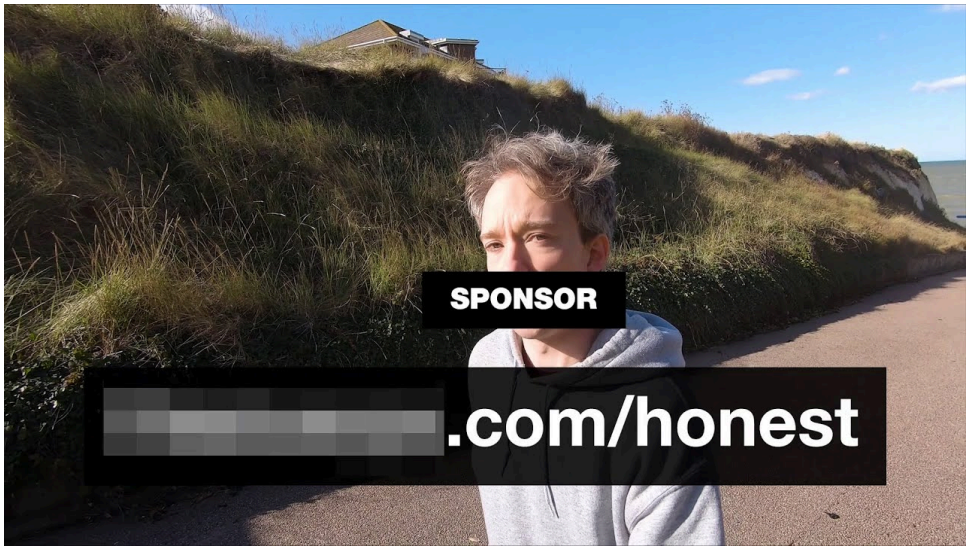
Virtual Private Networks

How they work and the pitfalls we've made for them

10.21.2026

Autumn Luzovich (she/they)

First, a convenient video



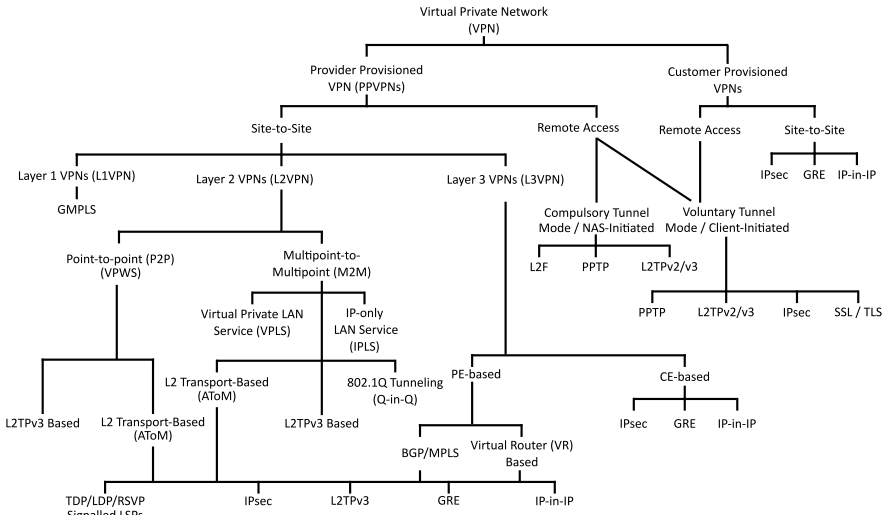
https://www.youtube.com/watch?v=WVDQEoe6ZWY

1 What Are They

Preface

VPNs are complicated

Preface (ii)

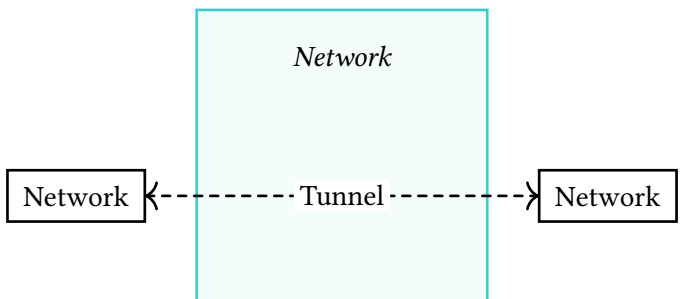


https://commons.wikimedia.org/wiki/File:VPN_classification-en.svg

At its simplest...

