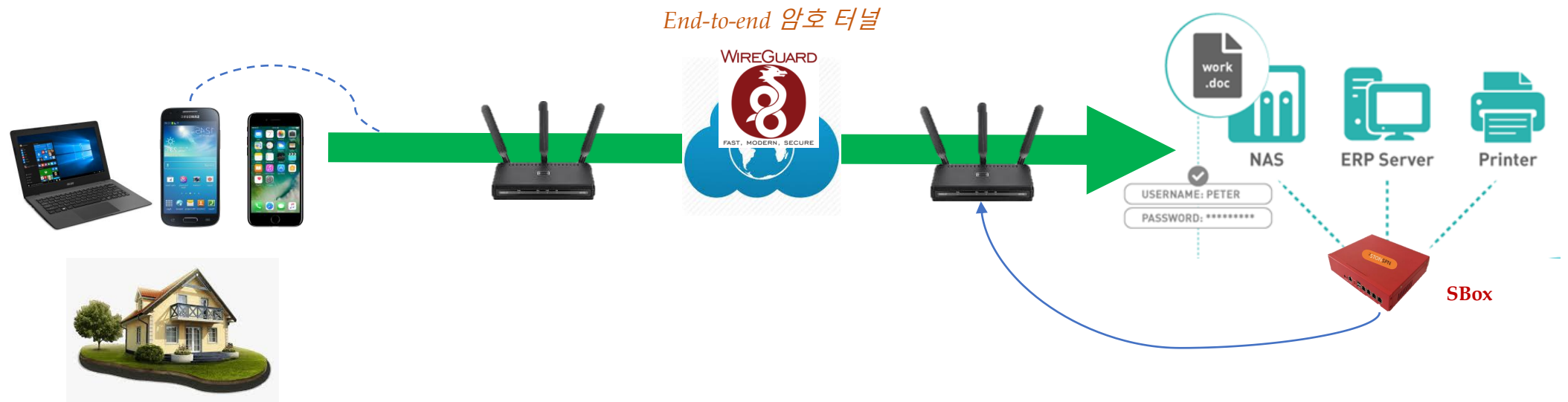
POS 결제 보안



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

3. EndSec(6) – Use Cases(7)

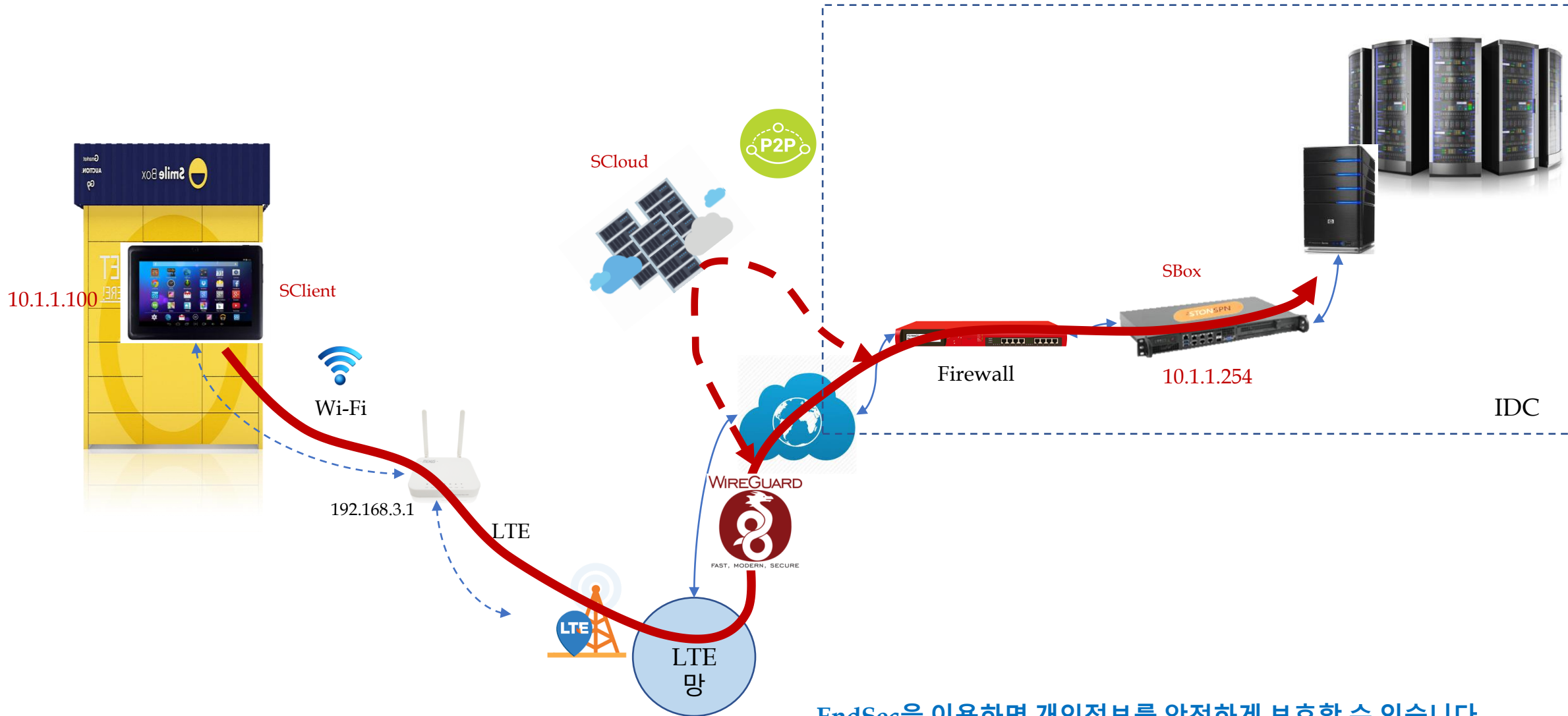
Online Shopping 보안



EndSec을 Online shopping에 필요한 개인 정보, 신용 카드 정보, 은행 정보, 주소 등을 안전하게 보호할 수 있습니다.

