

2ip SPN I-GUARD

DNS Security



(개발 계획)

2ip, Inc.

Doc. Revision: 0.5

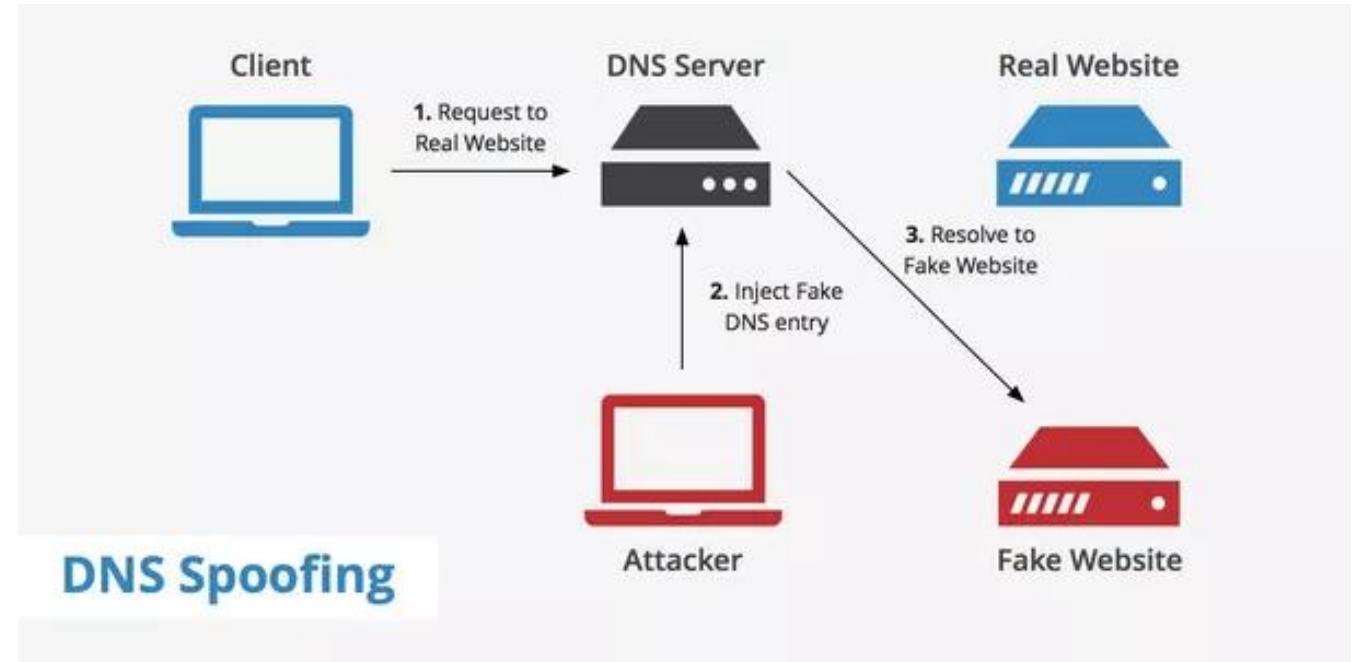
Copyright© 2018-2020, 2ip Inc. All Rights Reserved.

Contents

- 1. Phishing & Pharming Attack
- 2. DNS Sinkhole
- 3. POS-GUARD DNS Filter
- 4. I-GUARD



1. Phishing & Pharming Attack(1)



Pharming Attack

1. Phishing & Pharming Attack(2)

파밍(Pharming)은 넓은 의미에서 피싱(Phishing)의 한 유형으로 분류할 수 있으며, 정확한 명칭은 'DNS Spoofing'이라고도 합니다. 파밍(Pharming) 즉, 'DNS Spoofing'은 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법으로, 컴퓨터가 웹 사이트를 찾을 때 공격자가 원하는 거짓정보로 응답해주는 공격방법입니다. 올바른 URL을 입력했다고 하더라도 잘못된 서버로 접속되게 되며, 이러한 측면에서 피싱보다 한 단계 진화한 형태의 새로운 인터넷 사기 수법이라고 할 수 있습니다.

피싱(Phishing)이 사용자들을 속여 낚는(Fishing)정도라면, 파밍(Pharming)은 도메인 자체를 속임으로 다수의 사용자에게 대규모 피해가 발생할 수도 있기 때문에 'Farming'이라는 의미에서 'Pharming'이라는 이름도 붙여졌다고 합니다.

(Farming이란 단어에는 '농장을 운영하여 농산물을 경작하고 추수한다'는 의미가 있다는 점에서, 단순히 한두 사람을 대상으로 하는 피싱과는 달리 (공격자 입장에서) 대규모 '개인정보의 추수'가 발생할 수 있다는 점에서 파밍이 더 위험할 것 같습니다 ^^;;)