Virtual Private Network (VPN)

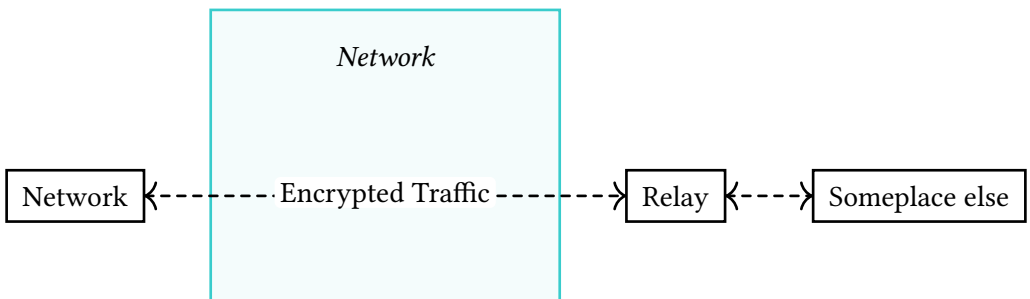
A non-physical way of “connecting” two networks together.



At its not-so simplest...

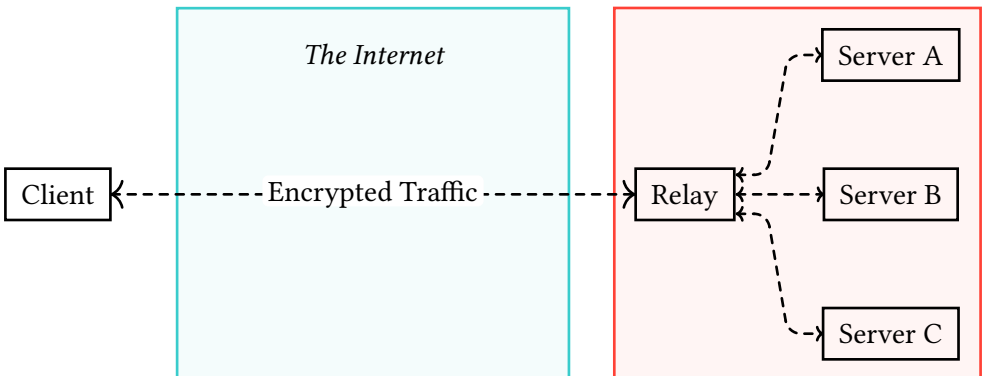
Virtual Private Network (VPN)

An encrypted connection between a client or network and a relay, which routes traffic someplace else.



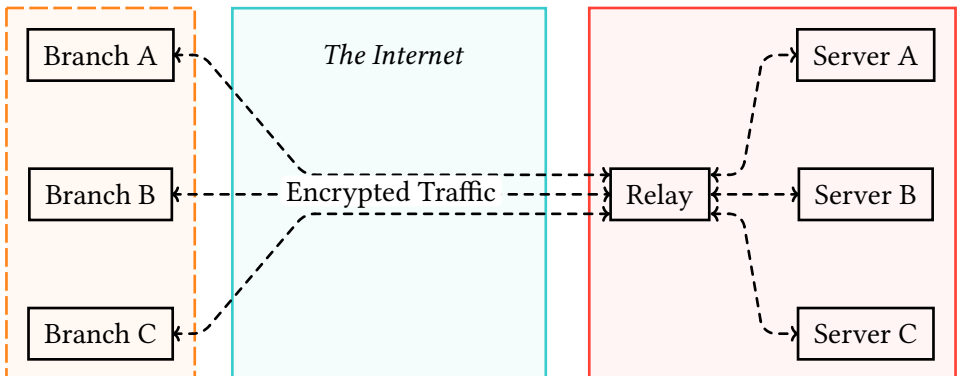
Some categories of VPNs

1.d.a Remote Access



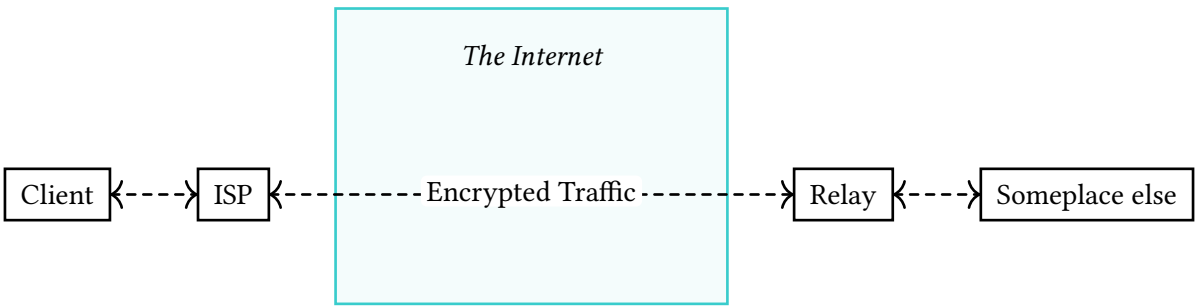
Some categories of VPNs (ii)

