Search...

What is Tailscale?

Tailscale is a mesh VPN (Virtual Private Network) service that streamlines connecting devices and services securely across different networks. It enables encrypted point-to-point connections using the open source WireGuard protocol, which means only devices on your private network can communicate with each other.

Unlike traditional VPNs, which tunnel all network traffic through a central gateway server, Tailscale creates a peer-to-peer mesh network (known as a tailnet). However, you can still use Tailscale like a traditional VPN by routing all traffic through an exit node.

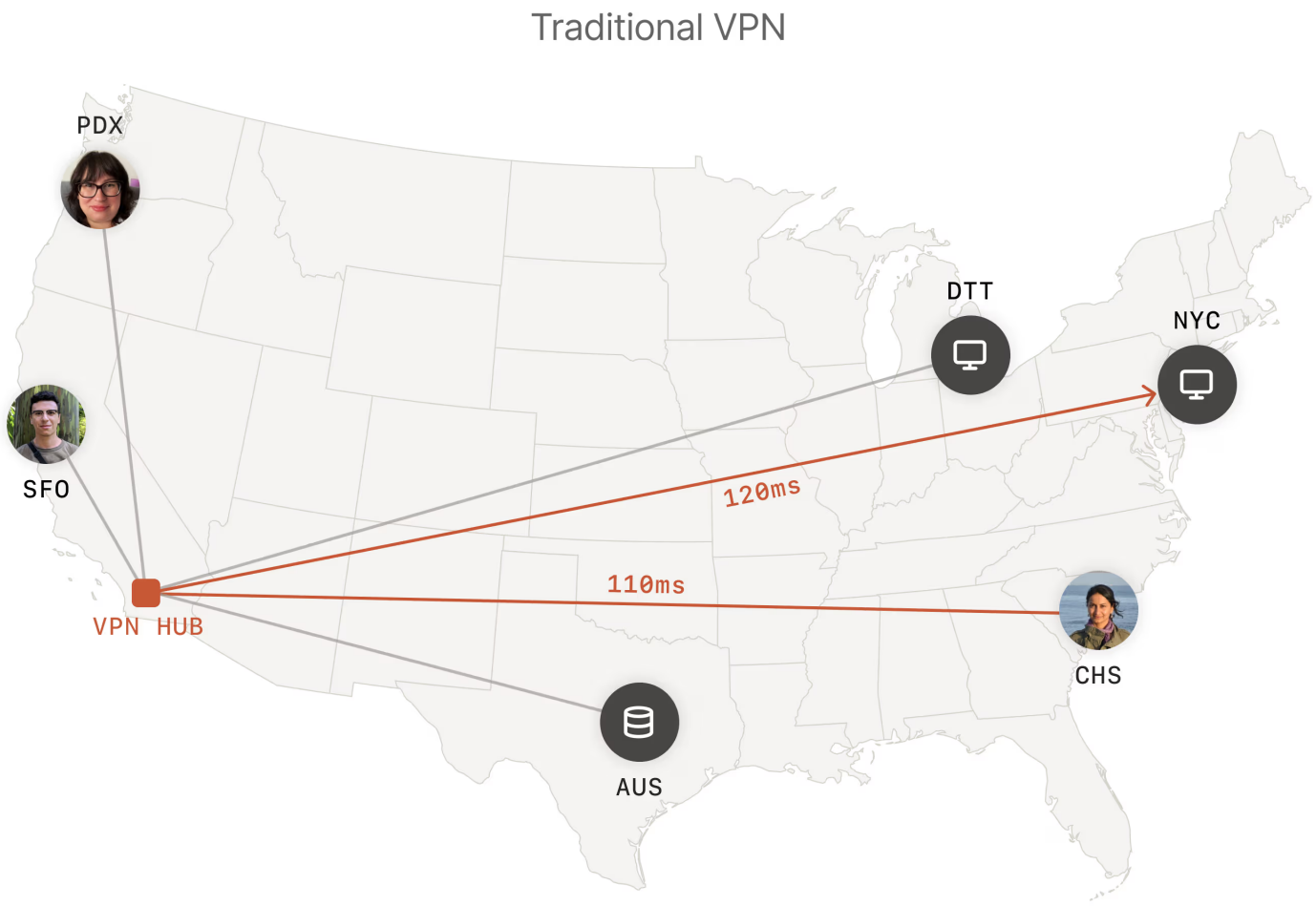

Figure 1(a). The central gateway may or may not be close to users, thus resulting in higher latency. Because traffic is centralized, it can also act as a bottleneck, slowing down connections further.

