NinjaDoH

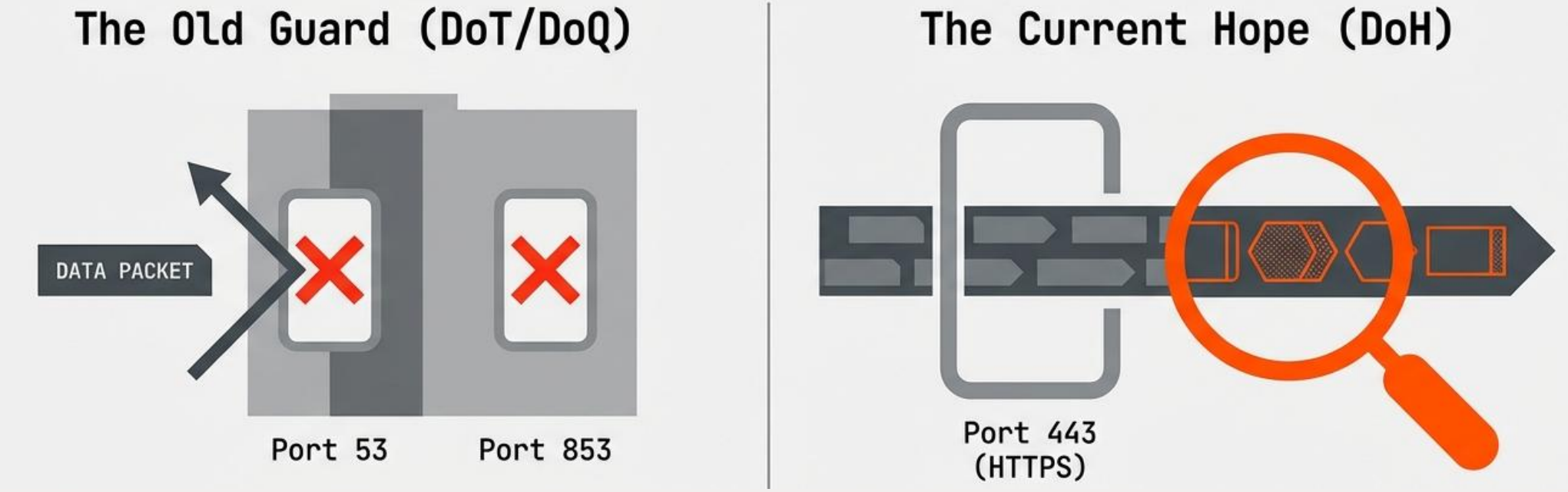
A Censorship-Resistant Moving Target DoH Protocol

MADWeb @ NDSS 2026

Scott Seidenberger, Marc Beret, Anindya Maiti (OU)

Raveen Wijewickrama, Murtuza Jadliwala (UTSA)

ENCRYPTION HIDES CONTENT, BUT NOT THE PATTERN.



Protocols that rely on static ports are easily blocked. DoH relies on masking DNS queries wrapped in HTTPS.

THE CENSORS STRIKE BACK.

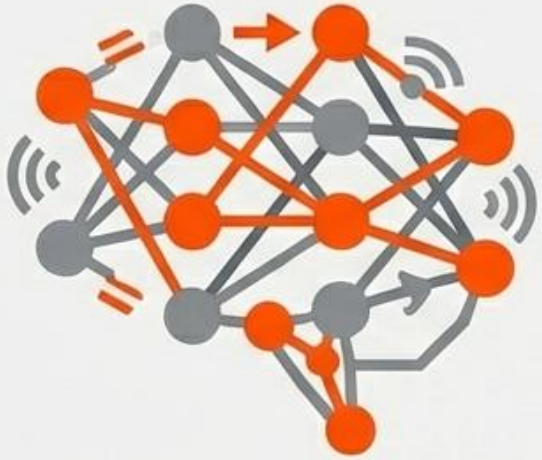
Blocklists

Databases of known DoH provider IPs and domains are blocked.

Deep Packet Inspection

Censors analyze for specific signatures of a DNS query.

Machine Learning



Measuring flow durations and packet inter-arrival times fingerprint traffic.

KEY CENSOR CONSTRAINTS.

1

Can’t block an entire hyperscaler “writ-large.”

This would cause cascading economic and basic usability problems.

2

No endpoint control.