1.d.b Site-to-Site

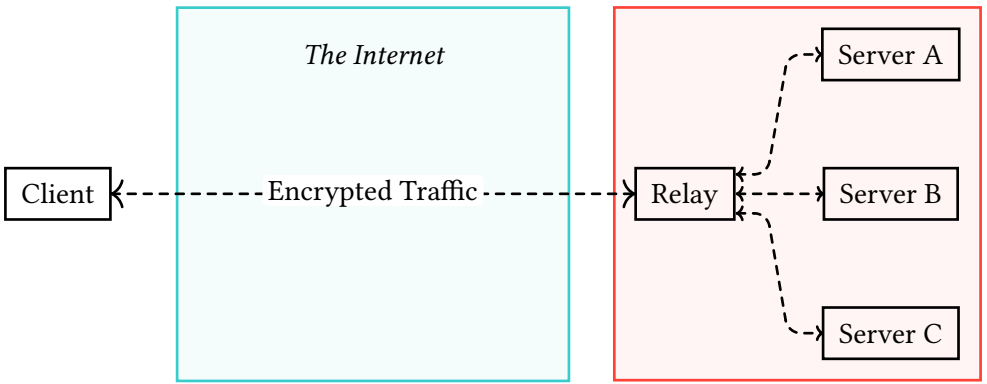


2 What They Can Do

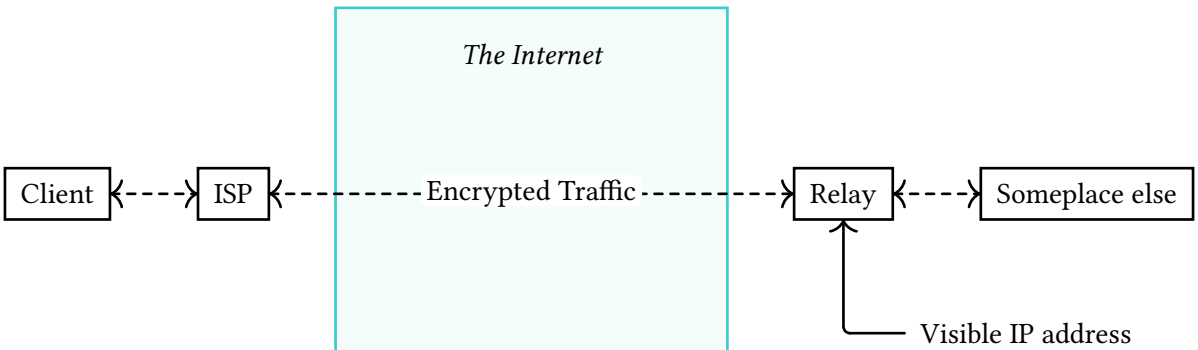
Keeping traffic private from your ISP



Connecting to internal resources

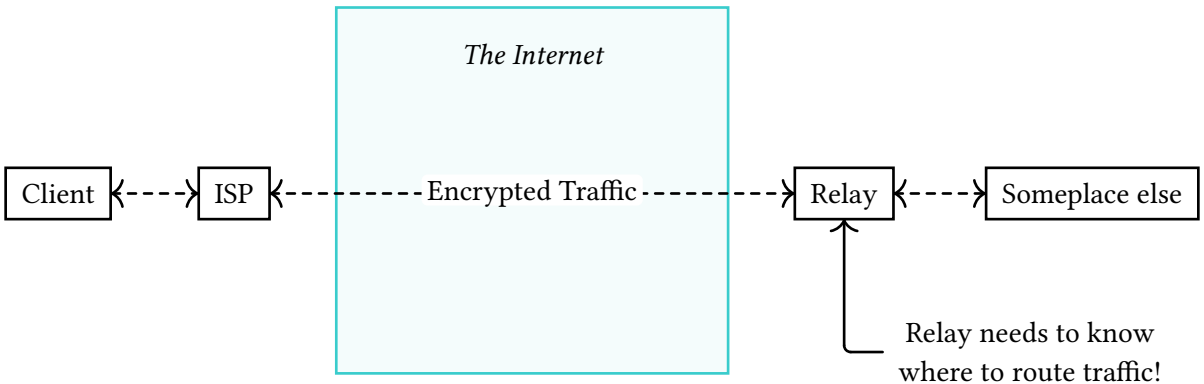


Accessing geo-restricted content



3 What They Can’t Do

Keeping traffic private from your VPN provider



Shielding your computer from all attacks

Sophisticated attack methods can still work

Shielding your computer from all attacks (ii)

