



Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure

Marcin Nawrocki, **Maynard Koch**, Thomas C. Schmidt, Matthias Wählisch

`marcin.nawrocki@fu-berlin.de`
`{maynard.koch, m.waehlisch}@tu-dresden.de`
`t.schmidt@haw-hamburg.de`

Which devices implement transparent DNS forwarding?
Misbehaving CPE devices in ISP networks.

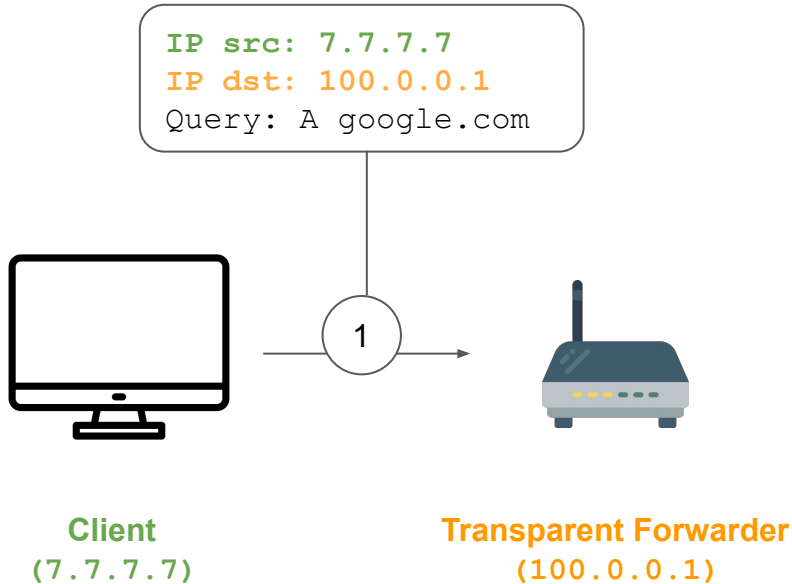


How do transparent forwarders work?

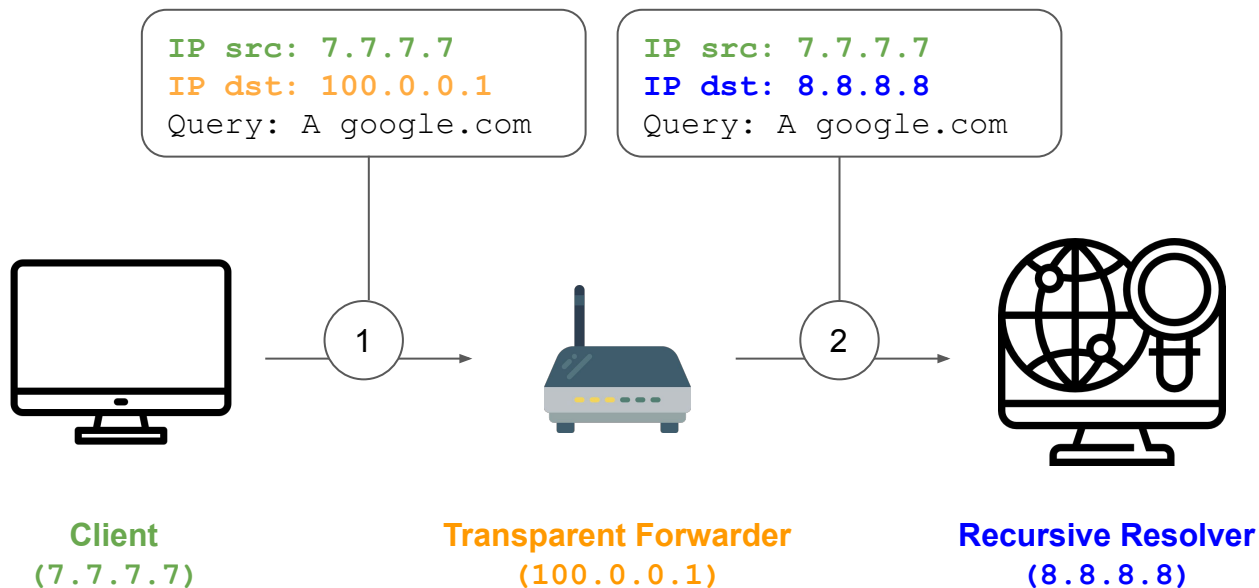


Client
(7.7.7.7)

