# 8 alternatives if you can't use a VPN

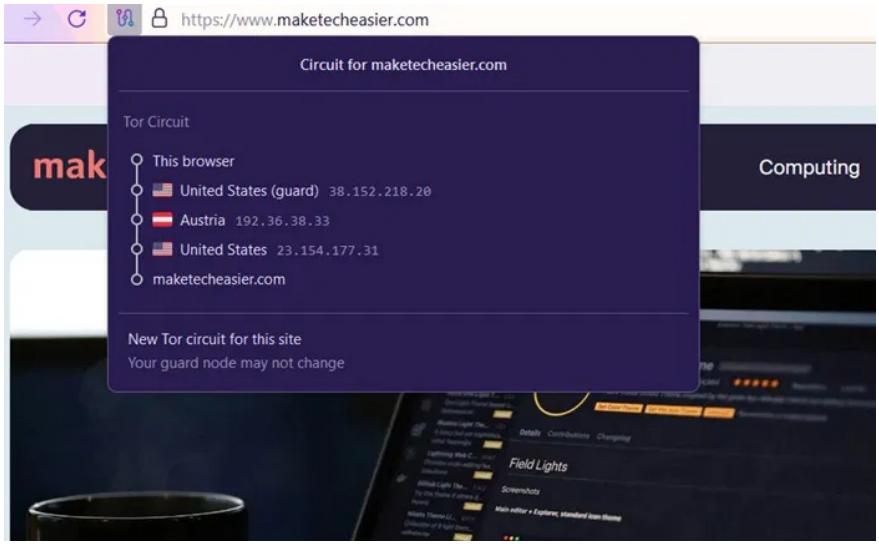
While they remain effective for many purposes, you might consider VPN alternatives when you can't access a particular website or app.

Virtual private networks (VPNs) are widely used to protect web browsing activity and user location, allowing you to bypass geographical barriers and censorship. However, they have drawbacks such as potential data leaks from outdated servers, data retention policies, VPN IP address blocking, and slower speeds. While they remain effective for many purposes, you might consider VPN alternatives when you can't access a particular website or app.

## 1. Onion Routing (Tor)

VPNs offer enhanced security with encryption, but this process only happens once per server. Instead of one-time encryption, try Onion Routing with the Tor Project, a popular alternative to VPNs. Tor encrypts your data multiple times and sends it through different volunteer-run servers.

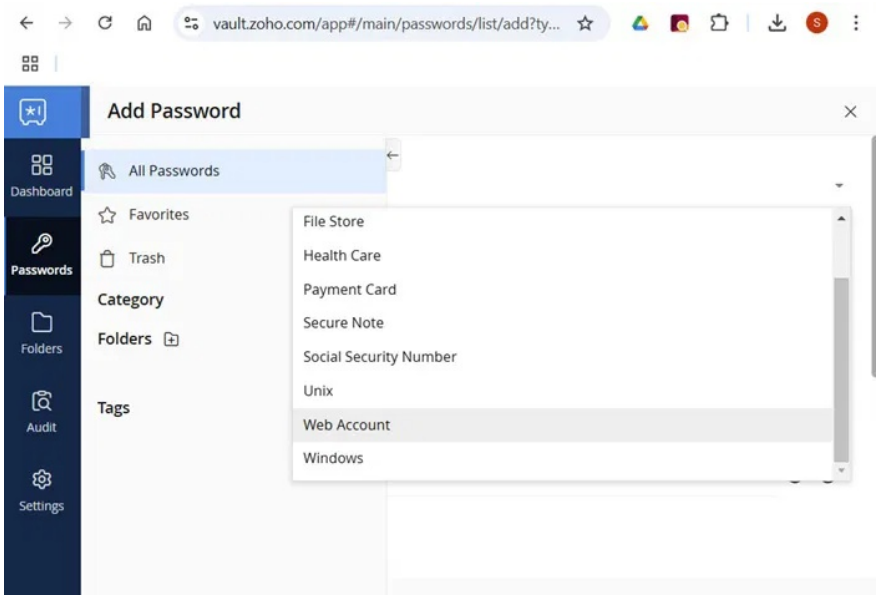
These servers don't know where the data is coming from, because each layer of encryption is peeled back, like an "onion." The weakness is Tor's input nodes, which Internet service providers (ISPs) can see, but everything after that is more secure and anonymous.