Cannot force SSL interception or block local installs of software.

3

Neutral Cloud Hyperscaler Provider.

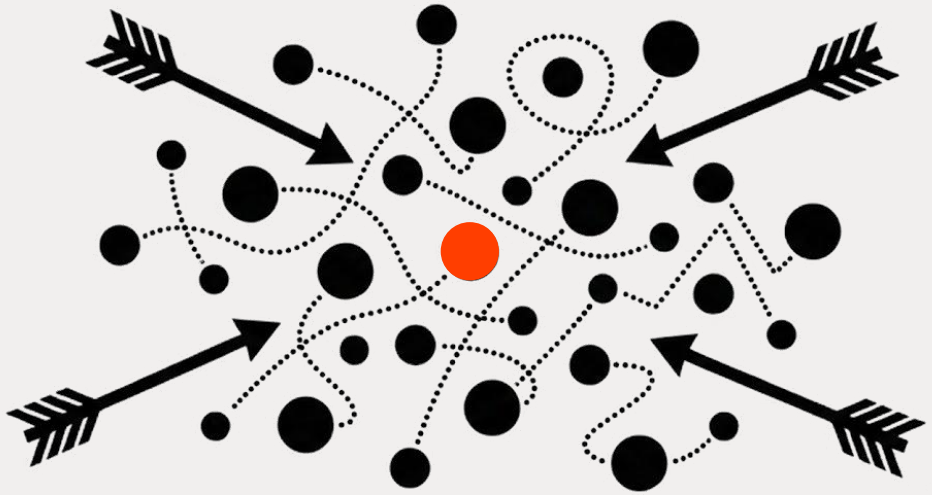
A colluding hyperscaler could identify NinjaDoH server instances.

CORE PHILOSOPHY

MOVING TARGET DEFENSE (MTD)

Static Defense

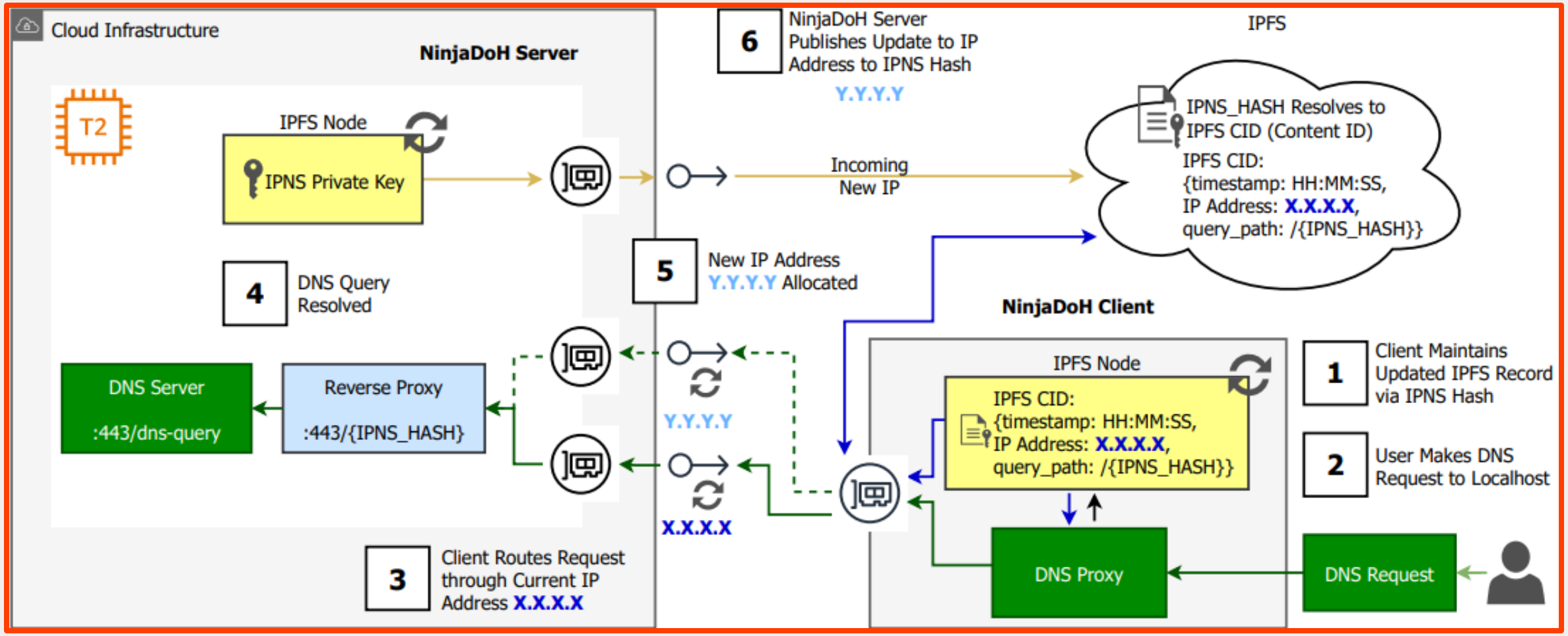
Static defenses rely on system hardening and “classic” security best practices.



