

2ip 2STON™ SPN *POS* GUARD

Simplified Version

2ip, Inc.

Doc. Revision: 1.5

Copyright© 2018-2020, 2ip Inc. All Rights Reserved.



Contents

- 1. POS 보안의 필요성
- 2. 2ip POS-GUARD 시스템
- 3. POS-GUARD Smart Firewall
- 4. POS-GUARD S/W 원격 Upgrade
- 5. POS-GUARD Specifications



1. POS(Point of Sale) 보안의 필요성(1)



POS 시스템, 악성코드에 대거 감염...윈도XP 등 구형 OS 이용이 빌미

노동균 기자



입력 2018.07.15 06:00

최근 2000년 출시된 윈도 XP를 기반으로 동작하는 판매시점 정보관리 시스템(POS)이 대거 악성코드에 감염되는 일이 발생했다. 2017년 금융자동화 기기(ATM) 악성코드 감염 사고도 보안에 취약한 구형 운영체제(OS)가 빌미가 됐다는 점에서 스마트폰이나 컴퓨터뿐 아니라 특수목적 시스템의 보안 관리 중요성이 부각된다.



IT Chosun 뉴스레터 구독

#신종 코로나 확산
과밀 접촉하다

코로나 바이러스 퍼지자 전염병 확산
이용자 급증

소셜미디어서 커지는 신종
코로나바이러스 공포

감염병 위기경보 '경계', 우한 입국자
전수조사 추진

접촉
적다

<POS 해킹 관련 기사 - 지상파 방송 3사 기사>

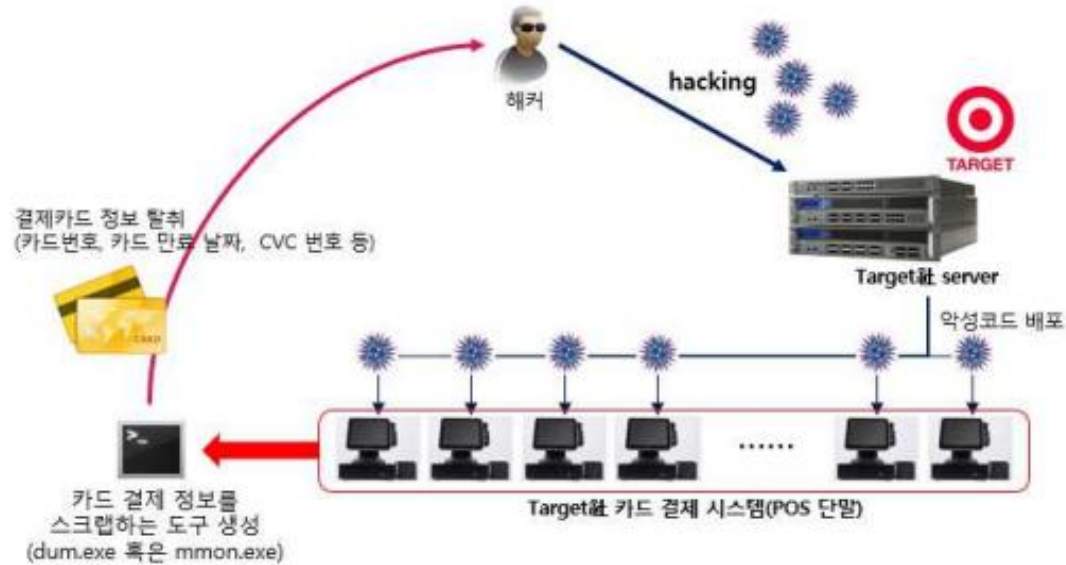
https://imnews.imbc.com/replay/2018/nwtoday/article/4694488_30187.html

<http://d.kbs.co.kr/news/view.do?ncd=3216445>

https://news.sbs.co.kr/news/endPage.do?news_id=N1002218984

POS 단말기에는 고객 이름, 카드번호 카드만료일, CVC/CVV 비밀번호, 매출, 거래 내역 등의 중요 정보가 들어 있다.

1. POS(Point Of Sale) 보안의 필요성(2)



<Target사 결제 카드 정보 유출 사고 개요도>

더욱이 해킹기술이 발달함에 따라 POS 시스템이 설치된 신용카드가맹점에서 카드회원의 개인정보가 유출되고 이를 복제하여 국내 및 해외에서 사용된 것으로 추정되는 사례가 빈번히 발생됨에 따라 모든 가맹점에서는 고객의 개인정보 관리 및 보호에 대한 문제점이 대두되고 있다.

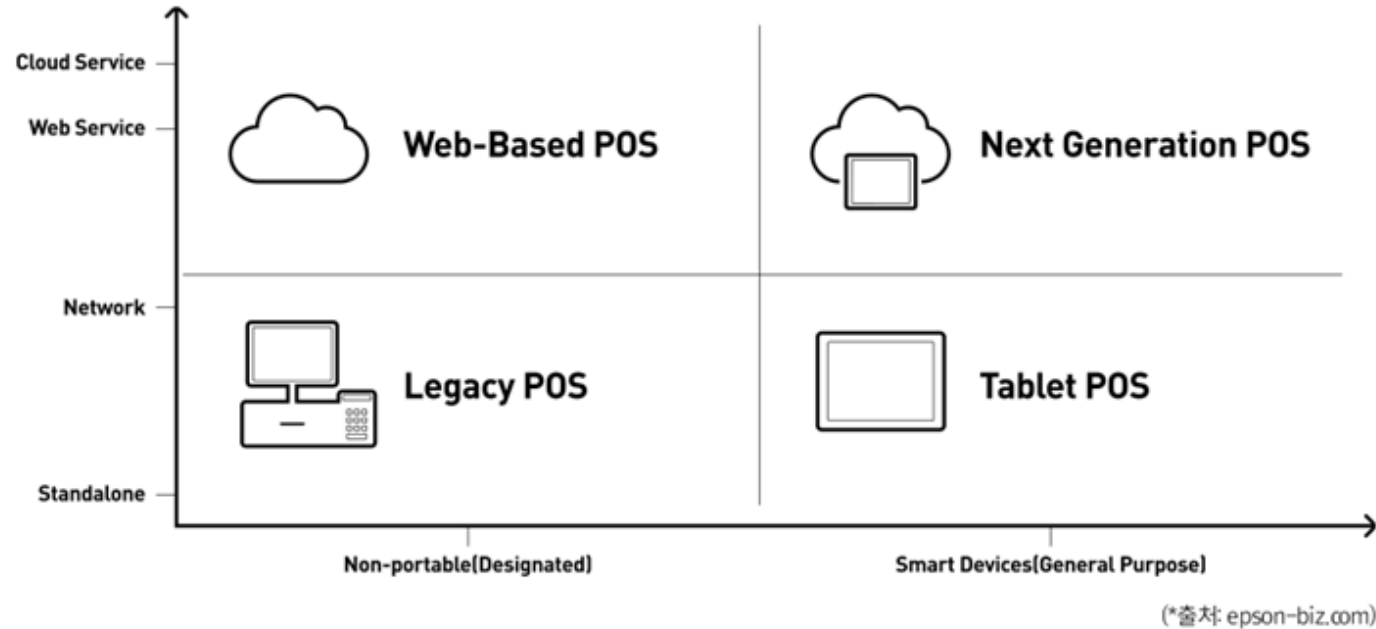
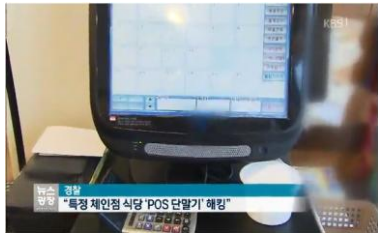
<카드 결제 정보>

▪고객 이름, 카드 번호, 카드 만료일, CVC/CVV 비밀번호

KISA KrCERT POS 해킹 악성코드 사례 보고서 중에서...

이와 같은 상황에서 POS로 인한 카드 정보 유출 사고를 예방하기 위해서는 우선적으로 ① POS 단말기의 업무 외 인터넷 사용을 금지하고, ② 카드사와의 통신과 같은 목적의 IP 및 포트를 제외한 모든 통신 라인에 대한 통제와 차단이 이루어져야 한다. 이는 외부로부터의 접근을 차단하여 악성코드가 유포되는 것을 막을 수 있다. 또한 ③ POS 단말기와 서버 간의 통신에 있어 송수신 되는 데이터는 암호화하여 처리하는 것이 필요하다.