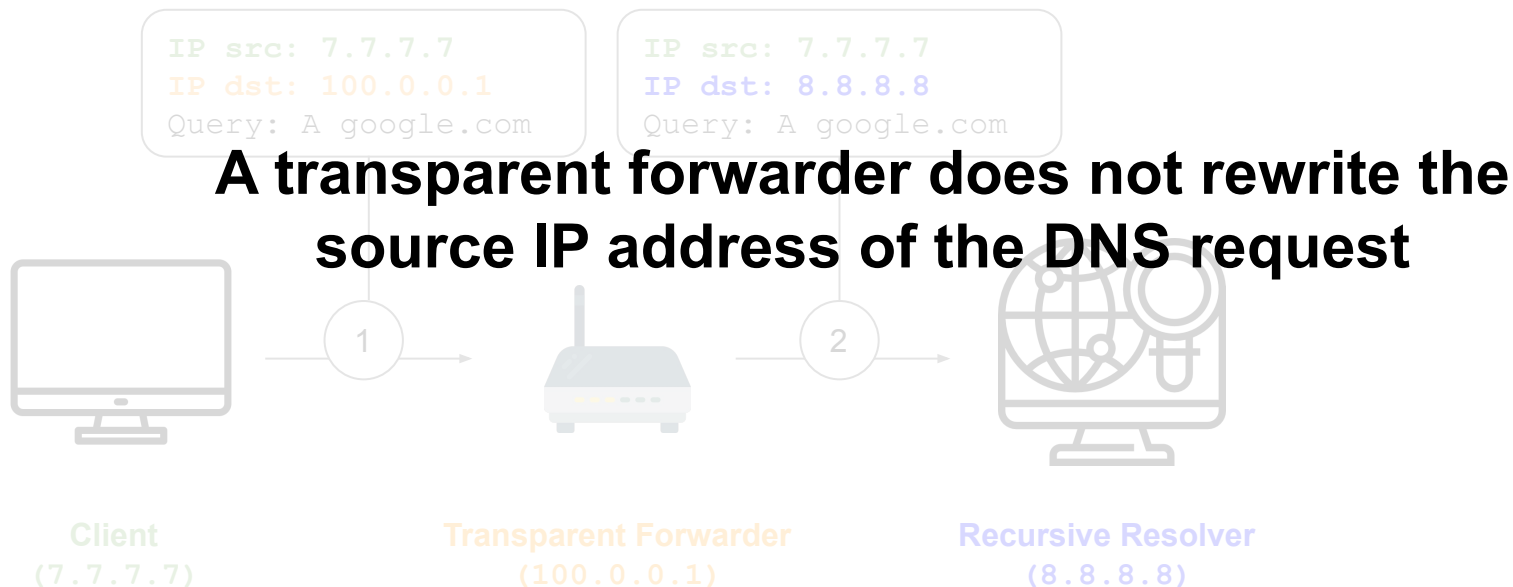
How do transparent forwarders work?



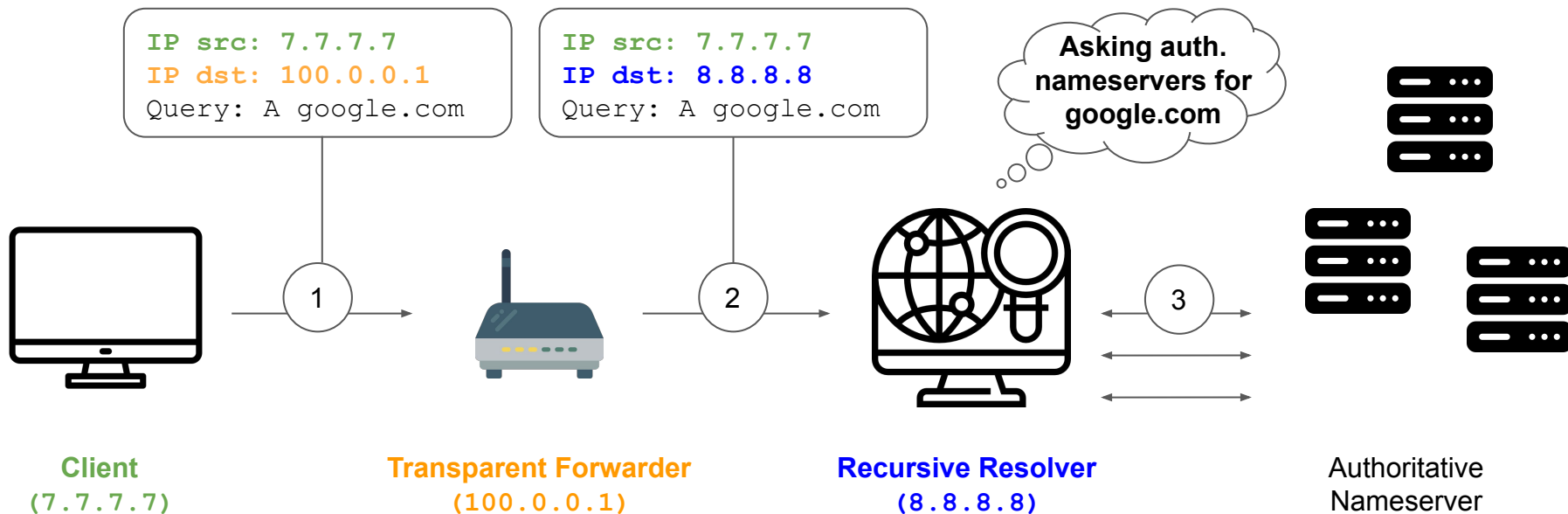
How do transparent forwarders work?



