Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

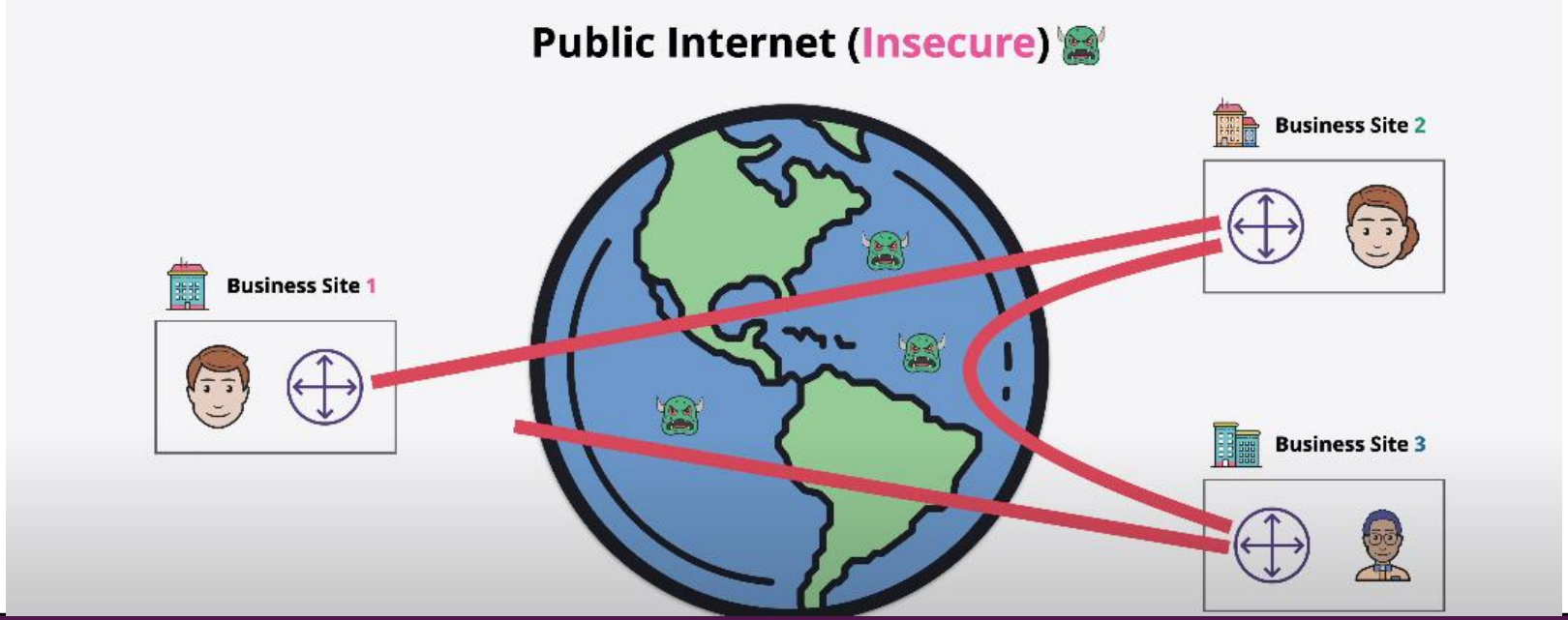
aNetSec.github.io

Spring 2025

IPsec

Why IP security?

- There is no built in encryption in IP protocol.
- Internet traffic route via different networks.
- Packets can be sniff in transmission.



