2ip SPN I-GUARD

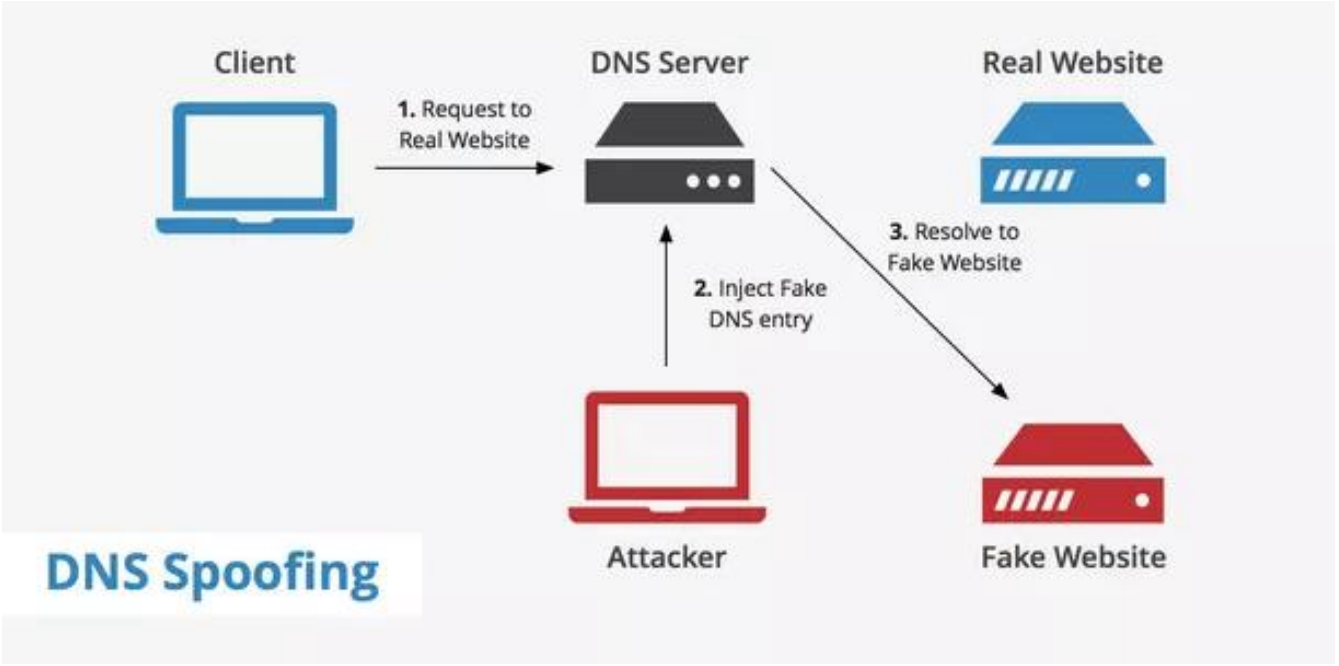
DNS Security

(개발 계획)

2ip, Inc.
Doc. Revision: 0.5

Contents

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(Phising)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)

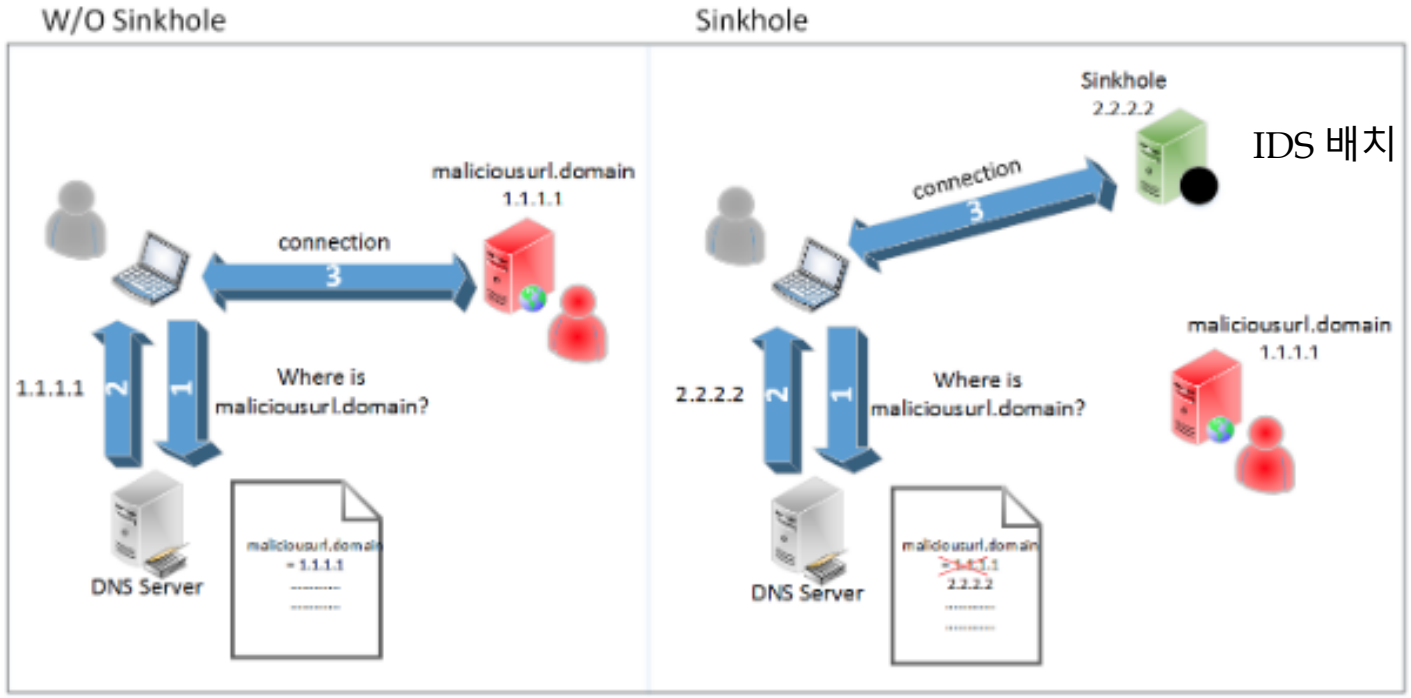
<인터넷 상의 피싱(phishing) 공격과 파밍(pharming) 공격 비교>