Malware and virus protection is only as good as the relay makes it

Other considerations

TLS already secures most requests over the Internet

Other considerations (ii)

Bad actors with access to the relay can compromise most security

Other considerations (iii)

3.c.a HSTS (HTTP Strict Transport Security)

- Per-website policy that prevents browsers from accessing insecure contents over HTTP on future requests
- Header `Strict-Transport-Security` designates length of policy and whether subdomains are included
- HSTS preloading applies policy to a designated list of sites before visiting

3.c.b HTTP blocking

- Web server blocks all requests over HTTP, requiring that they go over HTTPS
- Could limit access to content for devices that don't support HTTPS
- Exists by default within major SDKs (Software Development Kits) like Android and iOS
- Can be toggled on in most major browsers

3.c.c DNS Poisoning

- Penetrated, or rogue DNS server which returns unauthentic responses for queries
- Navigates requests towards malicious servers

4 Vulnerabilities Can Be Disastrous

CVE-2024-3400 — Palo Alto Networks' PAN-OS

Remote Code Execution

CVE-2024-9463/9464 — Palo Alto Networks' Expedition

Credential exposure

Who even uses Palo Alto Networks?

4.c.a Many companies

Including…

- NVIDIA
- Microsoft
- IBM
- Visa
- Wells Fargo
- UnitedHealth Group
- NBCUniversal
- ADT

4.c.c Many government entities

Including…

- U.S. Department of Defense

4.c.b Many, many universities

Including…

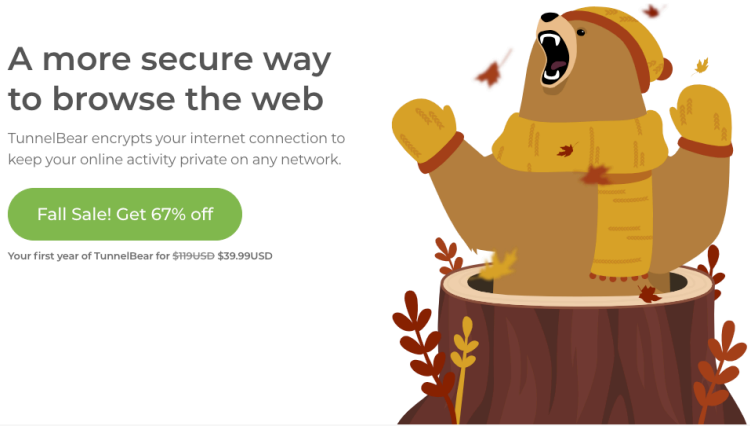
- MIT
- UC Berkeley
- School of Mines
- University of Pennsylvania
- University of Nebraska
- University of Maryland
- University of Wisconsin
- University of Louisville
- University of Denver
- Louisiana State University
- Colorado State University



That's us!

5 Commercial VPNs

TunnelBear



https://tunnelbear.com

TunnelBear (ii)



Change your IP address

Your IP address is kind of like a phone number that tells websites where you are and how to connect to your device. TunnelBear gives you a new IP, so all of your traffic looks like it's coming from somewhere else.



Block online tracking

Advertisers invade your online privacy by targeting your IP for ads. By changing your IP address, TunnelBear blocks common ways advertising trackers follow you around the internet.

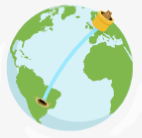


Stay safe on public WiFi

People love public Wi-Fi, but so do hackers. With simple tools, they can capture passwords and logins as they pass through a shared Wi-Fi point. Keep your accounts safe by encrypting your connection with TunnelBear.

https://www.tunnelbear.com/what-is-vpn#how-it-works

TunnelBear (iii)



Stay connected to home

Don't miss out on current events or local news when you're travelling. With servers in 47 countries, TunnelBear can help you stay connected to home as if you were there.



Stream video faster

Internet service providers regularly throttle services they compete with, but with TunnelBear, you can avoid throttling by keeping your browsing private from your service provider.



Bypass censorship

More governments are trying to censor news and communications outside their borders. TunnelBear can help bypass censorship by connecting to a server in another country, so you can get the information you need.

https://www.tunnelbear.com/what-is-vpn#how-it-works

TunnelBear (iv)



Travel securely

Don't trust the Wi-Fi in your hotel? TunnelBear's Grizzly-grade encryption lets you safely check your email, bank account, book flights and more—all without risking your personal information.



Protect your online privacy

Most websites ignore your Human Right to privacy. Whether it's your internet service provider monitoring your connection or advertisers tracking you, exercising your right to privacy is becoming more difficult. With TunnelBear VPN, all of your browsing is encrypted so no one else can see what you're doing.