**Tip** : If you're experiencing slow bandwidth due to restrictions imposed by your internet service provider (ISP) on Tor, try these methods to overcome the speed reduction .

## 2. Identity and Access Management (IAM)

Identity and Access Management (IAM) solutions are very popular in schools, companies, and other organizational networks. Their primary goal is to prevent data leaks by protecting user identities, not IP addresses. They serve as a robust alternative to VPNs by requiring multiple forms of verification before granting access to resources.




Microsoft's Entra ID and Google 's IAM are other reliable options for identity protection, but they currently don't offer free trials. There are many premium IAM solutions, such as IdentityForce. From previous work experience, people highly rate ScaleFusion for its excellent features.

## 3. Privileged Access Management (PAM)

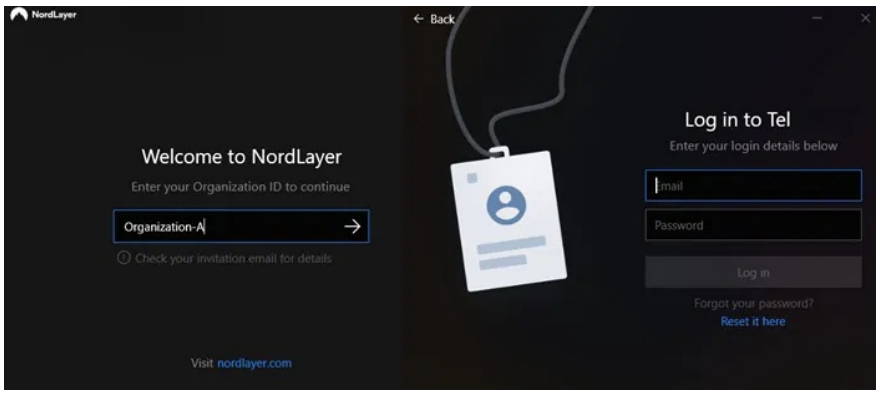
While IAM solutions are great for the average internet user, they don't meet the security needs of those with higher levels of access, such as network administrators, CEOs, or website owners who control user access. These accounts are prime targets for data thieves and hackers. For example, the 2024 NPD data leak exposed millions of personal records.


ManageEngine PAM360 is an excellent PAM solution. It has a centralized password repository, similar to other IAM software. But it also offers additional features such as role-based password ownership and sharing, automatic password resets for expired privileged accounts to prevent leaks, and monitoring and logging of user sessions. You can access a free trial on the website.

**Important note** : If your VPN provider doesn't have a strict no-logging policy, such as ExpressVPN's data deletion upon server restart, your data is at risk of being leaked.