NinjaDoH

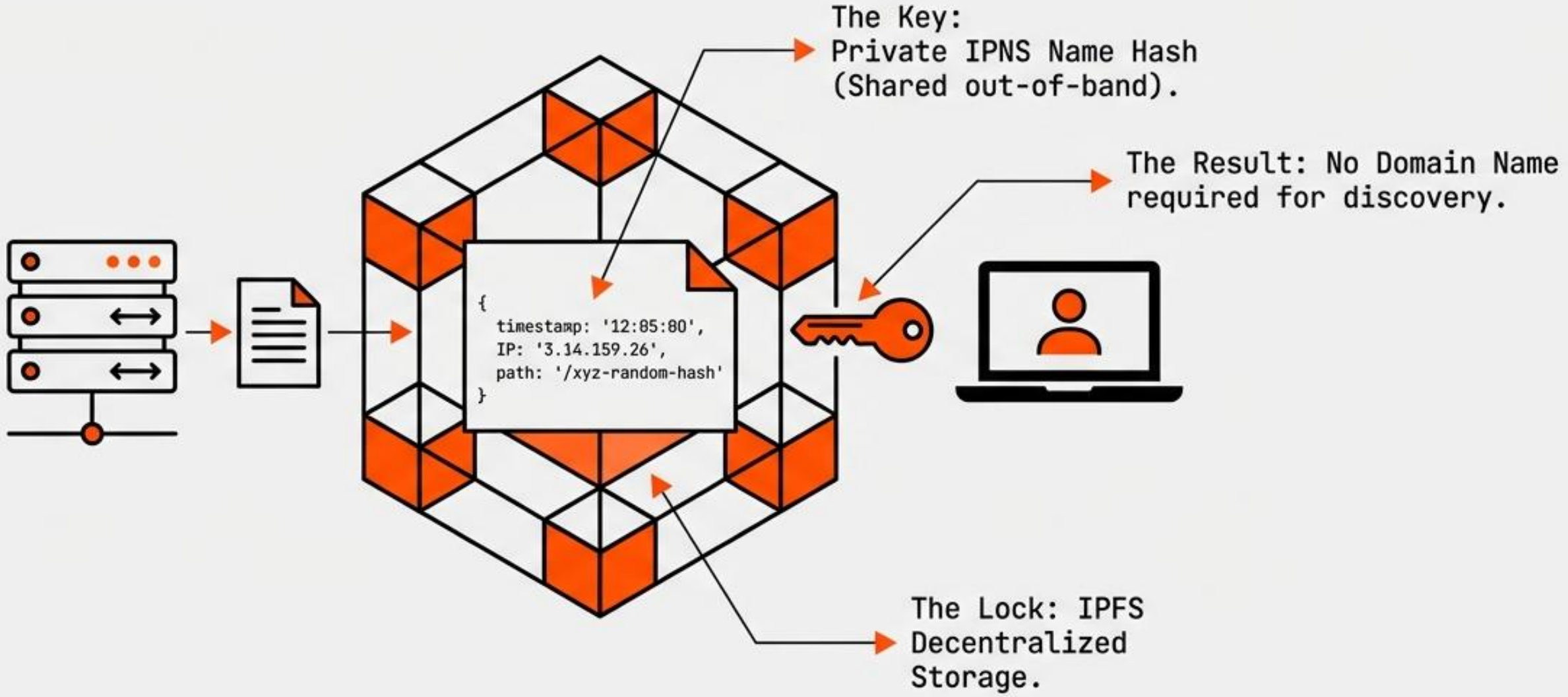
MTDs constantly change system characteristics that make targeting more difficult. **Stop the killchain at step one.**

SYSTEM OVERVIEW.