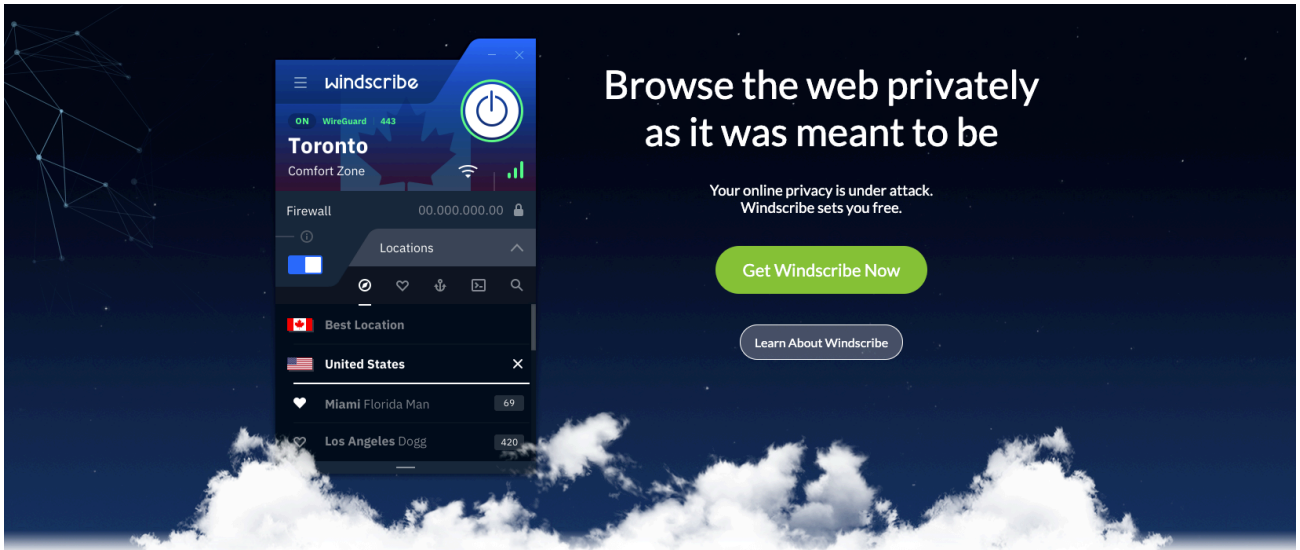


Peer-To-Peer

Internet service providers regularly slow, and even block, torrent connections on their networks. TunnelBear protects you from disconnects and blocks ISP from seeing your traffic, so they can't slow it down.

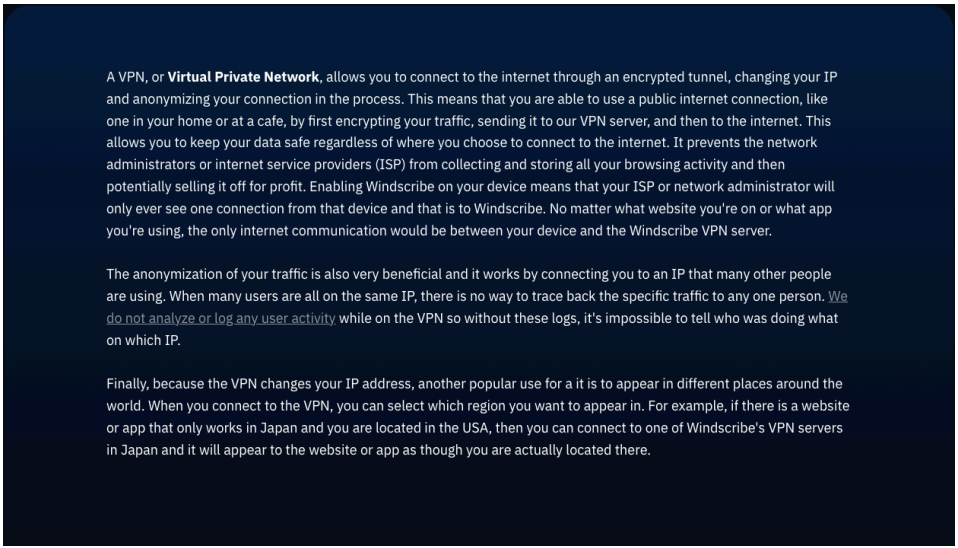
https://www.tunnelbear.com/what-is-vpn#how-it-works

Windscribe



https://windscribe.com

Windscribe (ii)