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

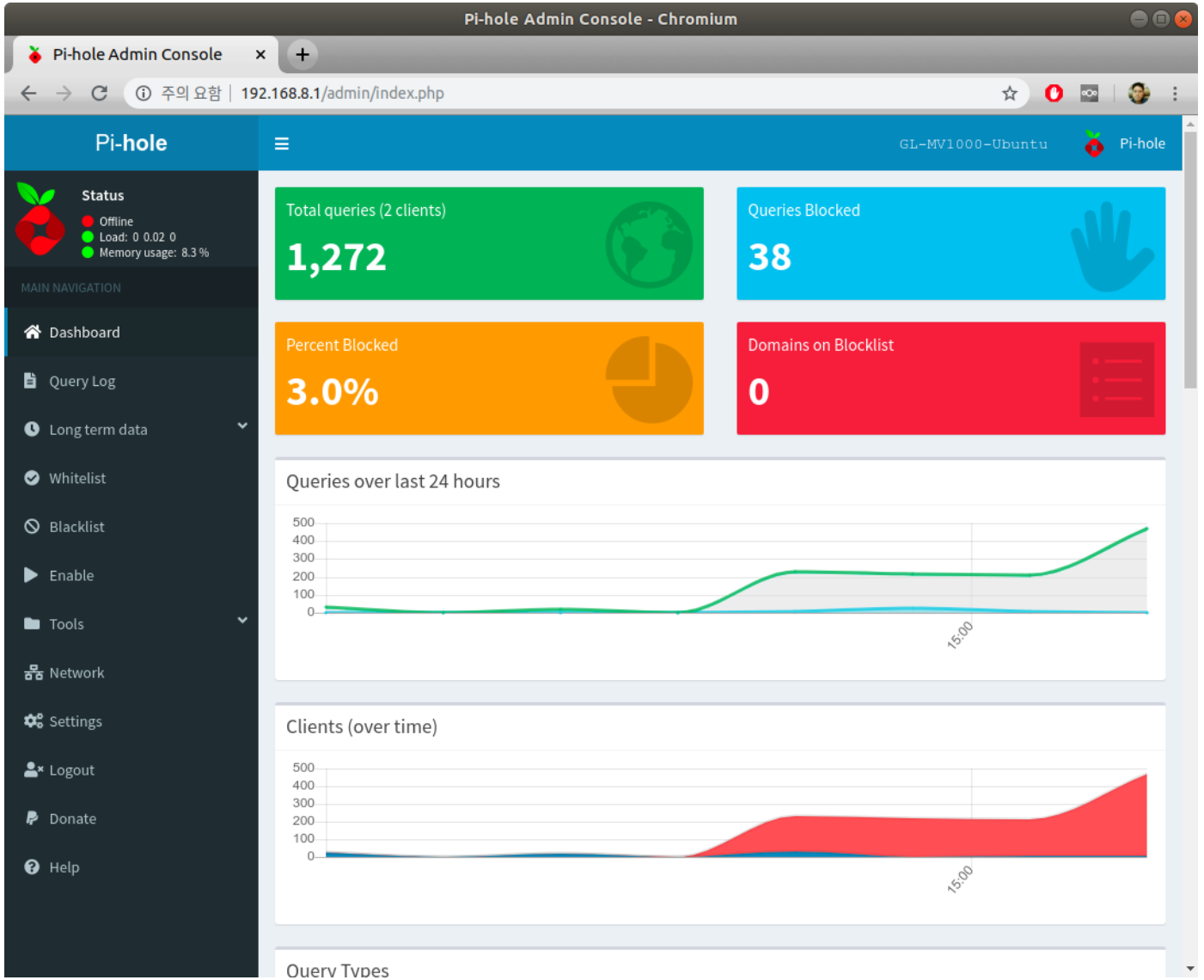
- Black hole DNS or IP sinkhole
- 차단 목적도 있지만 유해 트래픽을 분석하는 목적도 있음.