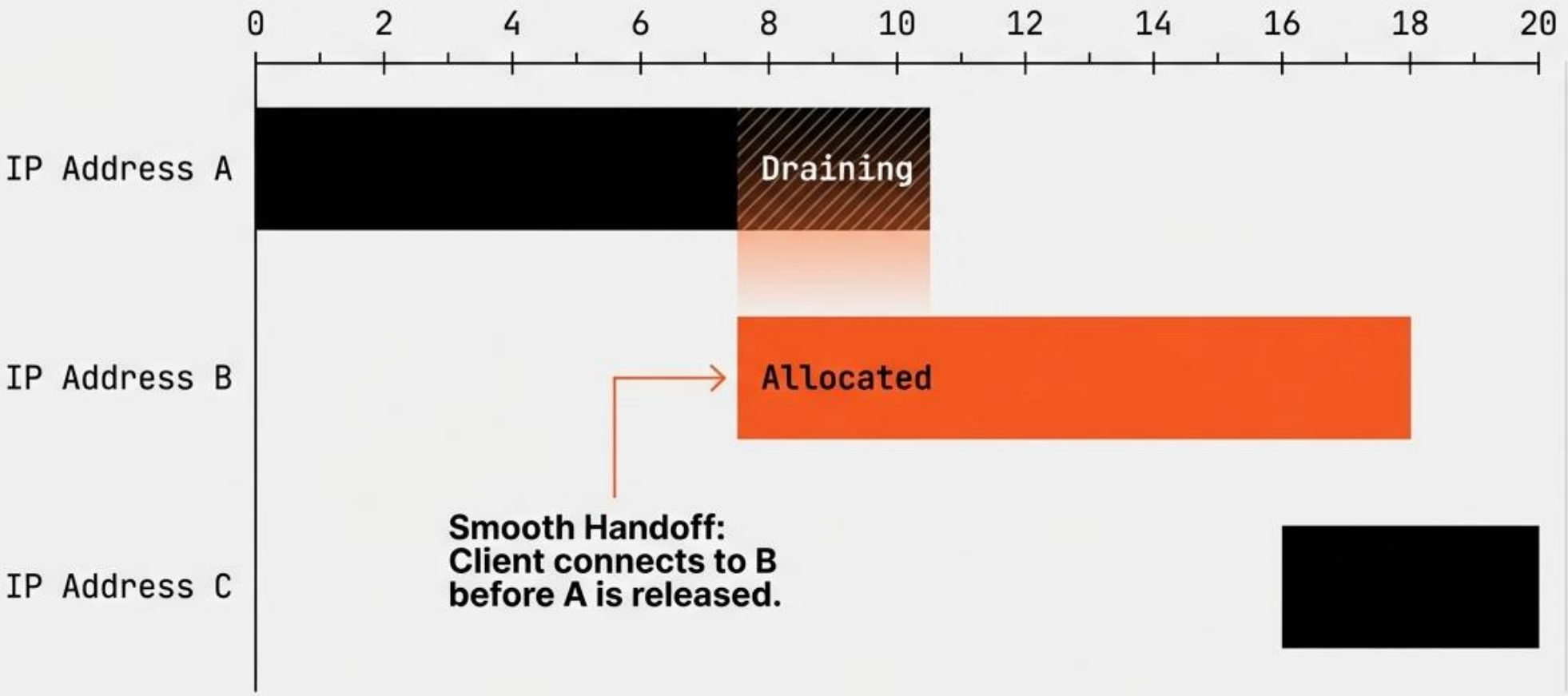
THE SECRET SIGNAL

DECENTRALIZED DEAD DROP.



ZERO DOWNTIME ROTATION

THE LADDER.



Not a load balancer.

Same server, multiple network interfaces each with its own IP.

Old IP remains active for a smooth handoff.

SECURING CLIENT HANDSHAKE.

PRIVATE CERTIFICATE AUTHORITY

Problem: Public CAs are too slow for quick rotation intervals.

Solution: Use on-the-fly, self-signed certs trusted by the local client proxy.

~~https://1.2.3.4/dns-query~~

https://3.14.15.9/k51qzi5uqu5…

QUERY PATH RANDOMIZATION

Problem: The RFC for DoH calls for a standard query path that creates a fingerprint.