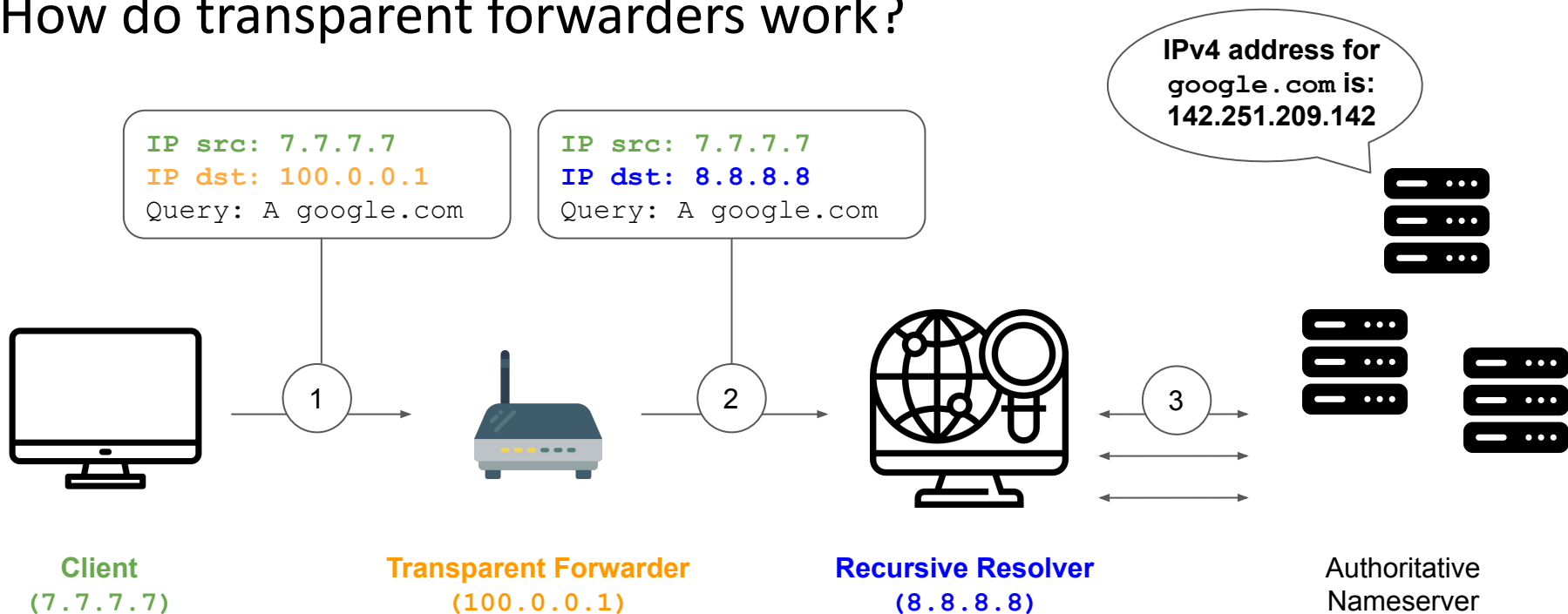
How do transparent forwarders work?



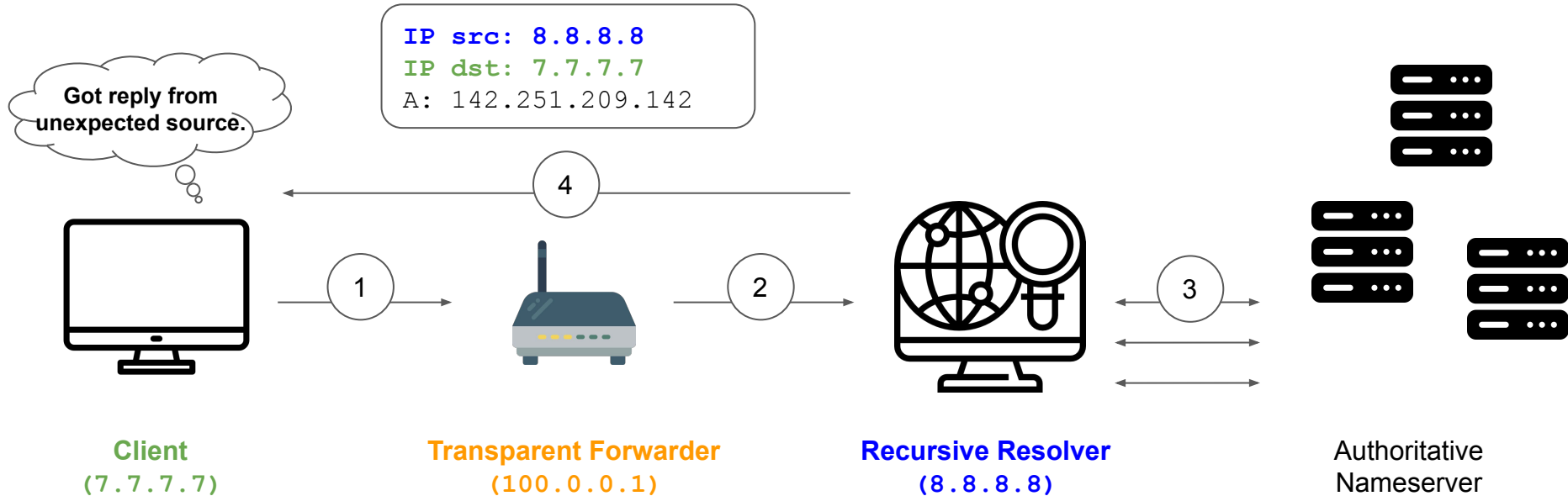
How do transparent forwarders work?



How do transparent forwarders work?



How do transparent forwarders work?







Why should we care? Open DNS enables amplification attacks!

Leading to unwanted traffic and unexpected traffic shifts.



Our controlled experiment confirms that transparent DNS forwarders fell of the radar.

	Censys	Shadowserver	Shodan	Our Scans
# ODNS	1.75M	1.8M	1.6M	2M
Transparent forwarders detected				 (31% forwarders)

M. Nawrocki, M. Koch, T. C. Schmidt, M. Wählisch, ACM CoNEXT, 2021,
<https://doi.org/10.1145/3485983.3494872>

Why do common scan campaigns miss transparent forwarders?