1. Phishing & Pharming Attack(3)

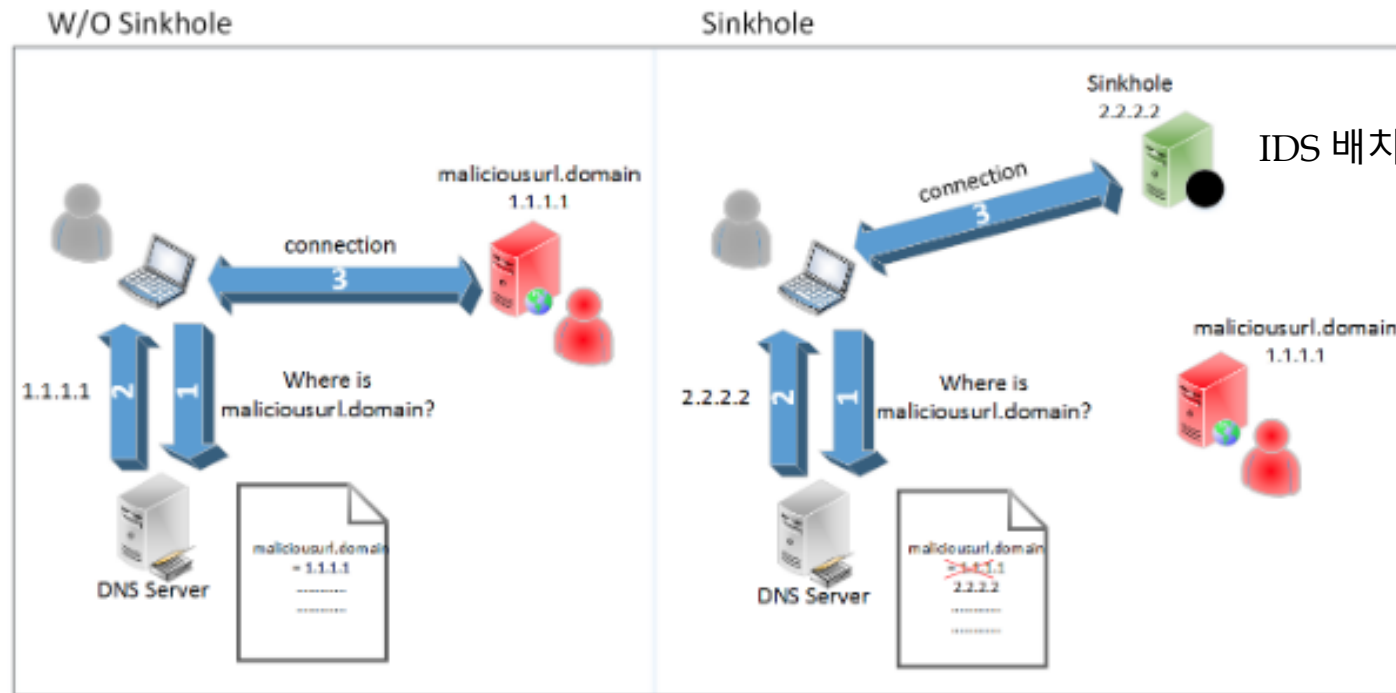
<인터넷 상의 피싱(phishing) 공격과 파밍(pharming) 공격 비교>

구분	피싱(phishing) 공격	파밍(pharming) 공격
주된 목적	- 가짜 사이트로 유도해 개인정보 탈취	- 가짜 사이트로 유도해 개인정보 탈취
공격방식 (인터넷)	- 실제 도메인네임과 유사한 가짜 도메인네임을 사용 - 진짜처럼 위장된 가짜 사이트로 접속하여 개인정보 입력 유도	- 조직, 목적, 분류 등 명칭을 영문약자로 표현한 최상위 도메인
공격특징	- 주로 이메일, SMS 등에 첨부된 링크를 통해 접속을 유도	- 정상 도메인 입력만으로도 공격이 가능하므로 별다른 유인매체가 불필요
위험성	- 사용자가 세심한 주의를 기울이면 공격탐지, 피해방지가 가능	- 실제 도메인네임이 그대로 사용되므로 공격탐지 곤란 - 사용자가 많은 캐시 DNS서버에 공격성공 경우, 피해범위 광범위

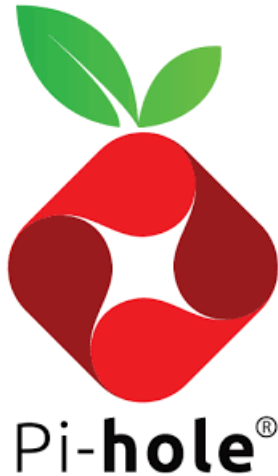
2. DNS Sinkhole(1)

DNS Sinkhole

- Black hole DNS or IP sinkhole
- 차단 목적도 있지만 유해 트래픽을 분석하는 목적도 있음.