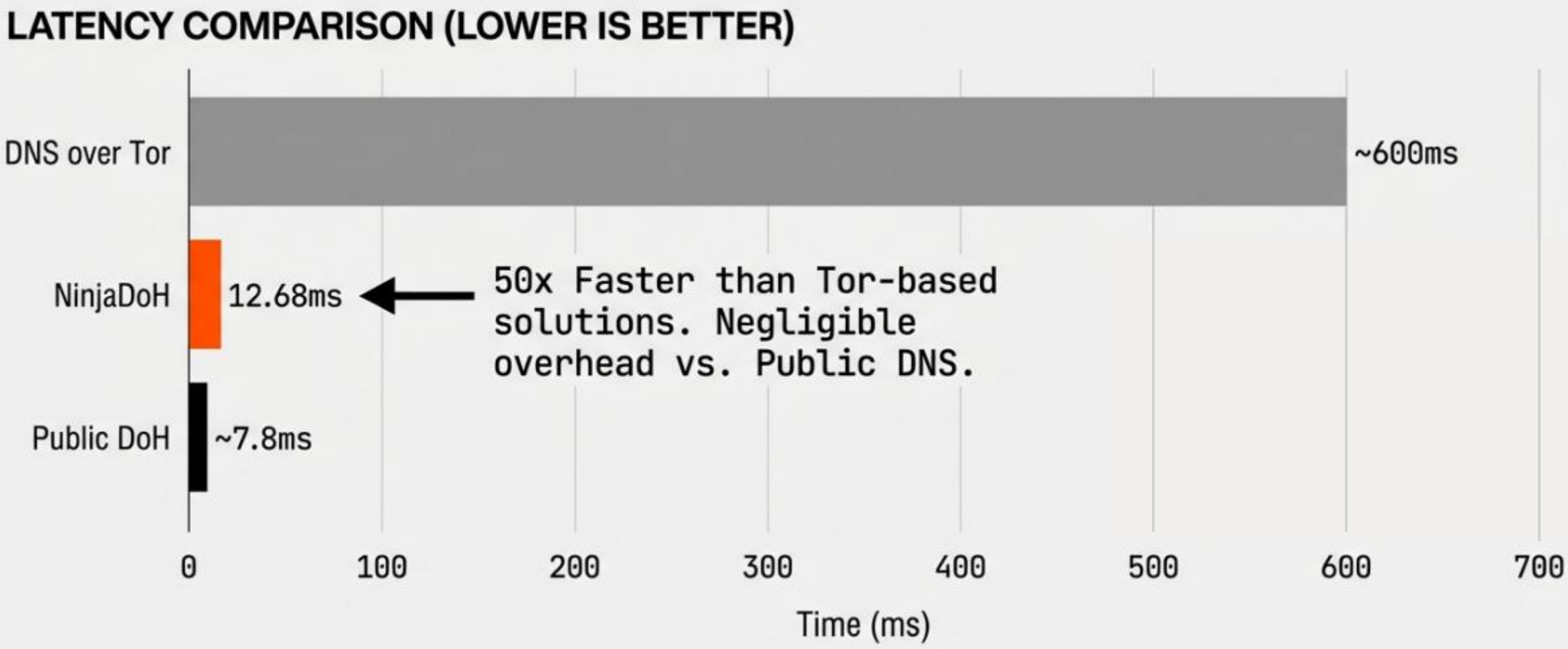
Solution: We use a randomized query path on the IPNS hash. **Prevents active probing.**

EVADING LISTS.

Domain Blocking	BYPASSED ✅
IP Blocking	BYPASSED ✅
SNI Blocking	BYPASSED ✅
Application ID	BYPASSED ✅
Strict IP Allowlisting	BLOCKED ❌

Requires blocking all unknown traffic (Economically Unfeasible for ISPs).

PERFORMANCE.