IPsec goals

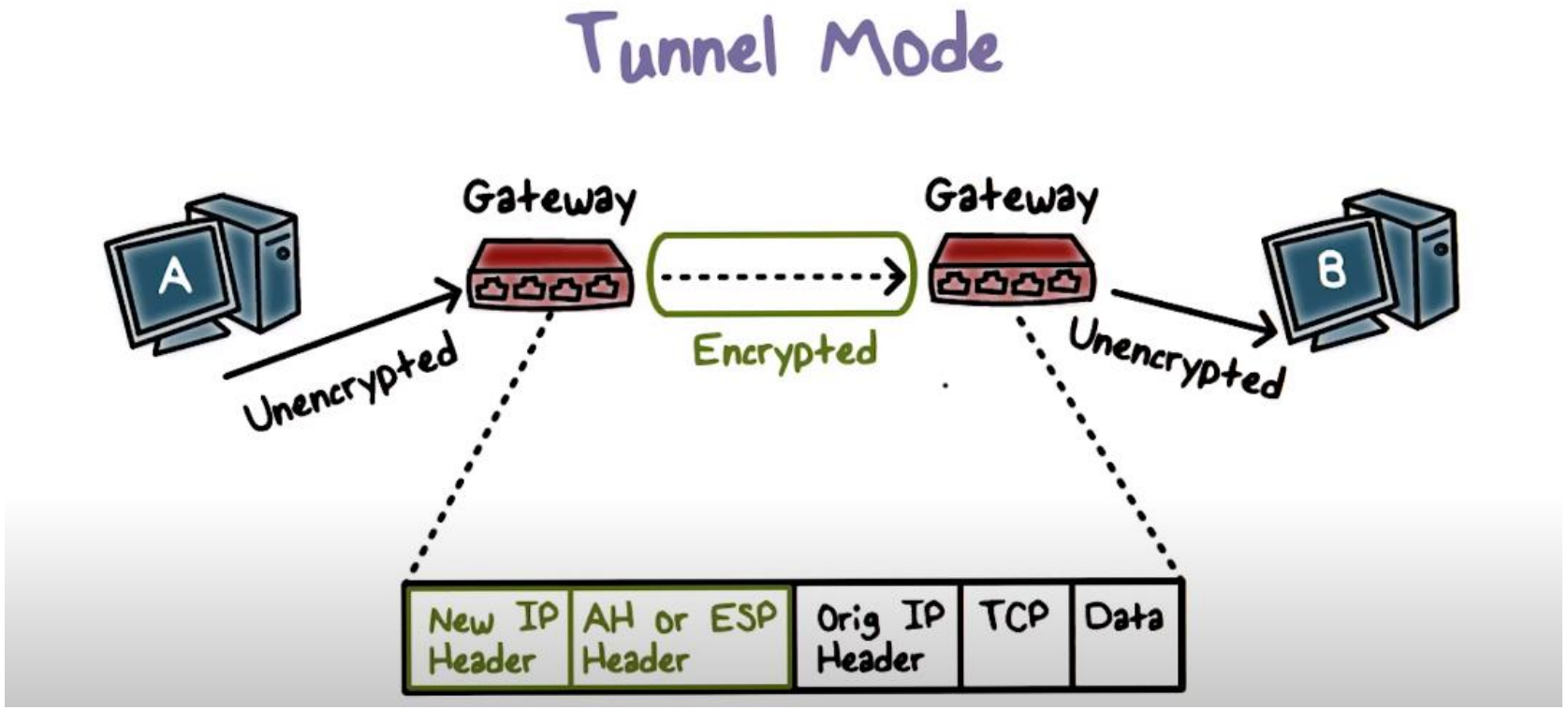
- IPsec: Internet Protocol Security.
- Preserve CIA.

IPsec modes

- IPsec operates in two main modes, each serving different purposes and use cases:
  - **Transport Mode**
  - **Tunnel Mode**