3. EndSec(6) – Use Cases(8)

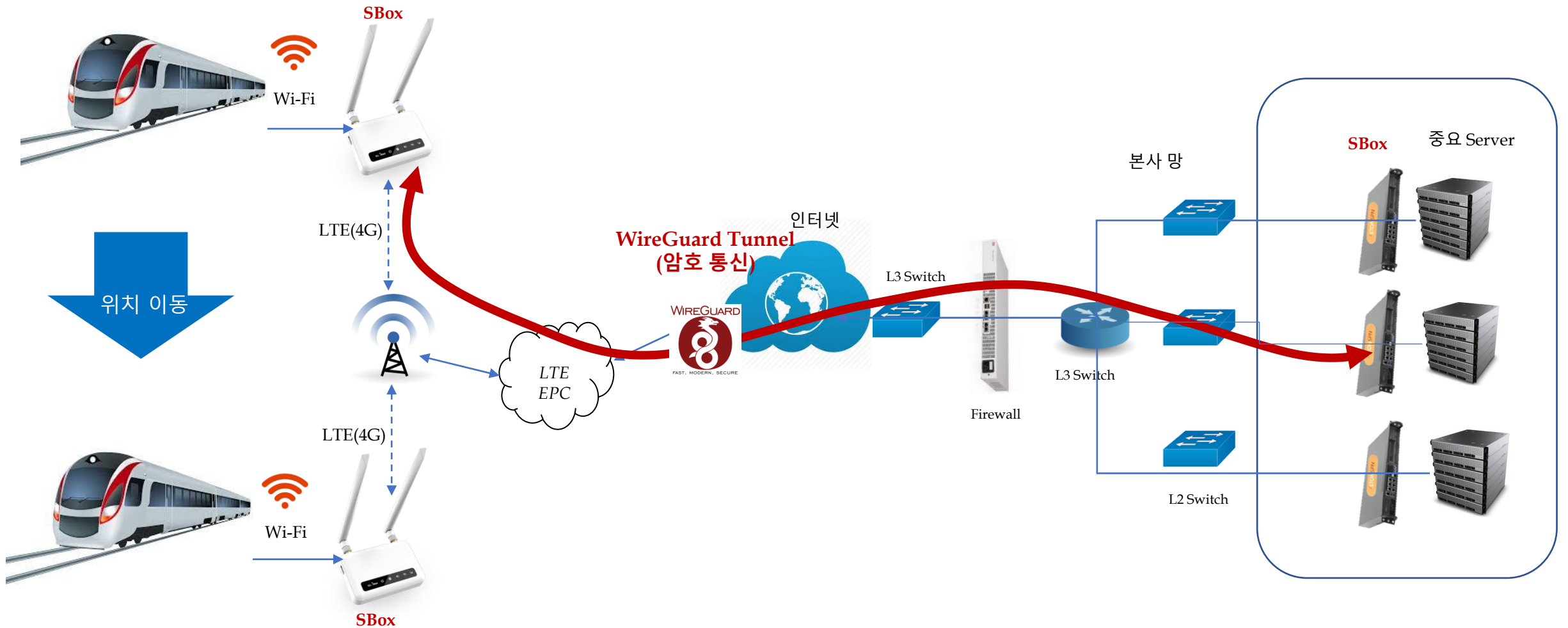
무인택배함 보안



EndSec을 이용하면 개인정보를 안전하게 보호할 수 있습니다.

3. EndSec(6) – Use Cases(9)

LTE 이동 데이터 보안

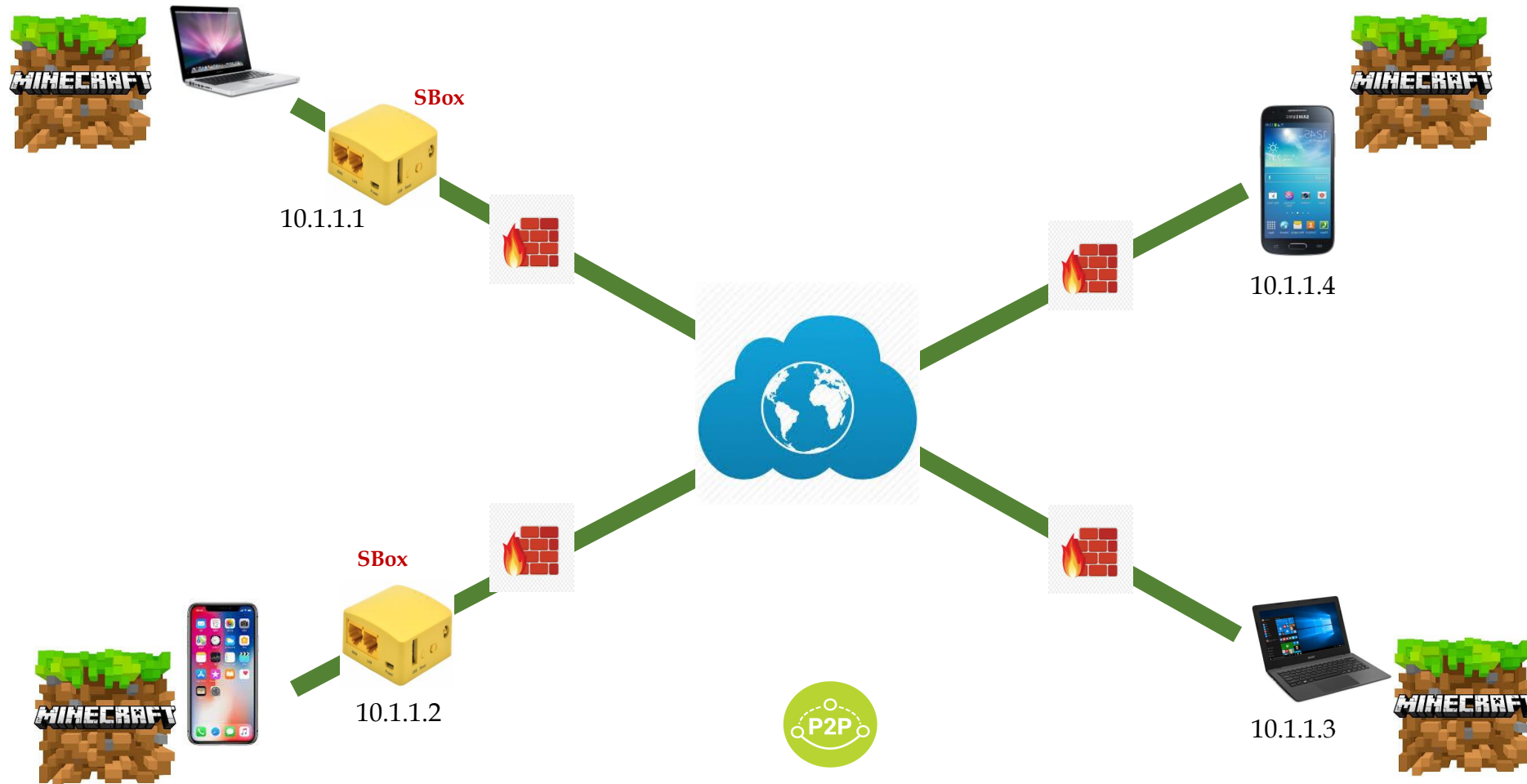


달리는 기차 위에서도 안전하게 회사 서버에 접속하여 업무를 볼 수 있습니다.

3. EndSec(6) – Use Cases(10)

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)

중형 SBox & SClients

중형 SBox & SClients

SiOS

Windows

SClient S/W

SAndroid

WebUI

CLI

SBox

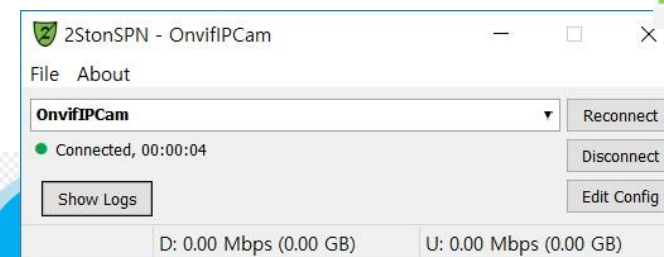
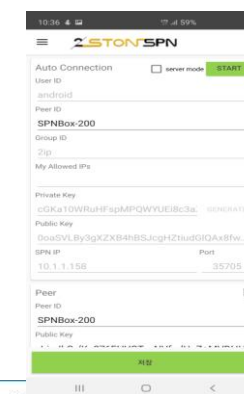
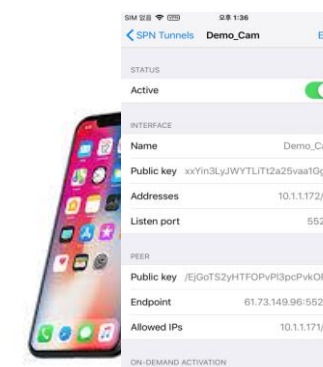
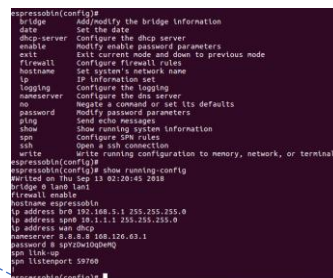
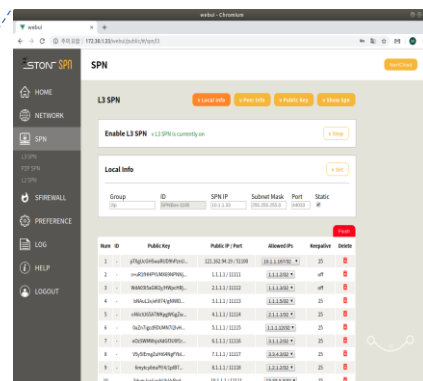
중형 Security Gateway