1. POS(Point of Sale) 보안의 필요성(3)

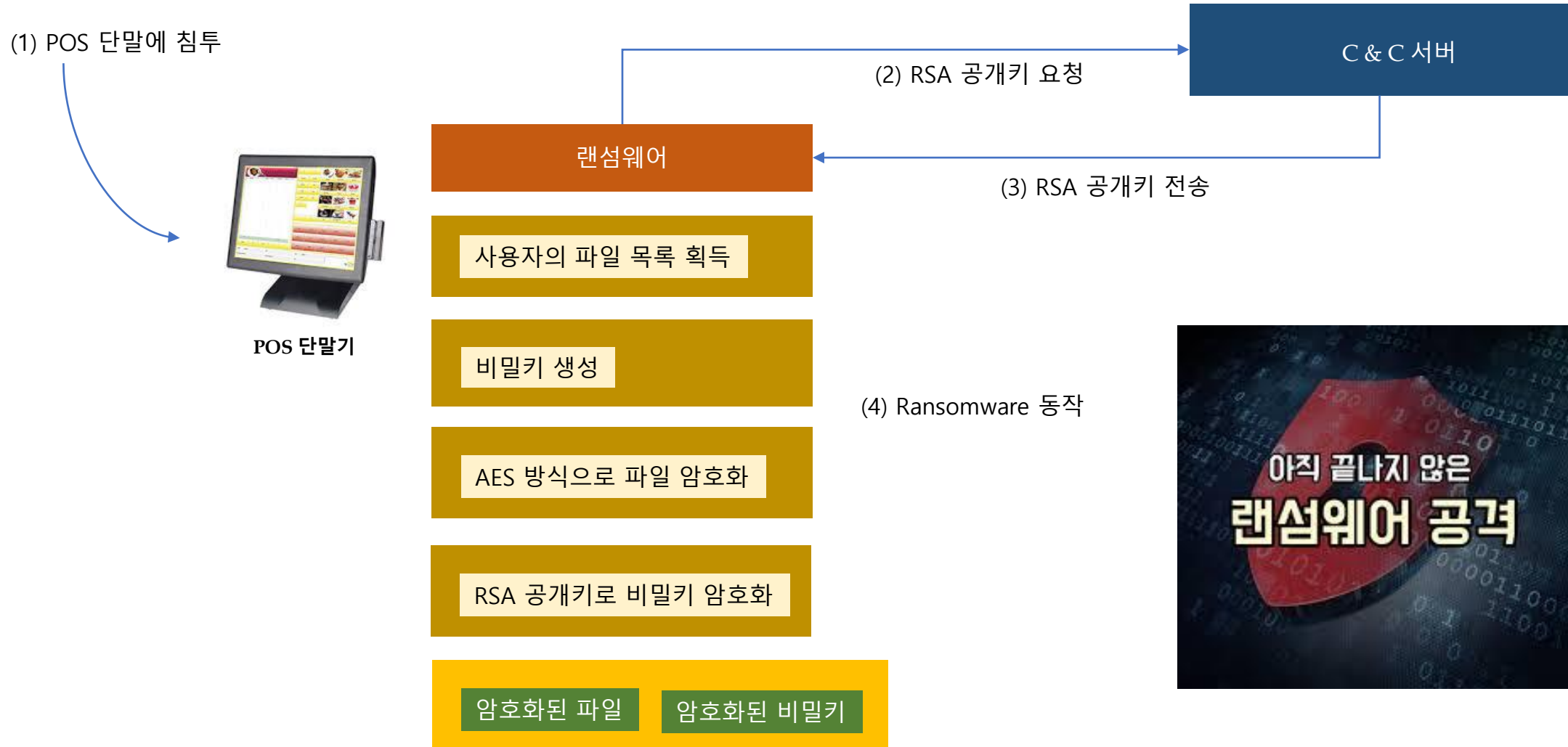


국내 POS 기기 80% 이상
MS 윈도 XP Professional,
XP Embedded, XP POS Ready

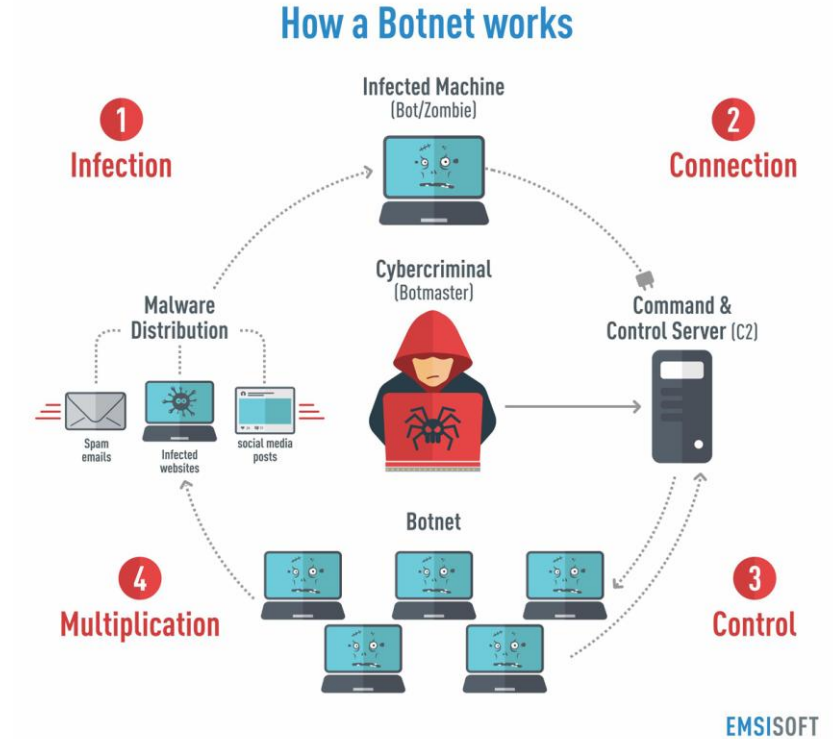
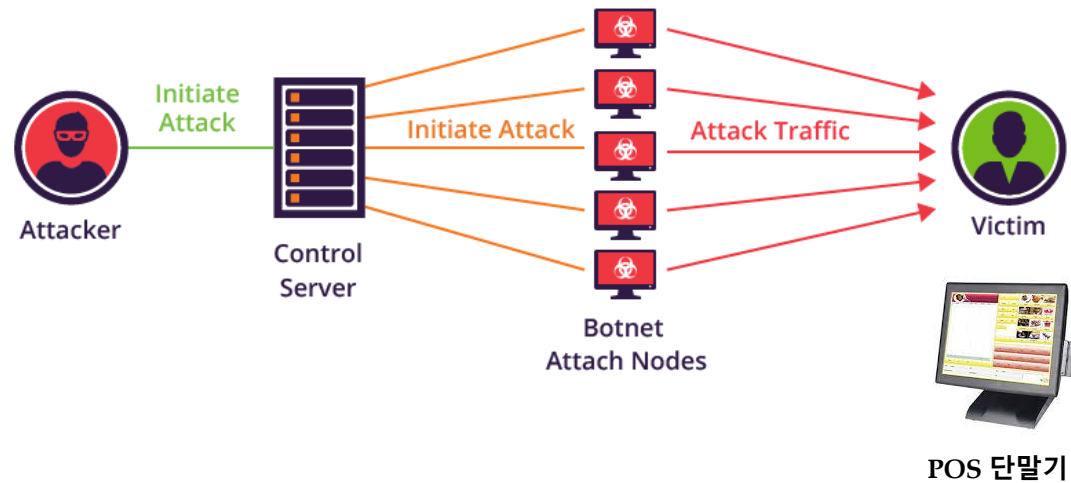


Embedded Linux
Android(Tablet)

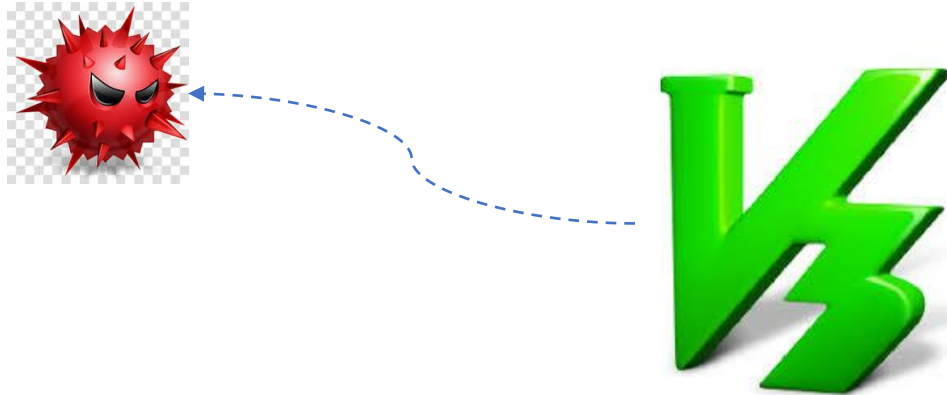
1. POS(Point Of Sale) 보안의 필요성(4) - Ransomware



1. POS(Point Of Sale) 보안의 필요성(5) - Botnet 공격



1. POS(Point Of Sale) 보안의 필요성(6-1)



사후약방문 (死後藥方文) ! 이런 접근 방식이 답일까 ???

1. POS(Point Of Sale) 보안의 필요성(6-2)

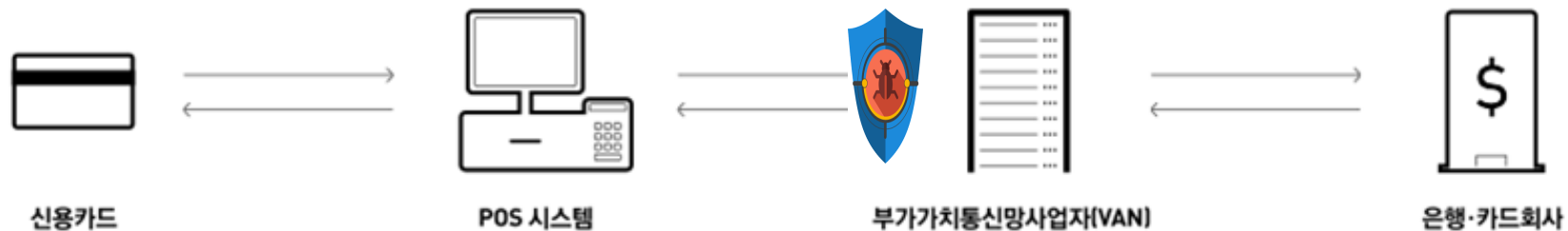


AhnLab EPS는 보다 진화된 방식이기는 하나, 역시 **사후약방문** !

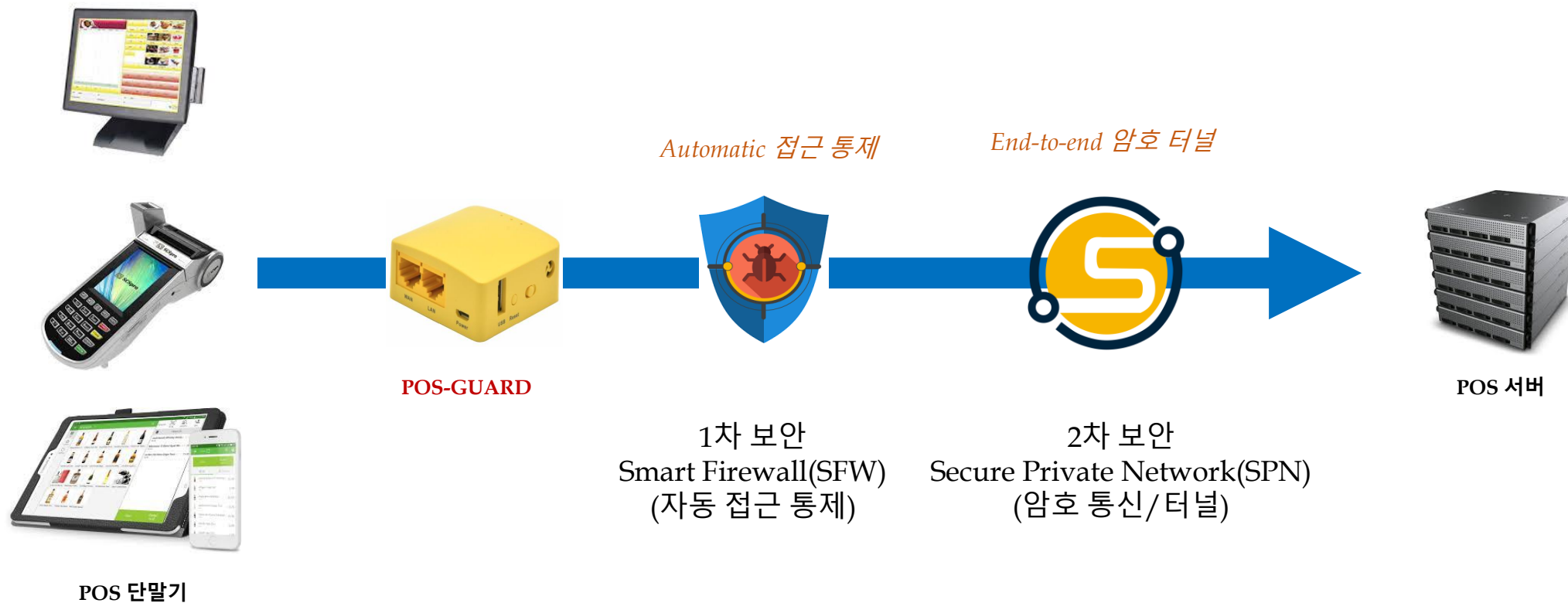
1. POS(Point Of Sale) 보안의 필요성(7)



- 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.




