



VPNalyzer

Systematic Investigation of the VPN Ecosystem

Reethika Ramesh, Leonid Evdokimov, Diwen Xue, Roya Ensafi

NDSS 2022





FTC Staff Report Finds Many Internet Service Providers Collect Troves of Personal Data, Users Have Few Options to Restrict Use



The uploader has not made this video available in your country.
Sorry about that.

Why Net Neutrality Can't Wait



PRIVACY INVESTIGATION —
FTC investigates whether ISPs sell your browsing history and location data
AT&T, Comcast, Verizon, T-Mobile, Google face probe into privacy and targeted ads.

THE WALL STREET JOURNAL.

NSA's Domestic Spying Grows As Agency Sweeps Up Data

Terror Fight Blurs Line Over Domain; Tracking Email



ISPs can now collect and sell your data: What to know about Internet privacy rules

Internet traffic is increasingly being **disrupted, tampered with, and monitored** by ISPs, advertisers, and other threat actors

VPNs are on the Rise

“From 2010 to year-end 2019, the use of VPNs has increased by **approximately four times**”

[Cybersecurity company PC Matic, 2020](#)

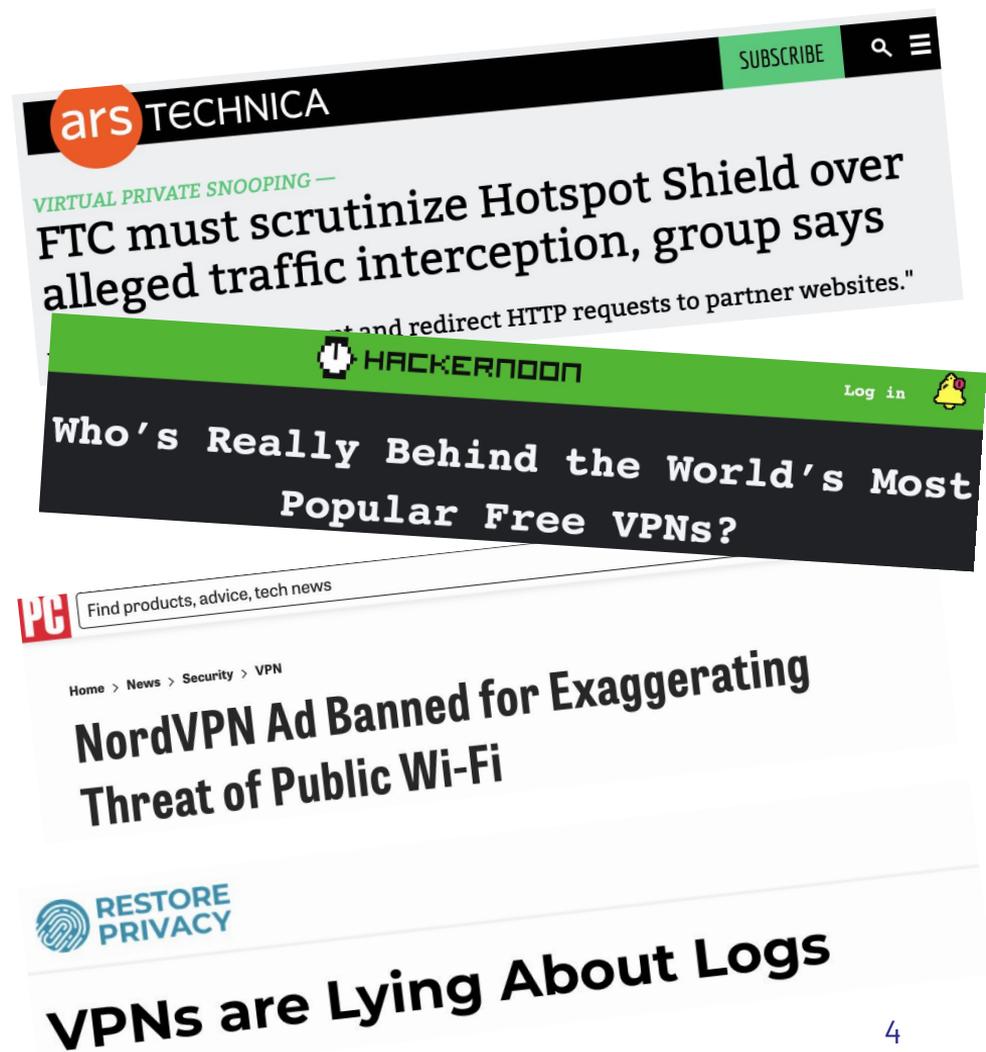
Commercial VPNs are a multi-billion dollar industry; most recently ExpressVPN was acquired for \$936 million

