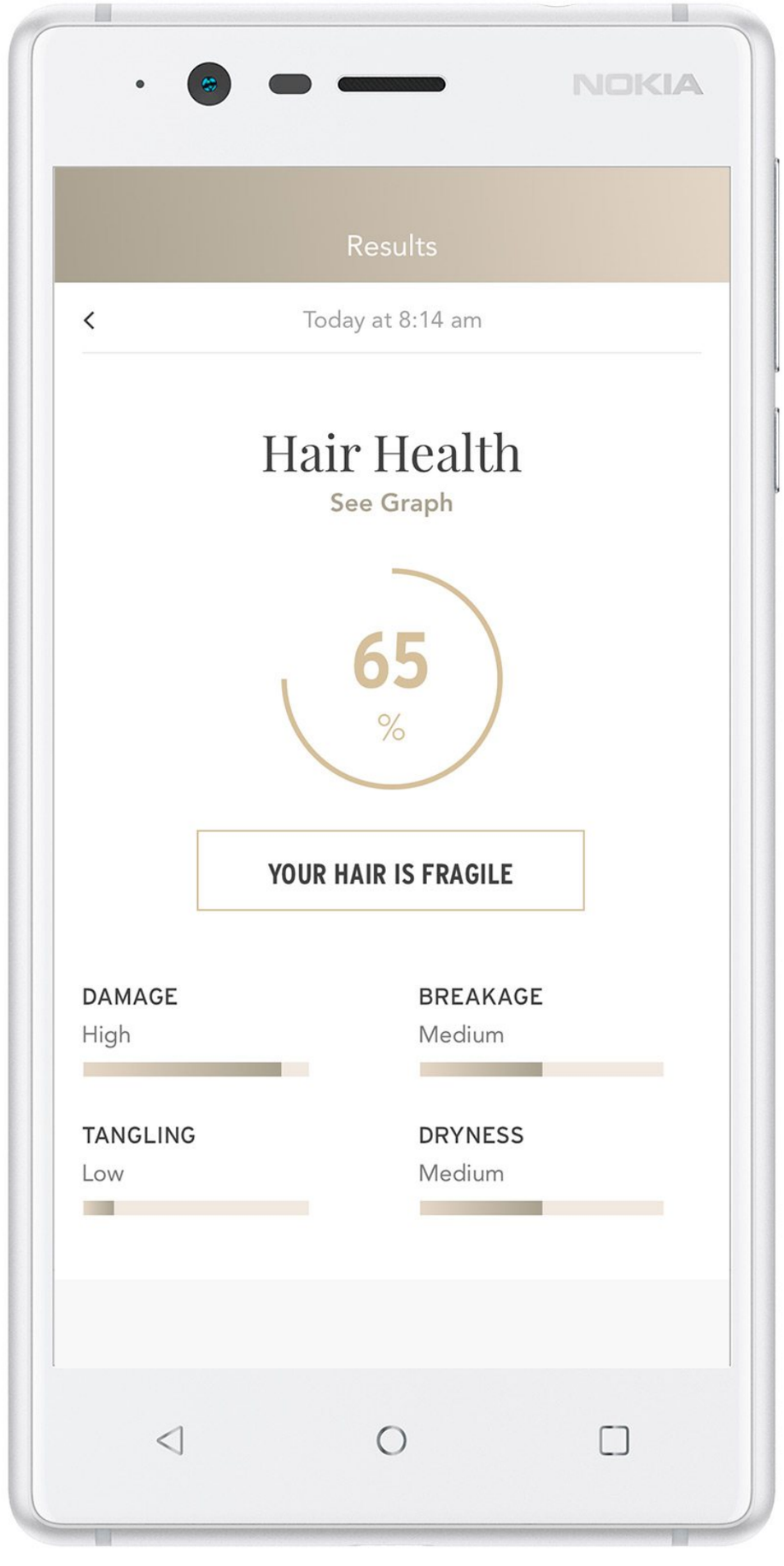
Een veiliger IoT met SPIN

Elmer Lastdrager

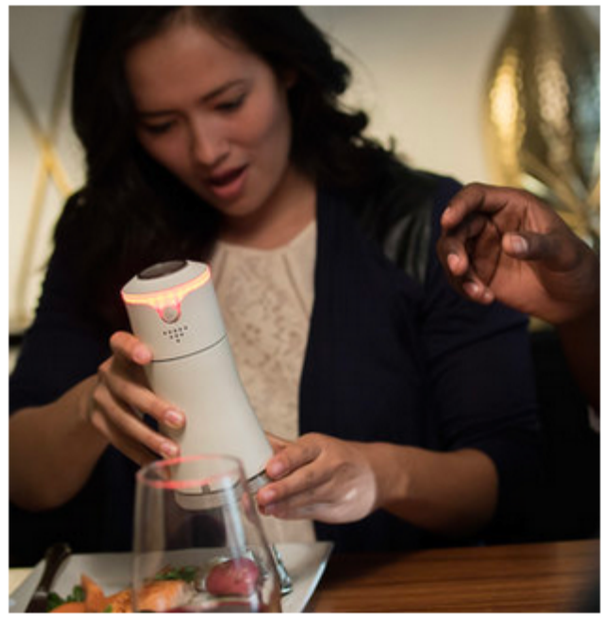
24 september 2019


KÉRASTASE


NOKIA
Results
Today at 8:14 am
Hair Health
See Graph
65
%
YOUR HAIR IS FRAGILE
DAMAGE
High
BREAKAGE
Medium
TANGLING
Low
DRYNESS
Medium

SMALT with voice

Connect SMALT with Amazon Echo and simply say “Alexa, dispense half a teaspoon of salt".