2. DNS Sinkhole(2) – Pi-hole(1)

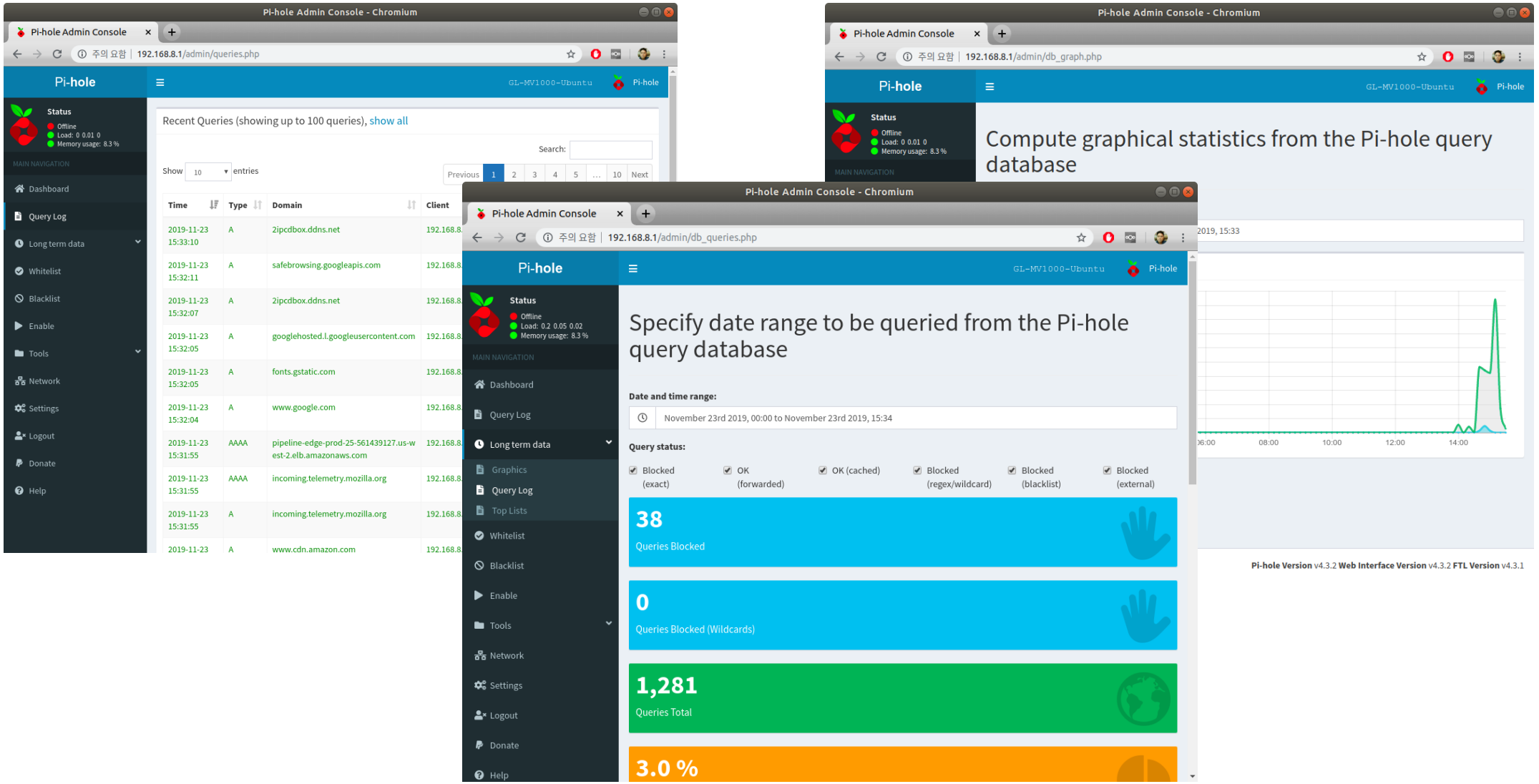
Pi-hole®

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



https://pi-hole.net/

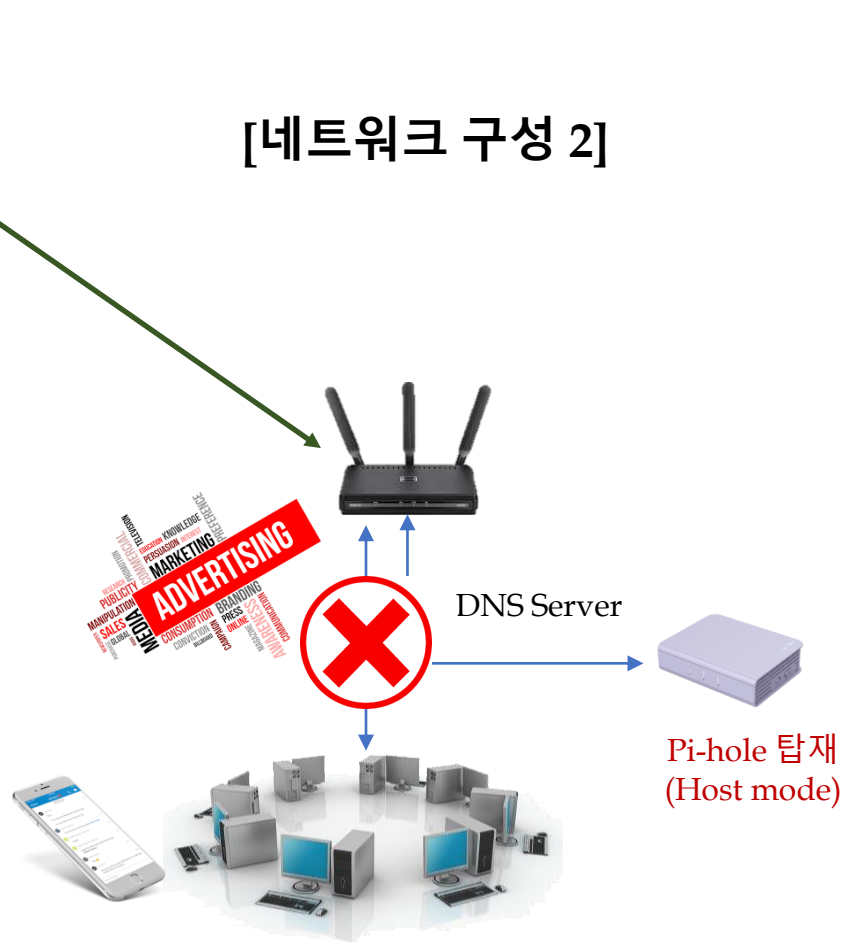
2. DNS Sinkhole(2) – Pi-hole(2)