[Reuters, Sep 2021](#)

Reasons for use?

Protection from surveillance, censorship circumvention, accessing work/school/university resources, entertainment etc

This multi-billion dollar industry is **laxly regulated**, rife with **hyperbolic claims**, and **remains severely understudied**



Towards a Systematic Investigation of VPNs

Previous reports are lab-based:

- ↪ Used **inconsistent heuristics**
- ↪ Involved a large amount of **manual effort**
- ↪ **Limited in the scale** and types of VPN products studied

Towards a Systematic Investigation of VPNs

Previous reports are lab-based:

- ↪ Used **inconsistent heuristics**
- ↪ Involved a large amount of **manual effort**
- ↪ **Limited in the scale** and types of VPN products studied

KEY CHALLENGES:

Rigor, Scale, Automation

Bringing transparency and better security to consumer VPNs requires a different approach



We built VPNalyzer

to address these challenges

Building VPNalyzer to Address Key Challenges

Modular, extensible test suite

Repeated VPN evaluations over time should not require starting from scratch

System should evolve alongside the VPN ecosystem: Validating VPN providers' fixes for issues reported as disclosures requires an updatable test suite

Building VPNalyzer to Address Key Challenges

Modular, extensible test suite

Repeated VPN evaluations over time should not require starting from scratch

System should evolve alongside the VPN ecosystem: Validating VPN providers' fixes for issues reported as disclosures requires an updatable test suite