Bring the flavor

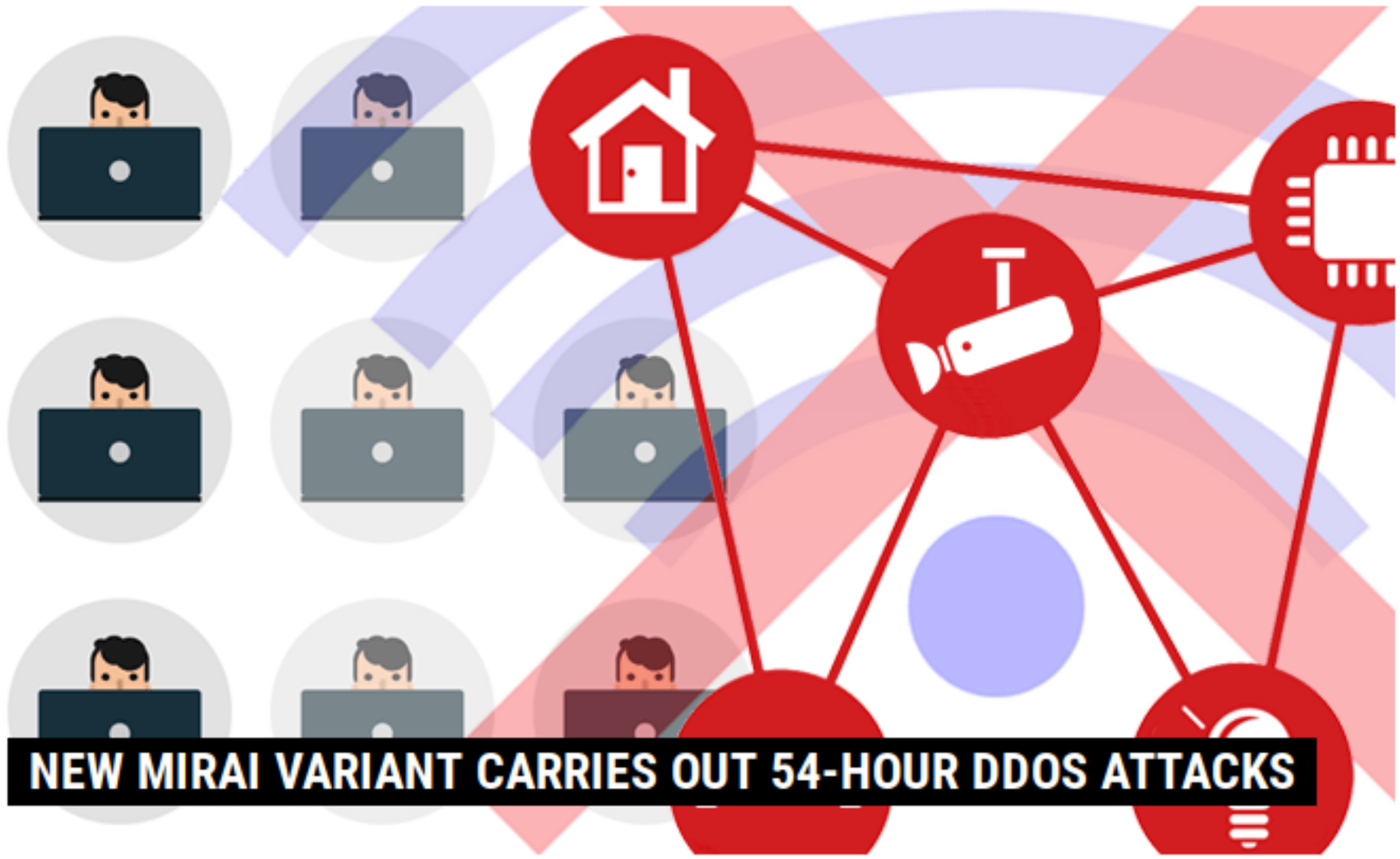
SMALT dispenses salt with a shake/pinch of your smartphone screen or simply turning the dial manually.

YOU GET CONNECTED!

AND YOU GET CONNECTED!

EVERYTHING GETS CONNECTED!


The "S" in IoT
stands for
SECURITY



by **Tom Spring**

March 30, 2017 , 2:50 pm

A variant of the Mirai malware pummeled a U.S. college last month with a marathon 54-hour long attack. Researchers say this latest Mirai variant is a more potent version of the notorious Mirai malware that made headlines in October, targeting DNS provider Dyn and the Krebs on Security website.

NETFLIX

WIRED

amazon.com

airbnb

BBC

CNN

HBO

SECURITY IS SEXY

By Darlene Storm, Computerworld | FEB 2, 2015 12:09 PM PT

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny

This is the third time news has circulated about some jerk hijacking a wireless Foscam camera/baby monitor and made his virtual intrusion known by talking. Please change the default password!

MORE LIKE THIS

Hacker strikes again: Creep hijacks baby monitor to scream at infant and...

2 more wireless baby monitors hacked: Hackers remotely spied on babies and...

Eerie music coming from wireless baby cam: is it a

EXCLUSIEF

Gluren in babykamers: duizenden slimme camera's in Nederland onveilig door lek

Aangepast: 21 september 2019 12:05

De camera's van Sumpple worden verkocht via grote webwinkels.

Kwaadwillenden kunnen meegluren met duizenden Nederlandse beveiligingscamera's en babyfoons. Door een lek liggen e-

Nieuws

Opvallend verkeer en gedrag bij smart-tv's en IoT-deurbellen

vrijdag 20 september 2019, 09:49 door **Redactie**, 27 **reacties**

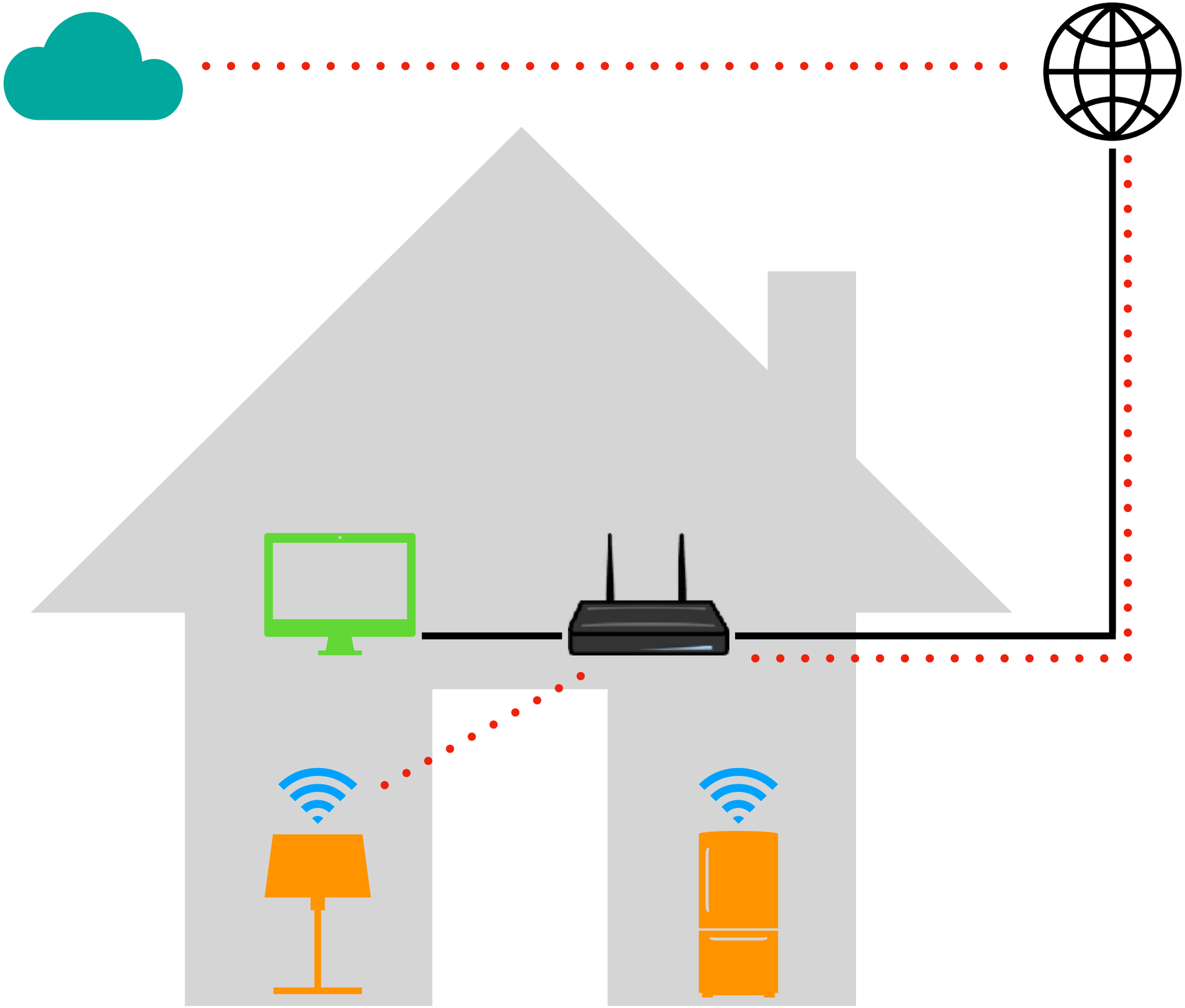
Smart-tv's die standaard verkeer naar Netflix sturen ook al heeft de gebruiker geen Netflix-account en IoT-deurbellen die opnames van voorbijgangers maken zonder dit aan de eigenaar te melden. Het zijn slechts enkele uitkomsten van een grootschalig onderzoek naar Internet of Things-apparaten (**pdf**).