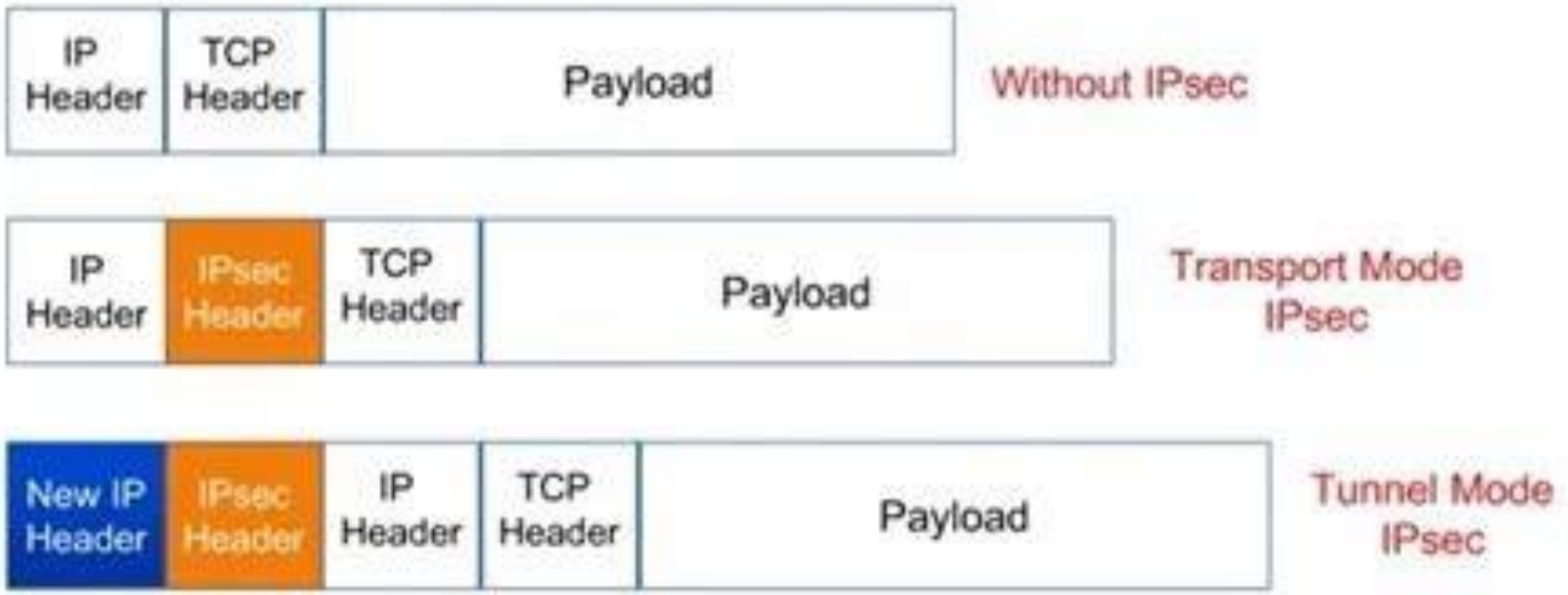
Tunnel Mode

- the entire IP packet is encapsulated within another IP packet



Transport Mode

- only the payload of the IP packet is encrypted



Compare

Transport Mode

1. Only the payload of the IP packet is encrypted and/or authenticated. The IP header remains intact and is not encrypted.
2. This mode is typically used for end-to-end communication between two hosts.

Tunnel Mode

1. The entire original IP packet is encapsulated within a new IP packet.
2. This mode is commonly used for site-to-site VPNs, where traffic between two networks is secured.
3. Tunnel mode is ideal for scenarios where multiple users or devices from a network need to communicate securely with another network.

Two IPsec protocols

- Authentication Header (AH) protocol [RFC 4302]
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP) [RFC 4303]
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

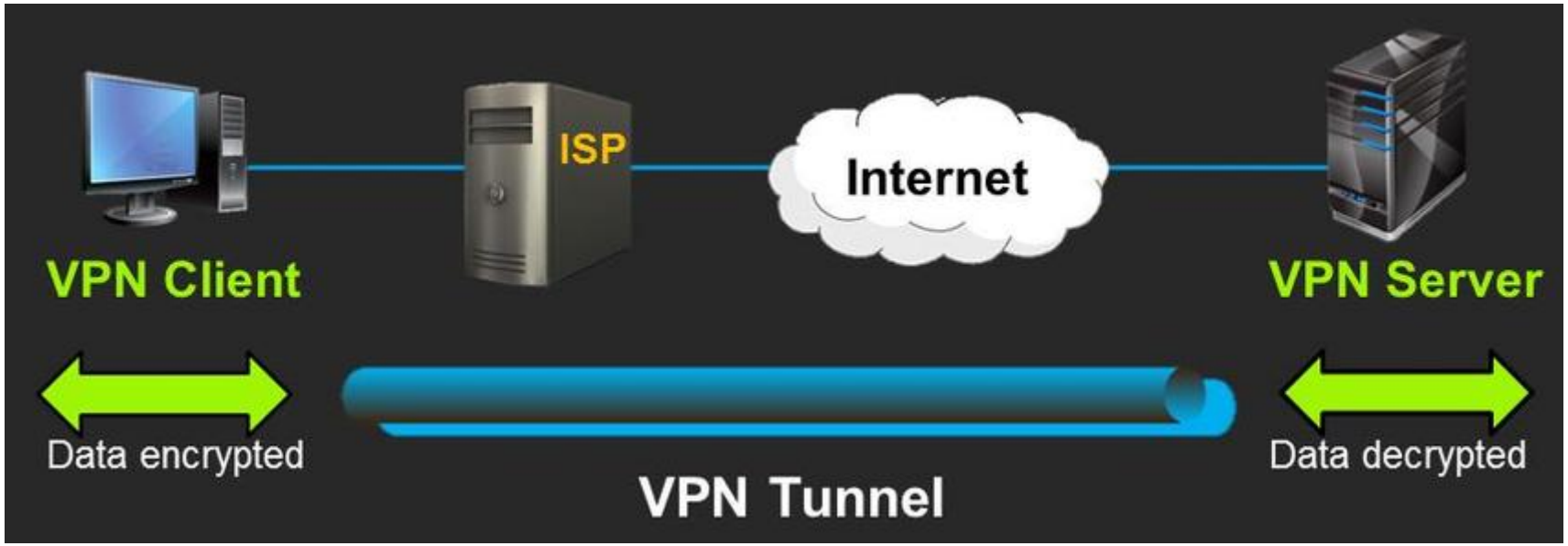
IKE (Internet Key Exchange)