SBox-1400



SBox-3000



3. EndSec(8) - 전략

- 기본 전략

- ✓ 제품의 성격 상, 유관 업체(예: Coldchain 업체, POS 제조사, 원격 진료 업체, Home Network 제품 개발사, Online shopping 업체 등)와의 긴밀한 관계를 통해 Project 형태로 진행하는 것이 타당해 보임.
- ✓ 많은 것을 벌리기 보다는 1~2군데 확실한 시장을 개척하는 것이 중요할 듯 보임.

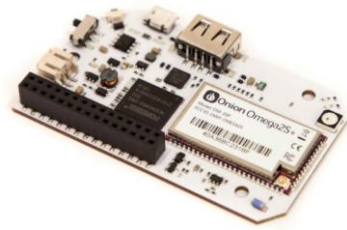
- 참고 사항

- ✓ HTTPS를 사용하여 Web 기반으로 서비스하는 경우와 자체 보안 기능을 무장한 제품과는 경쟁 관계에 놓이게 됨(이를 극복할 수 있어야 함).
- ✓ 신규로 시작하는 사업의 경우는 EndSec이 효과적일 것이나, 이미 HTTPS Web 기반으로 구현되어 있는 경우는 문제가 될 것임(EndSec의 장점을 부각시켜야 함).

4. IoT Security Gateway **SBox**

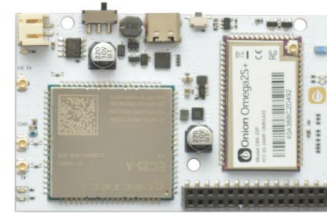


4. SBox(1) – Security Gateway Boards



SBox-OW

(Based on Omega2 Pro, WiFi to WiFi)



SBox-OL

(Based on Omega2 LTE, WiFi to LTE)



SBox-R

(Based on Raspberry Pi)



SBox-G

(Based on GrapeBoard)



SBox-E

(Based on ESPRESSObin)