# 4. Zero Trust Network Access (ZTNA)

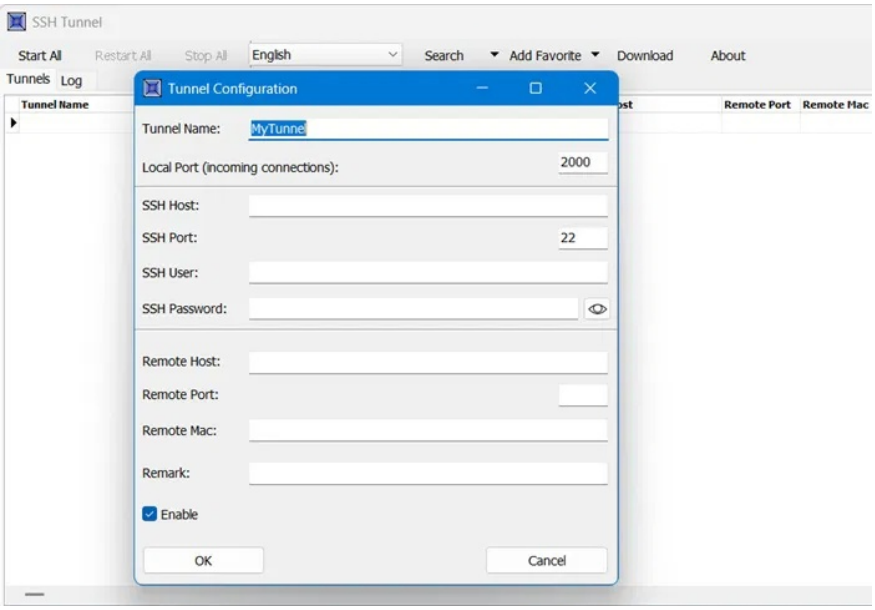
Most cyberattacks originate from the internet , but you can use Zero Trust Network Access (ZTNA) as a VPN alternative to mitigate the attack surface. Instead of using the regular internet, ZTNA relies on a private application network that neither internal employees nor external users are permitted to access. During access, everyone must independently authenticate themselves, hence the term 'zero trust'. The more sensitive the information, the stricter the authentication.



ZTNA is commonly used in healthcare organizations to meet regulations such as HIPAA. But ordinary internet users can also try it with applications like ZeroNet.

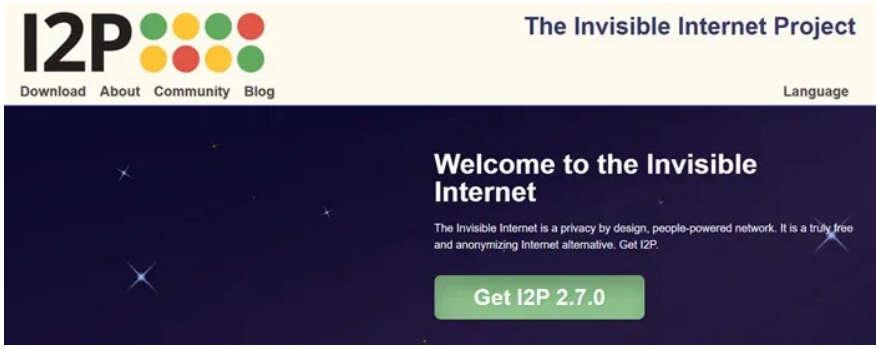
## 5. SSH Tunneling

While a VPN secures the entire network, sometimes you only need to secure a single application or port, or run a remote application securely. In these cases, you can use SSH tunneling (Secure Shell) to forward information from that specific application or port. The main goal of using SSH tunneling is to protect the identity of the remote computer, as you may not want it exposed on the internet.