- **Purpose**: IKE is a protocol used to set up a secure, authenticate.
  - Communication channel between two parties.
  - It is primarily responsible for the key exchange and the establishment of the parameters for IPsec.
- **IKE operates in two phases**
  - **Phase 1**: Establishes a secure, authenticated channel (IKE SA) between the two parties. This phase can use various authentication methods, such as pre-shared keys or digital certificates.
  - **Phase 2**: Negotiates the IPsec SAs that will be used for the actual data transmission.
- IKE is used in conjunction with IPsec to facilitate the secure exchange of keys and the establishment of security parameters necessary for IPsec to function.

VPN

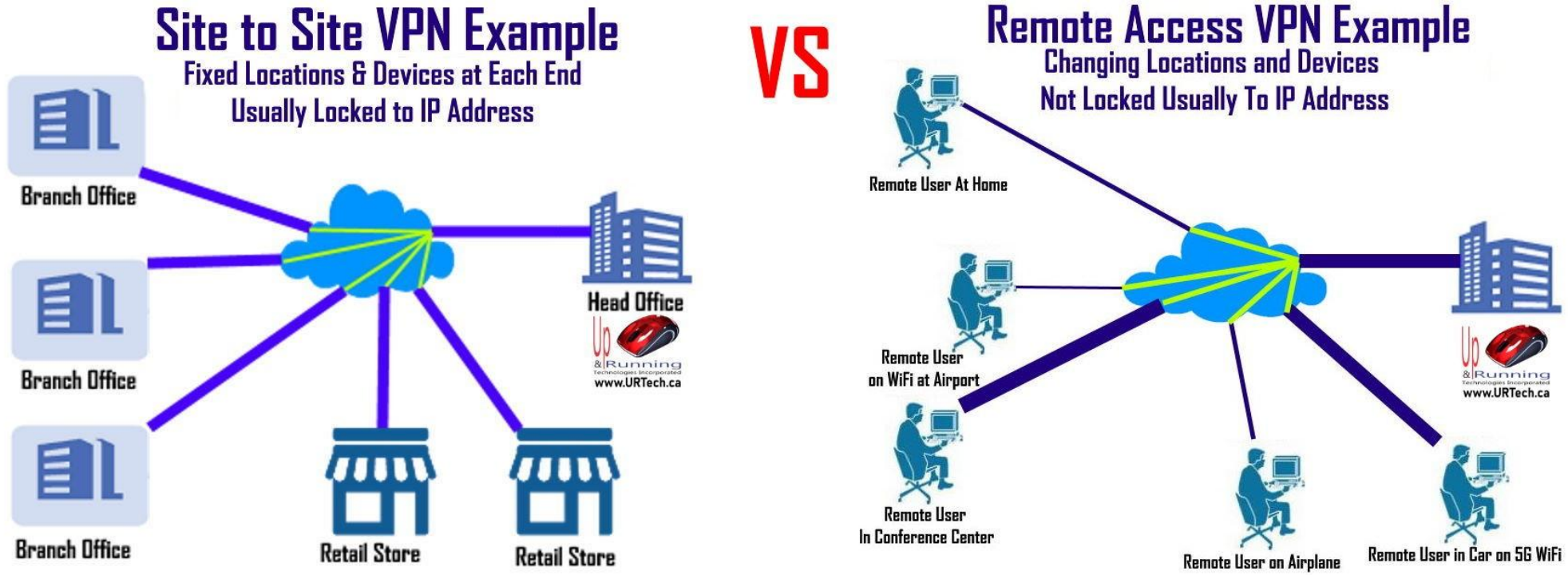
VPN: virtual private network

- VPN is a technology that creates a secure, encrypted connection over a less secure network, such as the Internet.
- It allows users to send and receive data as if their devices were directly connected to a private network.