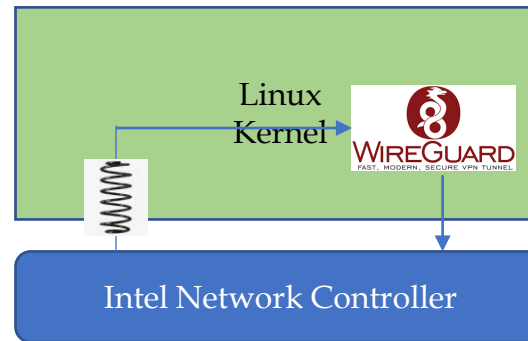
4. SBox(2) – Tiny Security Gateway



Gl.iNet Wireless Router + vIoTSec S/W

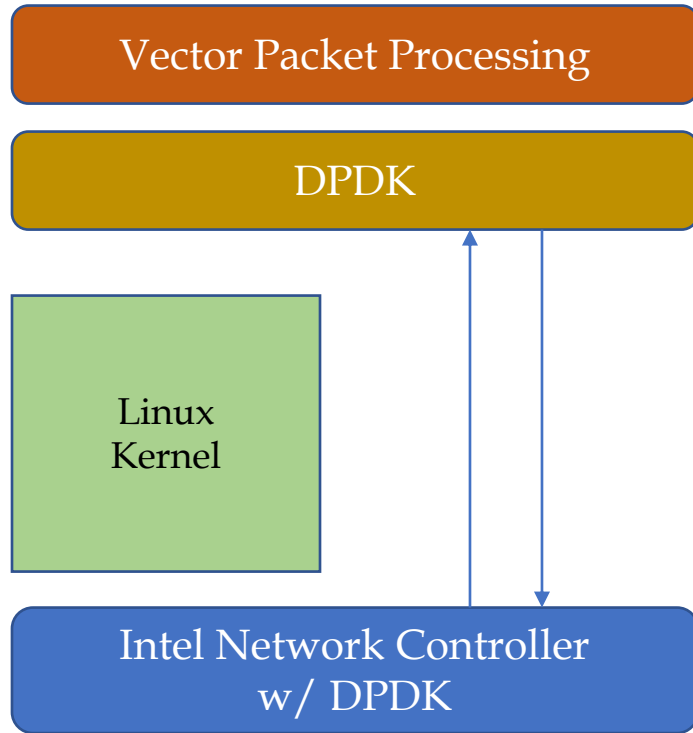
4. SBox(3) – Medium Security Gateway

Network Appliances powered by Intel CPU



Very Fast Security Gateway

4. SBox(4) – High Performance Security Gateway(1)



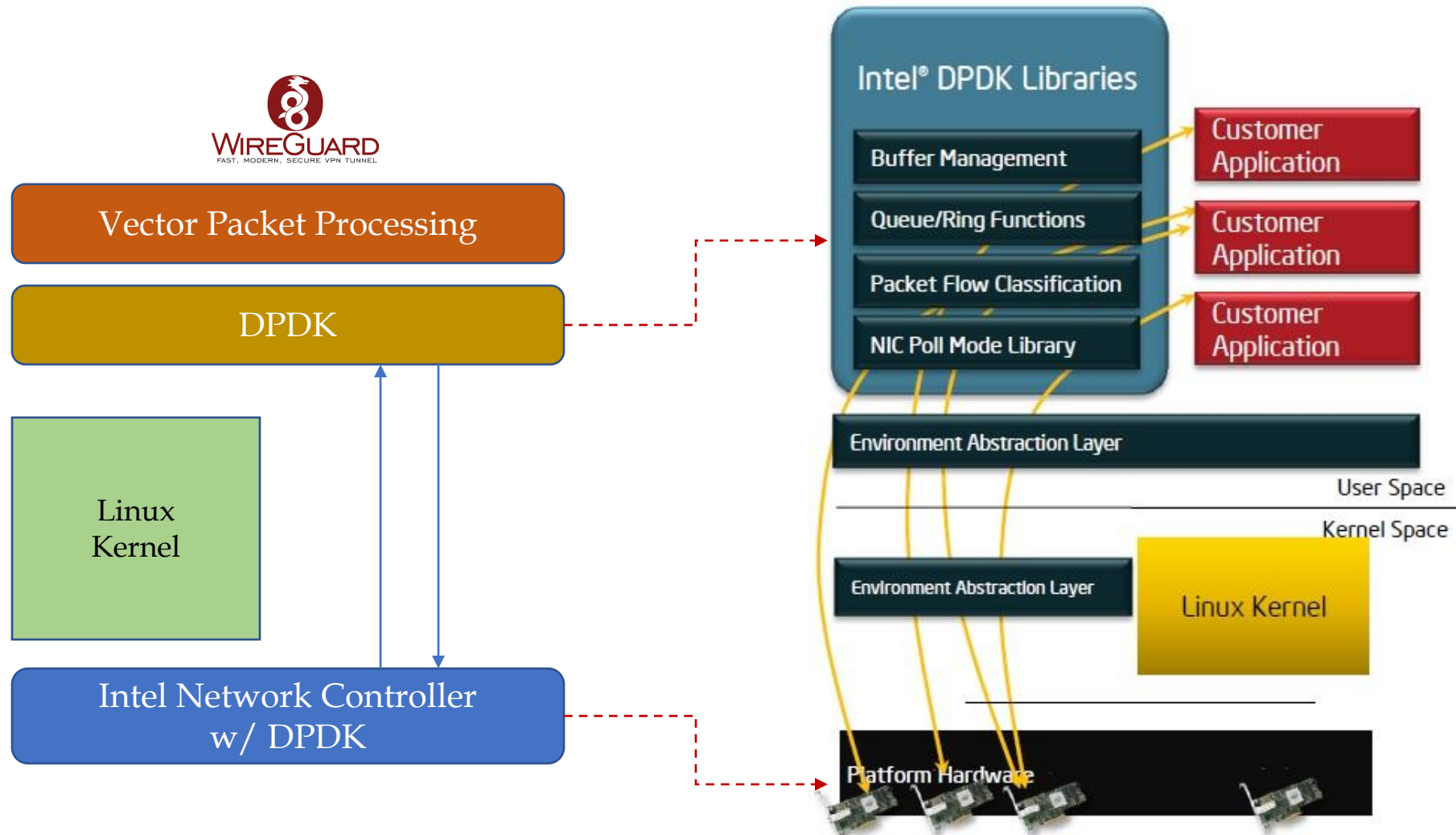
ASIC이나 FPGA를 사용하지 않고도 고성능의 Security Gateway를 만들 수 있습니다.

Network Appliances powered by Intel CPU

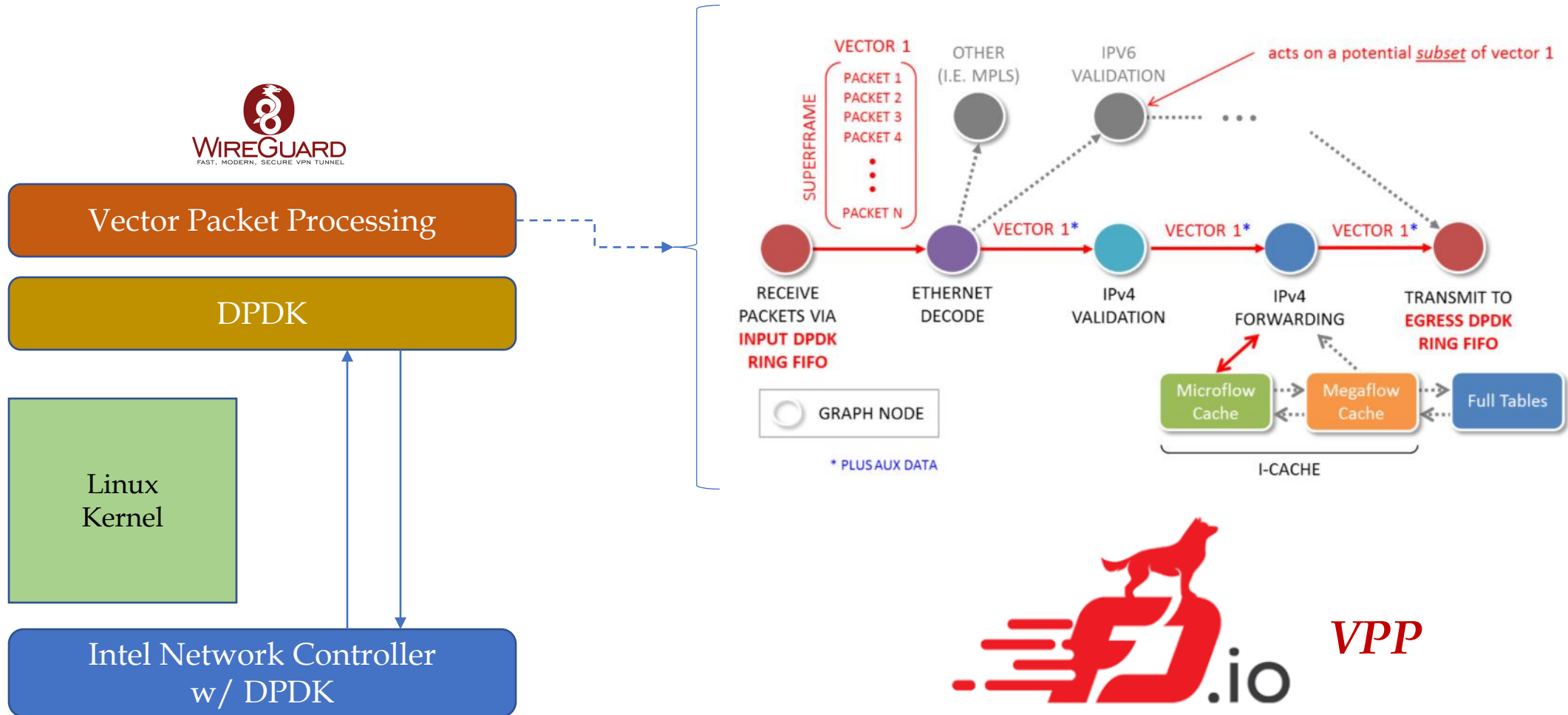


(H/W 제품 스펙은 변경될 수 있음)