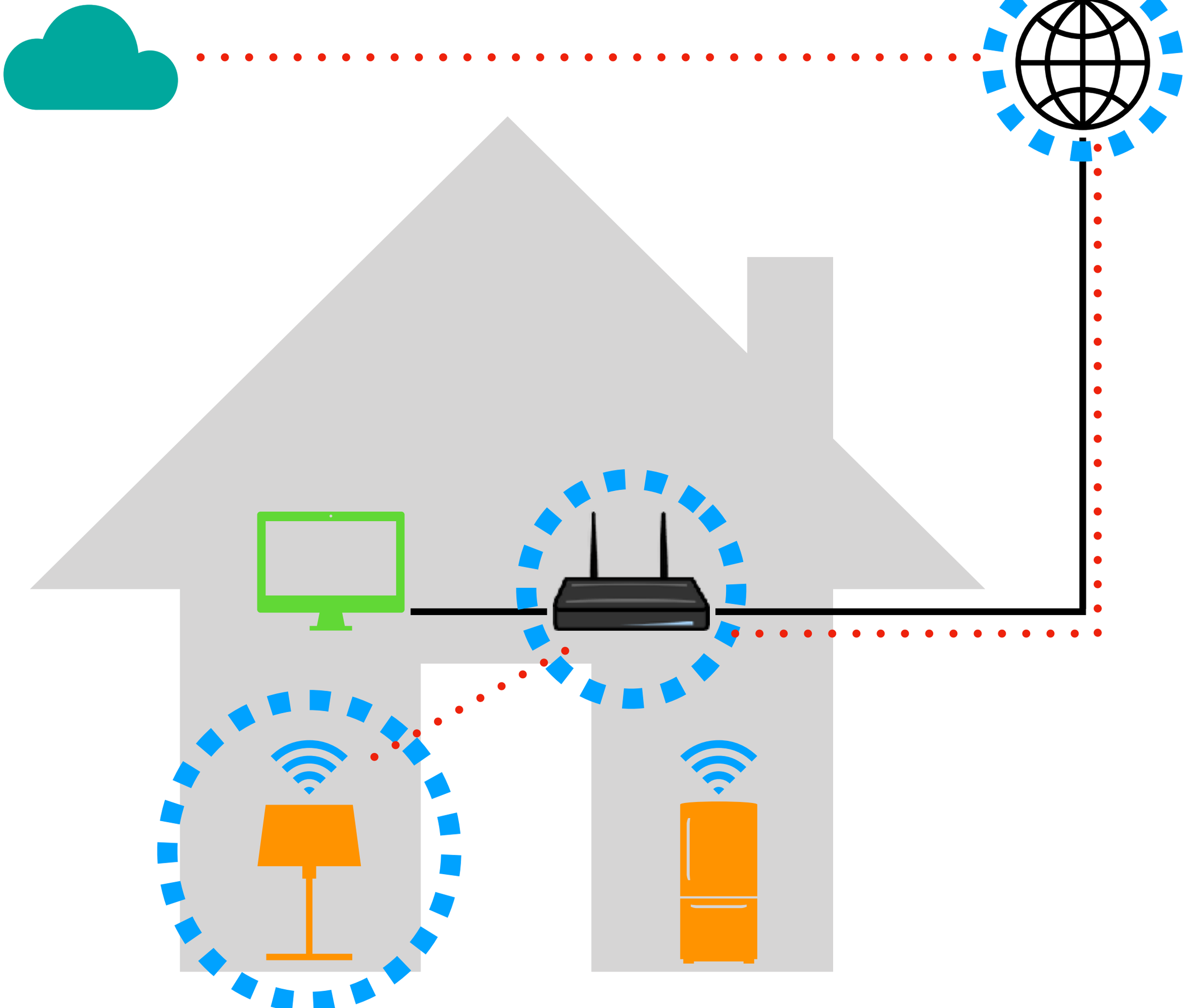
Het onderzoek werd uitgevoerd door onderzoekers van het Imperial College London en de Northeastern University. Het vond gedurende een periode van anderhalf jaar plaats en omvatte 81 IoT-apparaten, waaronder rijstkokers, koelkasten, lampen, speakers en televisies, die aan ruim 34.000 gecontroleerde experimenten in twee locaties, de Verenigde Staten en Verenigd Koninkrijk, werden blootgesteld. 72 van de 81 apparaten stuurden data naar een locatie die niet van de fabrikant was. Verder bleek dat 56 procent van de apparaten in de VS en bijna 84 procent van de apparaten die in het VK werden getest data naar locaties buiten hun regio stuurden.

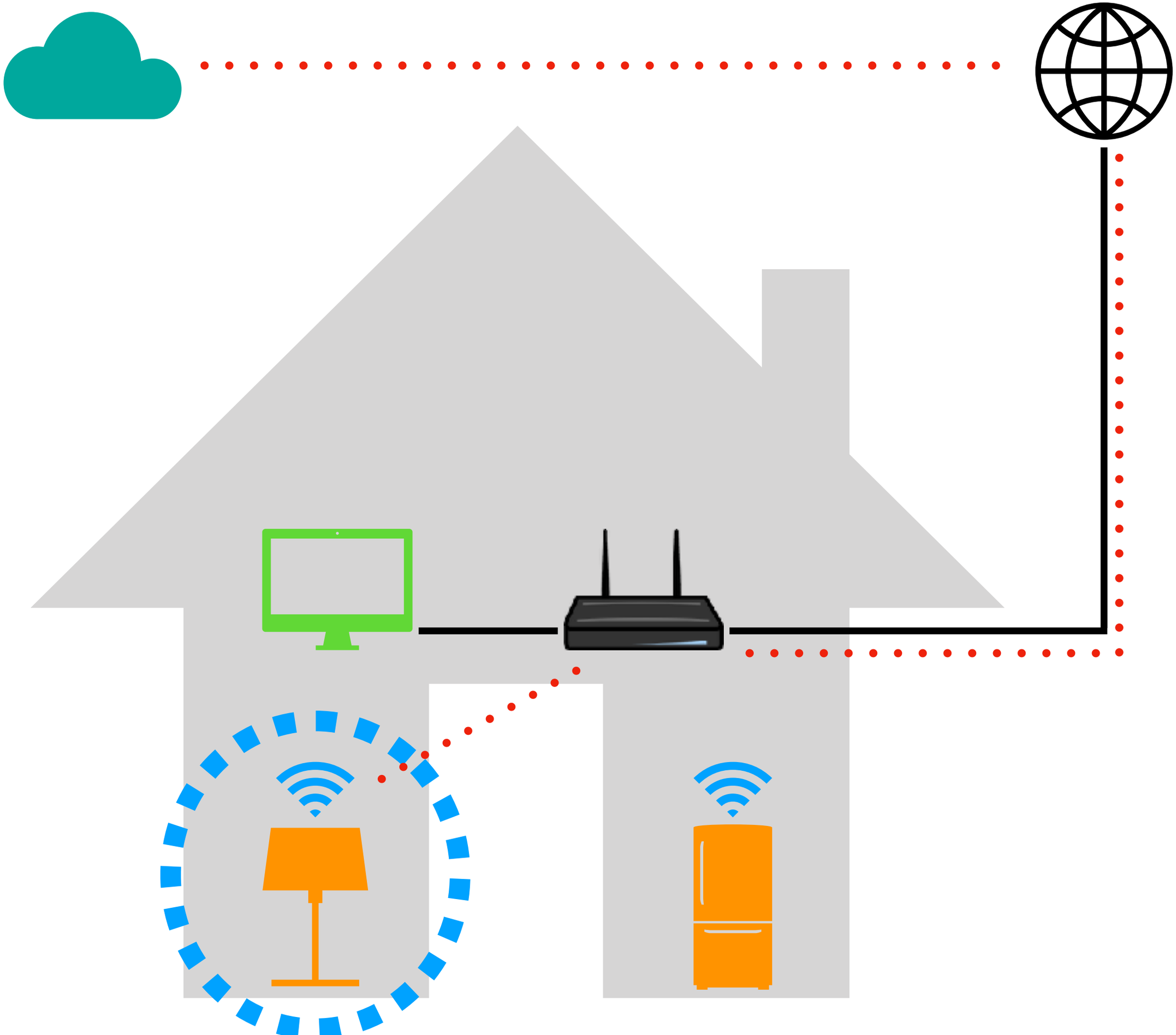
Alle apparaten blijken informatie via onversleutelde data te lekken en een passieve afluisteraar kan bij 30 van de 81 apparaten het gedrag van de gebruiker en het apparaat aan de hand van het verkeer afleiden, ongeacht of dit versleuteld is. Tevens blijkt dat tientallen van de apparaten bij het inschakelen data naar derde partijen versturen, waaronder Facebook, Google, Microsoft en Netflix. Tevens blijkt dat een klein aantal cloudproviders het meeste IoT-verkeer zien, waardoor ze een grote hoeveelheid informatie ontvangen over de apparaten die bij mensen thuis staan.