VPN Types

- **Site-to-Site VPN:** Connects entire networks to each other, allowing secure communication between different office locations.
- **Remote Access VPN:** Allows individual users to connect to a private network from a remote location.



VPN Protocols

- VPNs can use various protocols for security,
- Including IPsec, but also others like
  - SSL/TLS (used in SSL VPNs)
  - L2TP (Layer 2 Tunneling Protocol)
  - PPTP (Point-to-Point Tunneling Protocol)
  - OpenVPN
  - Wireguard

PPTP

- **PPTP (Point-to-Point Tunneling Protocol)**
- is a network protocol used to implement virtual private networks (VPNs).
- It was developed by a consortium led by Microsoft and is one of the oldest VPN protocols still in use today.
- Use fixed ports.
- PPTP has known security vulnerabilities, particularly in its encryption methods.
- No longer support in modern OS.

L2TP

- **L2TP (Layer 2 Tunneling Protocol)**
- Is a tunneling protocol used to support virtual private networks (VPNs)
- Was developed by a consortium of companies, primarily led by Cisco Systems and Microsoft.
- Combined with IPsec.
- Use fixed ports.
- Good encryption.
- Support in modern OS.

OpenVPN

- **OpenVPN** is an open-source VPN
- Provides a secure and flexible way to create point-to-point or site-to-site connections in routed or bridged configurations.
- It is widely used for secure communications over the Internet and is known for its strong security features and versatility.
- Open-source
- Works with TCP and UDP.
- Cross-Platform Compatibility
- Flexible encryption.
- Use one port (Not fixed port)
- Complex Setup
- Performance Overhead

WireGuard

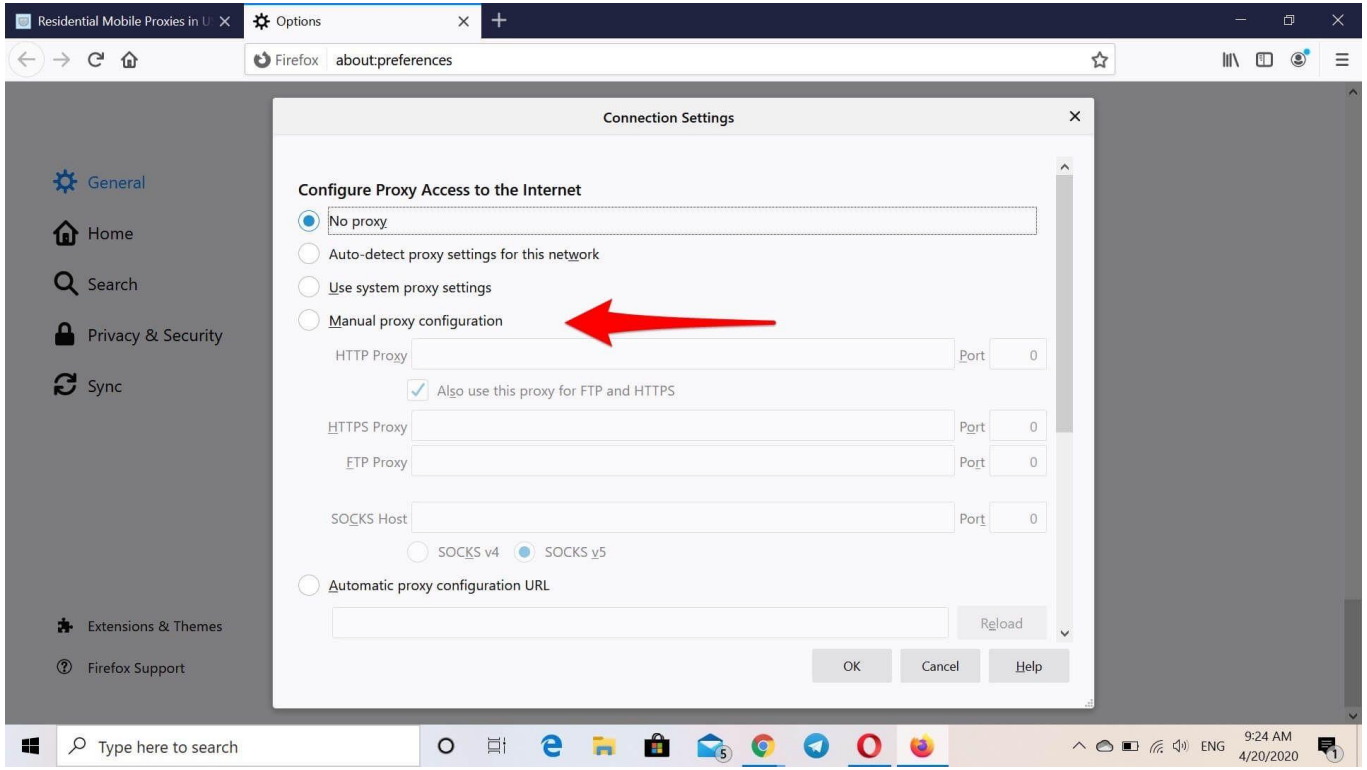
- **WireGuard** is a modern, open-source VPN protocol
- Designed to be simple, fast, and secure.
- It was created by Jason A. Donenfeld
- Performance and ease of use compared to older VPN protocols
- Open-source
- Works with UDP.
- Cross-Platform Compatibility
- Use one port (Not fixed port)
- Easy Setup
- Fast
- Limited Features