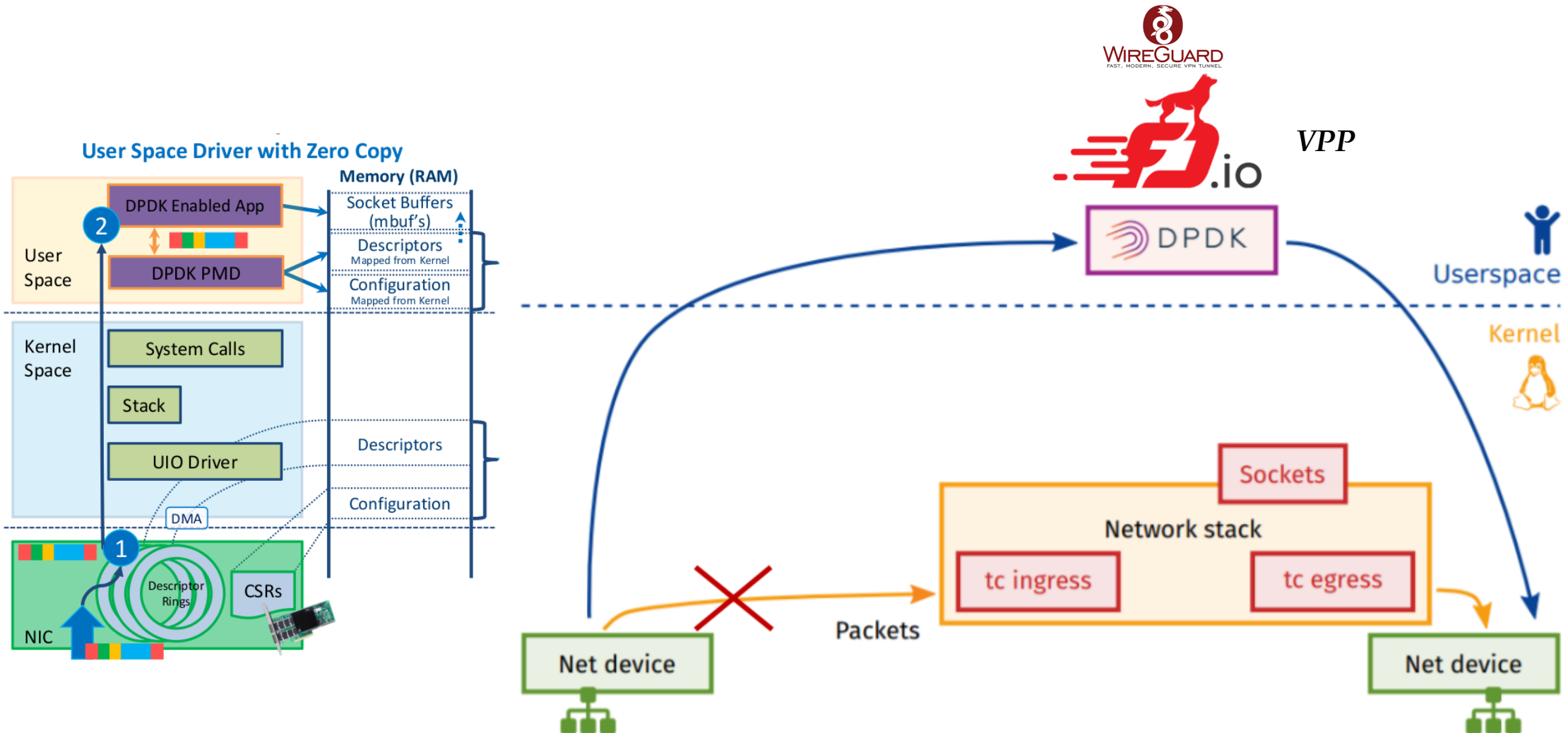
4. SBox(4) – High Performance Security Gateway(2)



4. SBox(4) – High Performance Security Gateway(3)



4. SBox(4) – High Performance Security Gateway(4)



5. IoT RTOS

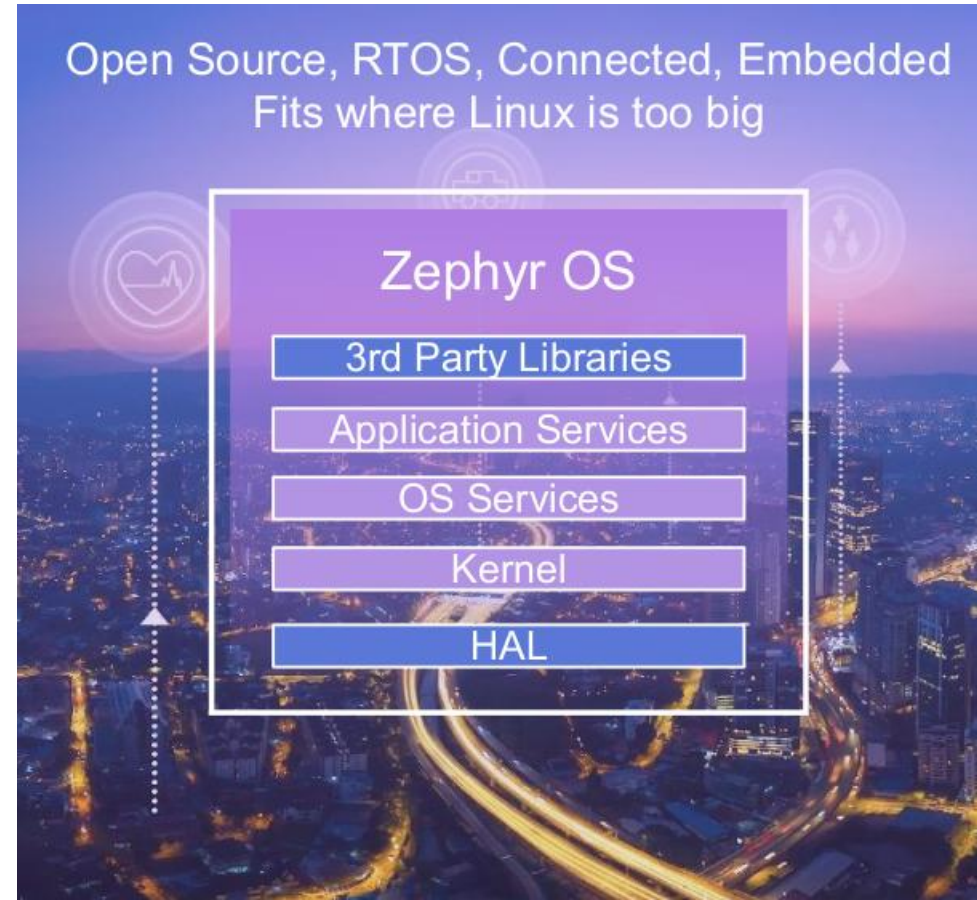
: Zephyr, mbed OS, FreeRTOS



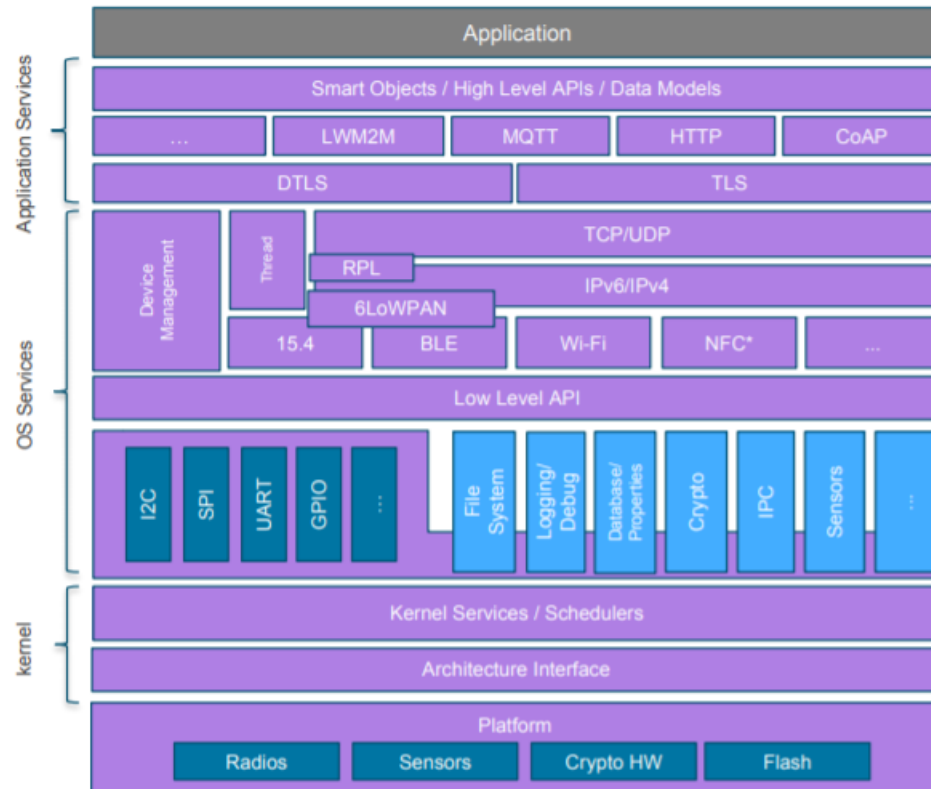
5. IoT RTOS(1) - Zephyr Project(1)



