

# Using Tailscale for Secure Networking

---

Linux Training Academy

# Lesson Overview

- What Tailscale is
- How Tailscale works
- Why it's a great choice for self-hosting environments

# A Quick Warning: Technical Details Ahead

- Technical deep dive ahead
- You don't **need** all the details to use Tailscale
- Want details? Stick around!
- Just want the setup? Skip to the next lesson.
- **Key takeaway:** Tailscale is easy, secure, and avoids complex networking configurations

# What Tailscale Does

- Creates a **secure, private network** connecting your devices.
- Works across different networks and locations.
- Devices communicate as if on the same network, no matter the distance.
- Supports **laptops, servers, phones, and more.**

# High-Level Overview of Tailscale

- A **private, secure network** that follows you anywhere.
- Simplifies remote access as if all devices are in the same location.
- Eliminates complex VPN setups like firewall rules and routing tables.
- **Easy installation** – just install and log in, no networking expertise needed.
- Devices automatically discover and securely connect.

# What Tailscale Is

- Creates a peer-to-peer **mesh VPN** for encrypted communication.
- **Direct, end-to-end encrypted connections** between devices.
- Unlike traditional VPNs, **it doesn't rely on a central server** for routing traffic.
- Secure data transmission over the public Internet—no risk of exposure.
- Captured network traffic appears as encrypted gibberish to outsiders.
- Tailscale refers to this network as a "**tailnet**" (Tailscale Network).

# What a VPN Is

- VPN (Virtual Private Network) creates a **secure, encrypted connection** over the internet.
- This connection is called a **tunnel** between a device and a remote VPN server.
- Ensures data protection from eavesdropping or tampering.



# Using a VPN on Public Wi-Fi

- VPN **encrypts all internet traffic** before leaving the device.
- **Useful for public Wi-Fi** in coffee shops, airports, and hotels.
- **Protects browsing, emails, and login credentials** from network snoopers.
- Attackers can only see meaningless, encrypted data.

# How VPN Encryption Works

- **Device encrypts** data before sending it to the VPN server.
- **VPN server decrypts** the data and forwards it to the destination.
- **Destination sees the VPN server as the source**, not the original device.
- Response is sent back to the VPN server, encrypted, and returned to the device.

# VPN Traffic Routing

- **Device appears** to be communicating directly with the destination.
- All traffic is actually routed through the **VPN server**.
- **Enhances privacy** by masking the original IP address.

# The Network Portion of a VPN

- **Devices** on different networks connect to the same VPN server and **appear on the same network** despite physical distance.
- **Enables access to shared resources**, internal services, and remote networks.
- Businesses use this for secure employee access to company servers.
- Individuals use it for connecting to self-hosted services securely.

# What a Mesh Network Is

- **Decentralized network** where devices (nodes) connect directly to each other.
- Unlike traditional VPNs, **no central server is required** for communication.
- Traditional VPNs use a hub-and-spoke system (central VPN server as a hub).
- Mesh networks allow **direct, encrypted connections** between devices.
- Reduces or eliminates the need for a centralized relay server.

# Tailscale's Mesh VPN

- Devices authenticate to a **tailnet**.
- Devices discover other connected devices.
- Direct communication occurs between devices **when possible**.
- If direct connections are blocked, Tailscale uses a relay server ( DERP).
- Tailscale uses NAT traversal to connect devices behind routers/firewalls.
- There's no complex setup—just install, log in, and connect securely.

# Benefits of Tailscale's Mesh VPN

- No central server to route all traffic
- **Direct, peer-to-peer communication** between devices
- Bypasses bottlenecks common in traditional VPNs

## Benefits of Tailscale's Mesh VPN, Continued...

- **Lower latency** due to direct connections
- **Enhanced performance** with efficient routing
- **Greater reliability** by reducing single points of failure
- Modern alternative to conventional VPN solutions

# Faster Connections with Lower Latency

- Direct device communication **eliminates central routing**
- No VPN server bottleneck **reduces delays**
- **Improved performance** for remote access & file transfers

## Improved Reliability and Redundancy

- **No single point of failure** like in traditional VPNs
- Dynamic traffic routing ensures **continued connectivity**
- **Devices remain connected** even if some go offline

# Simplified Firewall and Network Configuration

- **No** complex firewall rules or port forwarding required
- **No** need for static IPs or public internet exposure
- Devices automatically discover & **securely connect**