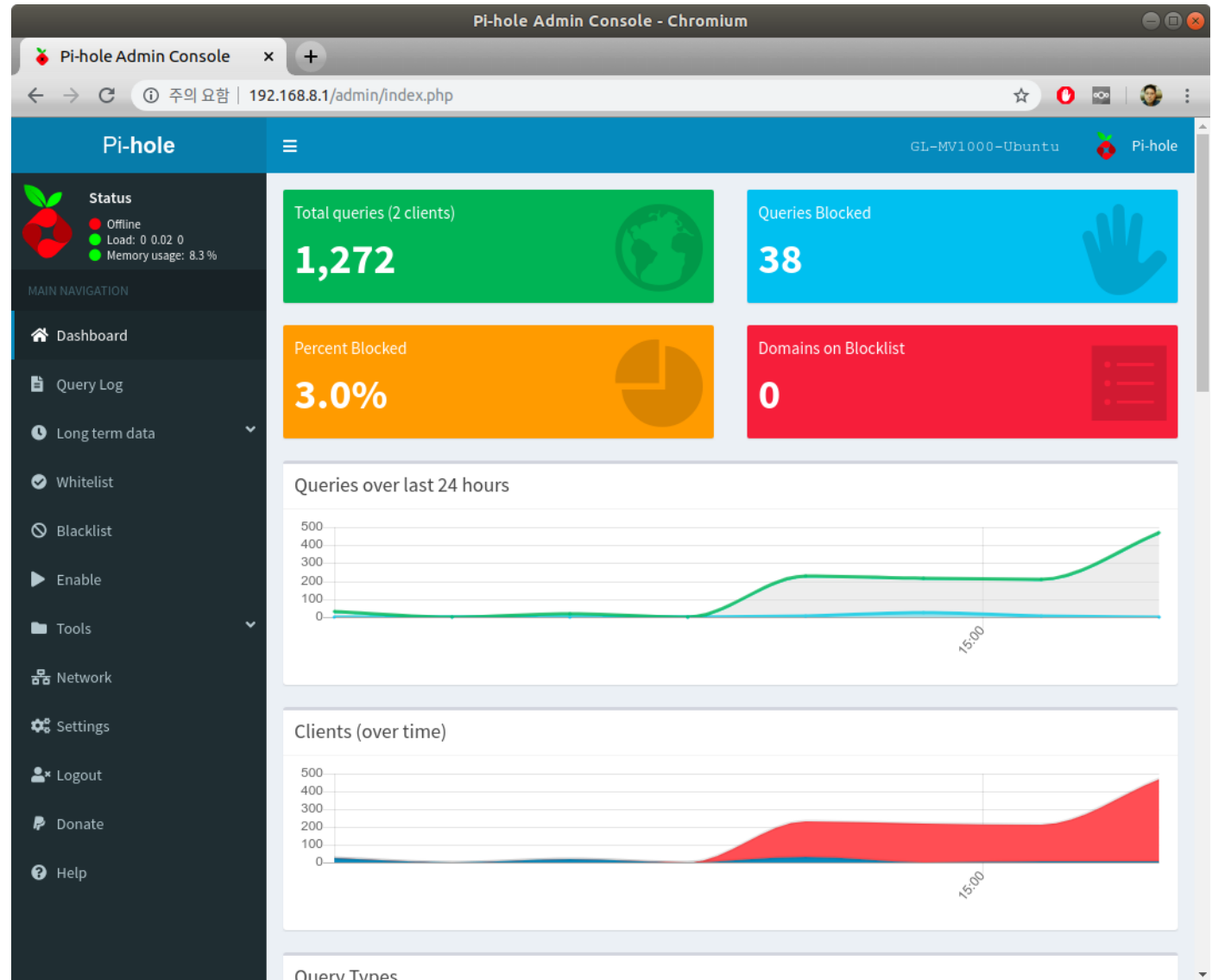


2. DNS Sinkhole(2) – Pi-hole(1)



- DNS sinkhole
- Network-wide Ad Blocking solution
- Open Source

<https://pi-hole.net/>



2. DNS Sinkhole(2) – Pi-hole(2)

Pi-hole Admin Console - Chromium

192.168.8.1/admin/queries.php

Pi-hole

Status

- Offline
- Load: 0 0.01 0
- Memory usage: 8.3 %

MAIN NAVIGATION

- Dashboard
- Query Log
- Long term data
- Whitelist
- Blacklist
- Enable
- Tools
- Network
- Settings
- Logout
- Donate
- Help

Recent Queries (showing up to 100 queries), [show all](#)

Show 10 entries

Search:

Time	Type	Domain	Client
2019-11-23 15:33:10	A	2ipcdbox.ddns.net	192.168.8
2019-11-23 15:32:11	A	safebrowsing.googleapis.com	192.168.8
2019-11-23 15:32:07	A	2ipcdbox.ddns.net	192.168.8
2019-11-23 15:32:05	A	googlehosted.l.googleusercontent.com	192.168.8
2019-11-23 15:32:05	A	fonts.gstatic.com	192.168.8
2019-11-23 15:32:04	A	www.google.com	192.168.8
2019-11-23 15:31:55	AAAA	pipeline-edge-prod-25-561439127.us-west-2.elb.amazonaws.com	192.168.8
2019-11-23 15:31:55	AAAA	incoming.telemetry.mozilla.org	192.168.8
2019-11-23 15:31:55	A	incoming.telemetry.mozilla.org	192.168.8
2019-11-23 15:31:55	A	www.cdn.amazon.com	192.168.8

Pi-hole Admin Console - Chromium

192.168.8.1/admin/db_queries.php

Pi-hole

Status

- Offline
- Load: 0.2 0.05 0.02
- Memory usage: 8.3 %

MAIN NAVIGATION

- Dashboard
- Query Log
- Long term data
- Graphics
- Query Log
- Top Lists
- Whitelist
- Blacklist
- Enable
- Tools
- Network
- Settings
- Logout
- Donate
- Help

Specify date range to be queried from the Pi-hole query database

Date and time range:

November 23rd 2019, 00:00 to November 23rd 2019, 15:34

Query status:

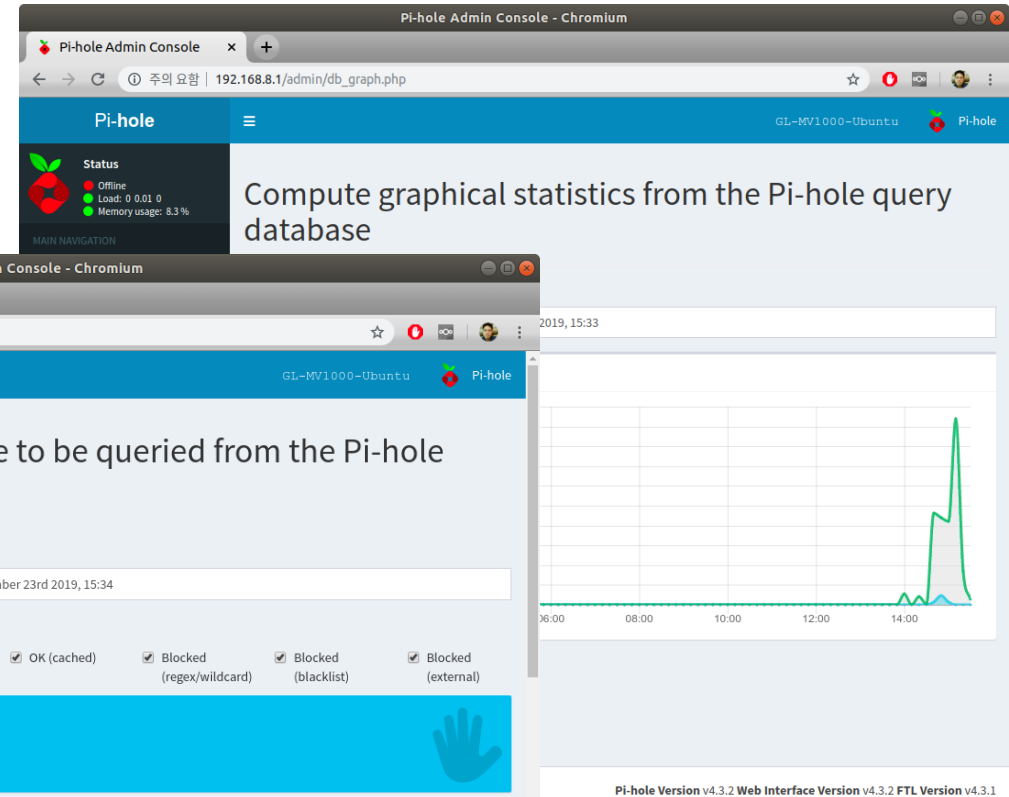
- ☒ Blocked (exact)
- ☒ OK (forwarded)
- ☒ OK (cached)
- ☒ Blocked (regex/wildcard)
- ☒ Blocked (blacklist)
- ☒ Blocked (external)