What to do?

- Better practices for manufacturers?
- Free **secure** software stacks?
- International policy, regulation, certification?
- Clear up accountability issues?
- Generate market demand for secure products?
- Quarantine bad actors (e.g. at ISP)?
- Educate users?
- Empower users?



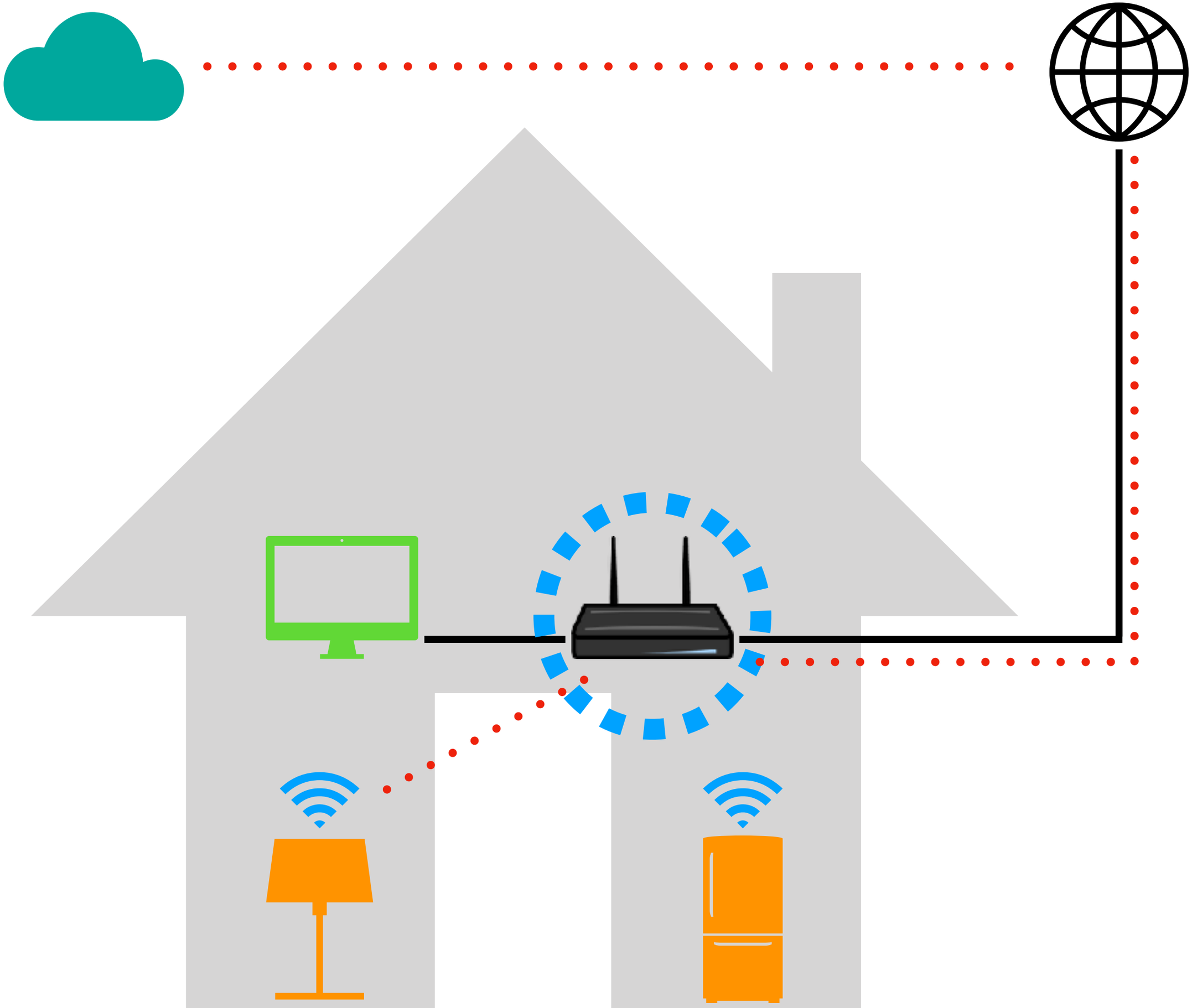




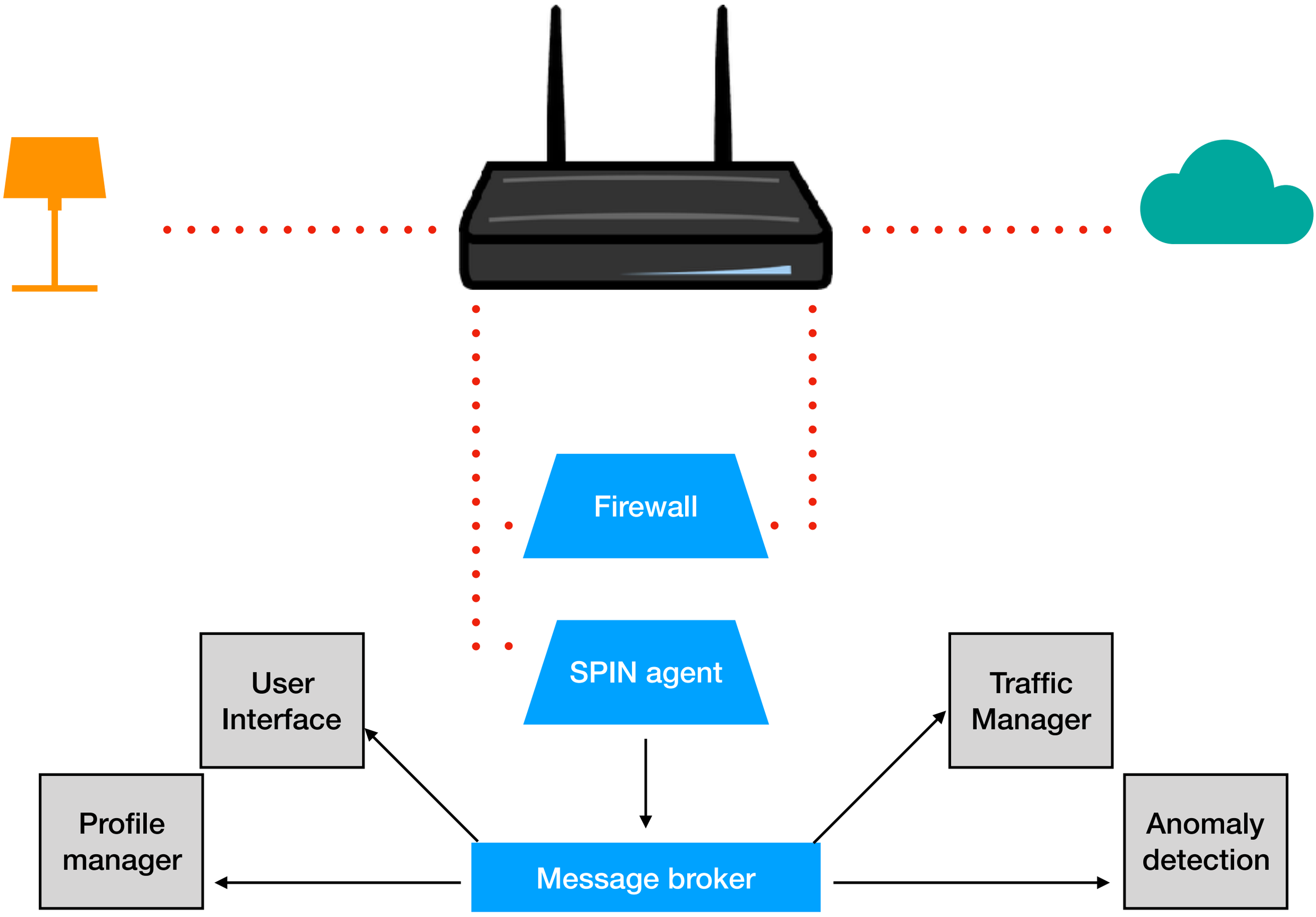
THE 5 RULES

1. No updates = no Internet
2. Force default password change
3. Patch
4. Bug bounty
5. Only collect and process RELEVANT data

F-Secure.



Security and Privacy for In-home Networks (SPIN)


Firewall
SPIN agent
User Interface
Traffic Manager
Profile manager
Message broker
Anomaly detection

Filter: tcp.stream eq 4 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
17	0.000000	192.168.8.100	192.168.8.101	TCP	54	49684 > http [ACK] Seq=1 Ack=1 Win=16
18	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
19	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
20	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
21	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
22	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
23	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
24	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
25	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