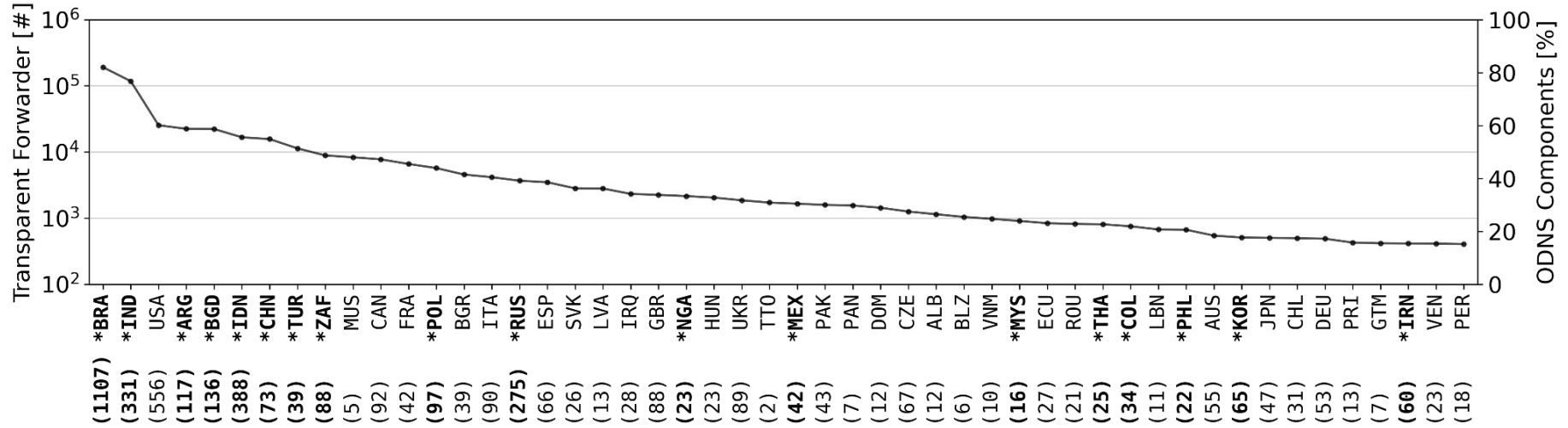
Due to efficiency reasons, scans use static queries and **only evaluate incoming traffic**.

This means that many scanning campaigns just consider the replying source address.



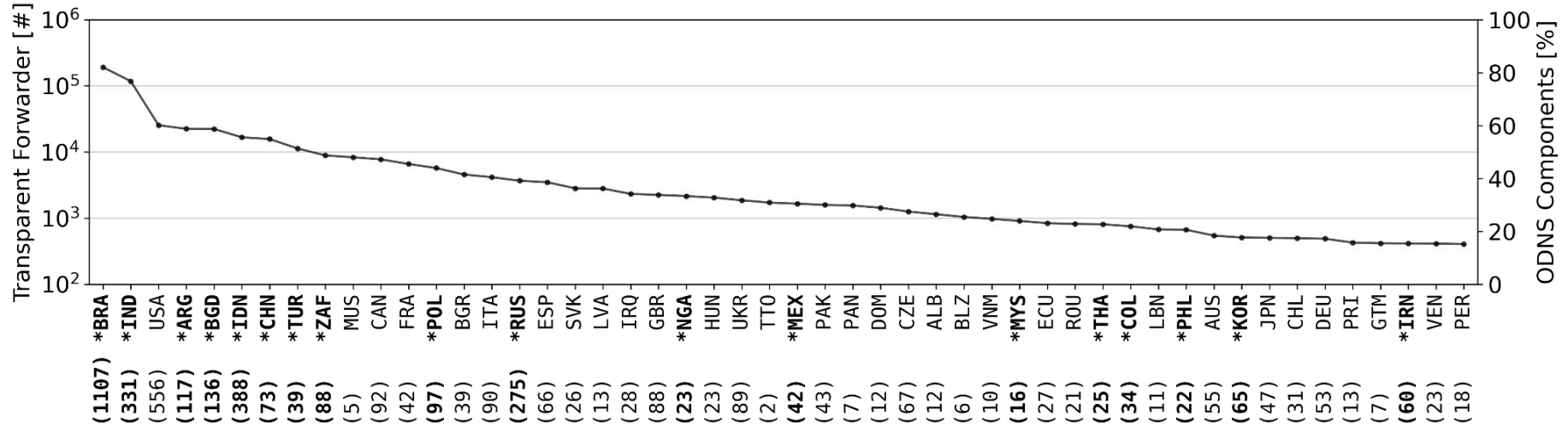
[http://bilder.hifi-forum.de/medium/610438/homer-simpson-doh_204826.gif]

Where is transparent forwarder deployment most popular?



Top 50 Countries Descending by Transparent Forwarders; * Emerging Markets and (#ASes) with a Transparent Forwarder

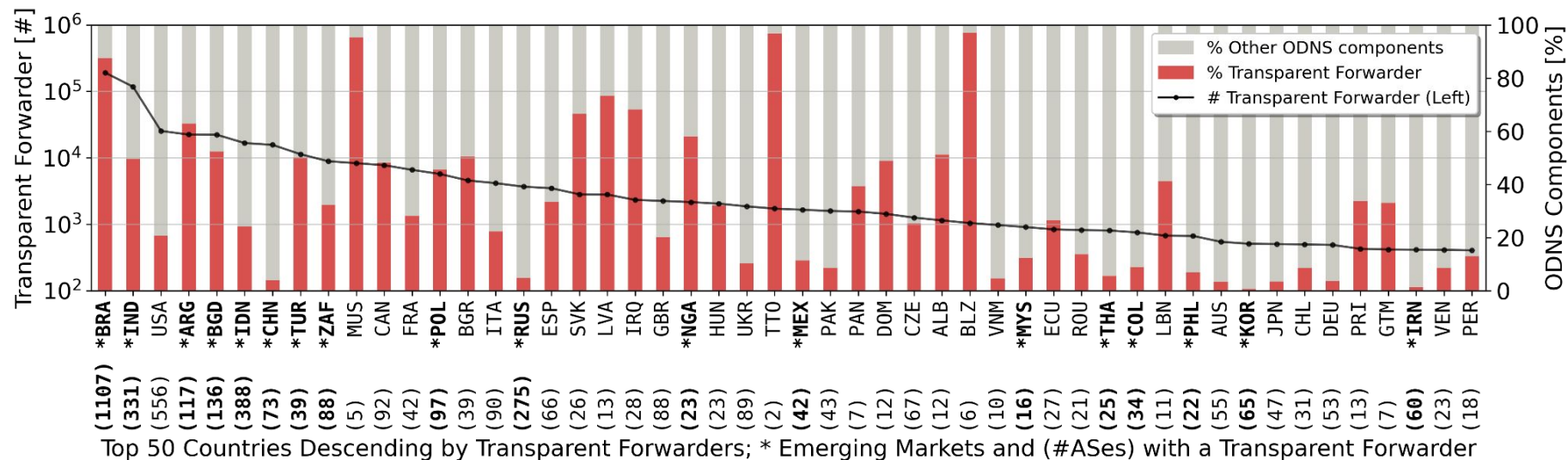
Where is transparent forwarder deployment most popular?