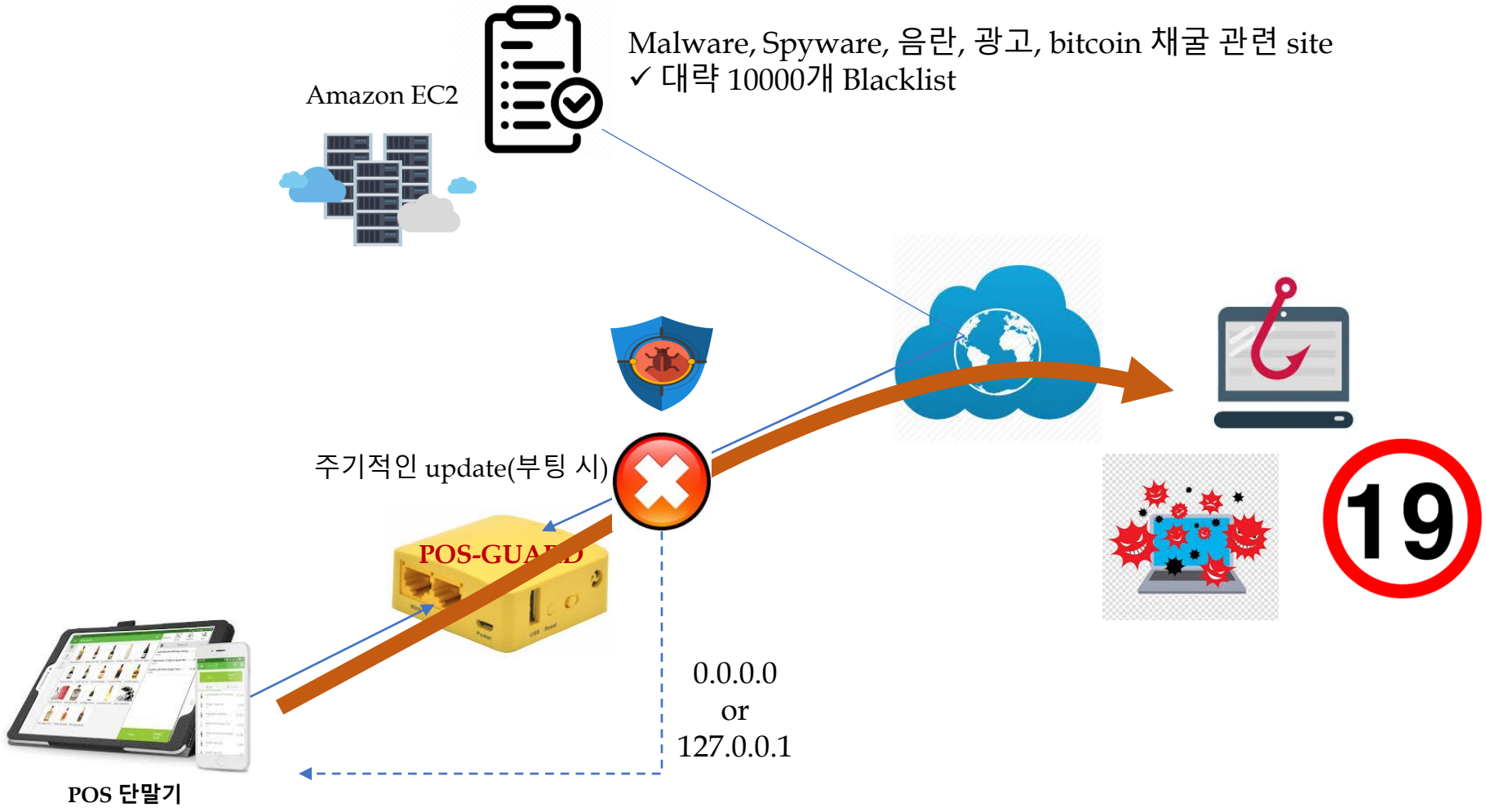
2. DNS Sinkhole(2) – Pi-hole(3)

[네트워크 구성 1]

[네트워크 구성 2]