31	0.000000	192.168.8.100	192.168.8.101	TCP	66	[TCP Out-Of-Order] 49684 > http [SYN]
36	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
37	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
38	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
39	0.000000	192.168.8.100	192.168.8.101	TCP	55	[TCP segment of a reassembled PDU]
40	0.000000	192.168.8.100	192.168.8.101	HTTP	56	Continuation or non-HTTP traffic

```
▶Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶Ethernet II, Src: AskeyCom_97:4c:bf (24:ec:99:97:4c:bf), Dst: Vmware_39:6e:6c (00:0c:29:39:6e:6c)
▶Internet Protocol Version 4, Src: 192.168.8.100 (192.168.8.100), Dst: 192.168.8.101 (192.168.8.101)
▶Transmission Control Protocol, Src Port: 49684 (49684), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
```

```
0000  00 0c 29 39 6e 6c 24 ec  99 97 4c bf 08 00 45 00   ..)9nl$. ..L...E.
0010  00 28 62 9d 40 00 80 06  06 19 c0 a8 08 64 c0 a8   .(b.@... .....d..
0020  08 65 c2 14 00 50 99 71  a0 1c 19 33 90 5c 50 10   .e...P.q ...3.\P.
0030  00 40 77 f8 00 00                                  .@w...
```

File: "Win8bulk/packets.pcap" ... Packets: 1528 · Displayed: 36 (2.4%) · Load time: 0:00.018 Profile: Def

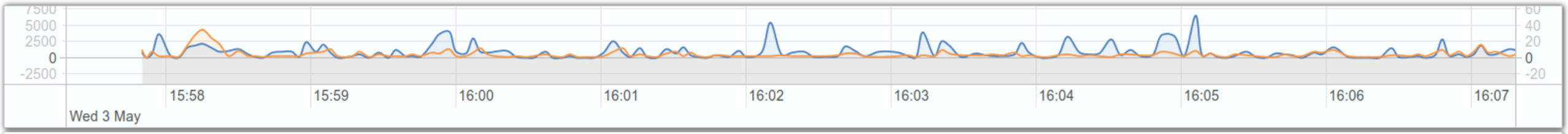
SPIN Traffic monitor pr... | SPIN Traffic monitor debu...