Top 50 Countries Descending by Transparent Forwarders; * Emerging Markets and (#ASes) with a Transparent Forwarder

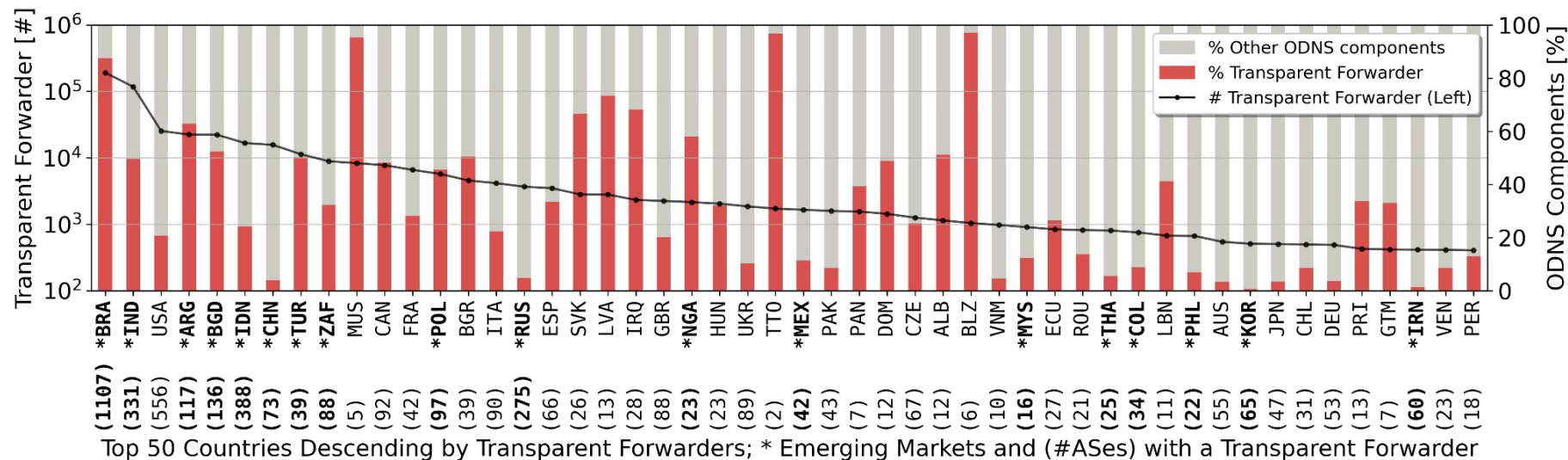
1. Countries classified as emerging markets are more likely to host transparent forwarders
2. In each country, multiple ASes host forwarders.

Where is transparent forwarder deployment most popular?



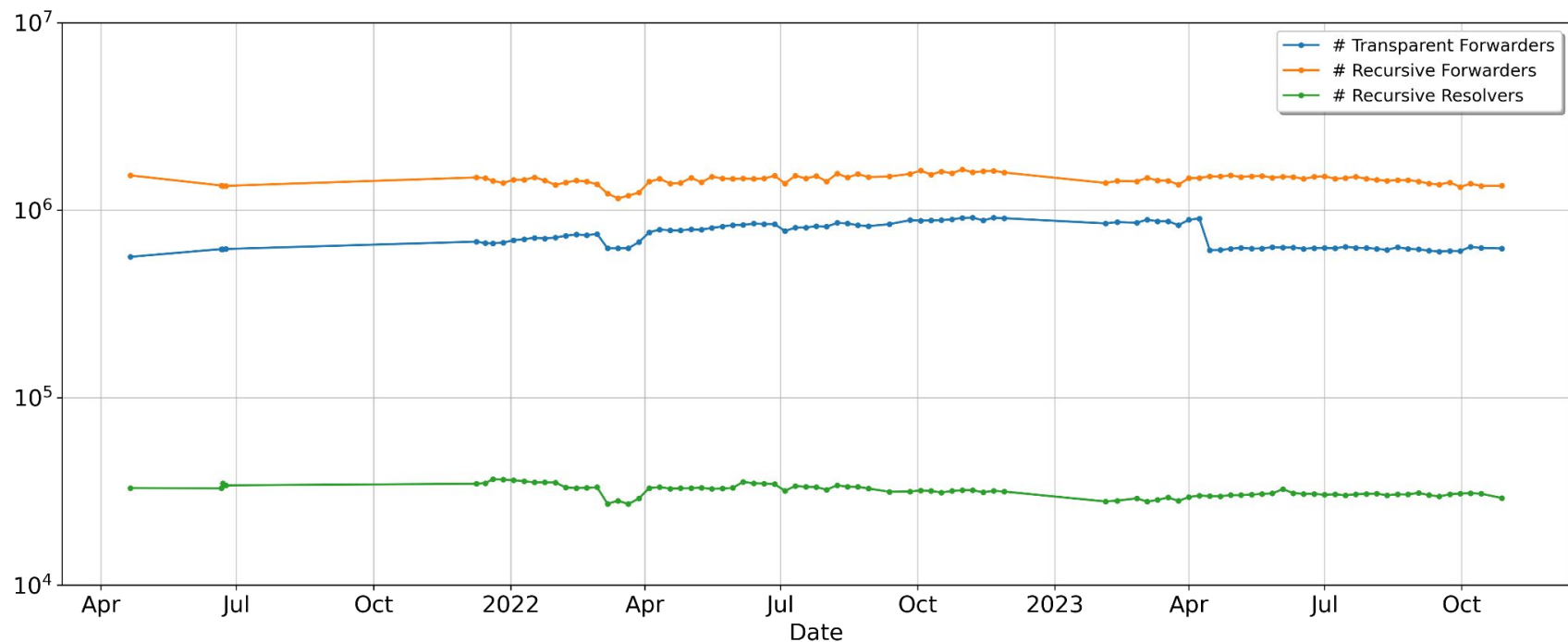
1. Countries classified as emerging markets are more likely to host transparent forwarders
2. In each country, multiple ASes host forwarders.