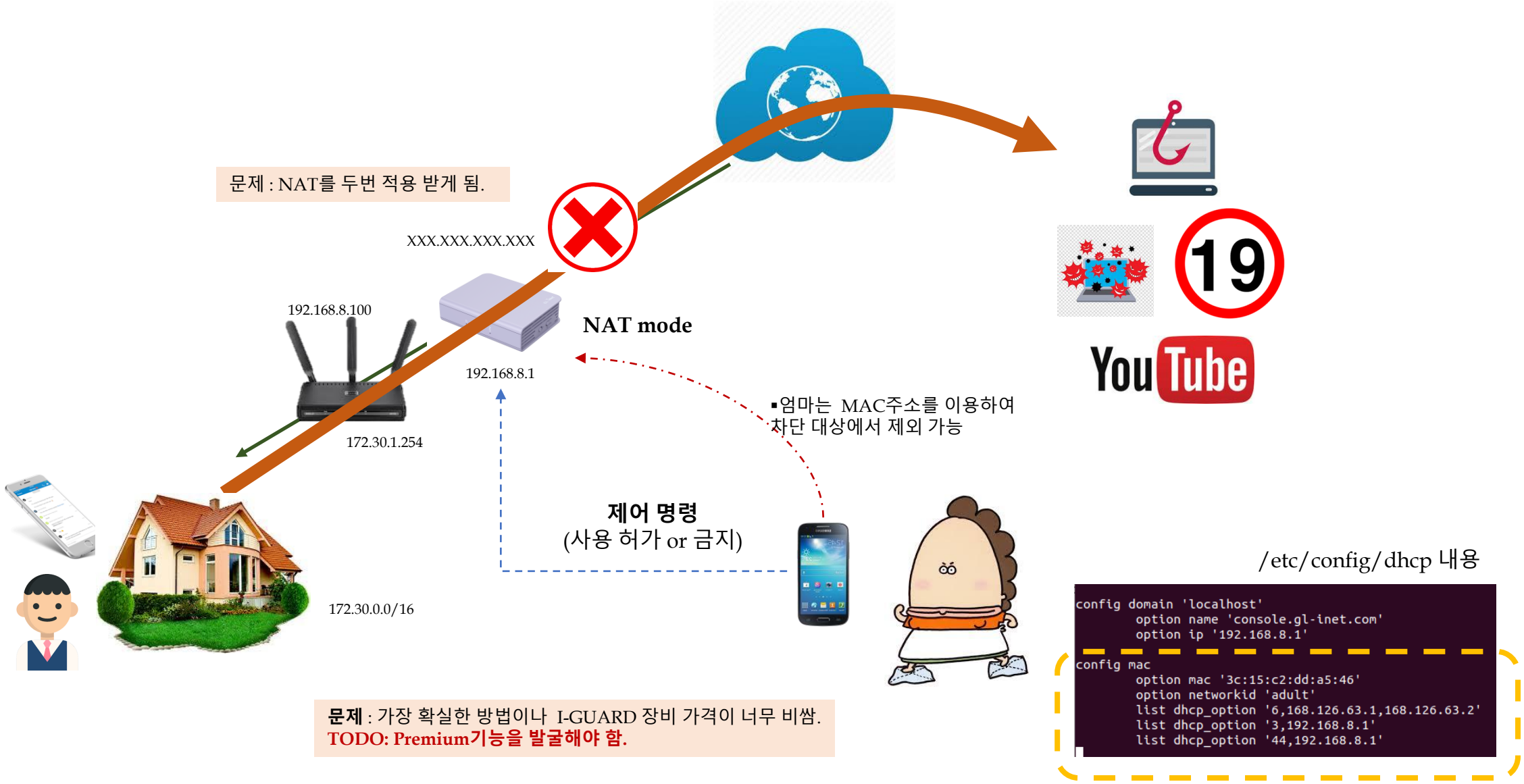


3. POS-GUARD DNS Filter



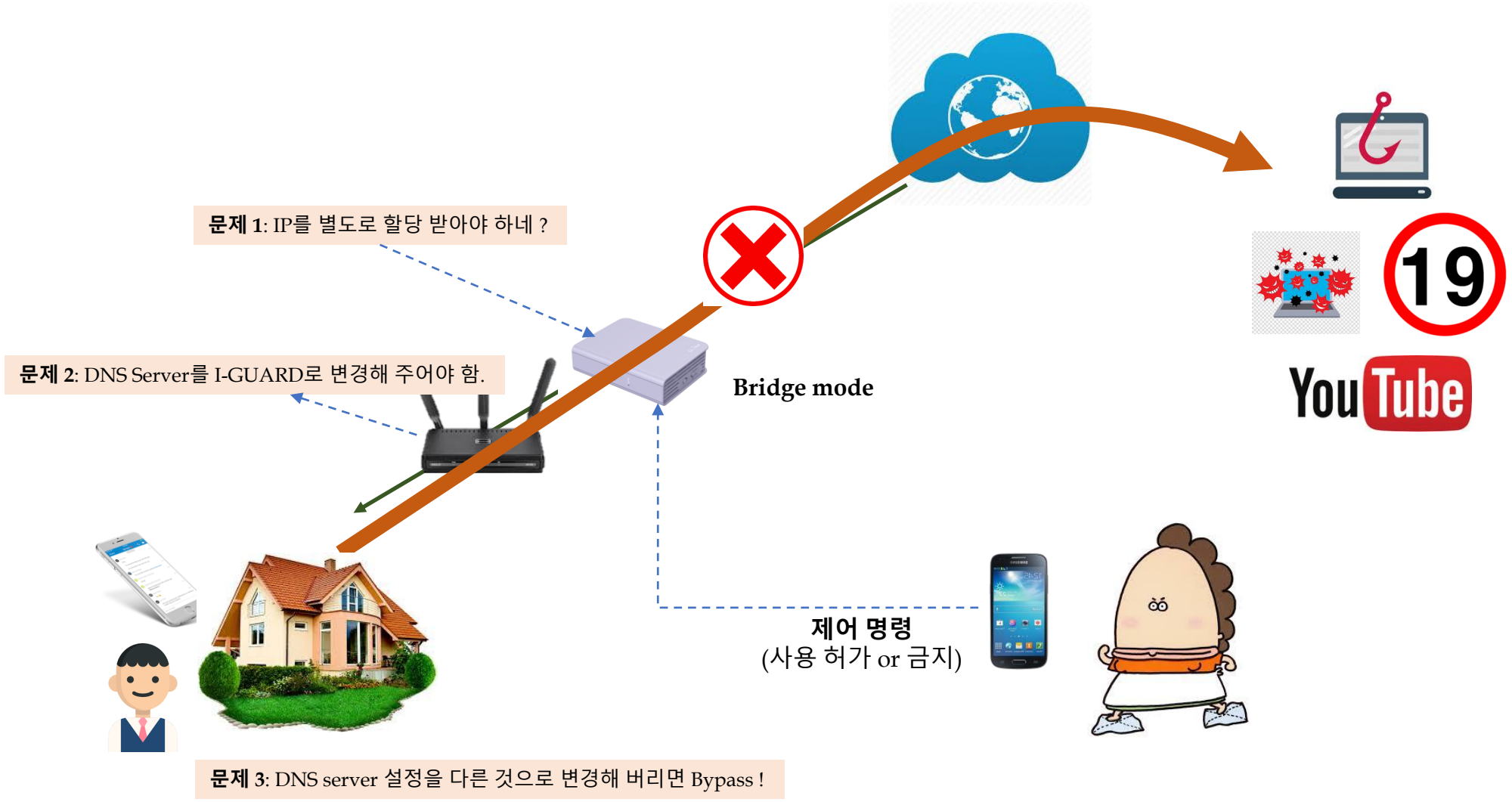
POS-GUARD는 Malware, Spyware, Phishing, 광고, bitcoin 채굴, 음란 site 등을 자동으로 차단해 줍니다.