38 Queries Blocked

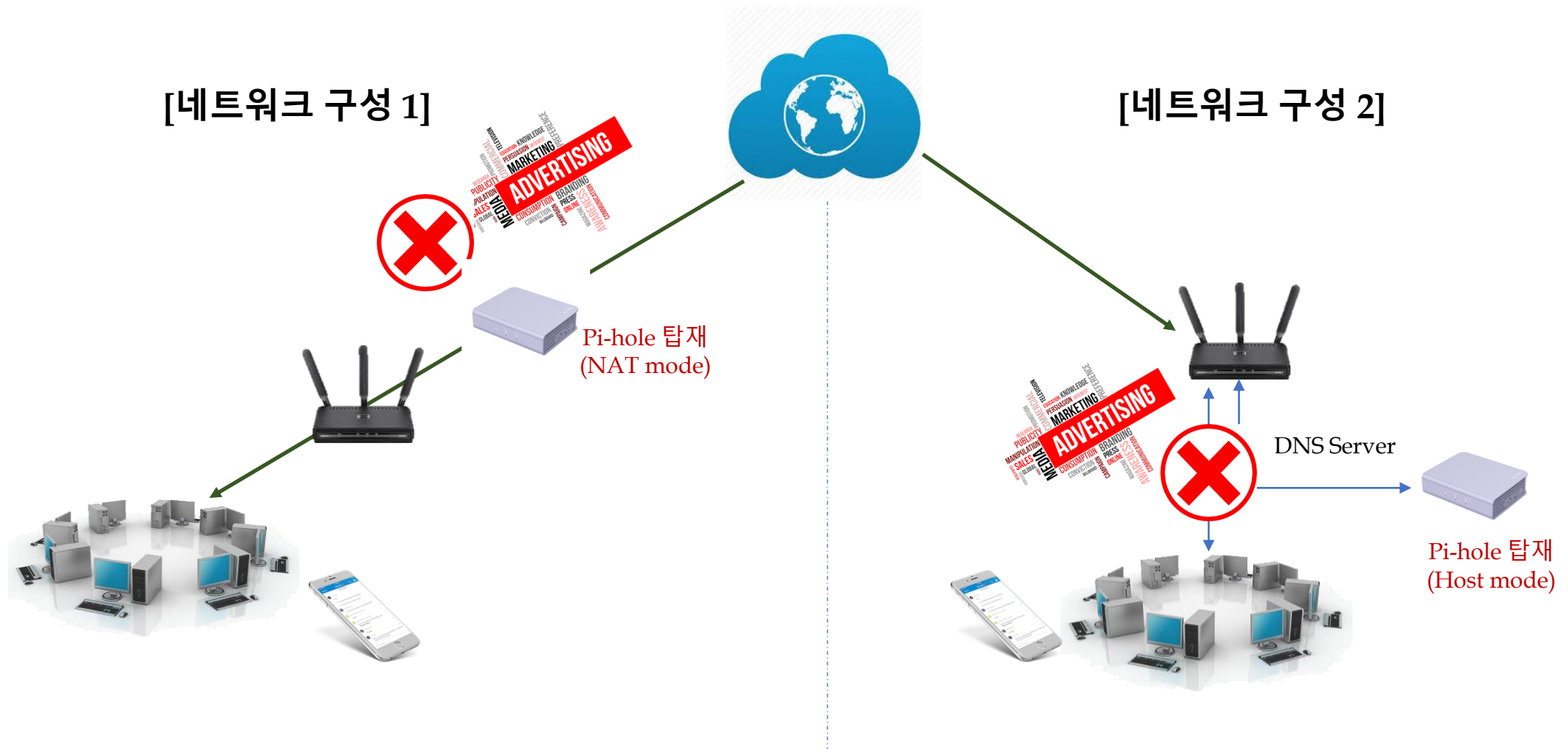
0 Queries Blocked (Wildcards)