2. 2ip POS-GUARD 시스템(1) - POS 단말 보안



참고: 2차 보안 기능인 SPN을 사용하기 위해서는 POS 서버 앞단에 SPN 장비가 설치되어 있어야 합니다.

2. 2ip POS-GUARD 시스템(2) - POS 단말 개통 절차



1. POS-GUARD에 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. POS-GUARD는 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.**

2. 2ip POS-GUARD 시스템(3) - 2가지 모델



POS-GUARD Lite

일반 POS 단말용



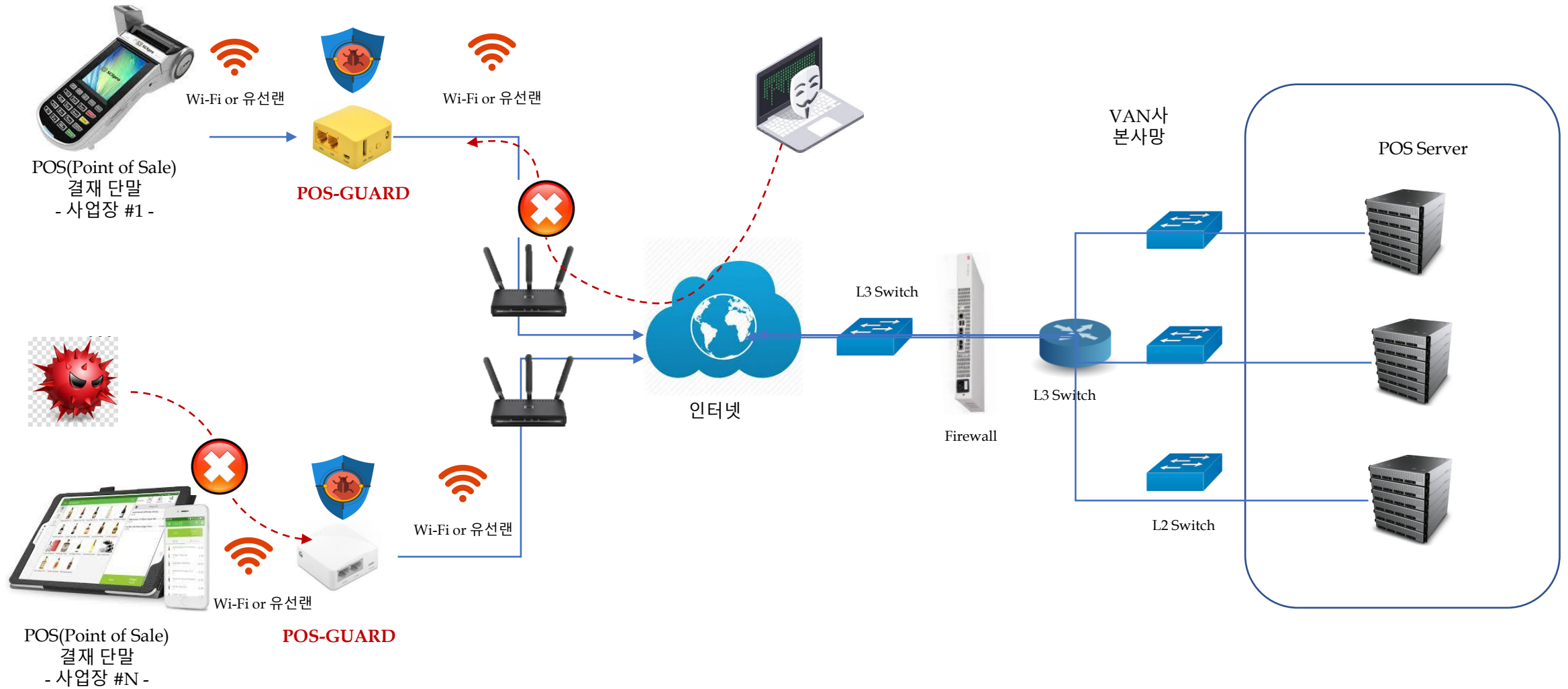
POS-GUARD Premium

복수개의 POS 단말 or Kiosk 용

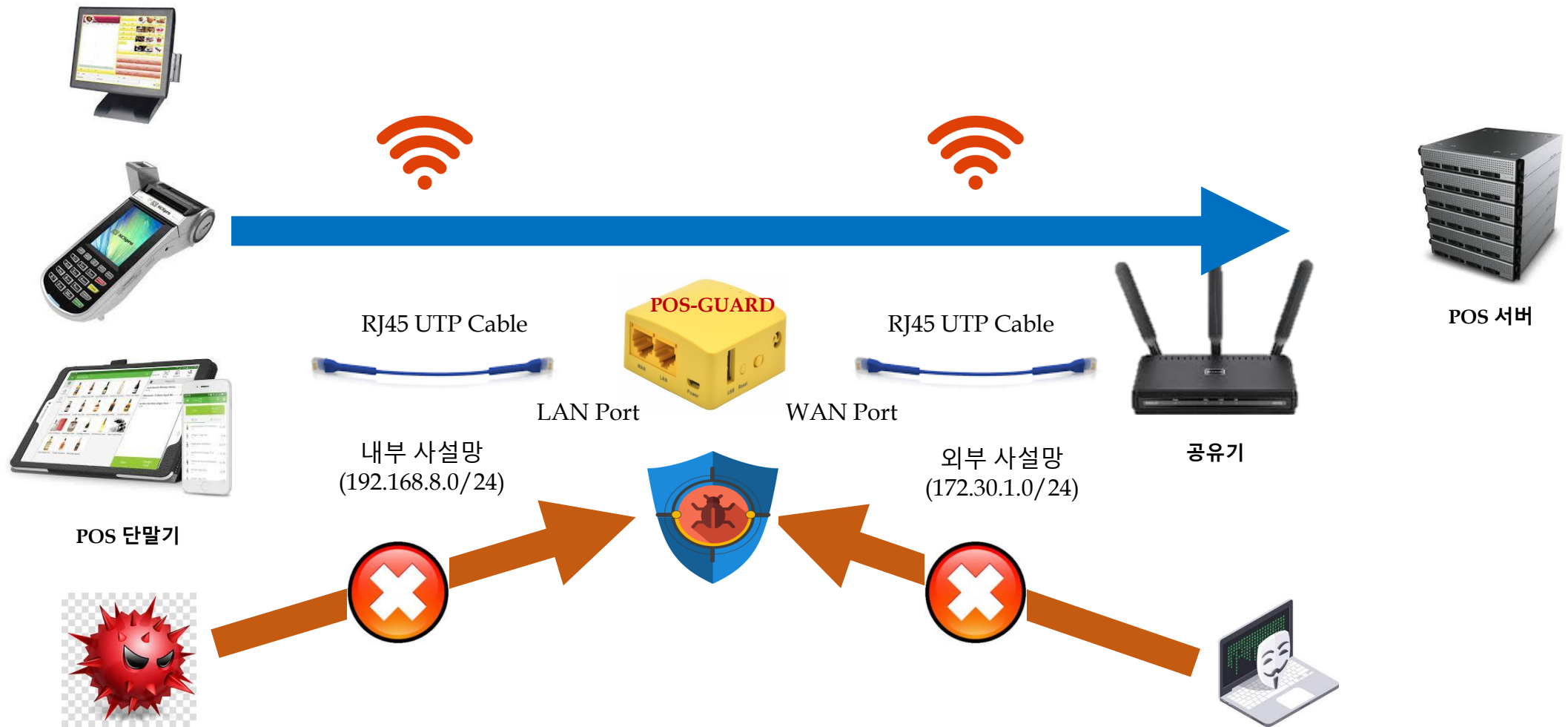
*POS***6GUARD**
Smart Firewall



3. P/G Smart Firewall(1) - 네트워크 구성(1)



3. P/G Smart Firewall(1) - 네트워크 구성(2)



3. P/G Smart Firewall(2) – 3단계 보안 모드(1)

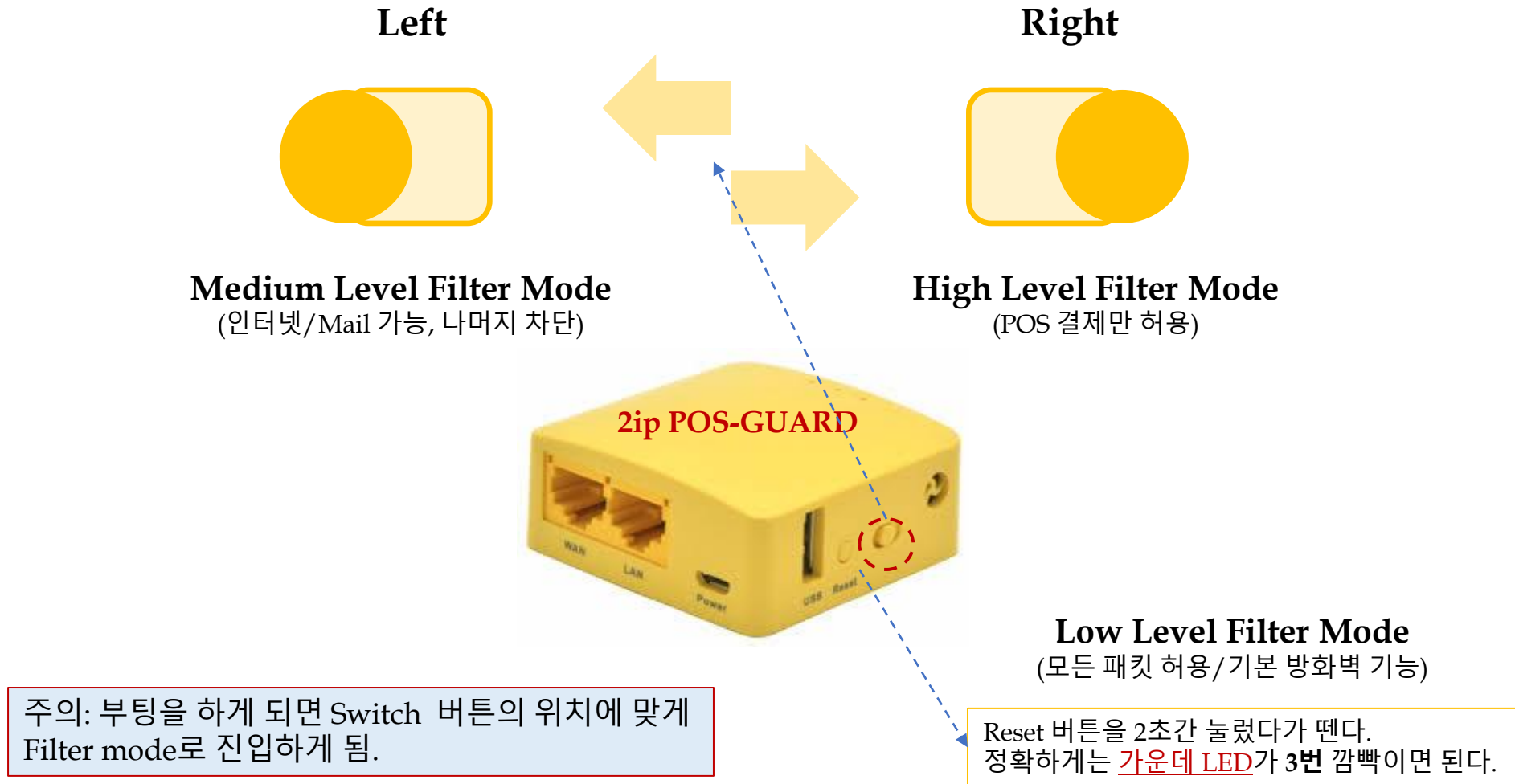
3단계 보안 모드



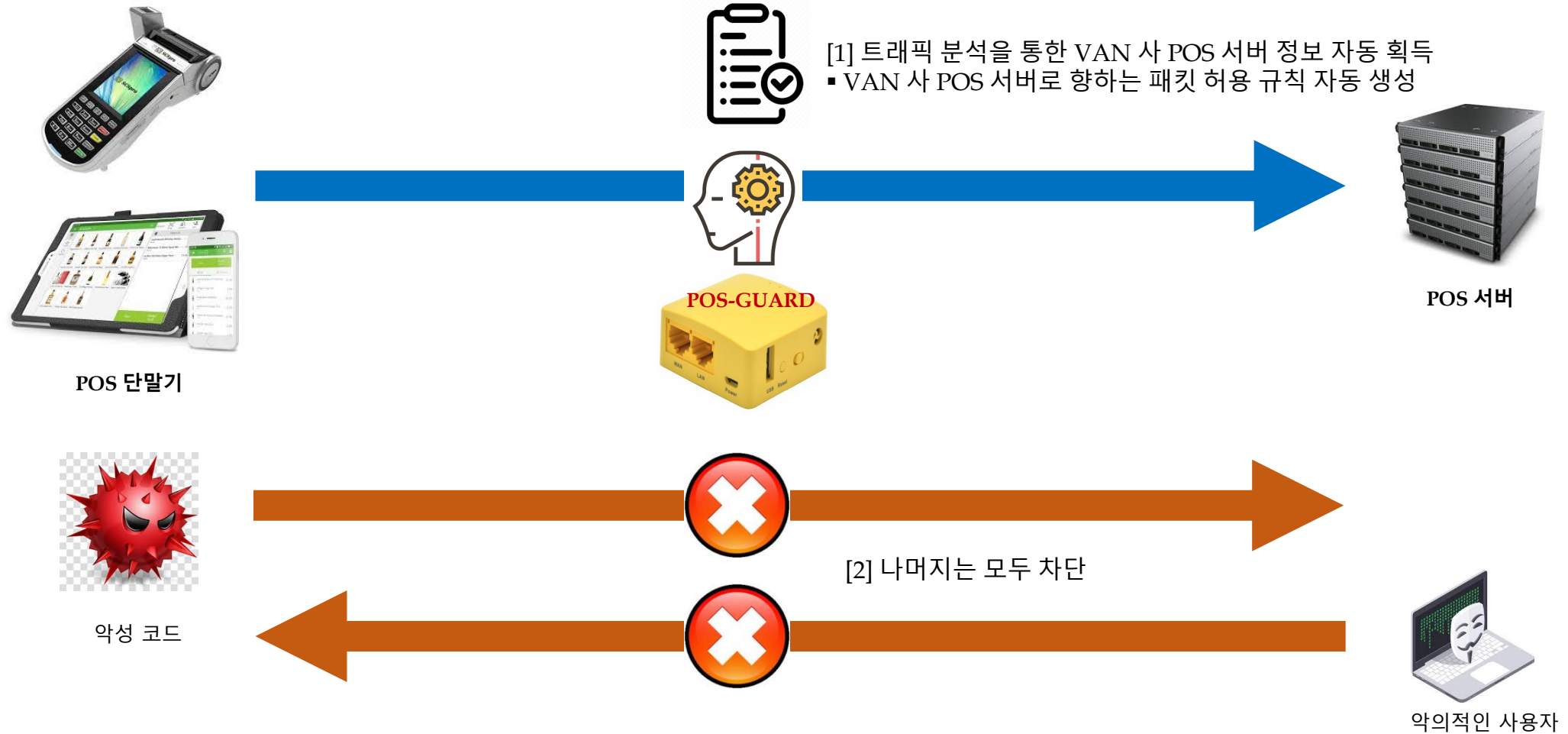
3. P/G Smart Firewall(2) – 3단계 보안 모드(2)

보안 모드	수행하는 내용(Smart Firewall)	비고