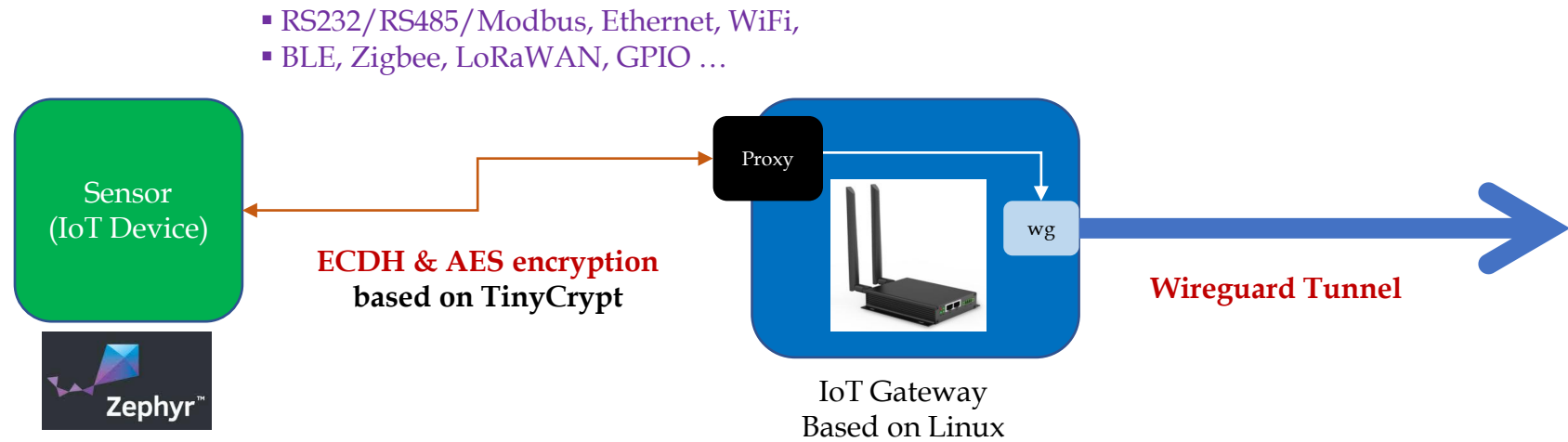
RTOS 계의 새로운 바람



5. IoT RTOS(1) - Zephyr Project(2)



5. IoT RTOS(1) - Zephyr Project(3)



IoT Device ~ IoT Gateway : ECDH & AES encryption based on TinyCrypt


5. IoT RTOS(2) – ARM MbedOS(1)


Bluetooth LE


Wi-Fi


6LoWPAN Sub-
GHz Mesh



NFC

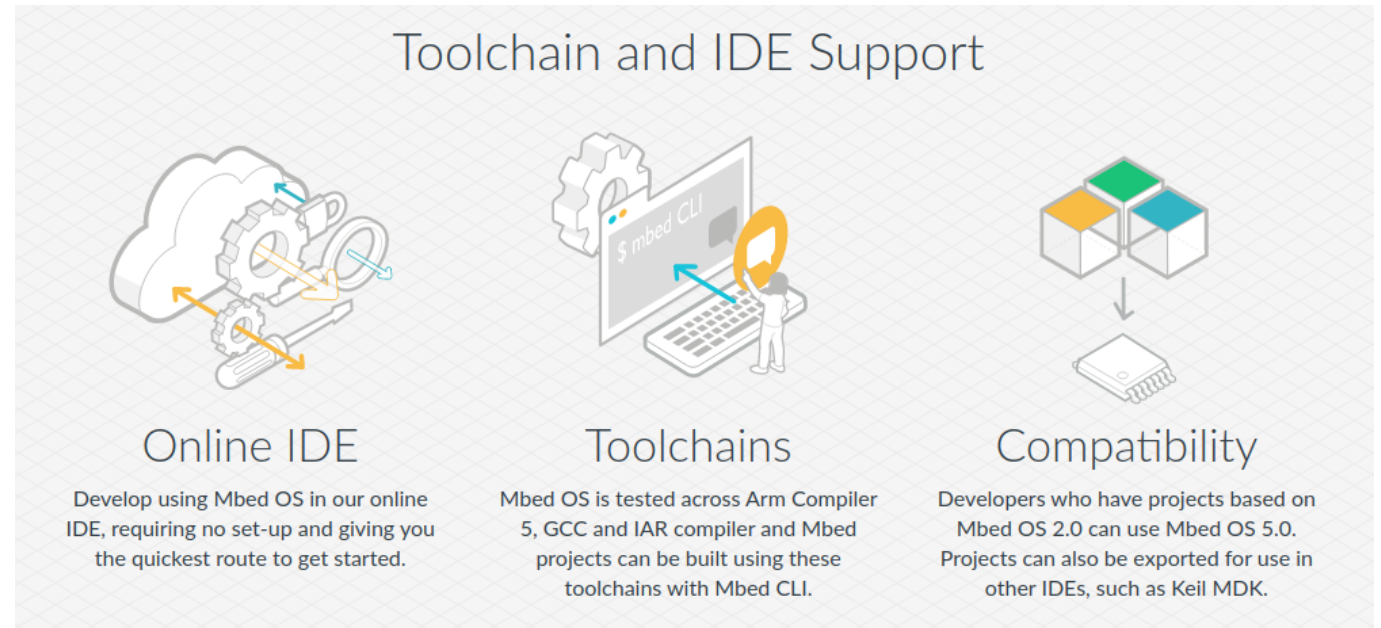

Thread


LoRa LPWAN

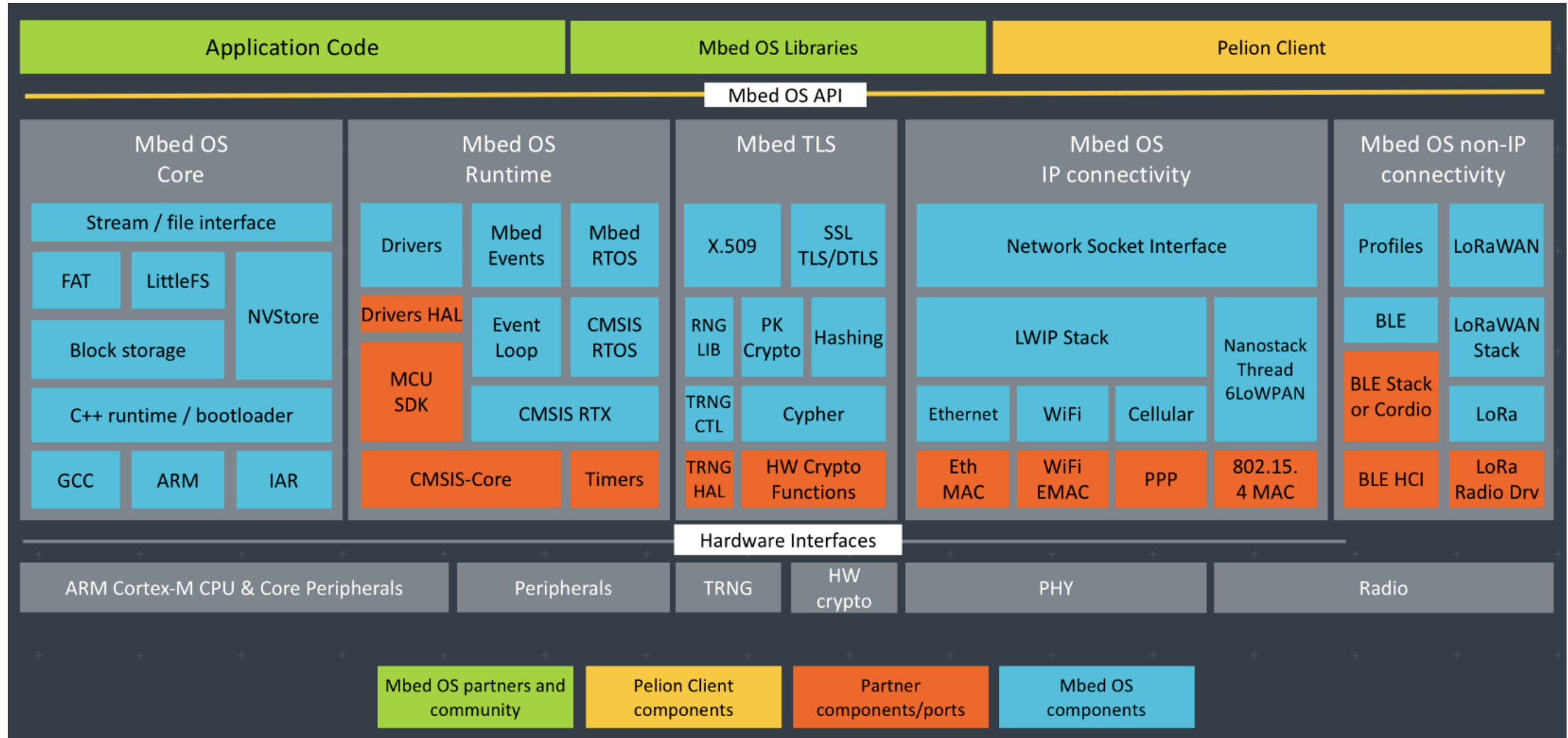

RFID


Ethernet

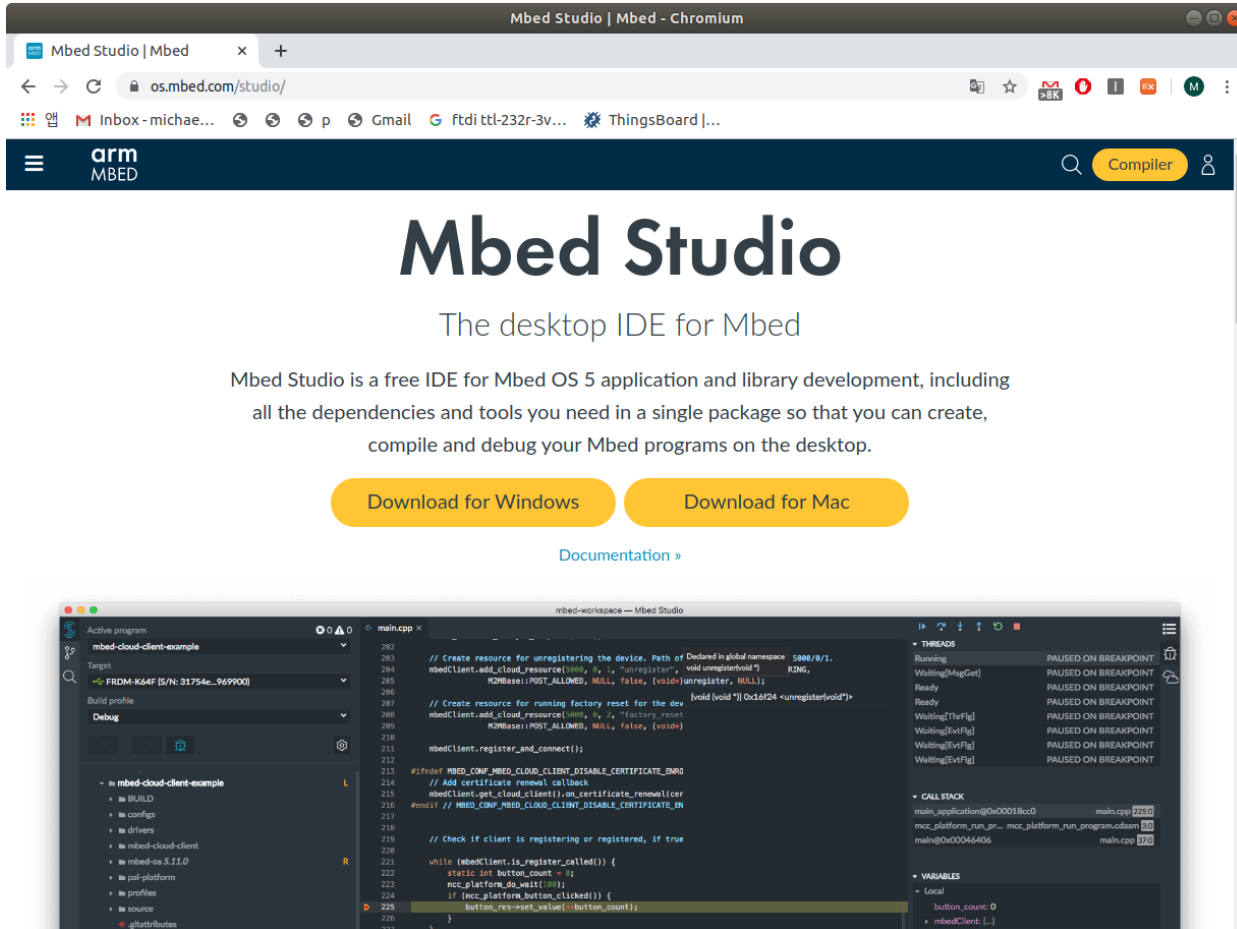

Cellular



5. IoT RTOS(2) – ARM MbedOS(2)



5. IoT RTOS(2) – ARM MbedOS(3)



Mbed Studio | Mbed - Chromium

Mbed Studio | Mbed

os.mbed.com/studio/

arm MBED

Mbed Studio

The desktop IDE for Mbed

Mbed Studio is a free IDE for Mbed OS 5 application and library development, including all the dependencies and tools you need in a single package so that you can create, compile and debug your Mbed programs on the desktop.