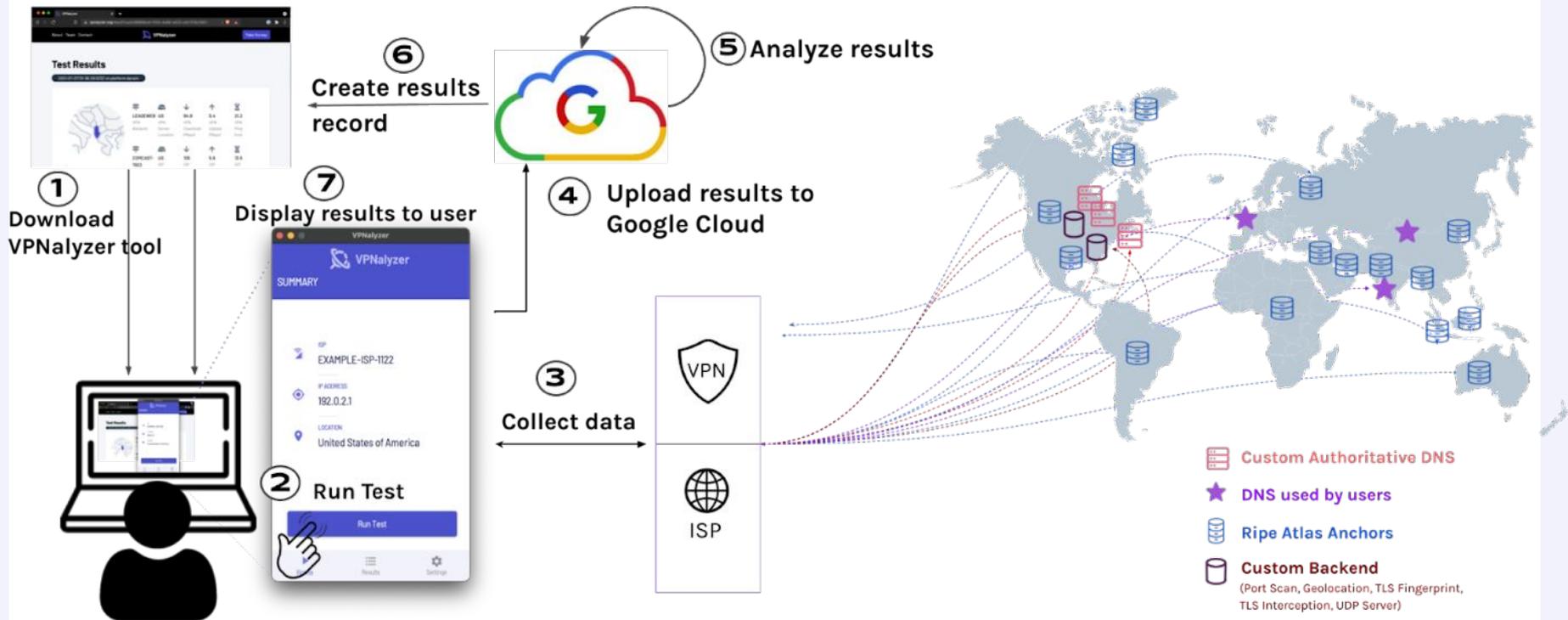
Facilitate Crowdsourced Data

Increasing number of VPN providers

Users have varied threat models and use cases, ranging from watching netflix to "anonymity"; they may prefer different VPN products

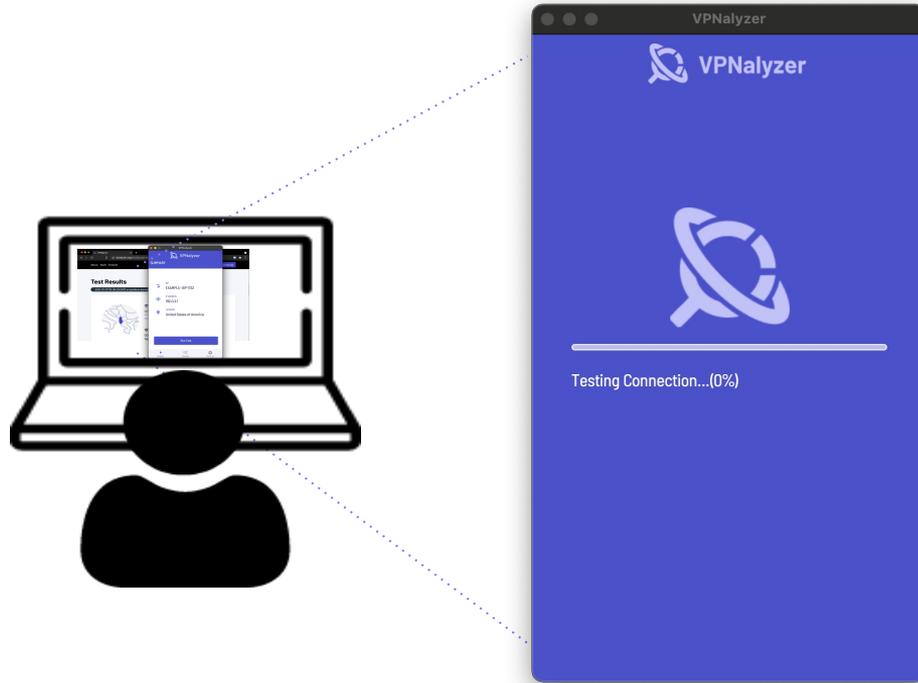


VPNalyzer System Design





Conducting the measurements

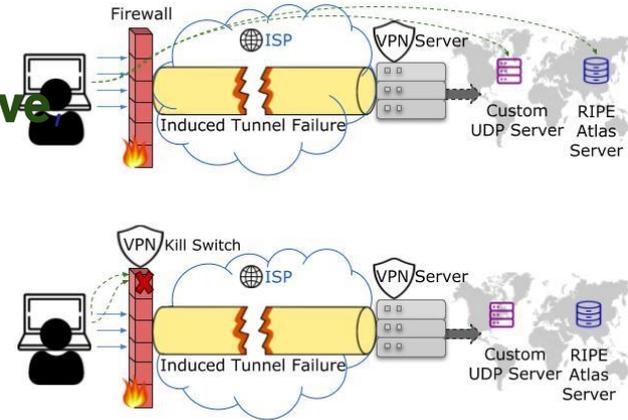




Detecting Traffic Leaks During Tunnel Failure

Overview: Conceptually, create an “allowlist” of specific hosts, cause a tunnel failure by blocking all traffic except to and from allowlist