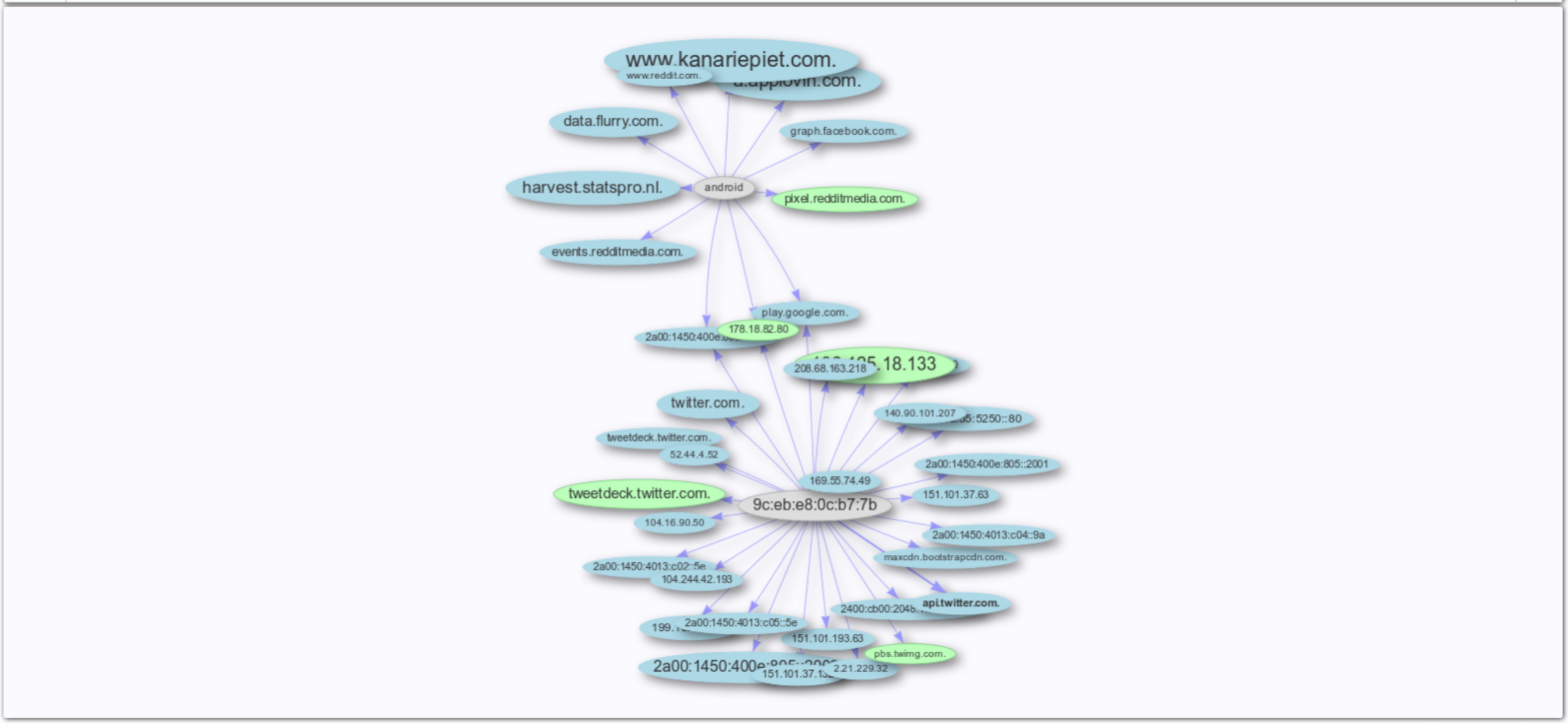
valibox./spin/graph.html

Search

Lock view | Show filter list | Connected

SPIN Traffic monitor prototype





Beta-release by SIDN Labs.

SPIN Traffic monitor prototype - Iceweasel

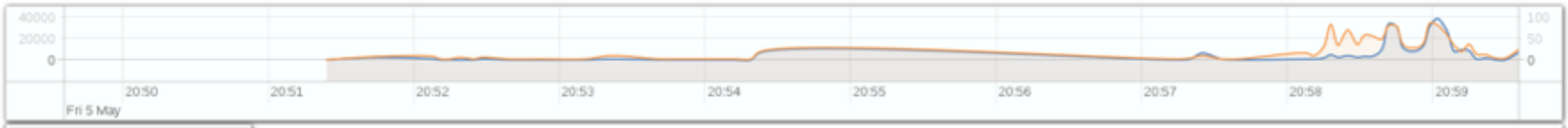
Restore Session | SPIN Traffic monitor prot...

turris/luci-static/spin/graph.html

Search

SPIN Traffic monitor prototype

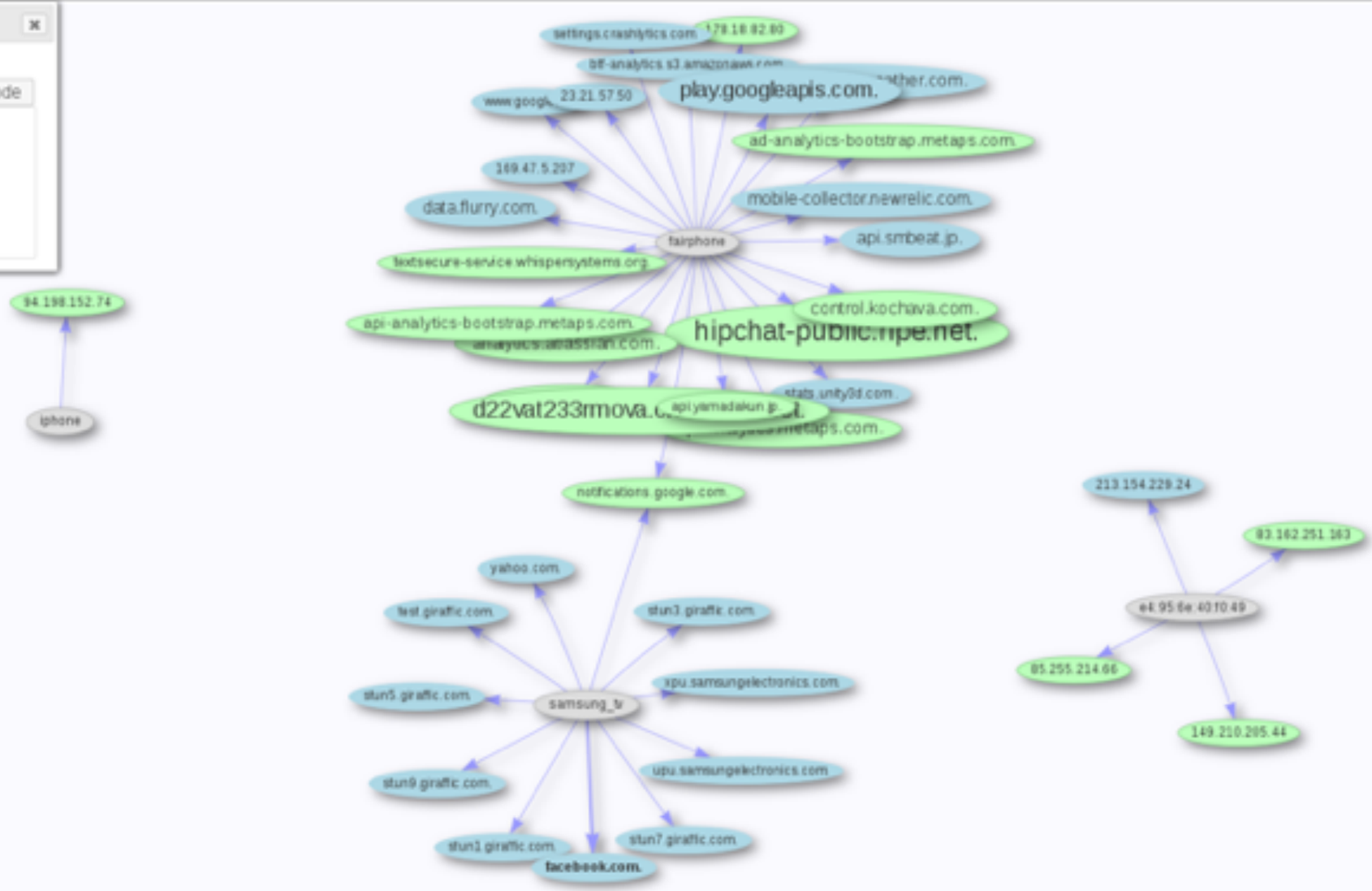
Unlock view | Show filter list | Connected