High Level 보안 모드 (Right button)	<ul style="list-style-type: none"> ▪ POS 결제 패킷만 허용 (자동 감지) ▪ 나머지는 모두 차단 <ul style="list-style-type: none"> ✓ POS 단말에서 외부망으로 나가는 패킷 ✓ 외부망에서 POS 단말로 들어오는 패킷 ✓ 공유기에 연결된 기기로부터 POS-GUARD 접근 차단 ✓ POS-GUARD에 Wi-Fi 연결 차단 	<ul style="list-style-type: none"> ▪ 정산, 발주 처리 관련 필드 시험해야 함. ✓ 대형 체인의 경우
Medium Level 보안 모드 (Left button)	<ul style="list-style-type: none"> ▪ POS 결제 패킷 허용 ▪ 웹(HTTP/HTTPS), GMAIL 송수신 패킷 허용 ▪ DNS Filter(Malware, Spyware, 음란, 광고, bitcoin 채굴 등 site 차단) ▪ TOP 30 IP 자동 획득 → 허용 ▪ 나머지는 차단 	<ul style="list-style-type: none"> ▪ 웹 서핑, 메일 수신을 통한 해킹 위협 있으니, 주의 요망 ▪ TOP 30 IP는 지정된 시간(예: 7일) 동안 자동으로 수집
Low Level 보안 모드 (Reset button)	<ul style="list-style-type: none"> ▪ 외부에서 접근하는 패킷 차단(기본 방화벽 모드) ▪ DNS Filter(Malware, Spyware, 음란, 광고, bitcoin 채굴 등 site 차단) ▪ 나머지모든 패킷 허용 	<ul style="list-style-type: none"> ▪ 특별한 경우가 아니면 사용을 해서는 안됨.

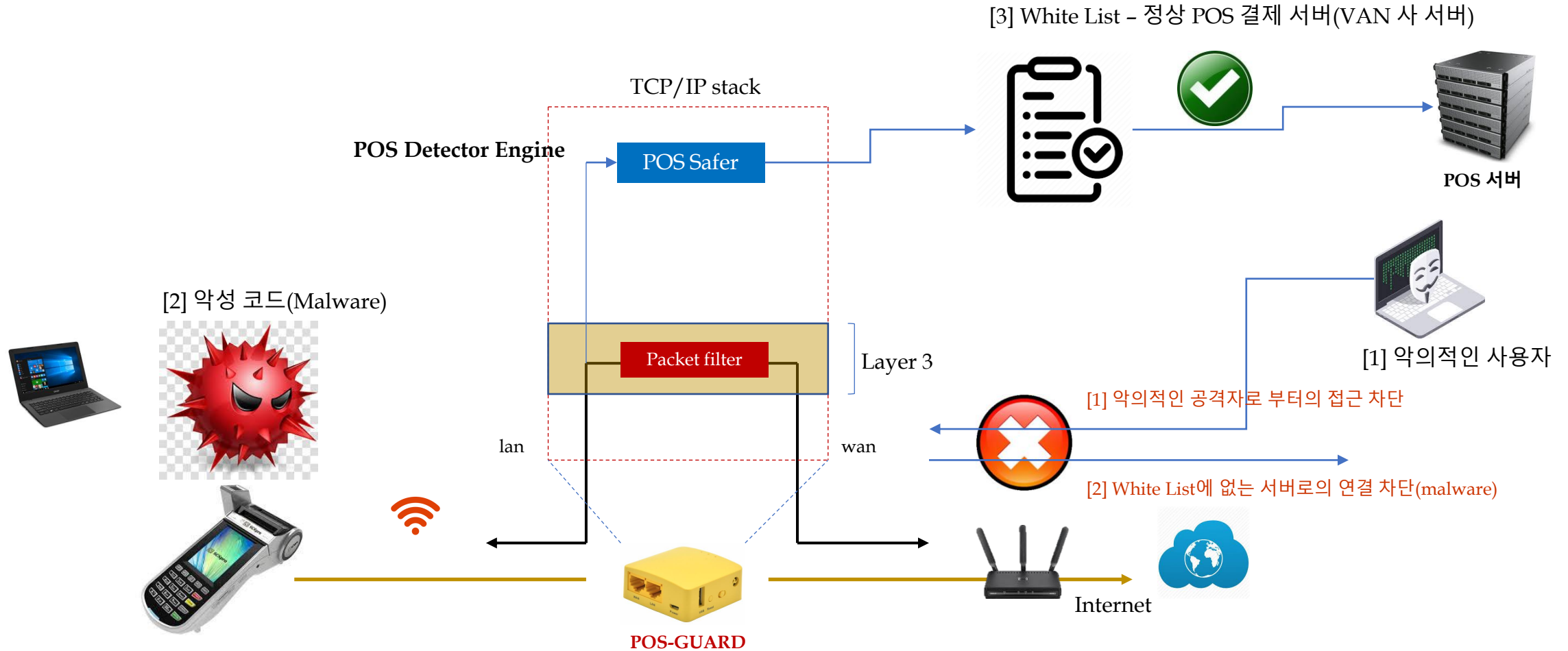
3. P/G Smart Firewall(2) – 3단계 보안 모드(3)