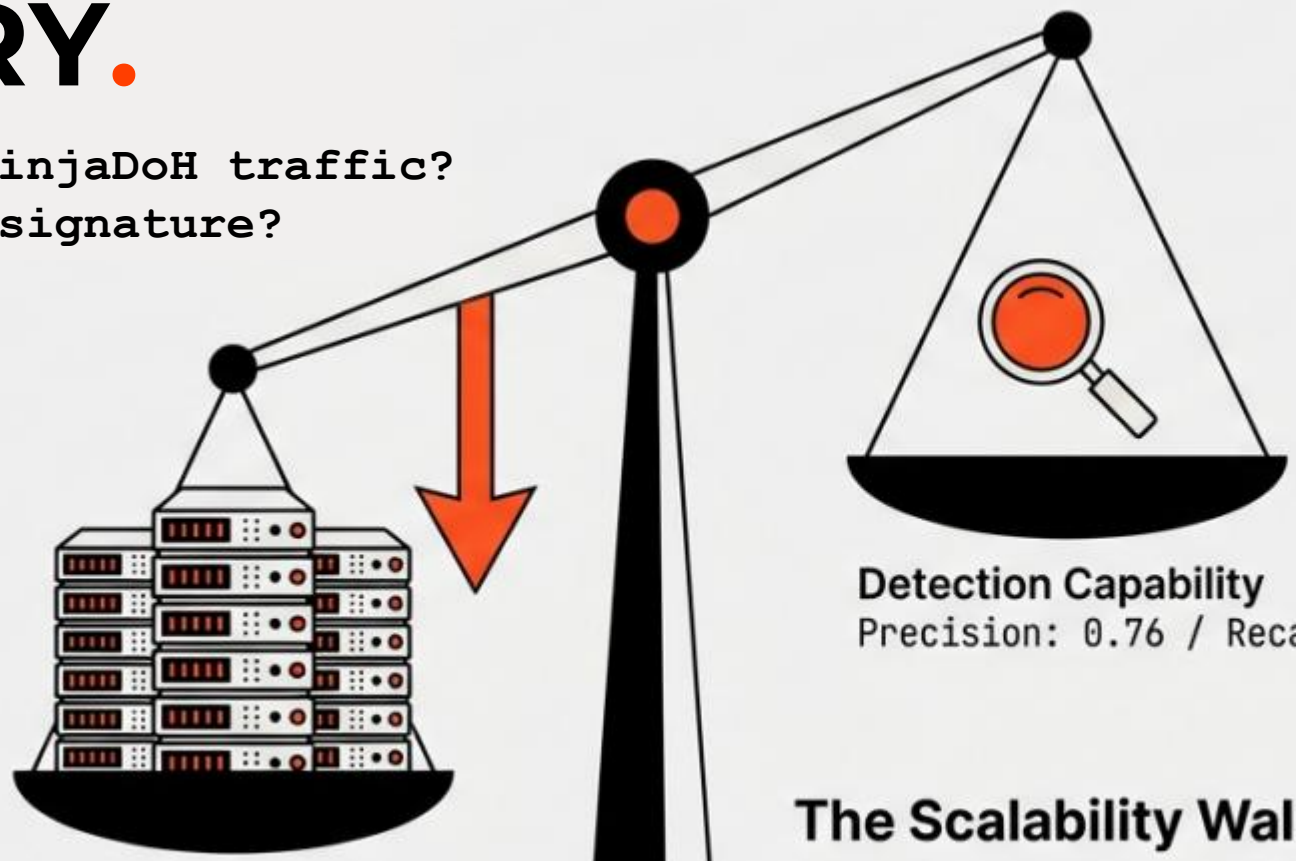


Privacy doesn’t require sacrificing a **usable internet connection.**

TACTICAL NOTE

THE ADAPTIVE ADVERSARY.

What if they train on NinjaDoH traffic?
Can they fingerprint a signature?



Detection Capability
Precision: 0.76 / Recall: 0.63.

Computational Cost
Must scan every flow in real-time.