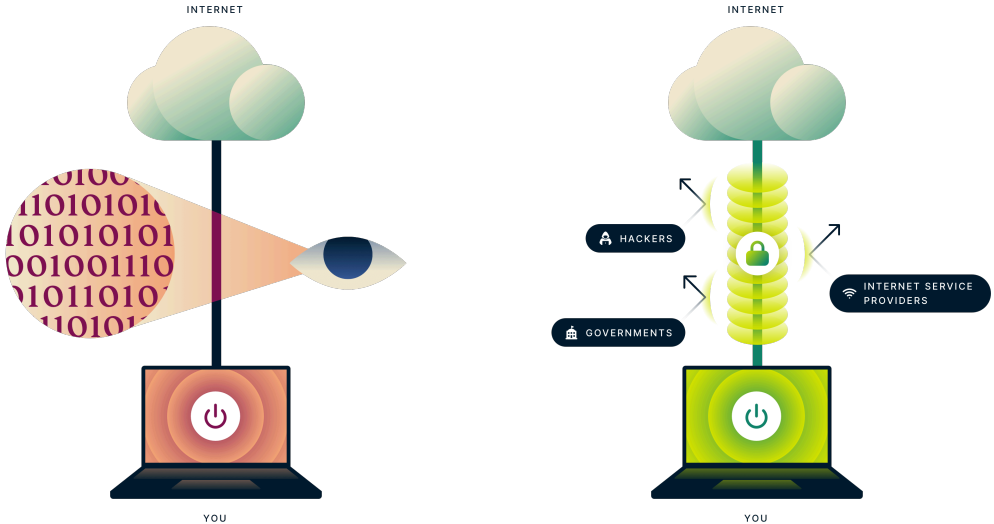
https://windscribe.com/knowledge-base/articles/what-is-a-vpn/

ExpressVPN



https://expressvpn.com

ExpressVPN (ii)



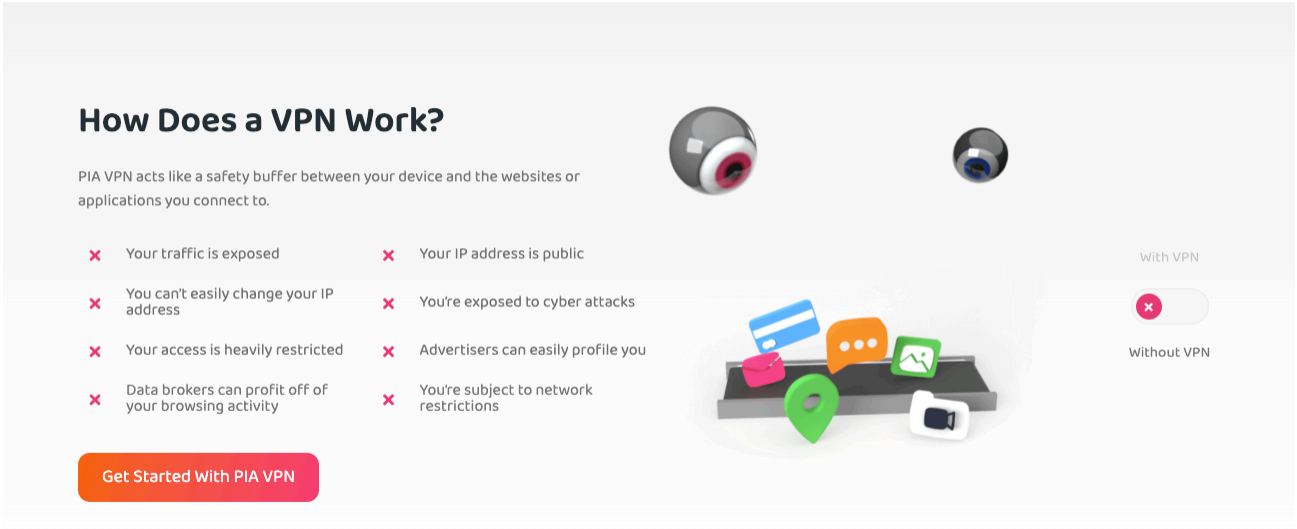
https://www.expressvpn.com/what-is-vpn#how-does-it-work

Private Internet Access



https://privateinternetaccess.com

Private Internet Access (ii)



https://www.privateinternetaccess.com/what-is-vpn

Private Internet Access (iii)

How Does a VPN Work?

PIA VPN acts like a safety buffer between your device and the websites or applications you connect to.