# No Public IPs, No Port Forwarding, No Exposure

- Traditional self-hosting risks public internet exposure
- To access remotely, you typically need to:
  - Expose a public IP address
  - Use port forwarding, increasing attack risks
  - Set up dynamic DNS (DDNS) for changing IPs

## How Tailscale Solves These Issues

- Private, encrypted tailnet replaces public IPs
- Unique private Tailscale IPs for **secure access**
- No need to open firewall ports or expose services

# Key Benefits of Tailscale's Approach

- **No external attack surface** – Services stay private
- No domain name or DDNS hassle – Uses stable private IPs
- **No router configuration needed** – Works behind NAT & firewalls

# Tailscale = Safer, Simpler, More Private

- **Eliminates security risks** from public exposure
- **Simplifies remote access** to self-hosted services
- **More private** than traditional networking solutions

# End-to-End Encryption for Maximum Security

- All traffic is **encrypted** using WireGuard
- **Secure** even on untrusted networks
- Tailscale never accesses decrypted traffic



# Easy Remote Access Without Exposing Services

- **Securely** access file servers, remote desktops, & web apps
- No need for public IPs, DDNS, or complex networking
- Each device gets a private tailnet IP

# Seamless Cross-Platform Support

- Works on **Linux, Windows, macOS, iOS, Android**
- Supports cloud instances for remote connectivity
- Easy device connectivity across different environments

# Automatic Handling of Restricted Networks

- Bypasses strict firewalls when direct connections fail
- Uses DERP relay servers as a fallback
- Ensures connectivity in **all network conditions**

# No Single Point of Failure

- Traditional VPNs rely on a single server
- Tailscale's distributed architecture **ensures reliability**
- Devices can connect even if parts of the network go down

# Easy Management

- **Minimal configuration required** – Tailscale automates networking
- **Web-based admin console** for managing devices
- Quickly check device status, rename, tag, or revoke access

# Tailscale's Exit Nodes: Secure Internet Routing

- A mesh VPN securely connects devices **without public exposure**
- Sometimes, routing all internet traffic through a trusted location is needed
- Tailscale's Exit Node feature enables this

# How Exit Nodes Work

- Routes all internet traffic through a specific device on your tailnet
- Similar to a traditional VPN, but using your own trusted device
- **Enhances security on public networks** & changes connection origin

## Real-World Use Case

- Useful when accessing **region-restricted services**
- Example: Logging into a bank account from a foreign country
- Using an Exit Node makes your connection appear as if it's coming from a different location.

## Free vs. Paid

- Tailscale offers a generous **free plan for individuals**
- The free plan includes up to **100 devices & 3 user accounts**
- Core features available at **no cost for personal use**
- **Ideal** for self-hosters

# Business Plans & Additional Features

- **Businesses must pay for Tailscale**
- Includes all free plan features plus:
  - External User Sharing for temporary access
  - More administrative controls & auditing
  - Unlimited user accounts for management

## How Tailscale Can Provide a Free Tier

- Costs are offset by charging small & large businesses
- Larger businesses pay higher fees
- **Efficient architecture** keeps costs low

# Cost-Efficient Architecture

- No need for centralized VPN servers
- Traffic flows **directly** between devices
- Minimizes reliance on costly infrastructure

# Wrapping Up

- Tailscale **simplifies** secure networking
- No need for port forwarding, public IPs, or exposure
- The Mesh VPN enables **direct, encrypted connections**
- Exit Nodes allow **secure internet traffic routing**
- The free plan is sufficient for most self-hosters

# Lesson Recap

- Tailscale is a modern, peer-to-peer mesh VPN that provides secure, private networking without the complexity of traditional VPNs.
- Devices connect using direct, encrypted tunnels whenever possible, avoiding the need for a central VPN server.
- A tailnet is a private network of authenticated devices, allowing seamless, secure communication between them.
- Self-hosting with Tailscale eliminates the need for public IPs, port forwarding, or exposing services to the internet, making remote access safer.

# Lesson Recap

- DERP servers relay encrypted traffic only when direct connections aren't possible, ensuring connectivity without compromising security.
- Exit Nodes allow internet traffic to be routed through a trusted device, making them useful for secure browsing and bypassing geo-restrictions.
- Tailscale's free plan includes all the features needed for personal self-hosting, while businesses pay for advanced security, access controls, and compliance tools.