[Download for Windows](#) [Download for Mac](#)

[Documentation »](#)

Active program: mbed-cloud-client-example

Target: FRDM-K64F [5/N: 31754e-969900]

Build profile: Debug

```
202 // Create resource for unregistering the device. Path of Declared in global namespace 5000/8/1.
203 mbedClient.add_cloud_resource(000, 8, 1, "unregister", void_unregister(void*) 0000,
204                               KDBase::POST_ALLOWED, NULL, false, (void*)unregister, NULL);
205
206 // Create resource for running factory reset for the dev
207 mbedClient.add_cloud_resource(000, 8, 2, "factory_reset",
208                               KDBase::POST_ALLOWED, NULL, false, (void*)
209                               [void(void*) 0x16224 <unregister(void*)]
210                               mbedClient.register_and_connect();
211
212 #ifdef MBED_CONF_MBED_CLOUD_CLIENT_DISABLE_CERTIFICATE_BN
213 // Add certificate removal callback
214 mbedClient.get_cloud_client().on_certificate_removal(
215     #endif // MBED_CONF_MBED_CLOUD_CLIENT_DISABLE_CERTIFICATE_BN
216
217 // Check if client is registering or registered, if true
218
219 while (mbedClient.is_register_called()) {
220     static int button_count = 0;
221     mbedClient.get_cloud_client().on_certificate_removal(
222         if (mbedClient.button_clicked()) {
223             button_count++;
224             button_count = 0;
225         }
226     }
227 }
```

THREADS

Running	PAUSED ON BREAKPOINT
Waiting[MagGet]	PAUSED ON BREAKPOINT
Ready	PAUSED ON BREAKPOINT
Ready	PAUSED ON BREAKPOINT
Waiting[ThrFg]	PAUSED ON BREAKPOINT
Waiting[EvtFg]	PAUSED ON BREAKPOINT
Waiting[EvtFg]	PAUSED ON BREAKPOINT
Waiting[EvtFg]	PAUSED ON BREAKPOINT

CALL STACK

main_application@0x00018cd	main.cpp 225
mcc_platform_run_pr...	mcc_platform_run_program.cdsam 10
main@0x00045406	main.cpp 225

VARIABLES

Local
button_count: 0
mbedClient: [...]



5. IoT RTOS(3) – FreeRTOS and ESP32(1)




ESP32

A feature-rich MCU with integrated Wi-Fi and Bluetooth connectivity for a wide-range of applications




5. IoT RTOS(3) – FreeRTOS and ESP32(2)

 **ESPRESSIF**


ESP-IDF

Espressif's official IoT Development Framework for the ESP32 and ESP32-S series of SoCs.

[Learn More](#)


ESP HomeKit SDK

Control your Home from your iPhone, iPad or Apple Watch.

[Learn More](#)

ESP-ADF

Espressif's official audio development framework for the ESP32 and ESP32-S2 SoCs.

[Learn More](#)

ESP-AT

Use our AT command firmware solution to go wireless.

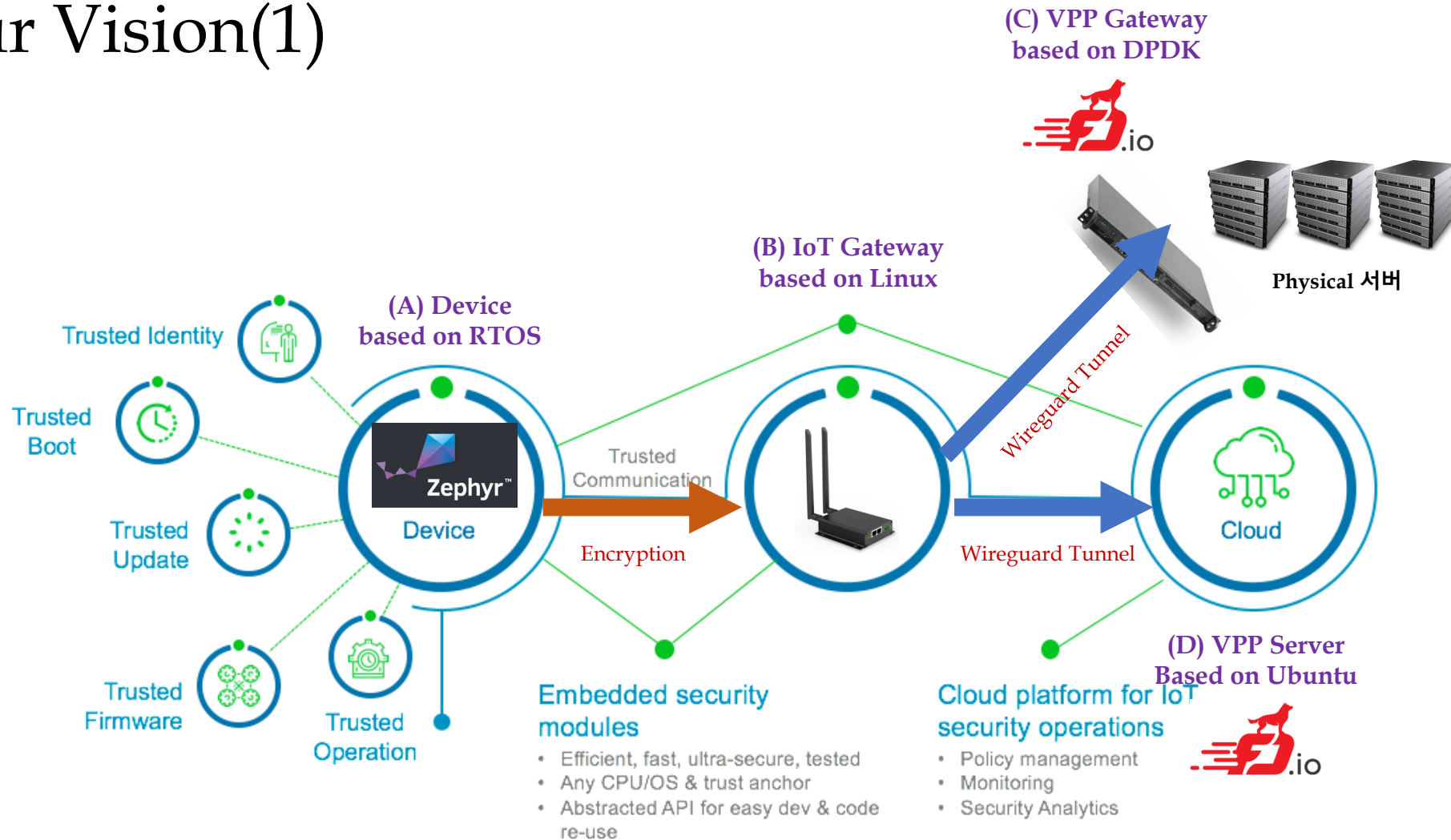
ESP-WIFI-MESH

Enable more nodes to directly connect to the same router.

ESP-TOUCH

Connect your device to Wi-Fi through Smart Config on your phone.

6. Our Vision(1)



From IoT devices to cloud or physical servers

6. Our Vision(2)

- 1) IoT Sensor ~ IoT Gateway ~ Server(Cloud) 구간의 안전한 암호 통신 Infra & Solution 제
공
 - ✓ *Sensor + IoT Gateway(SBox) + Server Gateway(SBox) + Mobile Viewer*
- 2) Embedded Linux & Wireguard 기반 Secure Gateway 개발 및 연구
 - ✓ *Tiny Gateway based on OpenWrt, Medium Gateway based on Ubuntu Core*
- 3) DPDK & VPP 기반 고성능 Secure Gateway 개발 및 연구
- 4) RTOS 기반 IoT Device 및 Protocol 개발 및 연구
- 5) 암호 통신 Protocol 개발 및 연구
- Scope: **Connectivity & Security**
- Motto: **Let's connect all IoT devices safely !**

Let's connect all IoT devices safely !

We Secure the Internet of Things with vIoTSec !



Thank You