3. P/G Smart Firewall(3) – Auto IP Filter(1)

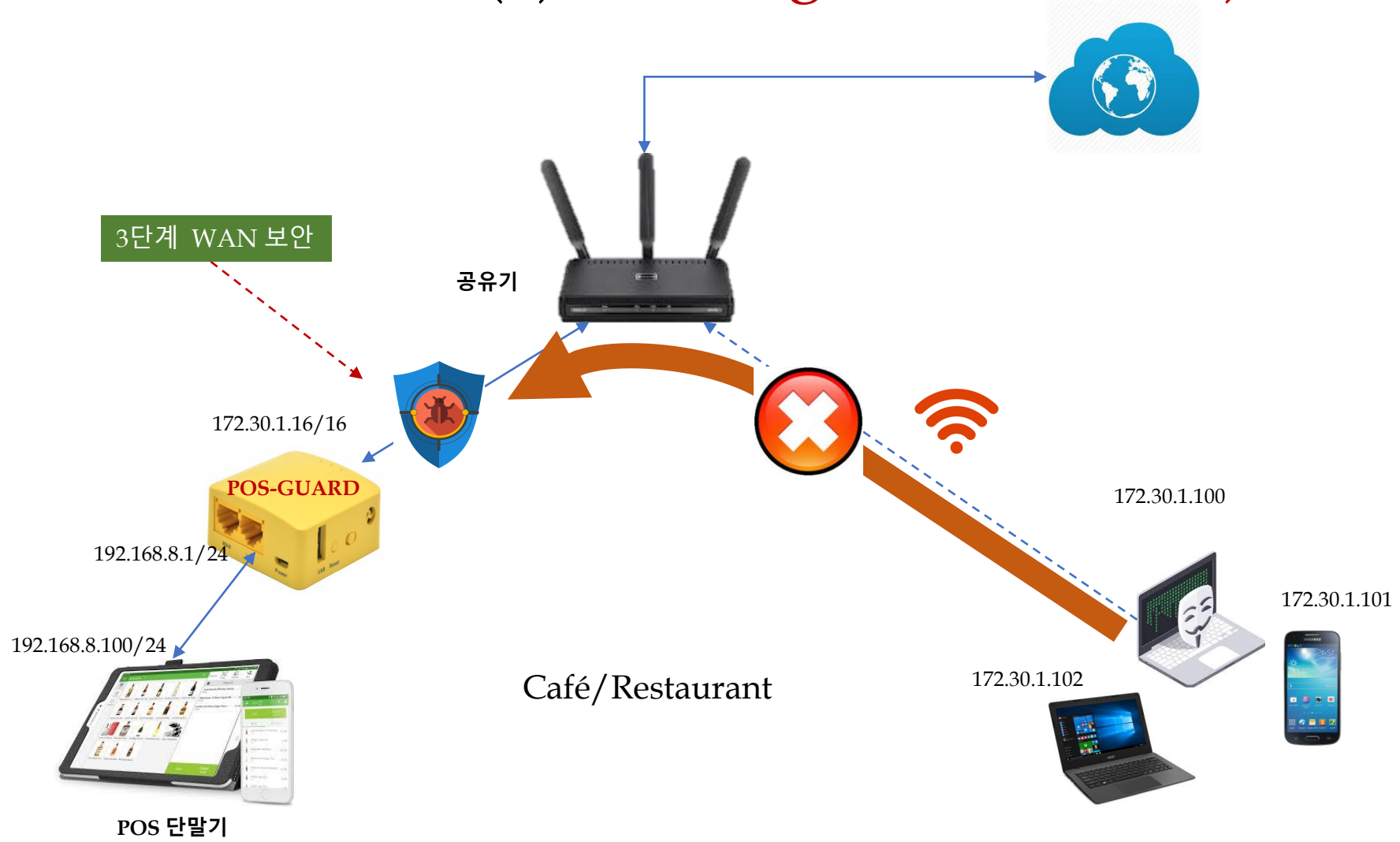


3. P/G Smart Firewall(3) – Auto IP Filter(2)



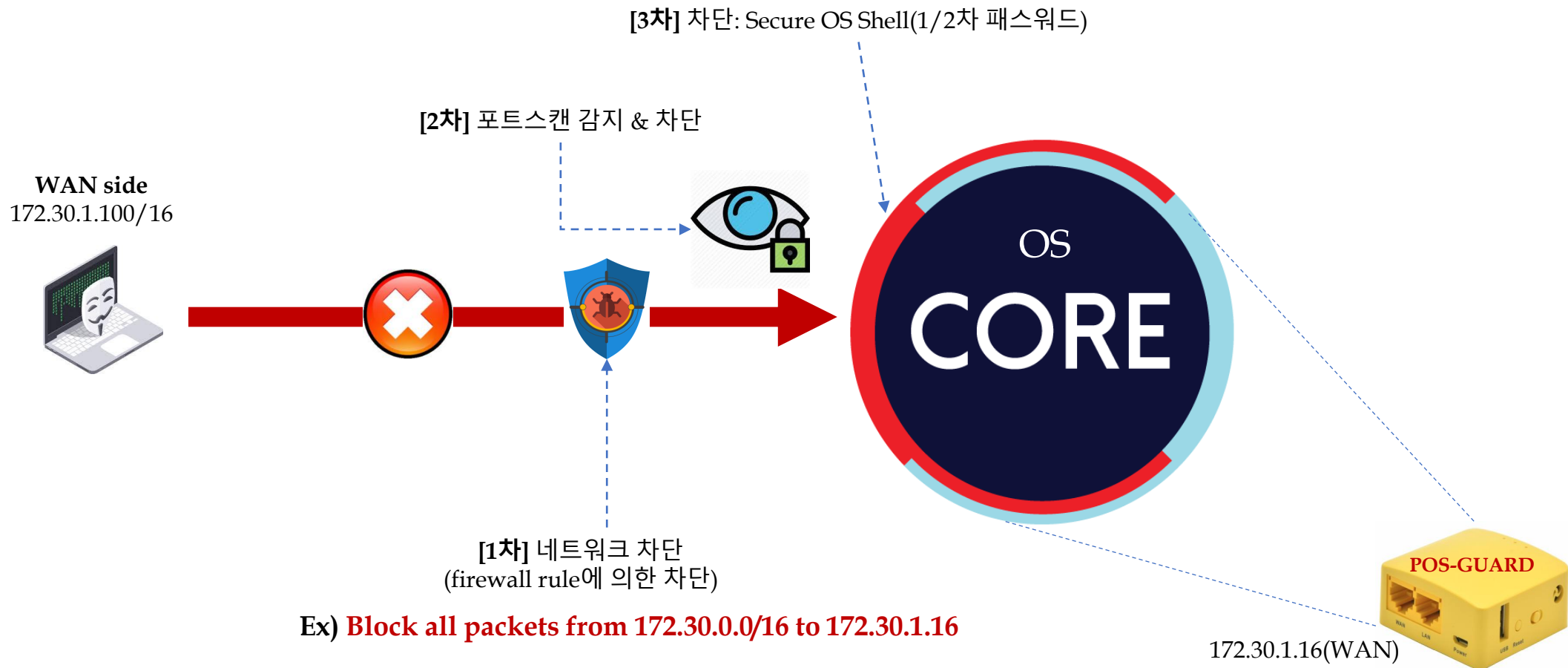
PG Auto IP Filter는 허가된 POS 서버를 제외한 모든 패킷을 차단하여 잠재적인 보안 위협을 자동으로 막아 줍니다.

3. P/G Smart Firewall(4) - Strong WAN 보안(1)



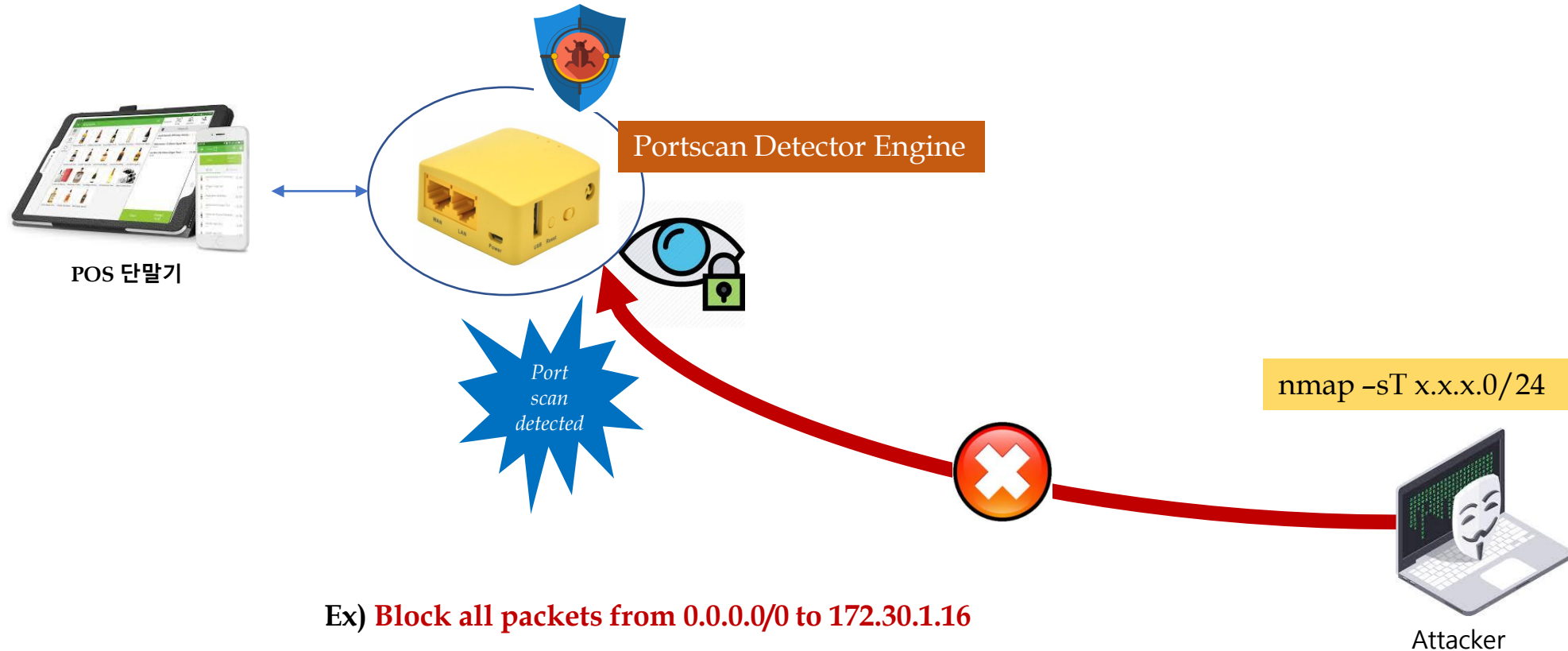
POS-GUARD는 공유기에 연결된 외부 공격자로 부터의 해킹 시도를 자동으로 차단(원천 봉쇄)합니다.