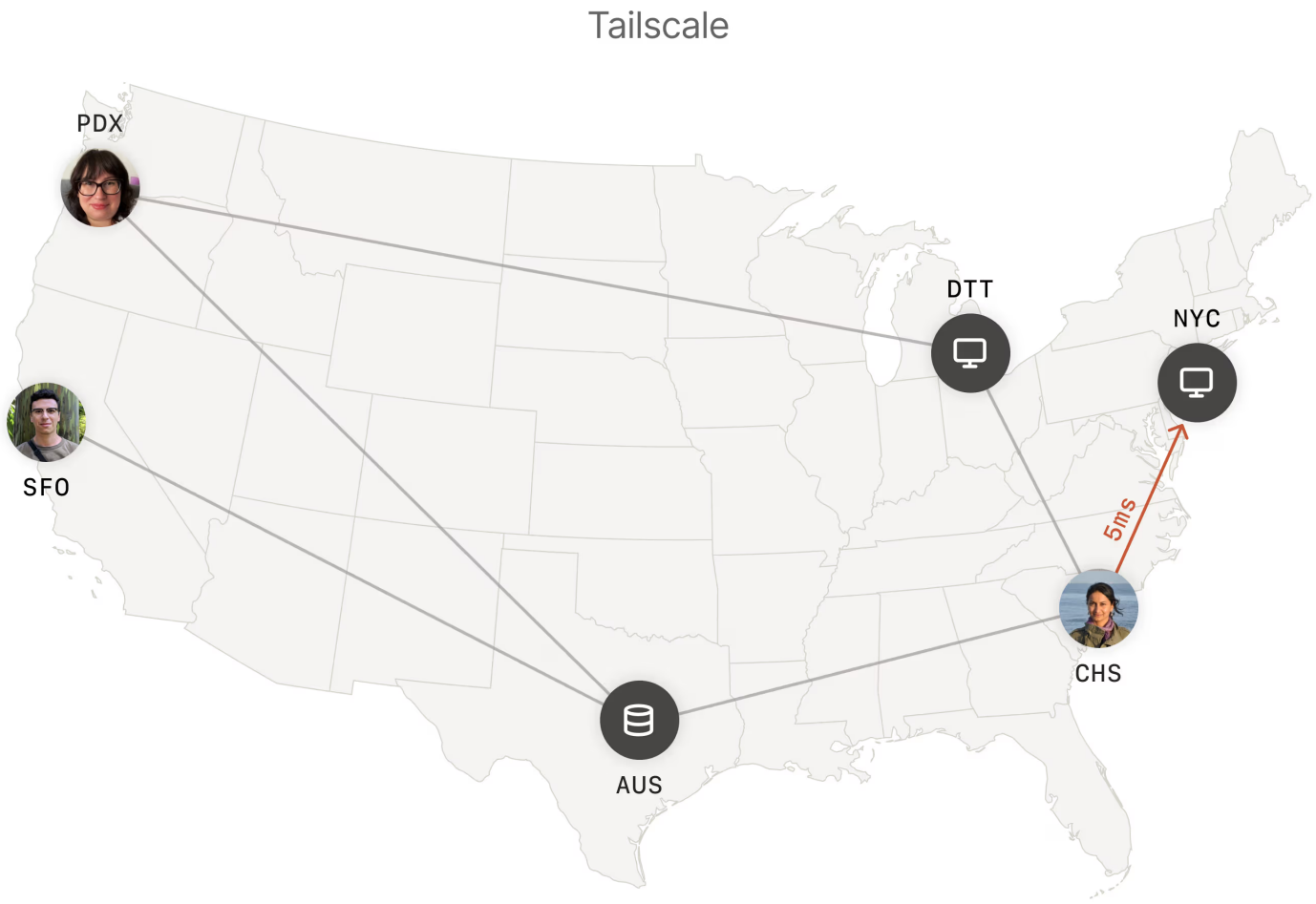

Figure 1(b). With Tailscale, each device is connected to the other directly, resulting in lower latency.

The Tailscale approach avoids centralization where possible, resulting in both higher throughput and lower latency as network traffic can flow directly between devices. Additionally, decentralization improves stability and reliability by reducing single points of failure.

The benefits

Some key advantages of Tailscale include secure and private connections between devices, a flexible network topology, and a streamlined setup. Tailscale is also cross-platform, infrastructure agnostic, highly configurable, and has a collection of features and integrations.

Streamlined setup

Although Tailscale is highly configurable, it's easy to get started. Unlike traditional VPNs that require extensive configuration, server setup, and networking expertise, you can deploy a Tailscale network (known as a tailnet) in minutes. After you create an account, authenticating two or more devices automatically creates a tailnet with a sensible set of default access policies.

Connections between tailnet devices work seamlessly across firewalls and Network Address Translation (NAT) without requiring port forwarding or complex firewall rules. This "zero config" approach dramatically reduces the technical barriers to implementing secure networking, making it accessible to technical and non-technical users.

Security and privacy

The Tailscale security model is built on modern, proven technologies and best practices such as end-to-end encryption and a zero-trust architecture. At its core, Tailscale uses WireGuard, a state-of-the-art VPN protocol known for its security and performance. This foundation is enhanced by Tailscale's commitment to compliance, security policies, and security features such as access control policies and Tailnet Lock.

Scalability and adaptability

Tailscale's flexible architecture is designed to grow seamlessly with your organization's needs. Whether you're scaling from a small team to a large enterprise or expanding across multiple geographic locations, Tailscale maintains its performance and security characteristics at scale. The distributed nature of its architecture means that adding new devices or users doesn't create bottlenecks that typically plague traditional VPN solutions.

Who's it for?

With its low barrier to getting started, versatility, and powerful capabilities, Tailscale seamlessly scales from personal use to enterprise deployments. Developers can use it to share work-in-progress features with their team, home lab enthusiasts can use it to access their media servers remotely, and businesses can use it to secure their distributed workforce—all without the hassle and overhead of traditional VPN setup and maintenance.

To learn more, take a deep-dive into how Tailscale works, learn about Tailscale use cases, or check out what people say about Tailscale.

Get started

Getting started is as simple as creating an account, installing the Tailscale client, and logging into two or more devices. Visit the quickstart guide to learn more.

To stay in touch, sign up for our newsletter. You can also follow us on Twitter, Hachyderm, or YouTube.

Last updated Sep 30, 2025