- Your traffic is encrypted
- Your IP address is private
- You can easily change your IP address
- You can bypass network restrictions
- You have more protection from cybercriminals
- You enjoy unrestricted access to the internet
- Advertisers will struggle to profile you
- Data brokers can't profit from your browsing activity

Get Started With PIA VPN

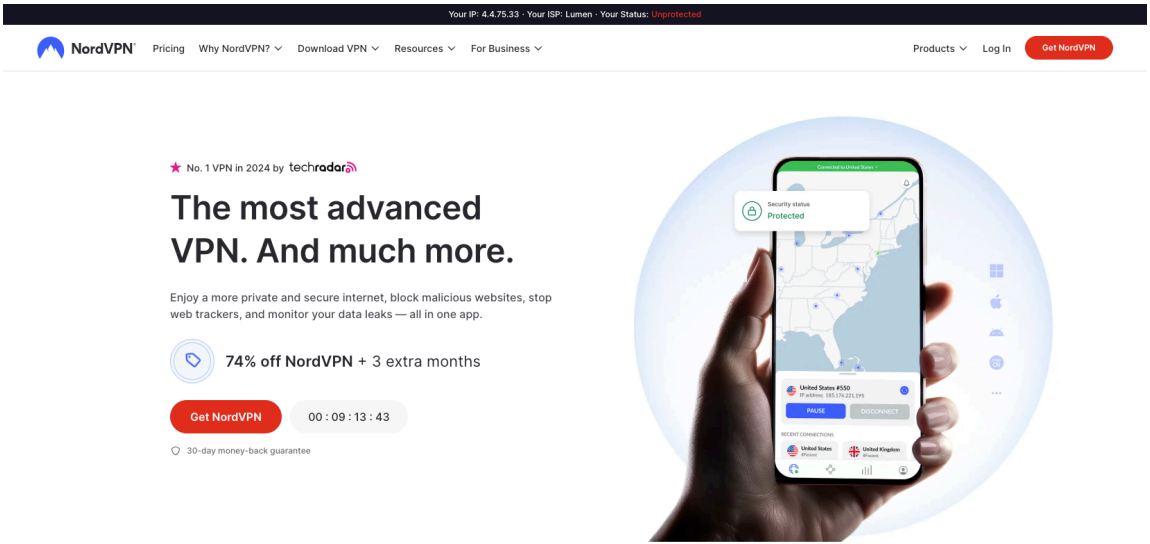


With VPN

Without VPN

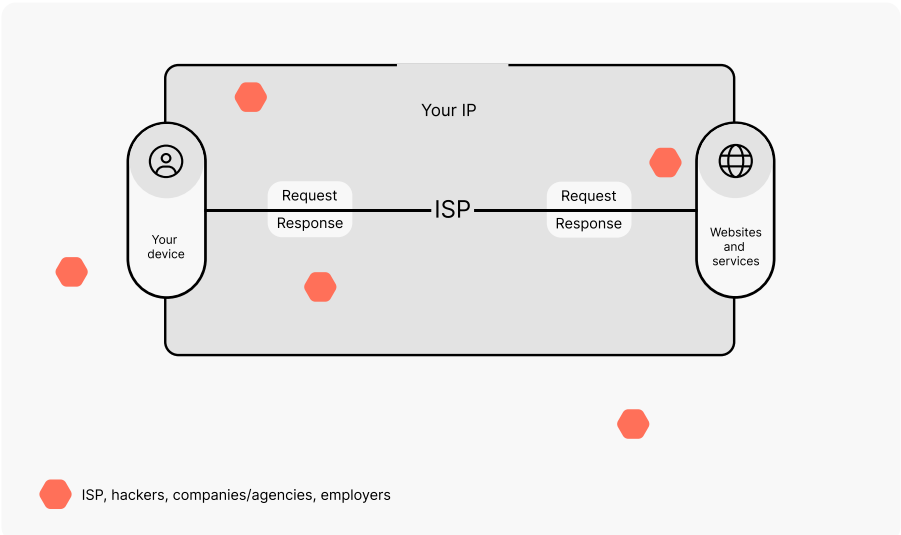
https://www.privateinternetaccess.com/what-is-vpn