3. P/G Smart Firewall(4) – Strong WAN 보안(2)



외부(WAN 포트)로 부터 POS-GUARD에 침투하기 위해서는 3단계의 방어막을 뚫어야만 합니다.

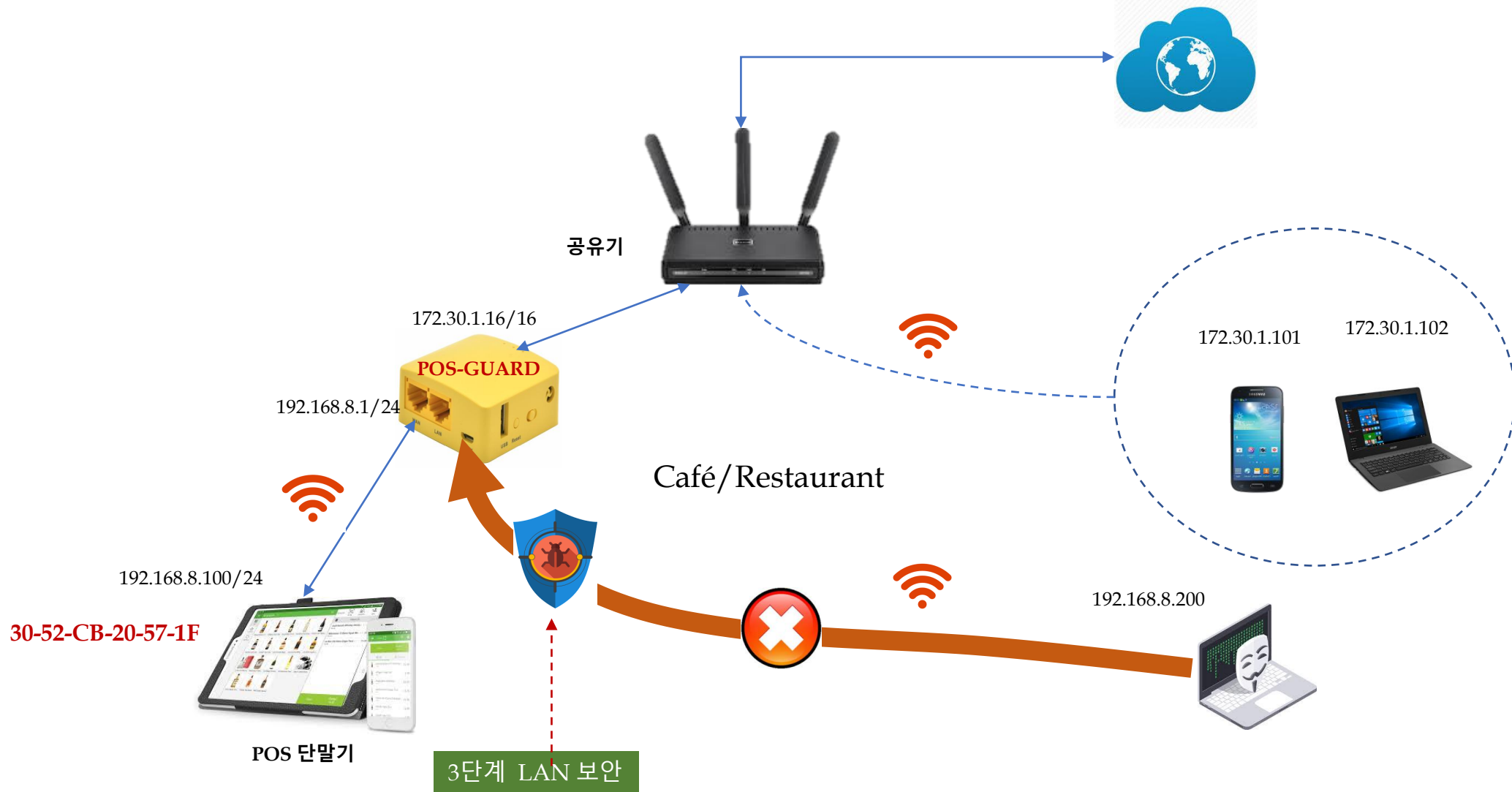
3. P/G Smart Firewall(4) – Strong WAN 보안(3)



<Portscan 감지 및 차단>

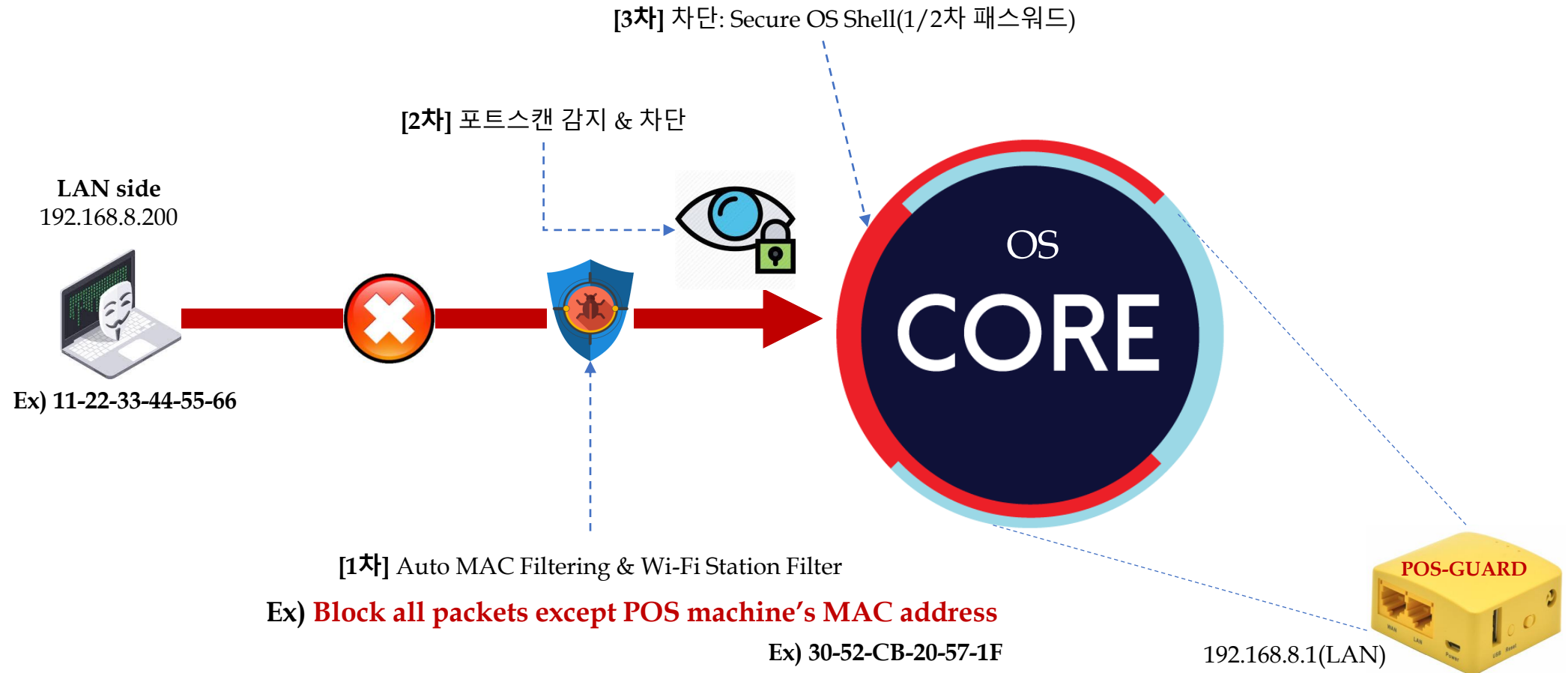
- ① 악의적인 attacker가 시도하는 port scan 공격을 자동으로 감지하고, 차단한다.
- ② Portscan 공격으로 간주된 IP에 대해 적용된 blocking rule은 2시간이 지나면 자동 해제된다.