1,281 Queries Total

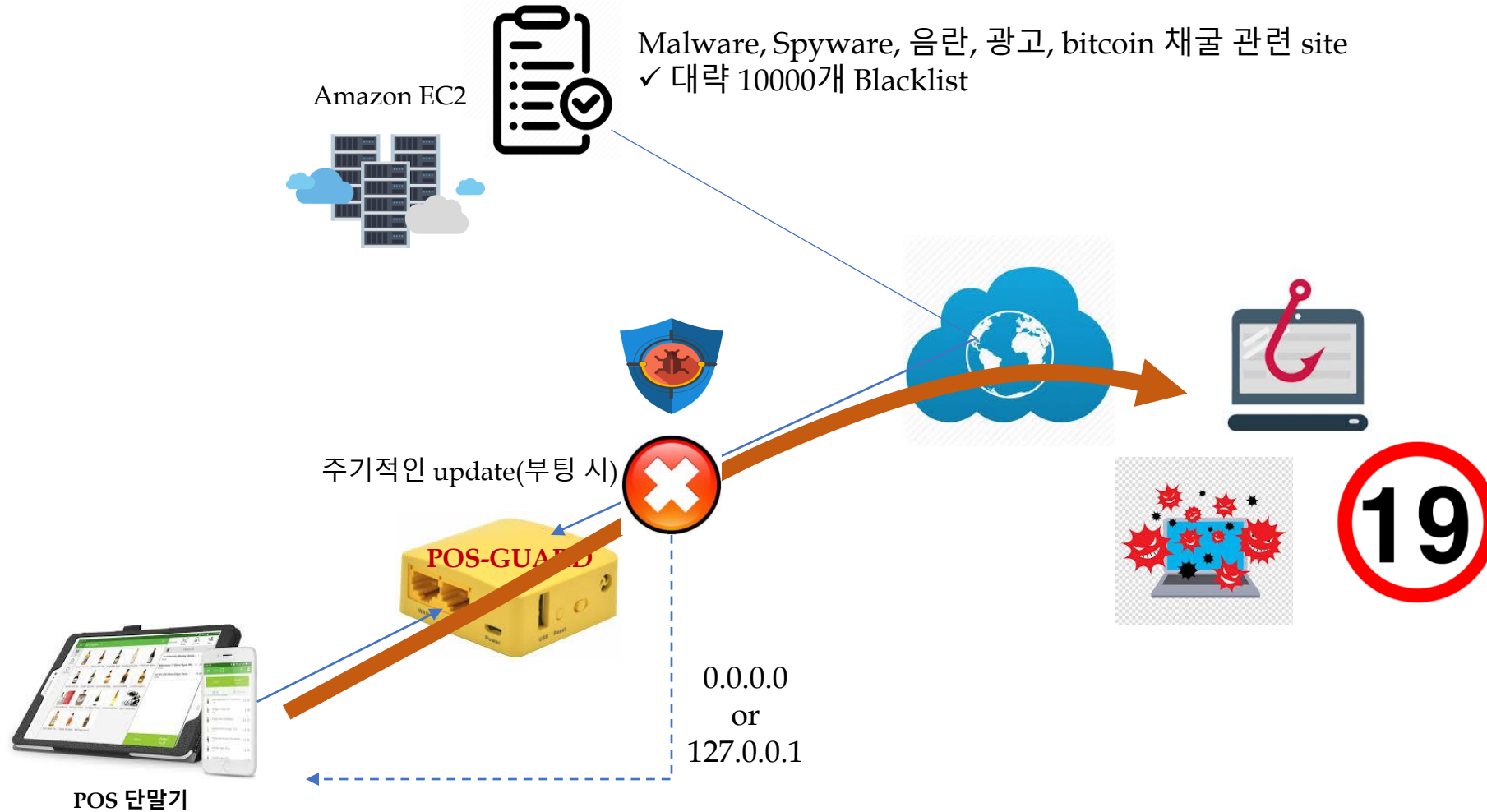
3.0 %



2. DNS Sinkhole(2) – Pi-hole(3)

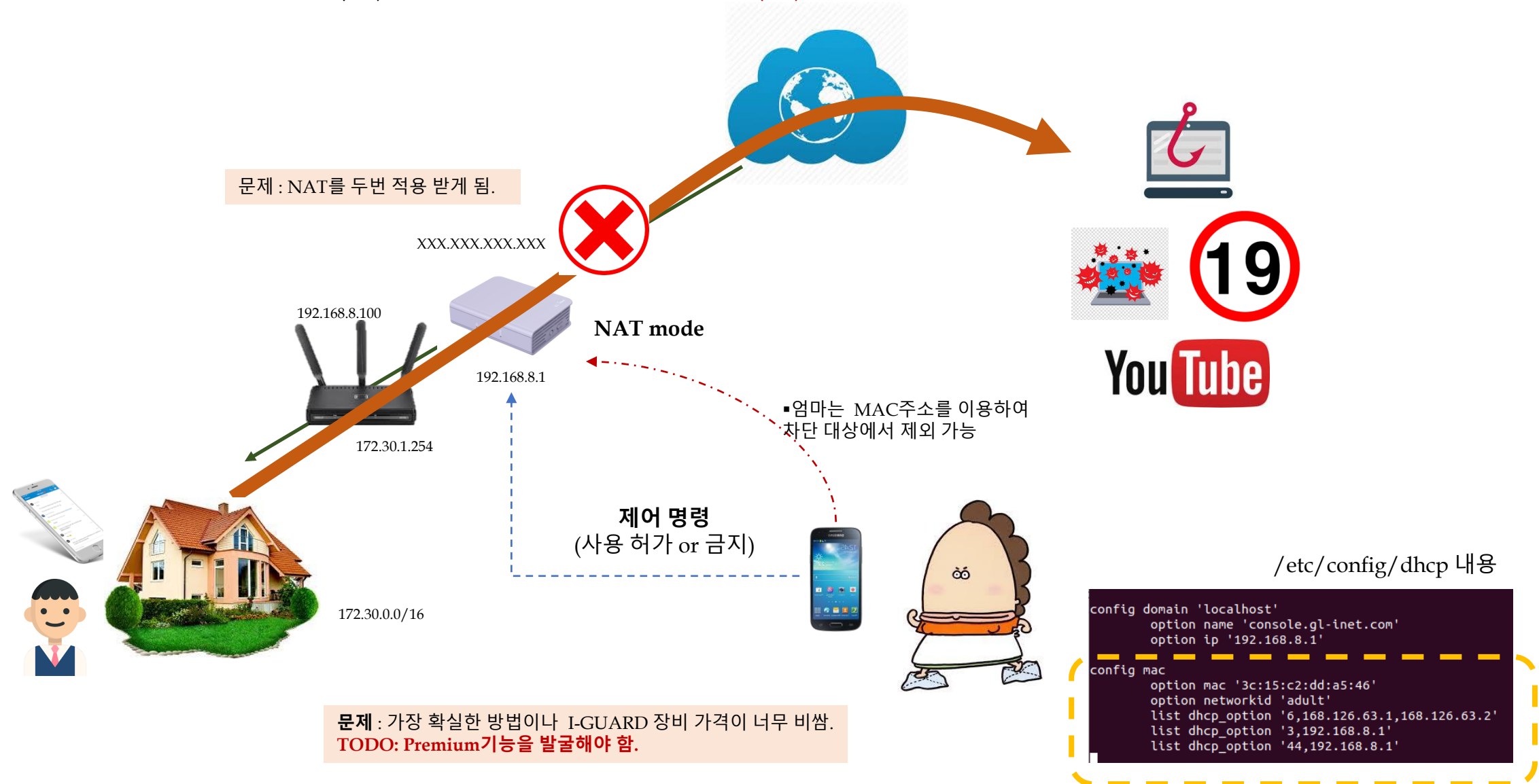