NordVPN



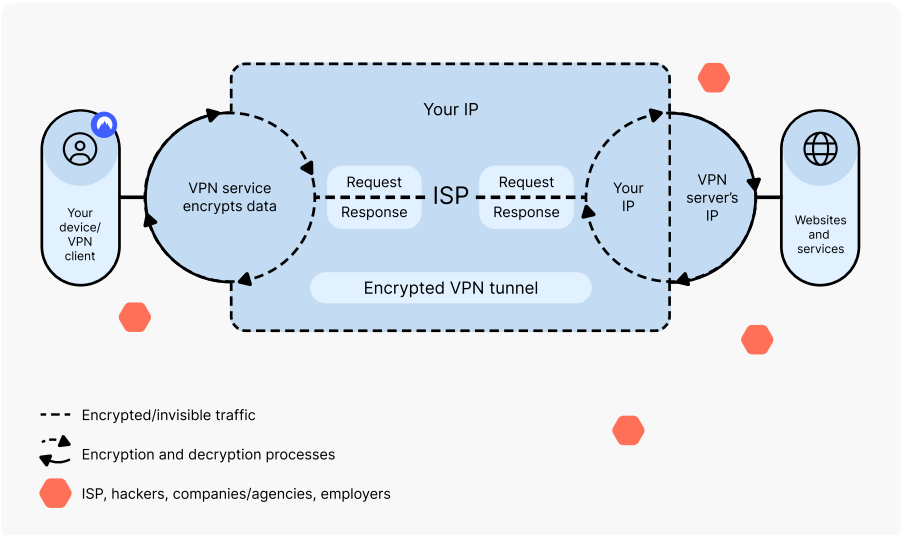
https://nordvpn.com

NordVPN (ii)



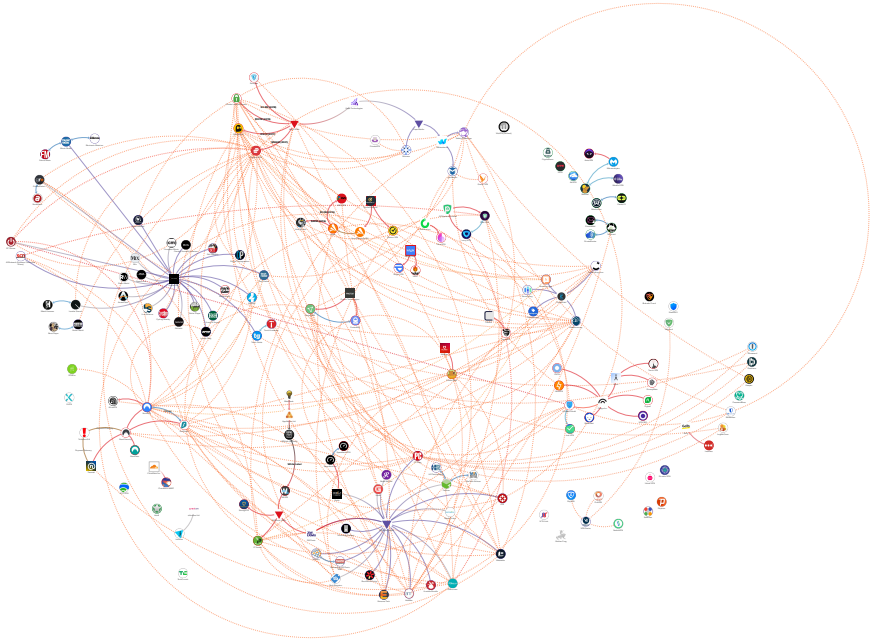
https://nordvpn.com/what-is-a-vpn/

NordVPN (iii)



https://nordvpn.com/what-is-a-vpn/

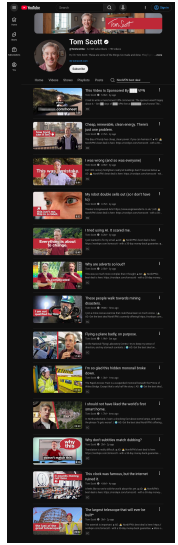
6 Conflicts of Interest



https://kumu.io/Windscribe/vpn-relationships

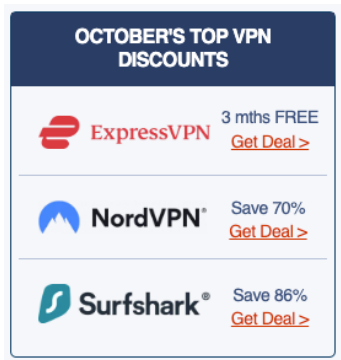
Back to Tom Scott

7 years later, after the initial “expose”, 12 NordVPN sponsorships were taken by Tom Scott…



References

- https://www.paloaltonetworks.com/cyberpedia/types-of-vpn
- https://www.fcc.gov/consumer-governmental-affairs/fcc-announces-effective-date-net-neutrality-order
- https://vulcan.io/blog/fixing-cve-2024-3400
- https://nvd.nist.gov/vuln/detail/CVE-2024-9463
- https://data.landbase.com/technology/palo-alto-networks-globalprotect
- https://bloomberry.com/data/palo-alto-global-protect



References (ii)

6.c.a Rabbit-hole content

- https://security.paloaltonetworks.com
- https://www.fcc.gov/document/fcc-restores-net-neutrality-0
- https://en.wikipedia.org/wiki/Virtual_private_network
- https://en.wikipedia.org/wiki/Transport_Layer_Security
- https://en.wikipedia.org/wiki/DNS_hijacking
- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://www.chromium.org/hsts/#preloaded-hsts-sites