3. P/G Smart Firewall(5) - Strong LAN 보안(1)



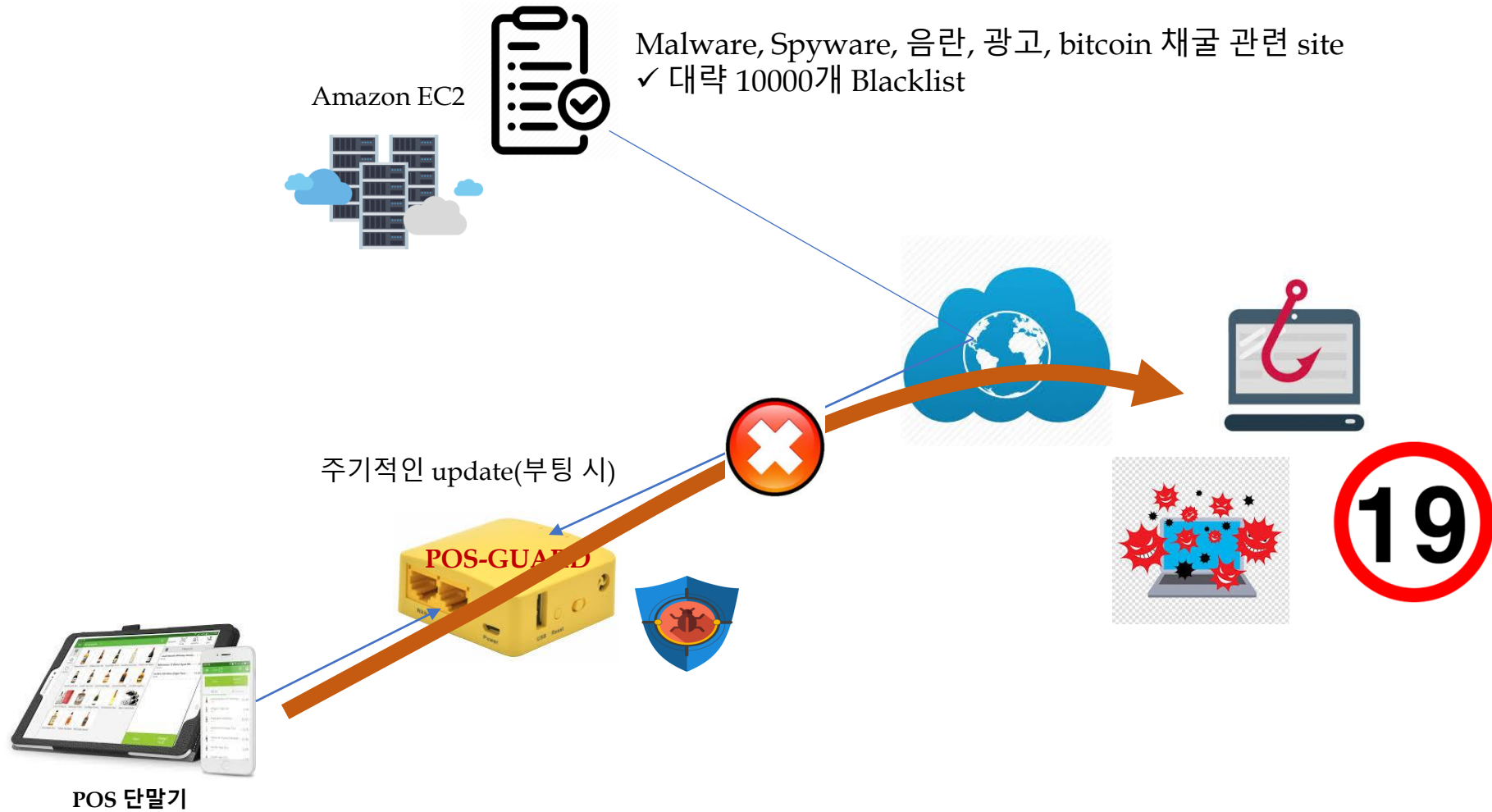
POS-GUARD는 악의적인 사용자가 POS-GUARD(LAN 포트)에 접속하려는 것으로 자동으로 차단합니다.

3. P/G Smart Firewall(5) – Strong LAN 보안(2)



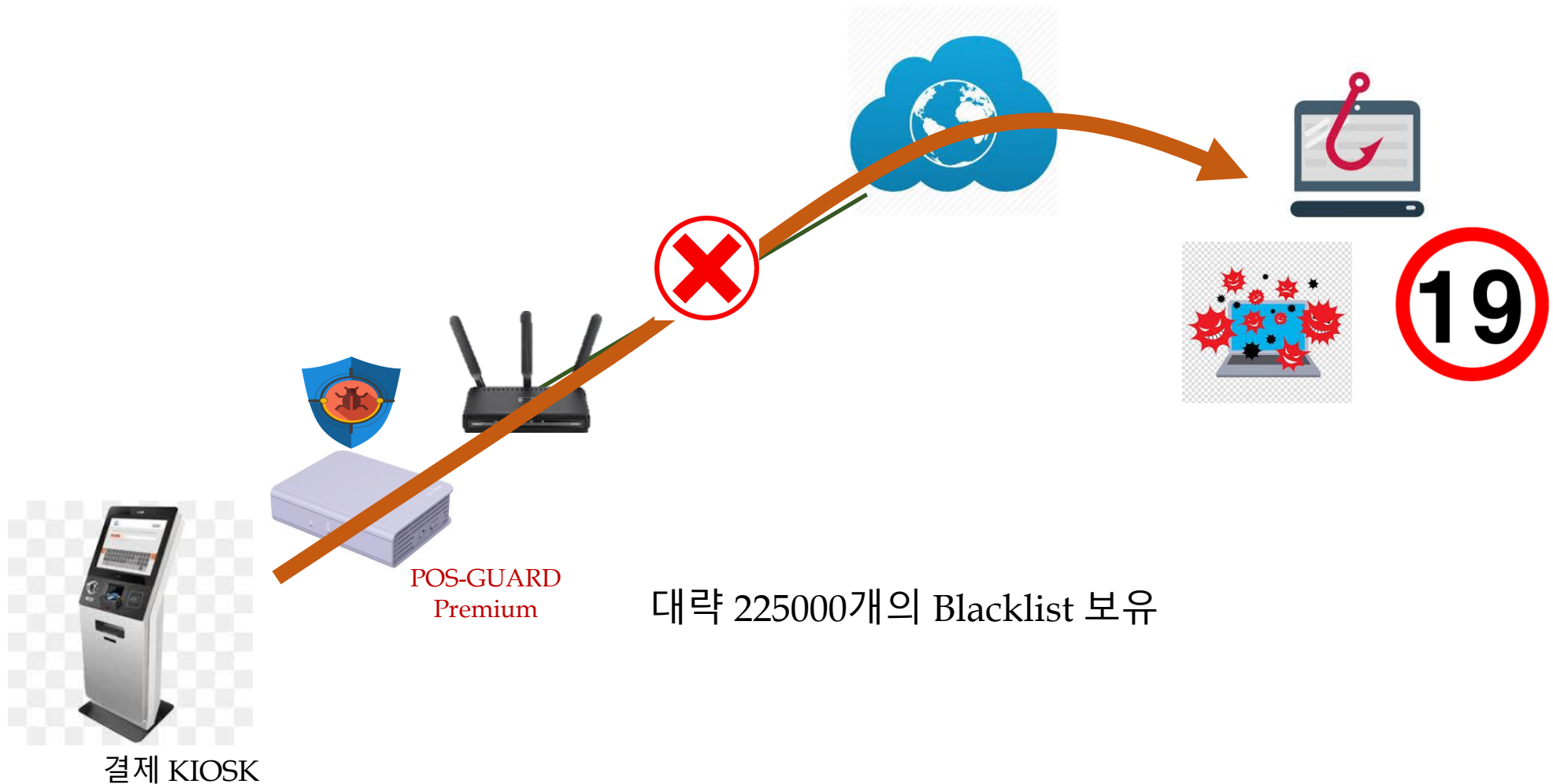
내부망(LAN 포트)로 부터 POS-GUARD에 침투하기 위해서는 3단계의 방어막을 뚫어야만 합니다.

3. P/G Smart Firewall(6) – DNS(a.k.a Blacklist) Filter(1)

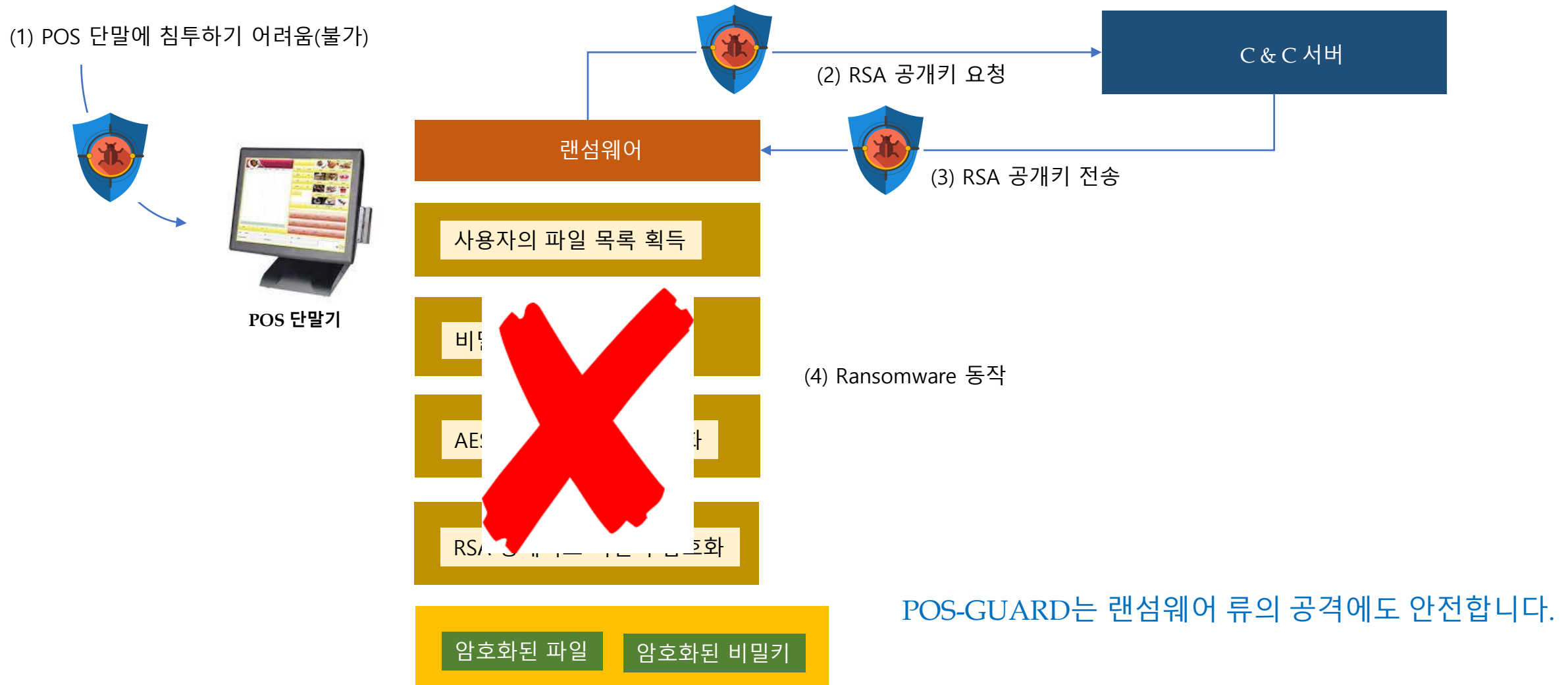


POS-GUARD는 Malware, Spyware, Phishing, 광고, bitcoin 채굴, 음란 site 등을 자동으로 차단해 줍니다.