4. I-GUARD(1) – NAT Mode(1)

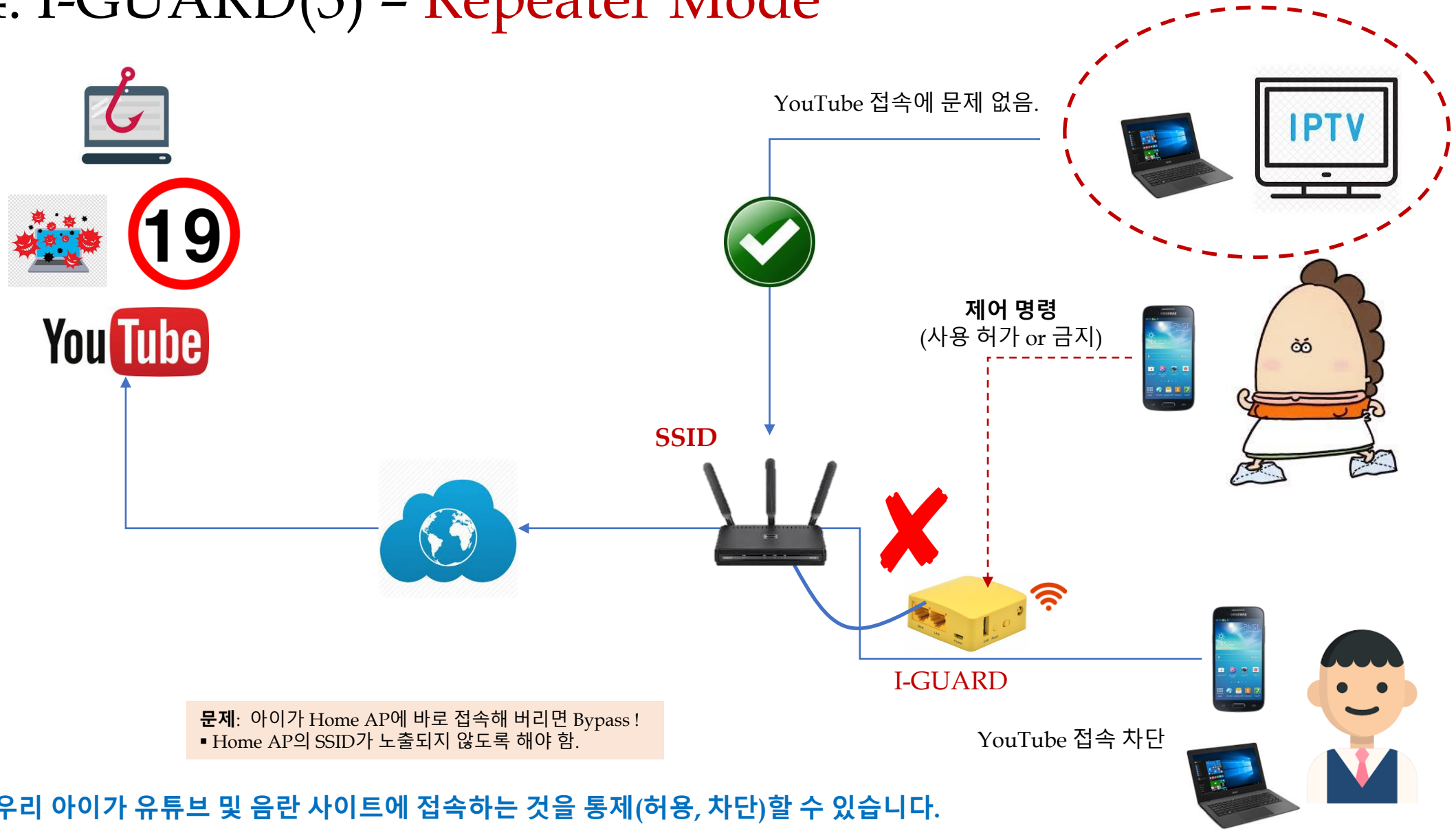


문제 : 가장 확실한 방법이나 I-GUARD 장비 가격이 너무 비쌈.
TODO: Premium기능을 발굴해야 함.

4. I-GUARD(2) – Bridge Mode