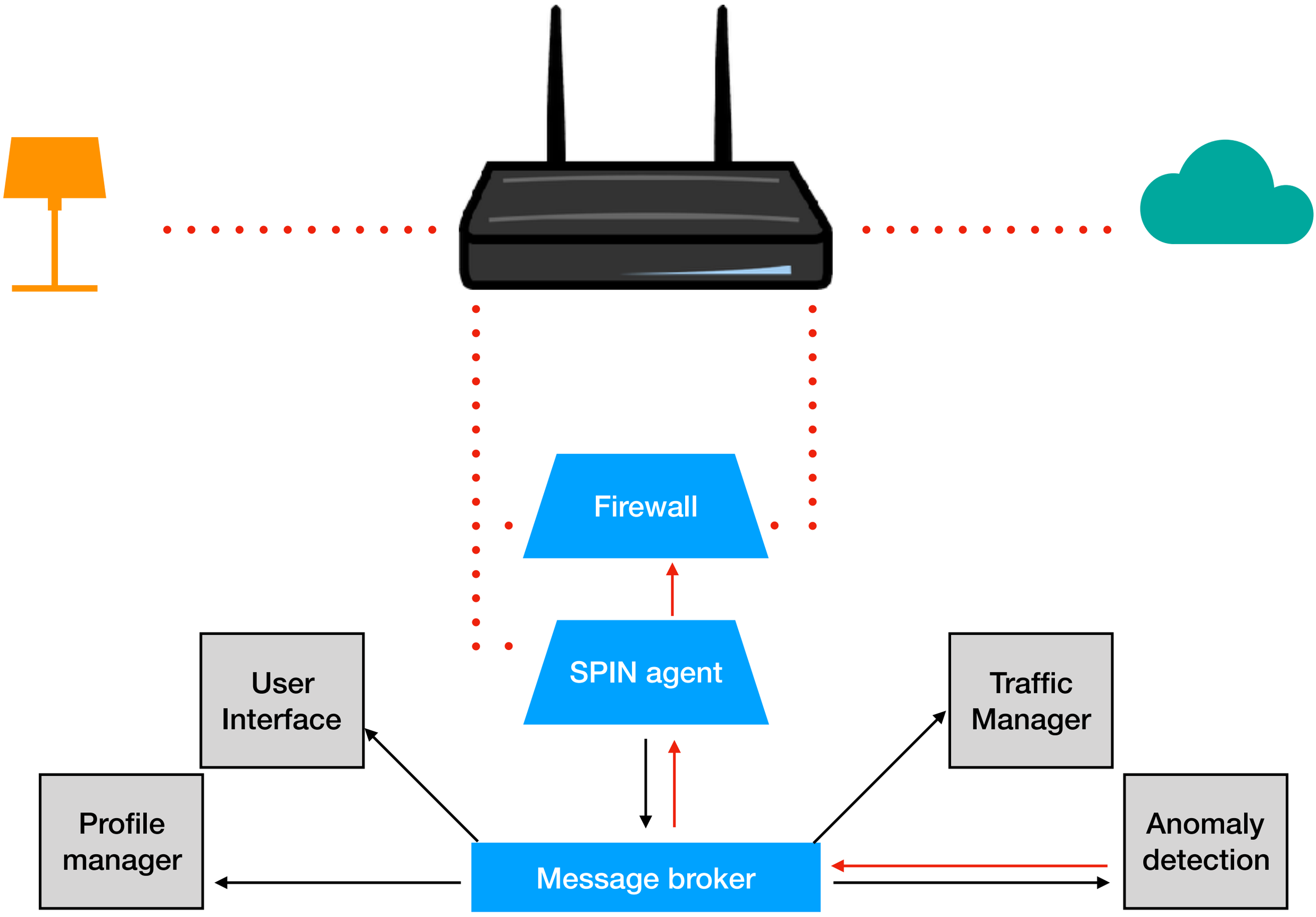
facebook.com.

Ignore this node | Rename this node | Block node

Node: 61
Connections seen: 5
Traffic size: 268
Last seen: Fri May 05 2017 20:58:11 GMT+0200 (CEST)
IP: 157.240.3.35
DNS: facebook.com.



Beta release by SIDN Labs.


Firewall
SPIN agent
User Interface
Profile manager
Message broker
Traffic Manager
Anomaly detection

PROPOSED STANDARD
Errata Exist

Internet Engineering Task Force (IETF)
Request for Comments: 8520
Category: Standards Track
ISSN: 2070-1721

E. Lear
Cisco Systems
R. Droms
Google
D. Romascanu

March 2019

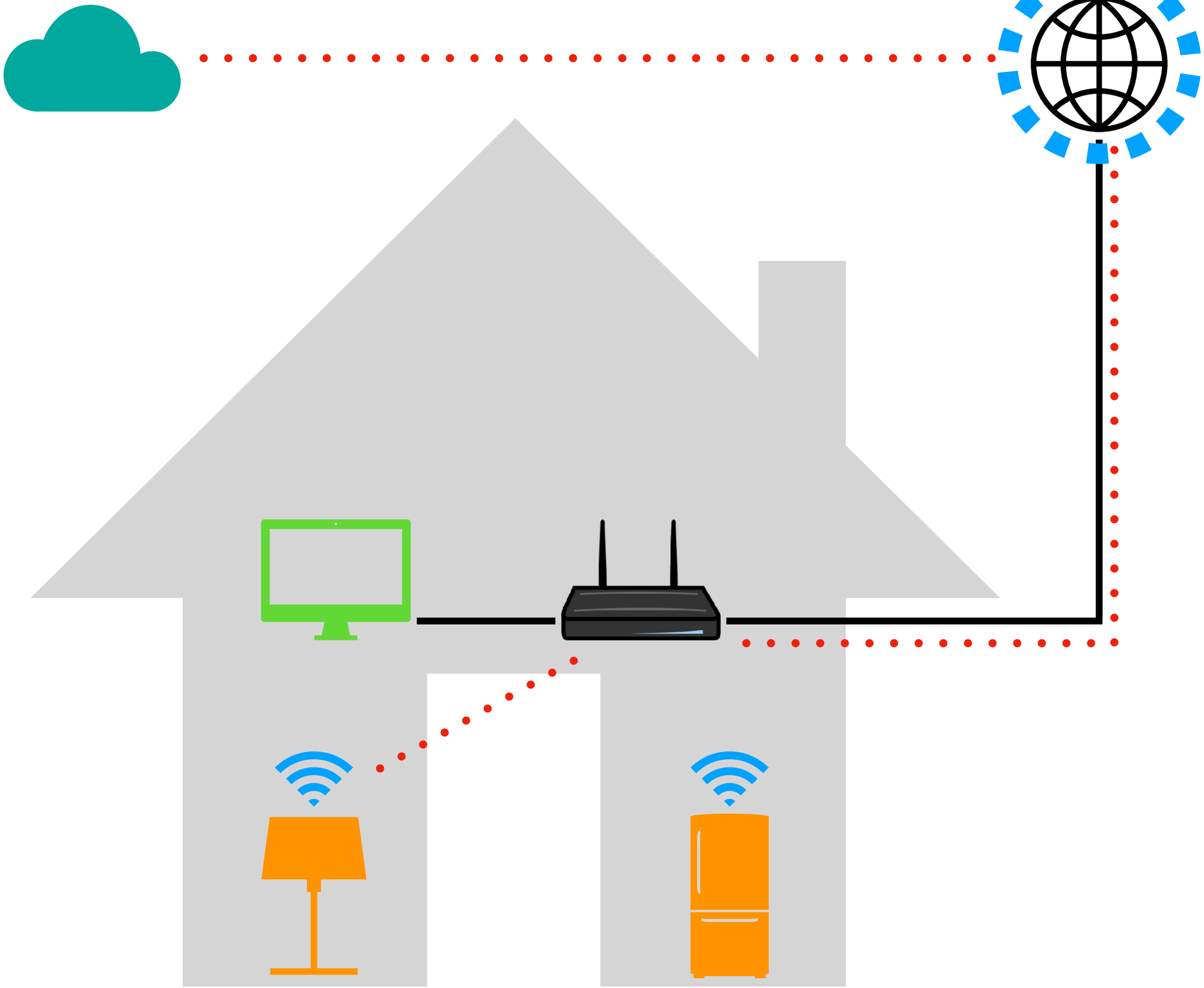
Manufacturer Usage Description Specification

Abstract

This memo specifies a component-based architecture for Manufacturer Usage Descriptions (MUDs). The goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. Later work can delve into other aspects.

This memo specifies two YANG modules, IPv4 and IPv6 DHCP options, a Link Layer Discovery Protocol (LLDP) TLV, a URL, an X.509 certificate extension, and a means to sign and verify the descriptions.

