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?

Where is google.com?

Client
(7.7.7.7)
How do transparent forwarders work?

IP src: 7.7.7.7
IP dst: 100.0.0.1
Query: A google.com

Client
(7.7.7.7)

Transparent Forwarder
(100.0.0.1)
How do transparent forwarders work?

1. Client (7.7.7.7)
2. Transparent Forwarder (100.0.0.1)
3. Recursive Resolver (8.8.8.8)

IP src: 7.7.7.7
IP dst: 100.0.0.1
Query: A google.com

IP src: 7.7.7.7
IP dst: 8.8.8.8
Query: A google.com
How do transparent forwarders work?

A transparent forwarder does not rewrite the source IP address of the DNS request.

Client (7.7.7.7) → Transparent Forwarder (100.0.0.1) → Recursive Resolver (8.8.8.8)
How do transparent forwarders work?

1. **Client** (7.7.7.7)
2. **Transparent Forwarder** (100.0.0.1)
3. **Recursive Resolver** (8.8.8.8)

**IP src: 7.7.7.7**
**IP dst: 100.0.0.1**
**Query: A google.com**

**IP src: 7.7.7.7**
**IP dst: 8.8.8.8**
**Query: A google.com**

Asking auth. nameservers for google.com
How do transparent forwarders work?

Client (7.7.7.7) → Transparent Forwarder (100.0.0.1) → Recursive Resolver (8.8.8.8) → Authoritative Nameserver

IP src: 7.7.7.7
IP dst: 100.0.0.1
Query: A google.com

IP src: 7.7.7.7
IP dst: 8.8.8.8
Query: A google.com

IPv4 address for google.com is: 142.251.209.142
How do transparent forwarders work?

1. **Client** (7.7.7.7)
2. **Transparent Forwarder** (100.0.0.1)
3. **Recursive Resolver** (8.8.8.8)
4. **Authoritative Nameserver**

Got reply from unexpected source.

- IP src: 8.8.8.8
- IP dst: 7.7.7.7
- A: 142.251.209.142
Why should we care? Open DNS enables amplification attacks!
Leading to unwanted traffic and unexpected traffic shifts.

Spoofed DNS Request → Unwanted DNS Response

https://www.flaticon.com/free-icon/loupe_622669 | https://www.flaticon.com/premium-icon/dns_1183595
https://www.flaticon.com/free-icon/devil_725040 | https://www.flaticon.com/premium-icon/sad_3129281
Our controlled experiment confirms that transparent DNS forwarders fell of the radar.

| # ODNS | Censys | Shadowserver | Shodan | Our Scans |
|--------|--------|--------------|--------|-----------|
| Transparent forwarders detected | × | × | × | ✓ (31% forwarders) |

M. Nawrocki, M. Koch, T. C. Schmidt, M. Wählsch, 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.
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?

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

![Graph showing the number of transparent forwarders, recursive forwarders, and recursive resolvers over time from April 2022 to October 2023. The graph is on a log scale with the y-axis ranging from $10^4$ to $10^7$. The number of transparent forwarders remains relatively stable, with a slight increase from April 2022 to July 2022. The number of recursive forwarders also remains stable, with a slight increase from April 2022 to July 2022. The number of recursive resolvers shows a slight decrease from April 2022 to July 2022, followed by a slight increase.]
Long-term ODNS measurement study

Large ISP added filter rules at their resolver → eliminated 280K transparent forwarders (decrease from 38% transparent forwarders to 31%)
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.
Weekly scan results and Open DNS classification: odns.secnow.net

https://doi.org/10.1145/3485983.3494872
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](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
(b) D = Transp. Fwd.; D uses shielded resolver
(c) DNS query gets intercepted by G
(d) NAT configuration at G rewrites source IP address

S Scanner  G Gateway  OR Open Rec. Resolver  SR Shielded Resolver  D Queried Device

DNS Transaction  Transp. Forwarding  Firewall