4. I-GUARD(3) – Repeater Mode

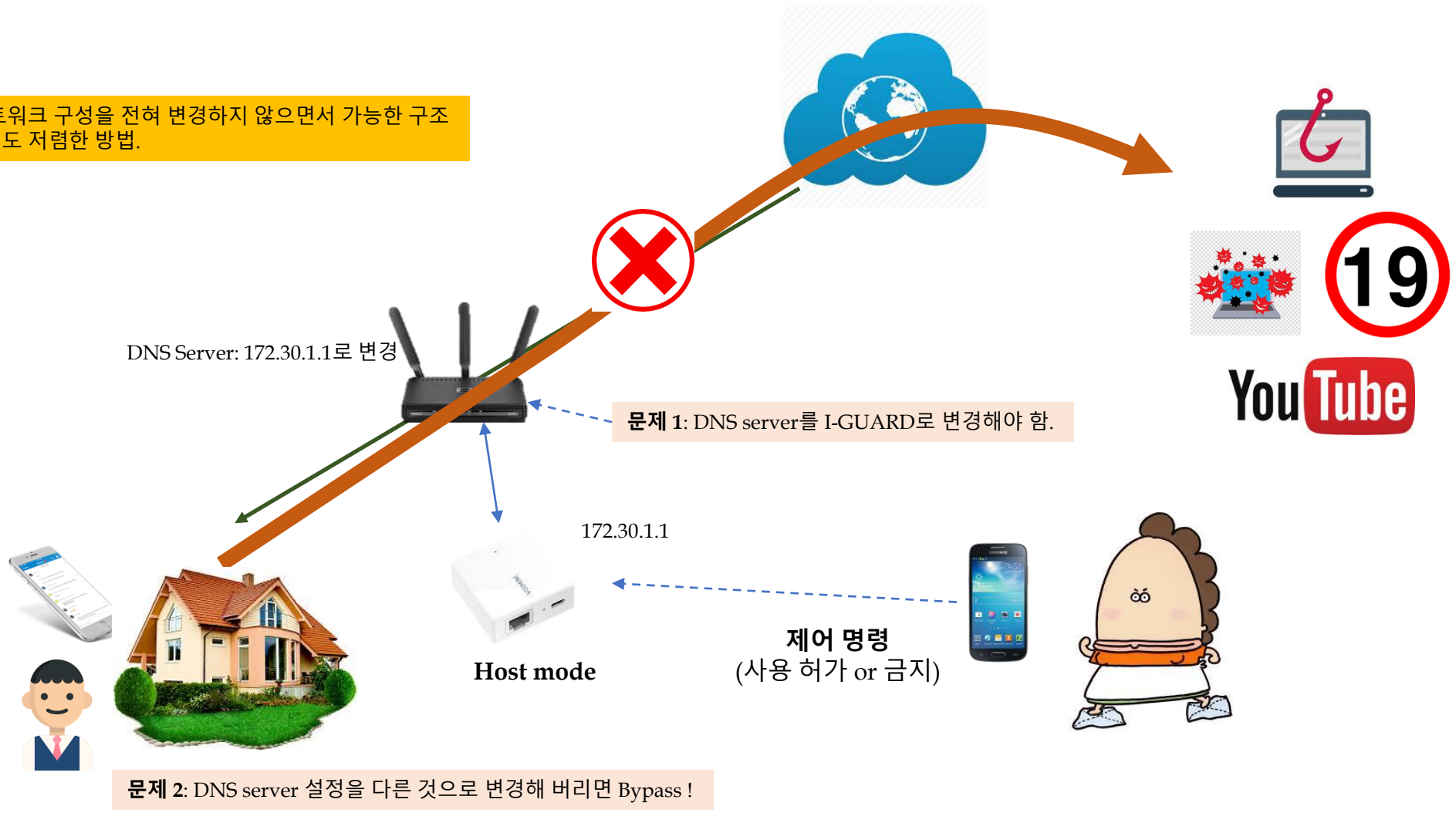


문제: 아이가 Home AP에 바로 접속해 버리면 Bypass !
- Home AP의 SSID가 노출되지 않도록 해야 함.