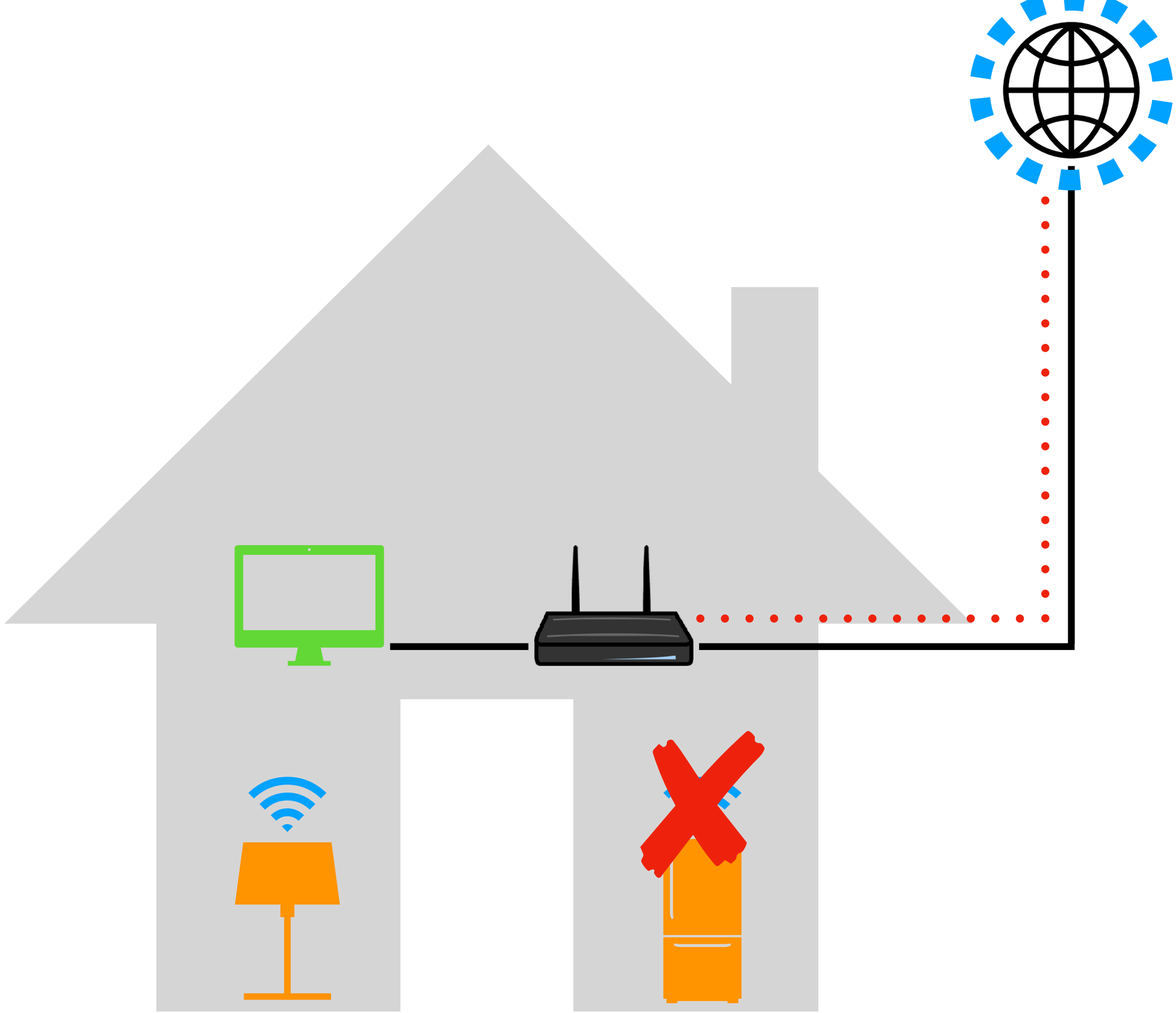
Status of This Memo



CAUTION

KEEP OUT

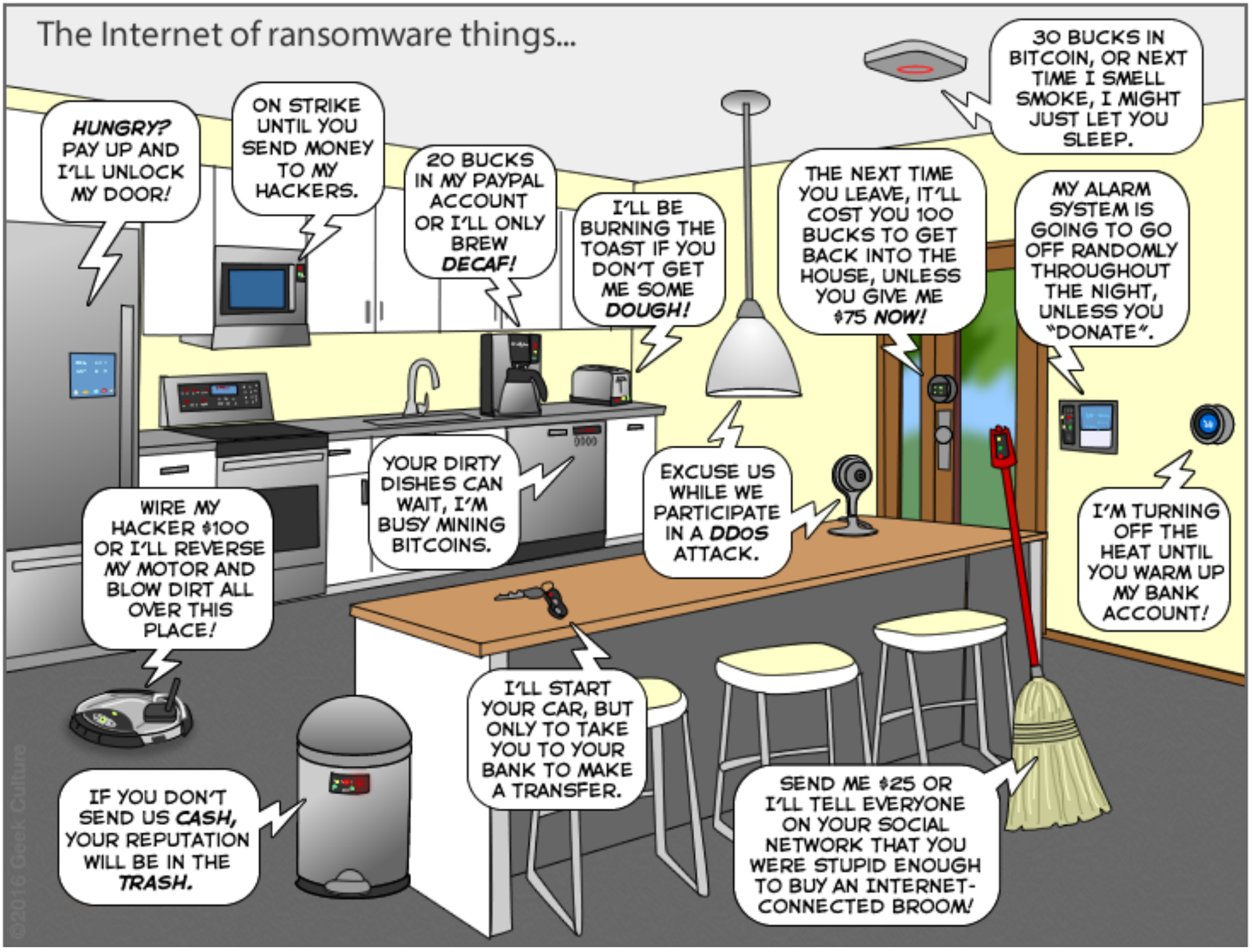
QUARANTINE




Max input: 230 V


sobo

The Joy of Tech™ by Nitrozac & Snaggy



elmer.lastdrager@sidn.nl
https://spin.sidnlabs.nl