Where is transparent forwarder deployment most popular?

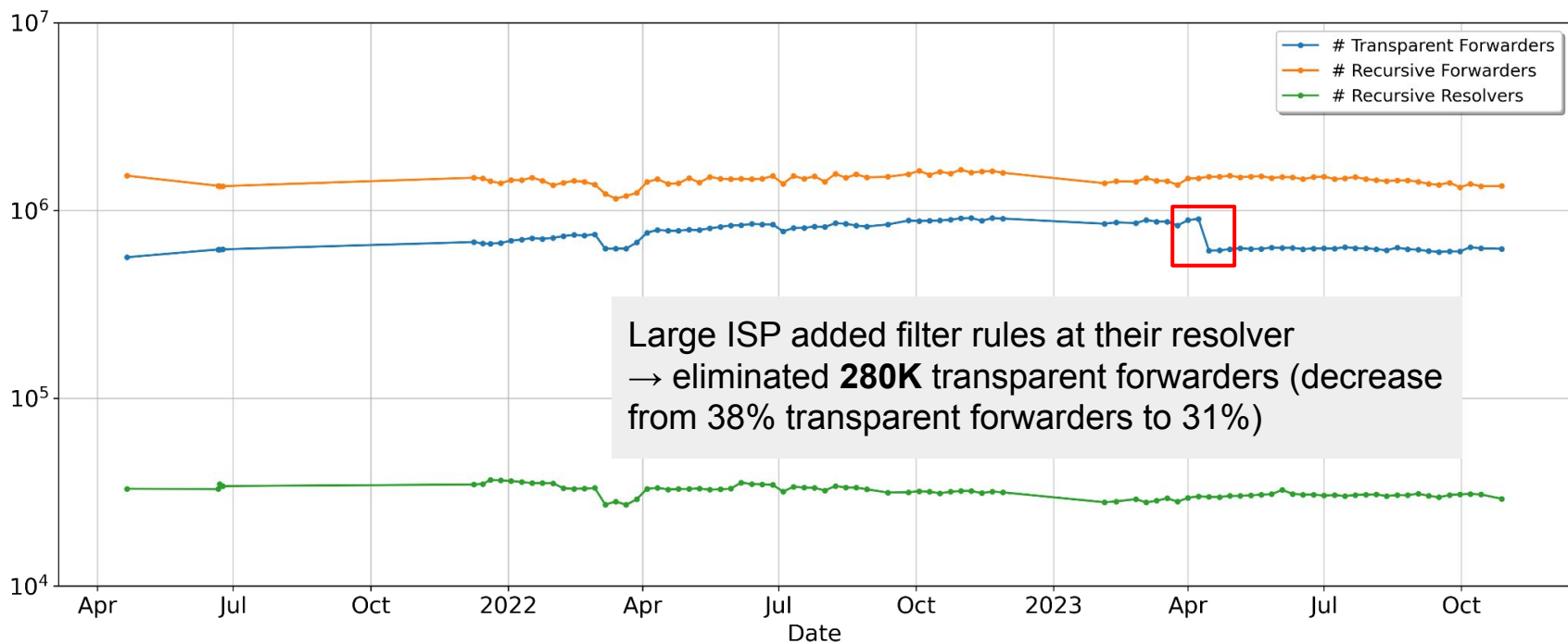


1. Countries classified as emerging markets are more likely to host transparent forwarders
2. In each country, multiple ASes host forwarders.
3. In some countries, the ODNS consists almost exclusively of transparent forwarders.

Long-term ODNS measurement study



Long-term ODNS measurement study



You ship transparent forwarders?

Please, talk to us. We would like to understand your implementations better.

We have identified **MikroTik** and **Cisco** devices that are misconfigured by default.



You are (unintentionally) hosting transparent forwarders?

1. Open transparent forwarders facilitate **DNS amplification attacks**
Even worse compared to recursive resolver
2. Open transparent forwarders allow attackers to **exploit anycast deployments**
Challenges PoP-based DDoS mitigation
3. Your AS forwards packets that look like **spoofed IP packets**
Attribution is challenging because these packets are triggered outside your AS

Solutions:
(1) Update filter rules, or
(2) Update transparent forwarders.



Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure

Marcin Nawrocki
marcin.nawrocki@fu-berlin.de
Freie Universität Berlin
Germany

Thomas C. Schmidt
t.schmidt@haw-hamburg.de
HAW Hamburg
Germany

Maynard Koch
maynard.k@fu-berlin.de
Freie Universität Berlin
Germany

Matthias Wählisch
m.waehlisch@fu-berlin.de
Freie Universität Berlin
Germany

ABSTRACT

In this paper, we revisit the open DNS (ODNS) infrastructure and, for the first time, systematically measure and analyze transparent forwarders, DNS components that transparently relay between stub resolvers and recursive resolvers. Our key findings include four takeaways. First, transparent forwarders contribute 26% (563k) to the current ODNS infrastructure. Unfortunately, common periodic scanning campaigns such as Shadowserver do not capture transparent forwarders and thus underestimate the current threat potential of the ODNS. Second, we find an increased deployment of transparent forwarders in Asia and South America. In India alone, the ODNS consists of 80% transparent forwarders. Third, many transparent forwarders relay to a few selected public resolvers such as Google and Cloudflare, which confirms a consolidation trend of DNS stakeholders. Finally, we introduce DNSRoute++, a new traceroute approach to understand the network infrastructure connecting transparent forwarders and resolvers.

CCS CONCEPTS

• Networks → Public Internet; Security protocols; Network measurement; • Security and privacy → Security protocols.

ACM Reference Format

Marcin Nawrocki, Maynard Koch, Thomas C. Schmidt, and Matthias Wählisch. 2021. Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure. In *The 17th International Conference on Emerging Networking Experiments and Technologies (CONECT '21)*, December 7–10, 2021, Virtual Event, Germany. ACM, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3485983.3494872>

1 INTRODUCTION

The open DNS infrastructure (ODNS) [37] comprises all components that publicly resolve DNS queries on behalf of DNS clients

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions.acm.org.
CONECT '21, December 7–10, 2021, Virtual Event, Germany.
© 2021 Copyright held by the owner(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9098-0/21/12...\$15.00
<https://doi.org/10.1145/3485983.3494872>

Table 1: Comparison of known open DNS components.

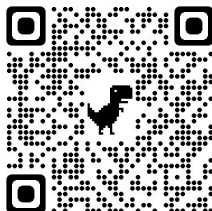
	2014	2020	2021			
	[26]	[1]	[8]	[39]	[38]	This Work
# Rec. Resolvers	n/a	20K	50K	n/a	n/a	32K (2%)
Forwarders						
# Recursive	n/a	1.4M	1.7M	n/a	n/a	1.5M (72%)
# Transparent	0.6M (2%)	n/a	n/a	n/a	n/a	0.6M (26%)
All ODNSes	25.6M	1.42M	1.75M	1.8M	1.6M	2.125M

located in a remote network. This “openness” makes the ODNS system a popular target for attackers, who are in search for amplifiers of DNS requests, for periodic DNS scan campaigns, which try to expose the attack surface, and for researchers, who want to learn more about DNS behavior.

Originally observed in 2013 [31], transparent DNS forwarders have not been analyzed in detail since then, but fell off the radar in favor of recursive forwarders and resolvers. This raises concerns for two reasons. First, the relative amount of transparent forwarders increased from 2.2% in 2014 to 26% in 2021 (see Table 1). Second, as part of the ODNS, they interact with unsolicited, potentially malicious requests.

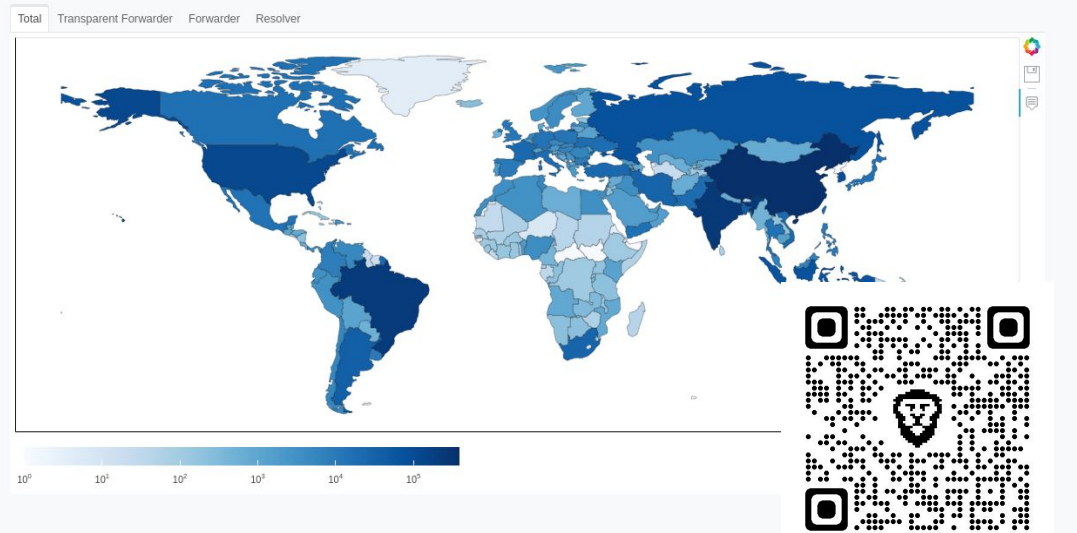
In this paper, we systematically analyze transparent forwarders. Our main contributions read as follows:

- (1) We ensure
- (2) We provide
- (3) We dive
- (4) We try
- (5) We leverage
- (6) We plot
- (7) We c
- (8) We th
- (9) We s