## 6. Garlic Routing (I2P)

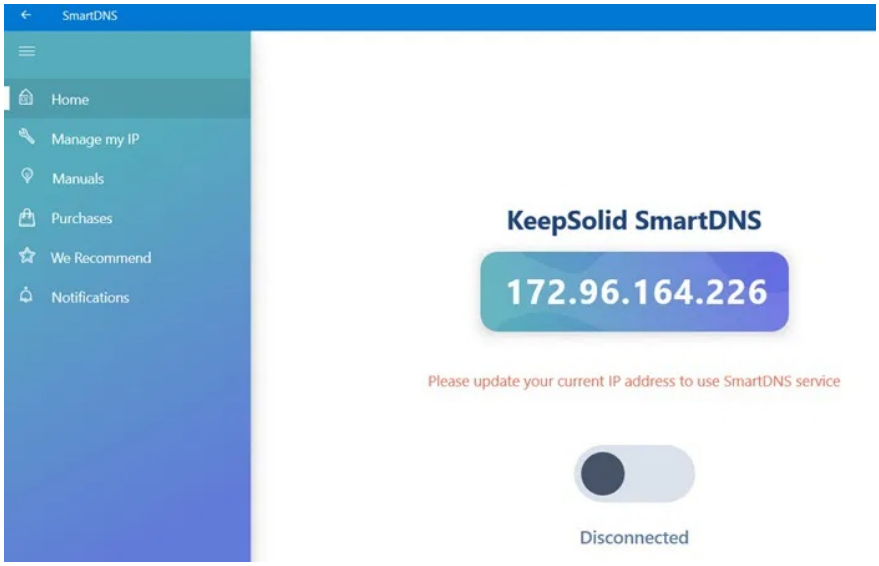
Similar to Tor's onion routing, garlic routing is another decentralized method for accessing remote servers, primarily used by a small group within the Invisible Internet Project (I2P), originally part of Freenet. Unlike Tor, which encrypts a single data stream multiple times across many different servers, garlic routing bundles multiple data streams together, each with its own layers of encryption, much like a clove of garlic.



There is no central server like in the case of Tor. Instead, I2P router consoles connect you to various websites on the network. You can find many I2P links (called 'eepsites') on this decentralized network for further access.

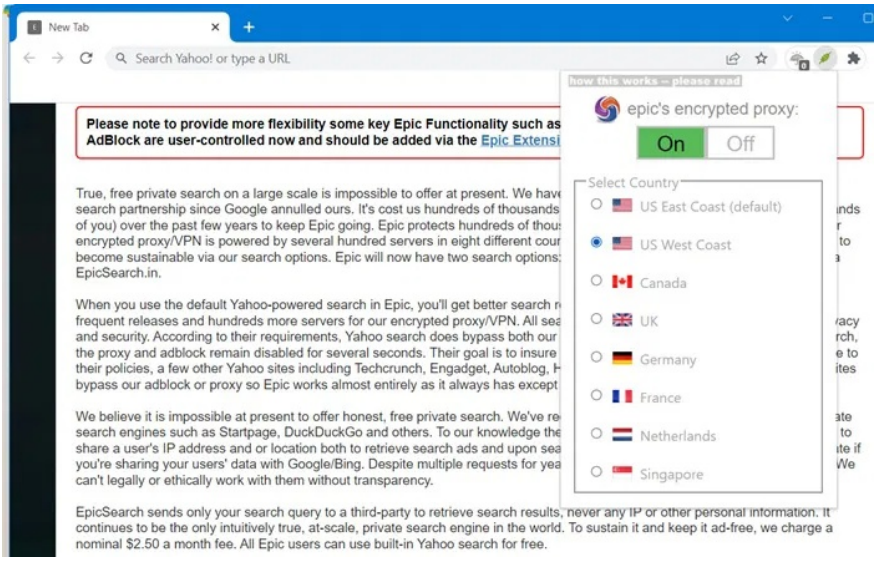
## 7. Smart DNS Solutions

Every time you access a website, your device sends a DNS request, which can expose your IP address through browsing activity. While VPNs aim to prevent DNS leaks, many VPNs, especially free ones, are ineffective. Smart DNS solutions are a more effective but lesser-known alternative to VPNs for bypassing geo-blocking restrictions on streaming sites like Netflix , and can sometimes succeed where VPNs fail.




## 8. Privacy-focused browser

This is a simple, straightforward solution that this article reserves for last. Instead of dealing with complex software and configurations, or paying for a VPN service, you can download a privacy-focused browser. These often incorporate many privacy-focused features, sometimes offering better anonymity than even a VPN. Some of the best options include Brave, Epic, Vivaldi, and Opera, each offering unique security features.




For example, the Brave browser has a feature called Fingerprint Randomization, which prevents websites from identifying and tracking your browsing activity. Even many advanced VPNs struggle with this, as their encryption isn't always adequate.

You finished reading the article "**8 alternatives if you can't use a VPN**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---