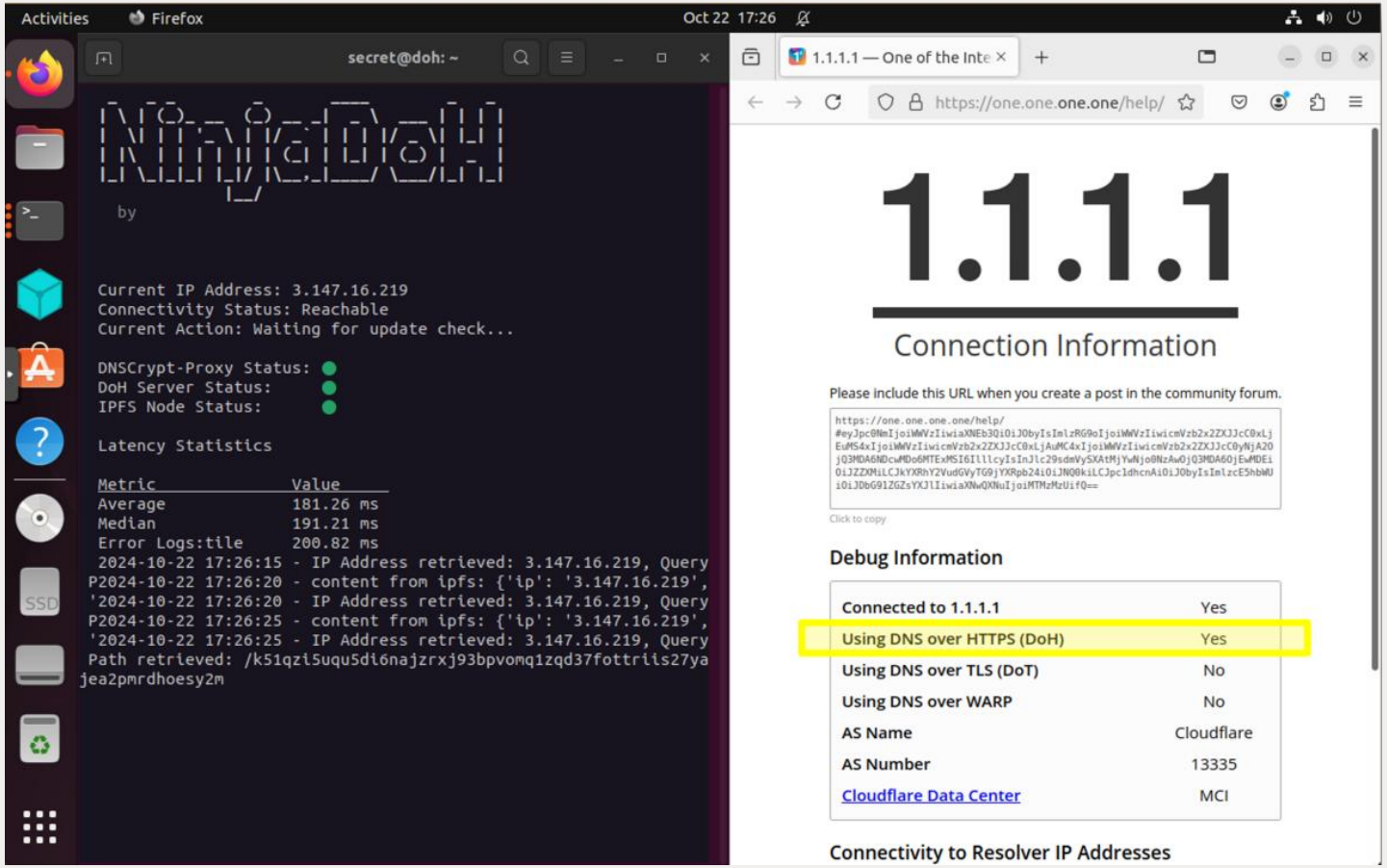
The Scalability Wall.

Even with a tailored model, the Poisson process simulation proves that scanning at ISP scale before the IP rotates is mathematically prohibitive.

DEMOCRATIZING ACCESS.

COST: ~$23.55 / Month

- Cheaper than a single-user enterprise VPN sub.
- Scalable for small groups.
- Client software is a small footprint with embedded IPFS client.
- **Future work:** One client serves the entire censored subnet.



BOOTSTRAPPING OTHER TOOLS.

Other tools like NetShuffle and SpotProxy have a "chicken and egg" problem.

A client needs **uncensored DNS** to find their entry nodes.

NetShuffle is an edge-network censorship resistance system that utilizes programmable switches to continuously scramble the mapping between domain names and IP addresses

SpotProxy employs instance rotation and cost arbitrage to frequently rotate proxy IP addresses across discounted cloud instances, creating a high churn rate that prevents effective enumeration and blocking

BE A NINJA

MAKE DISCOVERY A MOVING TARGET.

1

AGILE

Hyperscaler IP Rotation

2

DECENTRALIZED

IPFS key to the control plane. Point-to-point data plane.

3

RESILIENT

Assumes a challenging censor environment.

See **website** for artifacts, paper link, and more.

Thank you!