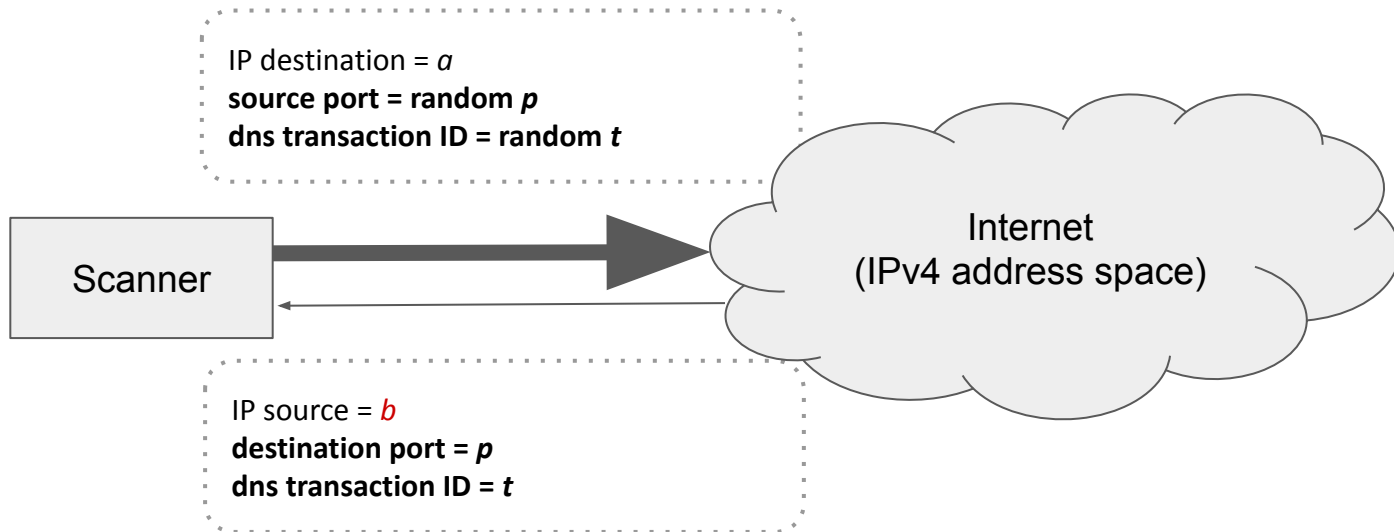
Weekly scan results and Open DNS classification: odns.secnow.net

Distribution of ODNS Components Worldwide



Backup

We detect transparent forwarders using transactional scans.



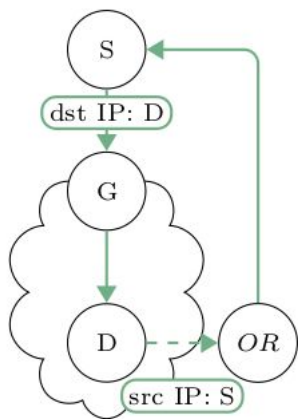
We follow the DNS transaction by correlating requests and responses via (client port, transaction ID) and a timeout. This is RFC1035-compliant and still efficient.

Regarding CPE devices that act as transparent forwarders

[<https://seclists.org/nanog/2013/Aug/132>]

- (1) Some CPE devices provide DNS resolution by just **forwarding** DNS requests to a predefined resolver, i.e., they do not implement a full resolver.
- (2) CPE devices usually implement NAT, i.e., at the **LAN interface**, they rewrite the source IP address and forward the incoming packet. This includes DNS requests.
- (3) CPE devices do not rewrite source IP addresses of incoming packets from a **WAN interface**.
- (4) Combining (1), (2), (3) means that (faulty) implementations also forward DNS requests received from the WAN interface without rewriting the source IP address.

Understanding which type of CPE devices are affected
will help to approach vendors and fix this bug.

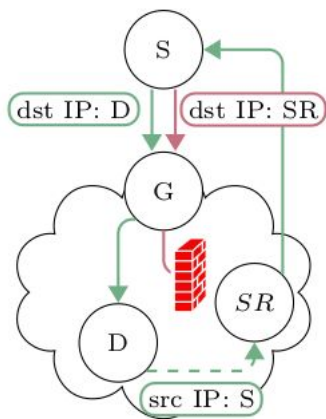


(a) D = Transp. Fwd.; D uses open resolver

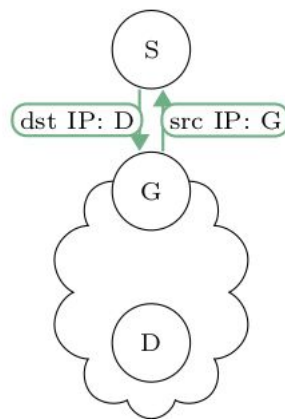
S Scanner

G Gateway

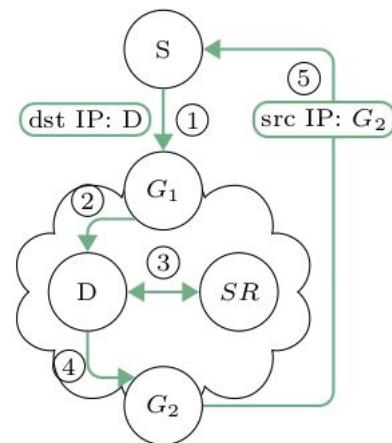
OR Open Rec. Resolver



(b) D = Transp. Fwd.; D uses shielded resolver



(c) DNS query gets intercepted by G



(d) NAT configuration at G_2 rewrites source IP address

D Queried Device

 DNS Transaction
  Transp. Forwarding
  Firewall