3. POS-GUARD DNS Filter

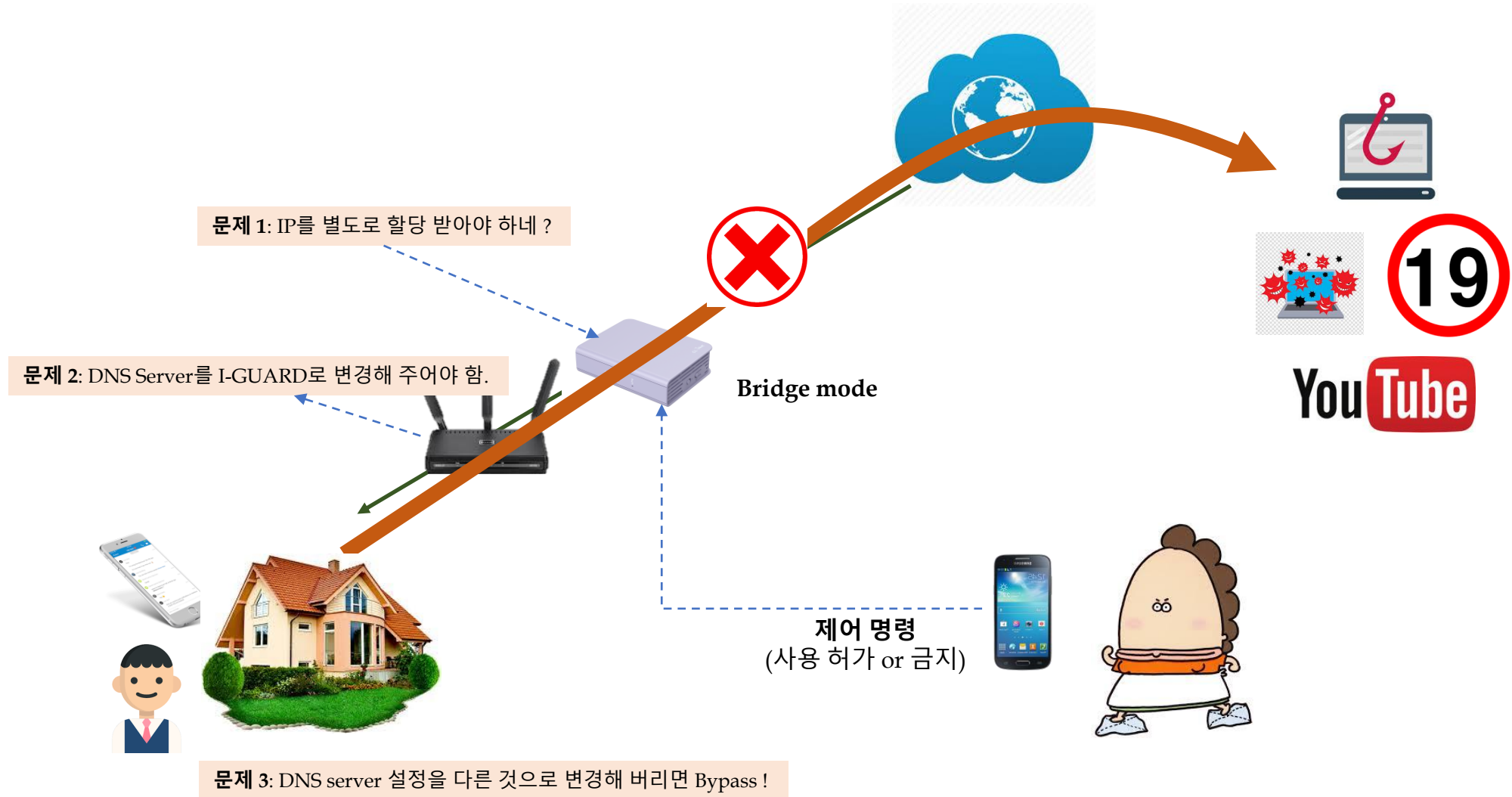


POS-GUARD는 Malware, Spyware, Phishing, 광고, bitcoin 채굴, 음란 site 등을 자동으로 차단해 줍니다.