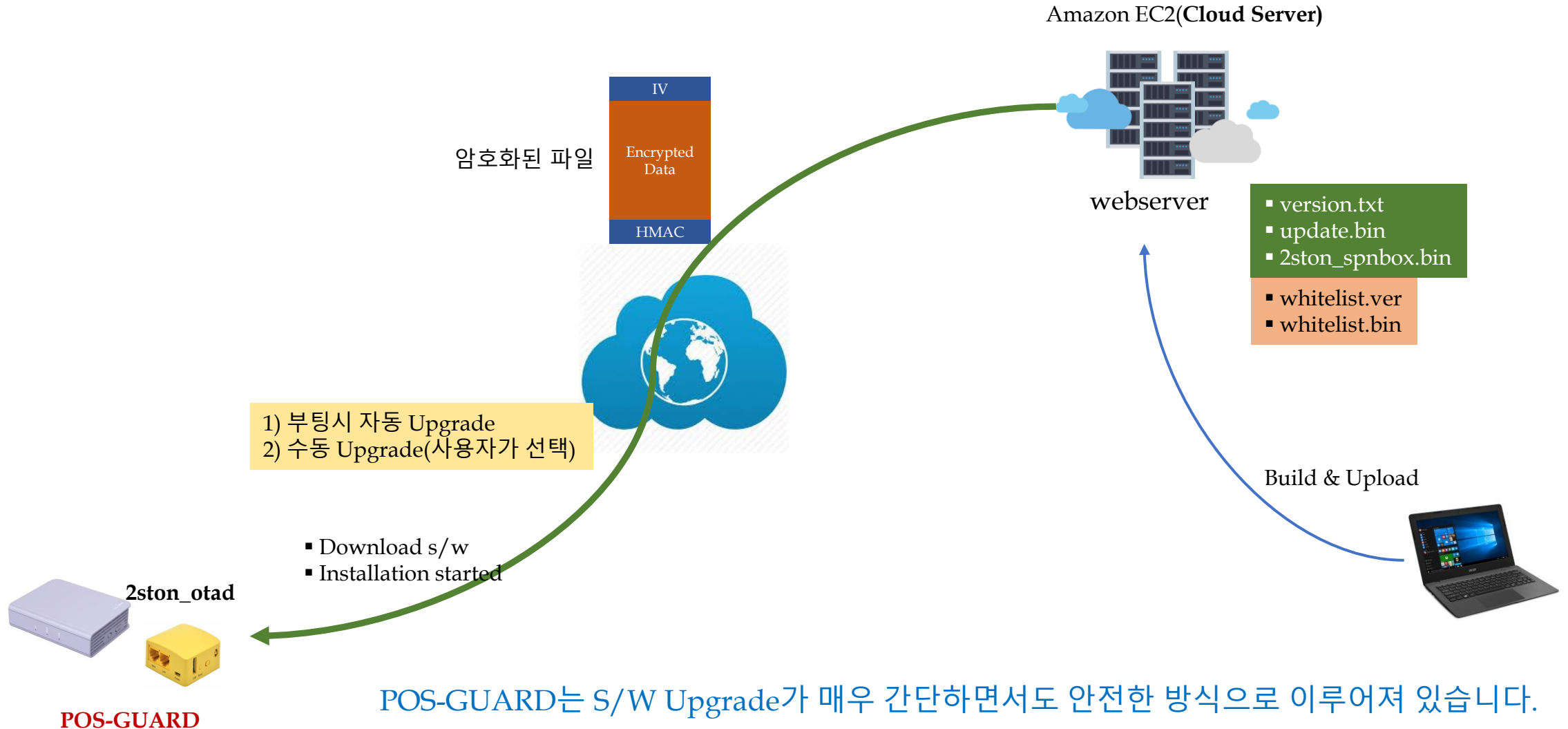
3. P/G Smart Firewall(6) – DNS(a.k.a Blacklist) Filter(2)



3. P/G Smart Firewall(7) – Ransomware 차단



4. POS-GUARD S/W 원격 Upgrade



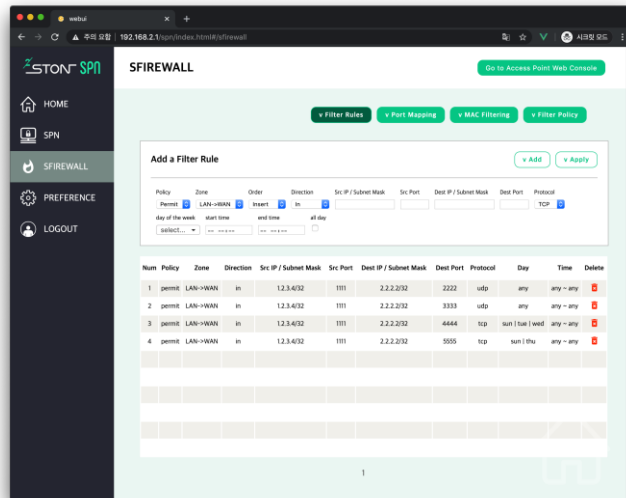
POS-GUARD는 S/W Upgrade가 매우 간단하면서도 안전한 방식으로 이루어져 있습니다.

5. POS-GUARD Specifications(1)



POS-GUARD Lite

(58 x 58 x 25mm)



Model Name	SPNBox-200
H/W 제조사	GLiNet
CPU	MTK 7628NN 580Mhz SoC
RAM	128MB DDR2
Storage	16MB NOR Flash
USB	1× USB 2.0
Wi-Fi	2.4Ghz, 802.11b/g/n, 300Mbps
Ethernet	10/100 Mbps(2 Ports)
Power Input	USB 5V/1A
Smart Firewall	Auto IP Filter, WAN Filter, LAN Filter, DNS Filter 3 Level Security Mode(High, Medium, Low)
NAT	NAT/Port Forwarding 제공
SPN(암호 통신)	L3 SPN: L3 Tunnel mode UDP 방식(NAT Traversal) End-to-End 구성 가능 P2P SPN 주의: SPN은 Peer가 존재해야 함.
Router Mode	Router, AP, Repeater mode 지원
Management	Web 기반 UI

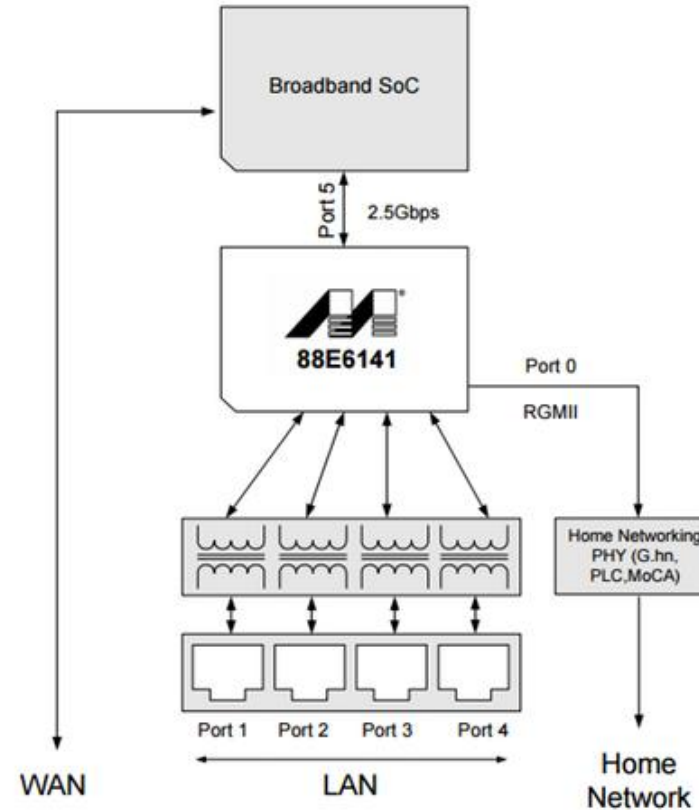
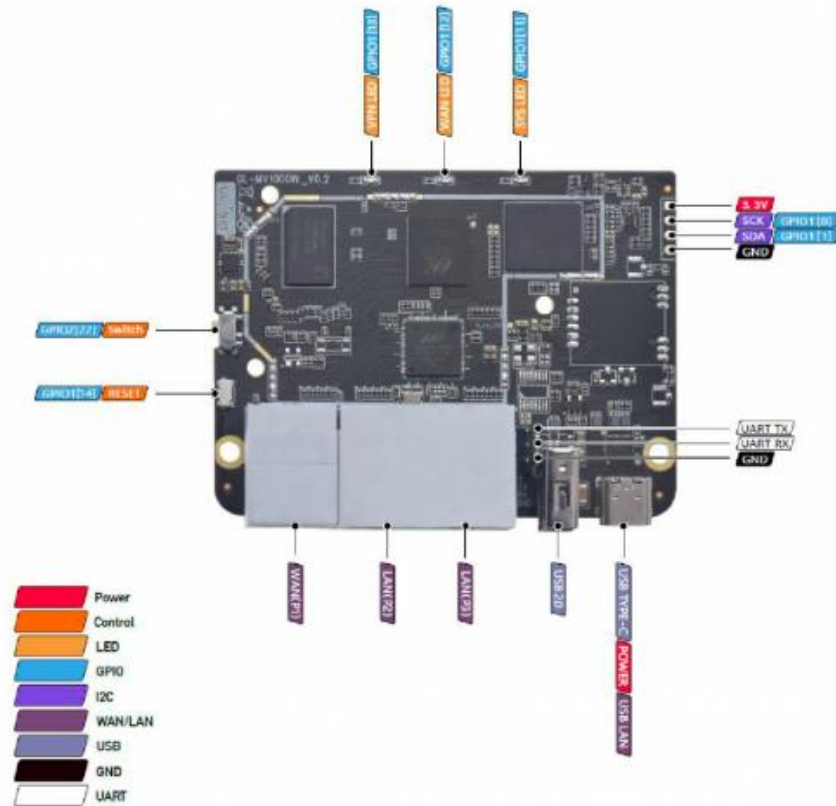
5. POS-GUARD Specifications(2-1)



POS-GUARD Premium
(88 x 68 x 24mm, 105g)

Model Name	SPNBox-900
H/W 제조사	GL.iNet
CPU	Marvell Armada 88F3720, Dual-Core ARM Cortex-A53 @ 1.0Ghz
RAM	DDR4 1GB
Storage	16MB NOR Flash + 8GB EMMC
USB	1× USB 2.0
Ethernet	3 x 10/100/1000 Mbps (Autosensing) : 2 LANs, 1 WAN
MicroSD card slot	1
Power Input	USB3.0 Type-C
Smart Firewall	Auto IP Filter, WAN Filter, LAN Filter, DNS Filter 3 Level Security Mode(High, Medium, Low)
NAT	NAT/Port Forwarding 제공
SPN(암호 통신)	L3 SPN: L3 Tunnel mode UDP 방식(NAT Traversal) End-to-End 구성 가능 P2P SPN 주의: SPN은 Peer가 존재해야 함.
Management	Web 기반 UI

5. POS-GUARD Specifications(2-2)



우수한 성능의 CPU(Marvell) & Switching chip(88E6141) 사용으로 Gigabit speed 보장

참고: LAN은 2개 포트만 사용함.

Thank You



We Secure the Internet of Things with 2STON™ SPN