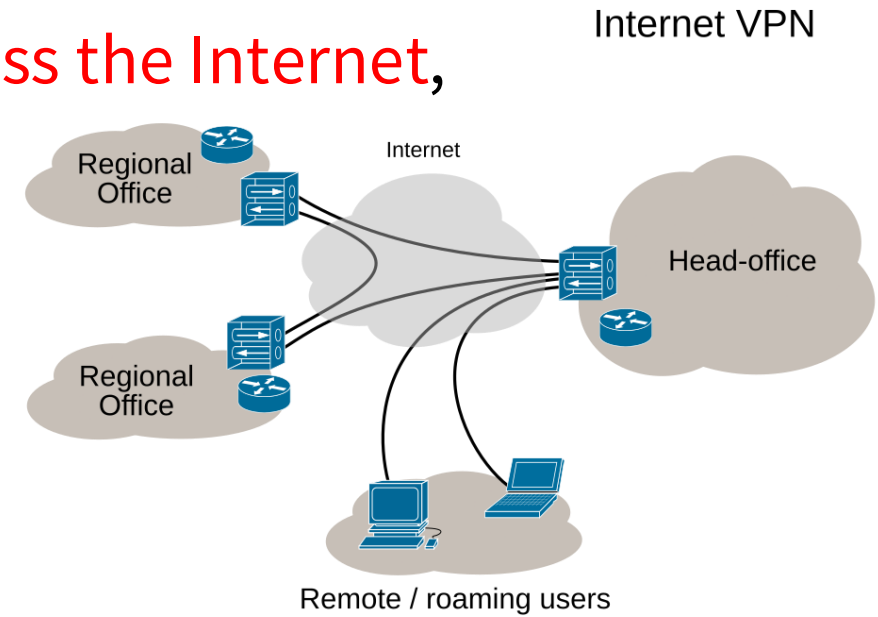
Virtual Private Network (VPN)

tsaimh (2024, 2026)
? (?-2023)

Source: https://en.wikipedia.org/wiki/Virtual_private_network

Introduction

- A virtual private network (VPN) is an overlay network that uses network virtualization to extend a private network across the Internet, via the use of encryption and tunneling protocols.
- In a VPN, a tunneling protocol is used to transfer network messages from one network host to another.



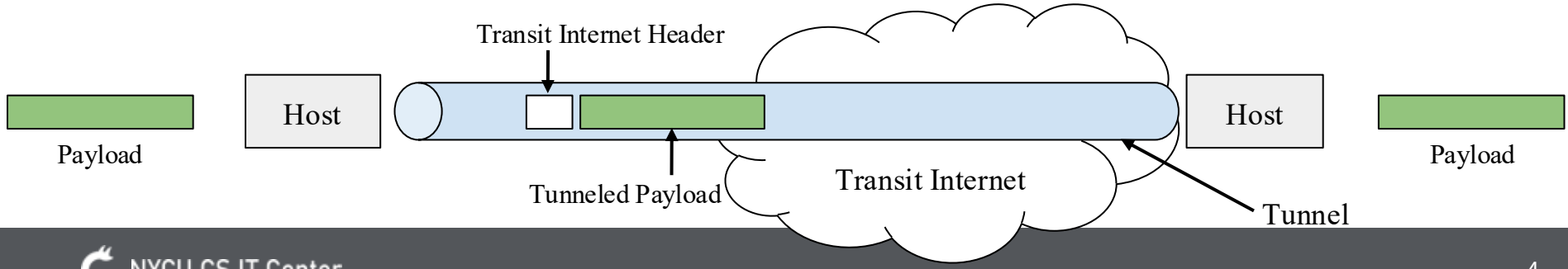
Source: https://surfshark.com/learn/what-is-vpn

Types of VPNs

- **Remote access VPNs (Host-to-network VPNs)** are commonly used by organizations to allow off-site users secure access to an office network over the Internet.
- **Site-to-site VPNs** connect two networks, such as an office network and a datacenter.
- **Consumer VPNs** route your internet traffic through a VPN server, which helps users bypass Internet censorship such as *geo-blocking* and users who want to protect their communications.

VPN Key Concept - Tunneling

- A VPN tunnel is a secure, encrypted connection between your device and a VPN server.
- Data sent through the tunnel is encapsulated (wrapped in additional encrypted layers), making your online activity private and unreadable to outside observers.



Source: https://surfshark.com/learn/what-is-vpn

Older VPN and Tunneling Protocols

- PPTP and LT2P/IPSec - Both PPTP (Point-to-Point Tunneling Protocol) and L2TP/IPSec (Layer 2 Tunneling Protocol/IPSec) are considered outdated tunneling protocols. While they can provide decent speeds, they can not offer the security or reliability of more modern protocols like OpenVPN, IKEv2, or WireGuard;
- SSTP -SSTP (Secure Socket Tunneling Protocol) is a tunneling protocol rather than a VPN protocol. This means it lacks the functionality of OpenVPN, IKEv2, and WireGuard. While considered relatively safe and easy to use, its code was never audited, and it has compatibility issues with certain operating systems, like macOS.

Source: https://surfshark.com/learn/what-is-vpn

Modern VPN Protocols

- IKEv2/IPSec. IKEv2 (Internet Key Exchange version 2), paired with IPSec, is widely and natively supported in modern OSs. It excels at speed, particularly when switching networks and at shorter-distance connections, making it popular among mobile users.
- OpenVPN/SSL VPN leverages existing SSL/TLS protocols to achieve high speed, strong security, and compatibility with various routers. It is a trustworthy choice but performs worse than IKEv2 and WireGuard.
- WireGuard is a protocol that has been built to outperform OpenVPN and IPSec in terms of power usage and performance, with **only 4,000 lines of code**. Currently, WireGuard is the fastest VPN protocol available.

Source: https://surfshark.com/learn/what-is-vpn

VPN Protocols

- The most popular ones:
  - OpenVPN
  - WireGuard
  - IKEv2/IPSec
- Older VPN and tunneling protocols
  - PPTP and L2TP/IPSec
  - SSTP

Source: https://en.wikipedia.org/wiki/Virtual_private_network

Reference

- Virtual Private Network (Wikipedia)
- What is VPN (SurfShark)
- Virtual Private Networking: An Overview (by Microsoft)