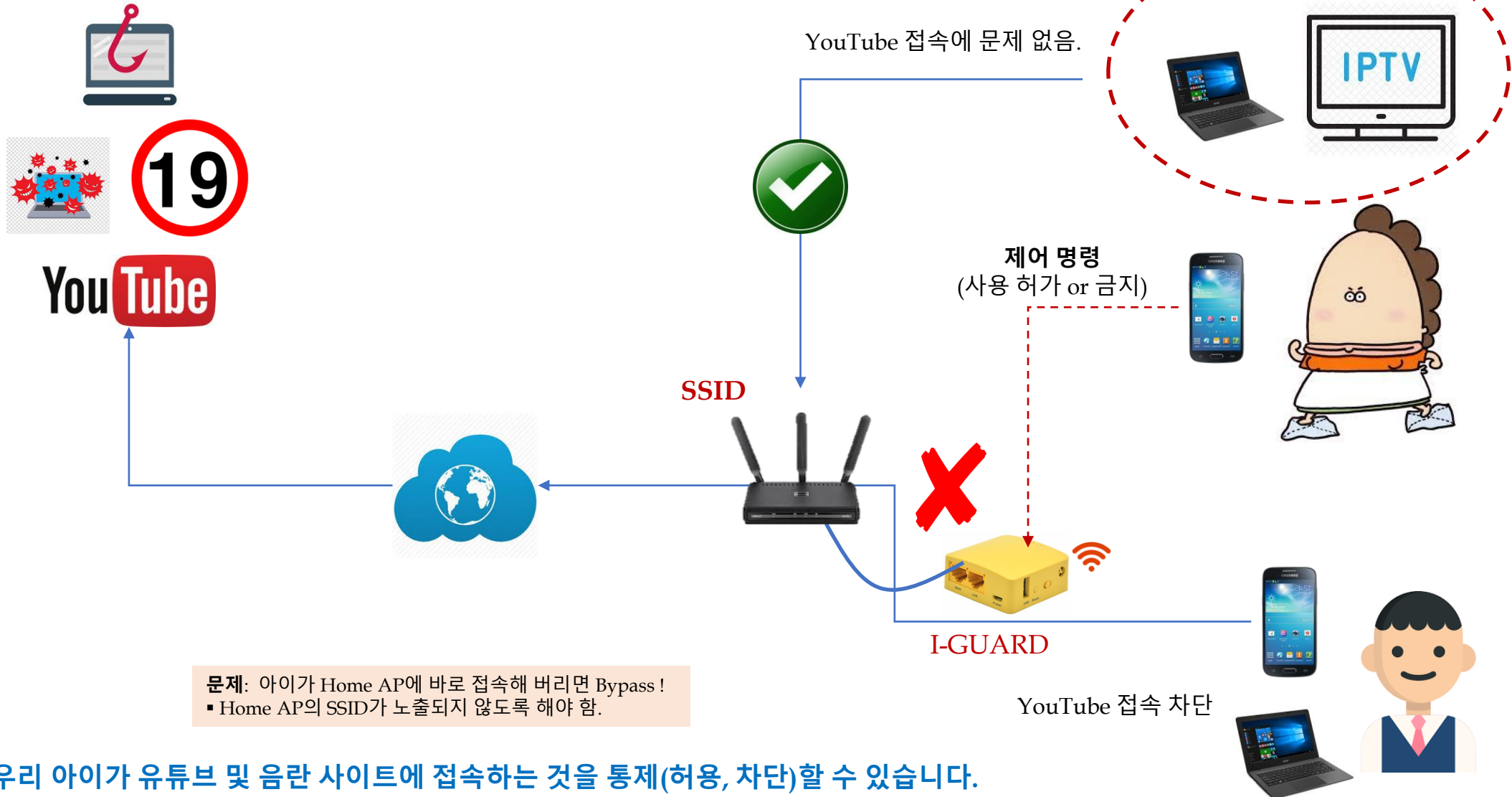
4. I-GUARD(1) - NAT Mode(1)



4. I-GUARD(2) – Bridge Mode

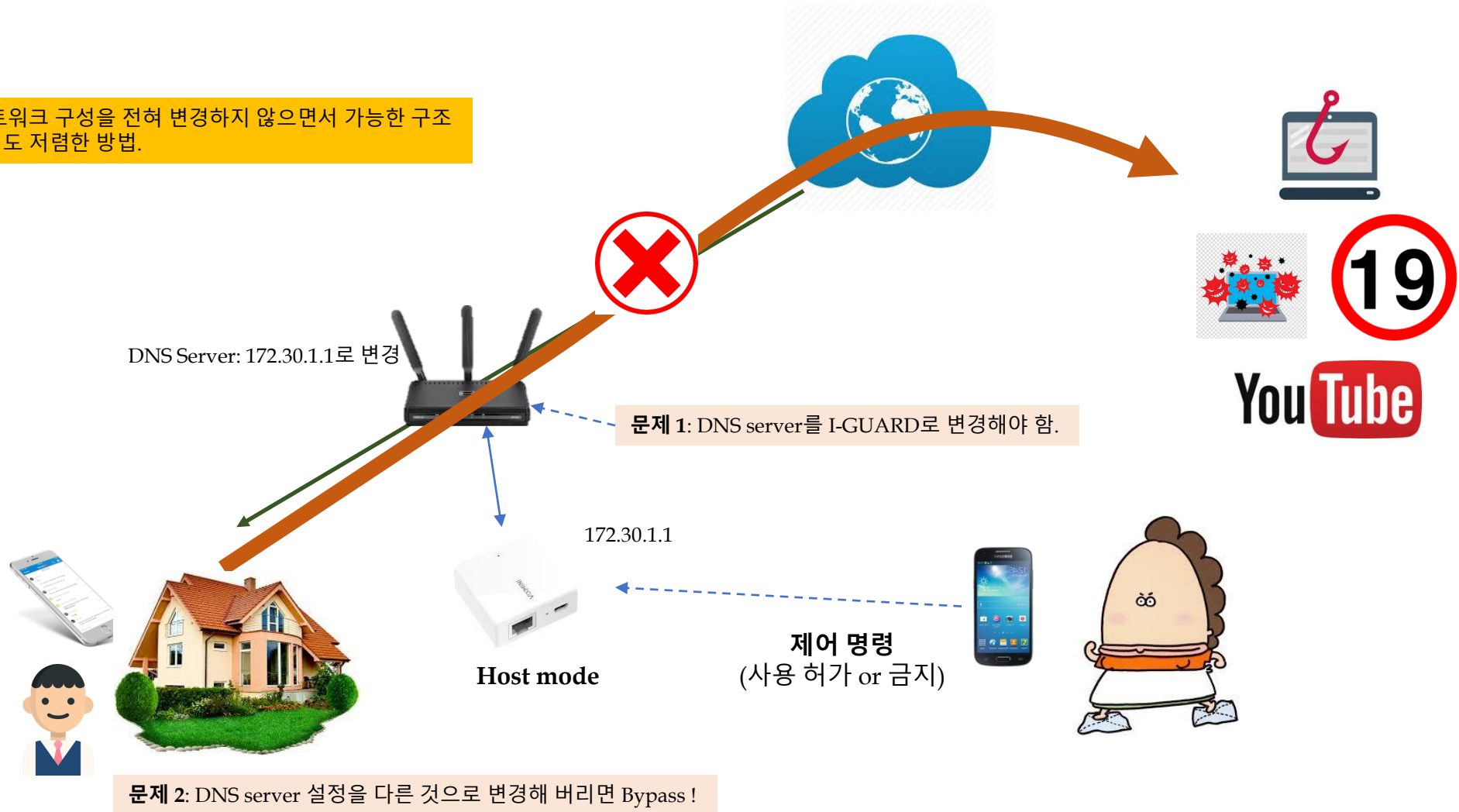


4. I-GUARD(3) – Repeater Mode



4. I-GUARD(4) – Host Mode

- 네트워크 구성을 전혀 변경하지 않으면서 가능한 구조
- 가격도 저렴한 방법.