If the VPN’s leak protection is **effective** the traffic to the hosts on the allowlist should also be **blocked**





Detecting Traffic Leaks During Tunnel Failure

- ↳ **Bootstrap via ISP:** Request administrative privileges, log firewall state before any changes, initiate sessions



Detecting Traffic Leaks During Tunnel Failure

↳ **Bootstrap via ISP**

↳ **VPN Case**

■ Initialization Phase

↳ Set up necessary platform-specific components



Detecting Traffic Leaks During Tunnel Failure

↳ **Bootstrap via ISP**

↳ **VPN Case**

■ Initialization Phase

↳ Set up necessary platform-specific components:

- Linux: Add chains for **iptables** and **ip6tables**
- Windows: Log version of **PowerShell** and **NetSecurity** module (Need PowerShell > 2.0)
- MacOS: Test custom anchors on **pf**, enable **pf**, and obtain token to revert it (**pfctl -X TOKEN**)



Detecting Traffic Leaks During Tunnel Failure

↳ **Bootstrap via ISP**

↳ **VPN Case**

- Initialization Phase

- ↳ Set up necessary platform-specific components
- ↳ Log the firewall state again



Detecting Traffic Leaks During Tunnel Failure

↳ **Bootstrap via ISP**

↳ **VPN Case**

- Initialization Phase
- Create Allowlist and Induce Tunnel Failure

RIPEstat Data API: Whats My IP

One of our custom UDP heartbeat servers (ServerA)

Authoritative nameservers and public DNS resolvers belonging to Cloudflare, Google, and OpenDNS



Detecting Traffic Leaks During Tunnel Failure

↳ **Bootstrap via ISP**

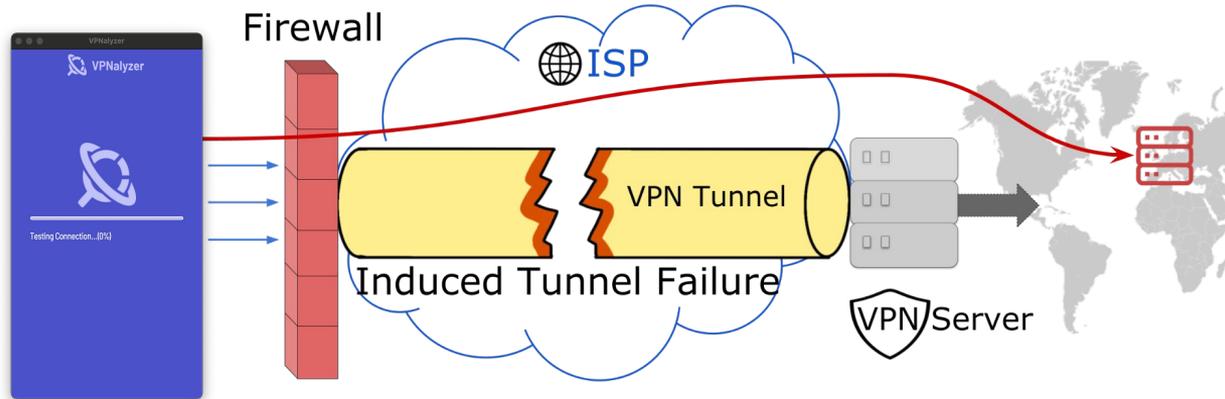
↳ **VPN Case**

- Initialization Phase
- Create Allowlist and Induce Tunnel Failure
 - RIPEstat Data API: Whats My IP
 - One of our custom UDP heartbeat servers (ServerA)
 - Authoritative nameservers and public DNS resolvers belonging to Cloudflare, Google, and OpenDNS
- Detection Logic

Traffic Leak Detection Logic

Probe for Possible Data Leaks:

- ↪ For 120s, periodically query the RIPEstat Data API: Whats My IP
- If some **data leak protection exists**, queries would time out
- If **there is no data leak protection**, query reaches endpoint and returns user's ISP IP





Detecting Traffic Leaks During Tunnel Failure

↳ Bootstrap via ISP

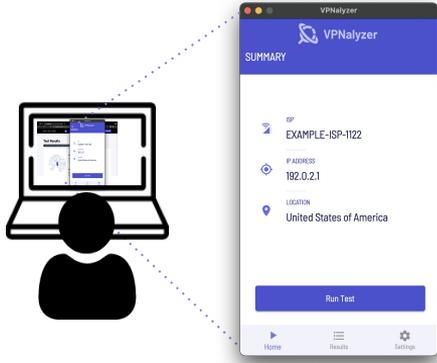
↳ VPN Case

- Initialization Phase
- Create Allowlist and Induce Tunnel Failure
- Detection Logic

↳ ISP Case

- No Measurements
- Log Firewall State

VPNalyzer Experiment Flow



1

Bootstrap via ISP

Request administrative privileges, initialize packet captures, fetch necessary resources, and log firewall state

2

Testing with the VPN on

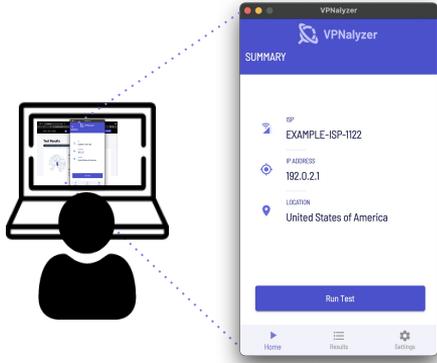
Test suite is triggered for *VPN* case:
We run Test {1 → X} serially

3

Testing with VPN off

Test suite is triggered again for *ISP* case:
We run Test {1 → X} serially as applies

VPNalyzer Experiment Flow



1

Bootstrap via ISP

Request administrative privileges, initialize packet captures, fetch necessary resources, and log firewall state

2

Testing with the VPN on

Test suite is triggered for *VPN* case:
We run Test {1 → X} serially

3

Testing with VPN off

Test suite is triggered again for *ISP* case:
We run Test {1 → X} serially as applies



What do we test with VPNalyzer?

Aspects of Service

Bandwidth and latency
Geolocation
RPKI validation

Misconfiguration and Leakages

DNS leaks
IPv6 leaks
Data leaks during tunnel failure

Security and Privacy Essentials

Port scanning
Router interface reachability
Presence of DNS proxy
QNAME minimization
DNSSEC validation
Lack of support for DoH
TLS Interception

VPNalyzer has a modular, extensible test suite currently containing 15 measurements

We tested **80 popular VPNs** with our VPNalyzer tool and uncovered several previously unreported findings

VPNalyzer in Practice: Testing 80 popular VPNs

- ↳ We tested random servers in each VPN provider, on Windows and MacOS
 - **58 paid** VPN providers
 - **18 free** VPN providers
 - **4 self-hosted** VPN solutions
(Algo, OpenVPN Access Server on AWS, Outline, Streisand)
- ↳ Some results for the same VPN provider may differ based on server selected

Traffic Leakages:

IPv6 Traffic

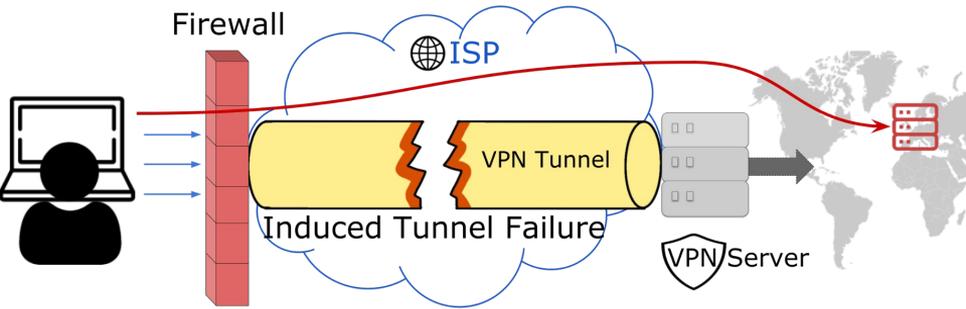
- Only 11 out of 80 VPNs support IPv6
- Five VPNs **leak IPv6 traffic** to the ISP by default
 - UMich VPN** is among them