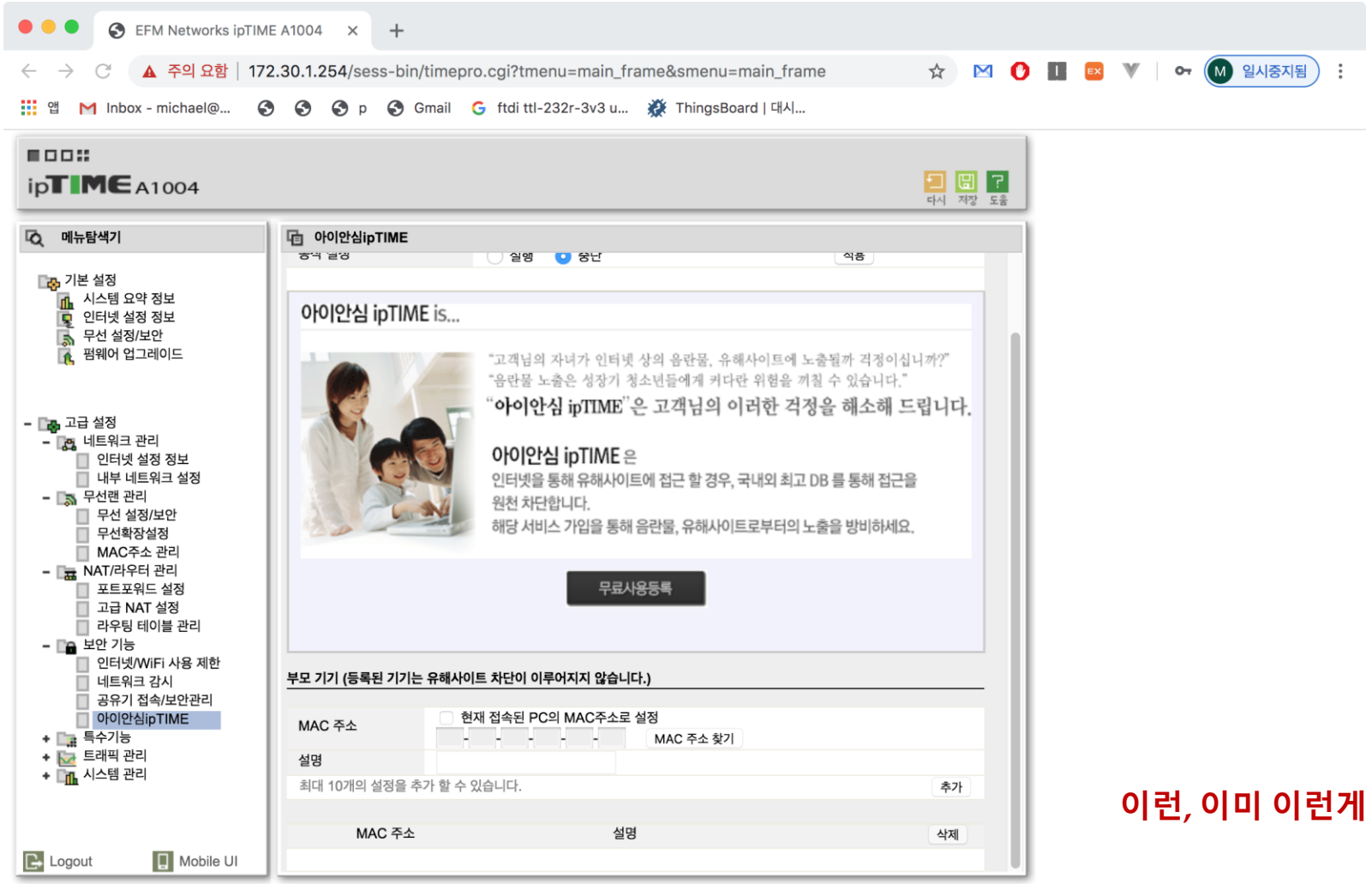
엄마는 우리 아이가 유튜브 및 음란 사이트에 접속하는 것을 통제(허용, 차단)할 수 있습니다.

4. I-GUARD(4) – Host Mode

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



4. I-GUARD(5) – IPTime 아이안심 기능



이런, 이미 이런게 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)

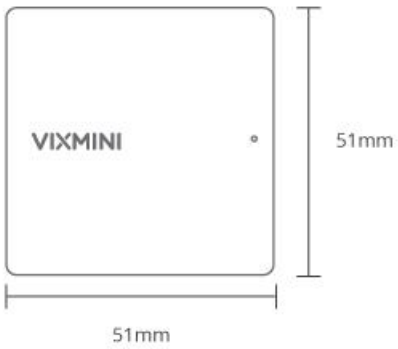
I-GUARD Premium

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