4. I-GUARD(5) – IPTime 아이안심 기능

The screenshot shows a web browser window with the address bar displaying "EFM Networks ipTIME A1004" and the URL "172.30.1.254/sess-bin/timepro.cgi?tmenu=main_frame&smenu=main_frame". The browser's address bar also shows a warning icon and the text "주의 요함". The browser's toolbar includes icons for back, forward, refresh, and search, as well as a search bar containing "M 일시중지됨".

The main content area of the browser displays the "아이안심ipTIME" (I-Guard) feature. The page title is "아이안심ipTIME". The page content includes a section titled "아이안심 ipTIME is..." with a sub-header "아이안심 ipTIME is...". Below this, there is a paragraph of text in Korean: "고객님의 자녀가 인터넷 상의 음란물, 유해사이트에 노출될까 걱정하십니까? 음란물 노출은 성장기 청소년들에게 커다란 위험을 끼칠 수 있습니다. '아이안심 ipTIME'은 고객님의 이러한 걱정을 해소해 드립니다." (Are you worried that your child will be exposed to obscene materials or harmful sites on the internet? Exposure to obscene materials is a great danger for growing teenagers. 'I-Guard ipTIME' solves your worries like this.)

Below the text, there is a button labeled "무료사용등록" (Free Registration). The page also includes a section titled "부모 기기 (등록된 기기는 유해사이트 차단이 이루어지지 않습니다.)" (Parent device (registered devices do not have harmful site blocking)). This section contains a table with columns for "MAC 주소" (MAC Address) and "설명" (Description). The table has a header row and a body row. The header row has "MAC 주소" and "설명" columns. The body row has "MAC 주소" and "설명" columns. The "MAC 주소" column has a checkbox for "현재 접속된 PC의 MAC주소로 설정" (Set to MAC address of currently connected PC) and a "MAC 주소 찾기" (Find MAC address) button. The "설명" column has a "추가" (Add) button. The table also has a "삭제" (Delete) button.

The left sidebar of the browser shows a menu with the following items: "메뉴탐색기" (Menu Explorer), "기본 설정" (Basic Settings), "시스템 요약 정보" (System Summary Information), "인터넷 설정 정보" (Internet Setting Information), "무선 설정/보안" (Wireless Setting/Security), "펌웨어 업그레이드" (Firmware Upgrade), "고급 설정" (Advanced Settings), "네트워크 관리" (Network Management), "인터넷 설정 정보" (Internet Setting Information), "내부 네트워크 설정" (Internal Network Setting), "무선랜 관리" (Wireless LAN Management), "무선 설정/보안" (Wireless Setting/Security), "무선확장설정" (Wireless Extension Setting), "MAC주소 관리" (MAC Address Management), "NAT/라우터 관리" (NAT/Router Management), "포트포워드 설정" (Port Forward Setting), "고급 NAT 설정" (Advanced NAT Setting), "라우팅 테이블 관리" (Routing Table Management), "보안 기능" (Security Function), "인터넷/WiFi 사용 제한" (Internet/WiFi Usage Restriction), "네트워크 감시" (Network Monitoring), "공유기 접속/보안관리" (Router Connection/Security Management), "아이안심ipTIME" (I-Guard ipTIME), "특수기능" (Special Function), "트래픽 관리" (Traffic Management), and "시스템 관리" (System Management).

The bottom of the browser window shows a "Logout" button and a "Mobile UI" button.

이런, 이미 이렇게 있네~

4. I-GUARD(6) - 지원 예상 모델(1)

Host Mode



I-GUARD Mini

Repeater Mode



I-GUARD Lite

아이가 사용하는 기기만 보호

NAT Mode(WAN side)



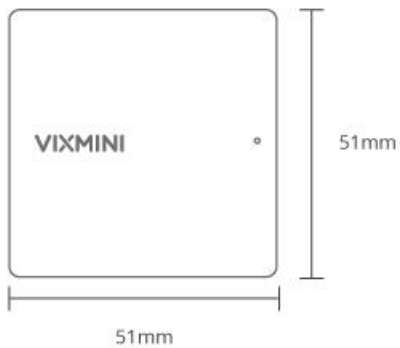
I-GUARD Premium

Home 네트워크 전체 보호

(*) I-GUARD Mini는 Repeater(Router) Mode로도 사용 가능함.

4. I-GUARD(6) – 지원 예상 모델(2)

I-GUARD Mini



4. I-GUARD(7) – TODO

- 1) I-GUARD Premium
 - 가격이 비싼 관계로 경쟁력 있는 추가 기능을 발굴해야 함.
- 2) I-GUARD Lite
 - Home AP의 SSID가 노출되지 않도록 하는 방안 모색해야 함.
 - **가격적인 면, 네트워크 구성 측면에서 이게 가장 합리적인 선택일 듯.**
- 3) I-GUARD Mini
 - 가장 저렴함. \$ 17.99, **I-GUARD Lite** 자리에도 위치할 수 있음.
- 4) Android/iOS App
 - 제어용 간단한 App: 오히려 이게 경쟁력이 될 수도 있겠음.

Thank You



We Secure the Internet of Things with 2STON™ SPN