Happy Eyeballs prefers connections over IPv6
If the IPv6 request completes first, user's connection would go through the ISP

Implemented in popular browsers and OSes
(Chrome, Firefox, Opera, OS X)

Traffic Leakages: During Tunnel Failure

Upon tunnel failure, 26 providers **leak traffic** to the user's ISP



By default, 26 VPNs lack protection during tunnel failure

Traffic Leakages: During Tunnel Failure

Upon tunnel failure, 26 providers **leak traffic** to the user's ISP

- ⇒ 18 leak all traffic, eight of these leak DNS traffic only
- ⇒ Five of these 26 are the ones that also leak IPv6

By default, 26 VPNs lack protection during tunnel failure



Traffic Leakages: Even with a Kill Switch Enabled

Even in their most secure setting, 10 providers **leak traffic** to the user's ISP upon tunnel failure

↪ Six of which even had a **"kill switch" feature** enabled

Even with a **"kill switch"**, six VPNs **leak traffic during tunnel failure**



Traffic Leakages: Insecure Default Configuration

Astrill VPN tunneled **only browser traffic** by default

Psiphon did **not enable “VPN mode”** by default

Default Configuration caused user's (non-browser) traffic to be exposed to the ISP



Findings: Security and Privacy Essentials

- ↪ Support for DNSSEC (54 of 80), Query Name Minimization (26 of 80) is non-uniform
- ↪ 14 VPNs signal to turn off DoH for Firefox users using Canary Domain **silently**



Configuring Networks to Disable DNS over HTTPS

Findings: Security and Privacy Essentials

- ↪ Support for DNSSEC (54 of 80), Query Name Minimization (26 of 80) is non-uniform
- ↪ 14 VPNs signal to turn off DoH for Firefox users using Canary Domain **silently**

Configuring Networks to Disable DNS over HTTPS

Although we disable it by default (using the canary domain), nothing prevents a customer from enabling it manually. So we don't block DoH, we just require users to "opt-in" to it.

We fully support the concept of DoH and that it in general boosts privacy by hiding a user's DNS traffic from their ISP. However, our customers already get more complete privacy protection using our DNS servers and so by default we disable DoH.

```
; <<>> DiG 9.10.6 <<>> use-application-dns.net
;
; Thank you for your report.
;
; We rely on the user using our DNS resolver in order to be able to provide DNS
; filtering (i.e. netshield). If the browser bypasses our resolver, we can't do so.
; Additionally, streaming also requires the user to use our DNS resolver.
;
;; QUESTION SECTION:
;use-application-dns.net.      IN      A

;; AUTHORITY SECTION:
use-application-dns.net. 10800 IN      SOA      use-application-dns.net.
nobody.invalid. 1 3600 1200 604800 10800

;; ADDITIONAL SECTION:
explanation.invalid. 10800 IN      TXT      "Proton no DoH"
```

Collaboration with CR

- ↳ Consumer Reports (CR) used our VPNalyzer tool for their own investigation to help recommend VPNs to their subscribers
- ↳ Served as a real-world evaluation of our tool

CR Consumer Reports 

[Become a Member](#) | [Donate](#)

Should You Use a VPN?

Virtual private networks can provide a layer of privacy and security, but many people don't need them

CR Consumer Reports 

[Become a Member](#) | [Donate](#)

VPN Testing Reveals Poor Privacy and Security Practices, Hyperbolic Claims

CR Consumer Reports 

[Become a Member](#) | [Donate](#)

Mullvad, IVPN, and Mozilla VPN Top Consumer Reports' VPN Testing

We evaluated 16 services for privacy and security, and these were the best VPNs overall

32



VPNalyzer

Systematic Investigation of the VPN Ecosystem

Reethika Ramesh, Leonid Evdokimov, Diwen Xue, Roya Ensafi

NDSS 2022