Other VPN protocols

- **SSTP (Secure Socket Tunneling Protocol)**
  - Developed by Microsoft, SSTP encapsulates PPP traffic over an SSL/TLS channel. It is primarily used on Windows systems.
- **L2F (Layer 2 Forwarding Protocol)**
  - Developed by Cisco, L2F is an older tunneling protocol that was designed to support VPNs. It is less commonly used today, as it has largely been replaced by L2TP.
- **SoftEther VPN**
  - An open-source, multi-protocol VPN software that supports various VPN protocols, including its own SoftEther protocol, as well as OpenVPN, L2TP/IPsec, SSTP, and more.
- **OpenConnect**
  - An open-source VPN client that was originally developed to support Cisco's AnyConnect SSL VPN.
- Vmess/Vless/Trojan, ... !!

Proxy Server

- A **proxy server** is an intermediary server that acts as a gateway between a client.
- Proxy types: HTTP, HTTPS, Socks v4,v5.



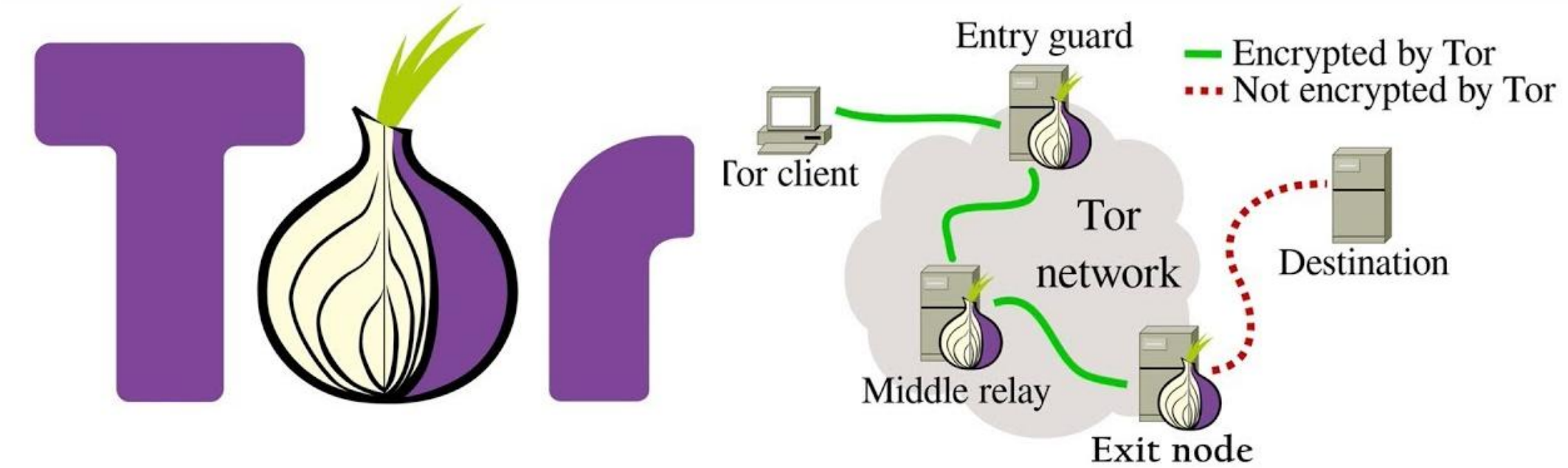
VPN vs Proxy Server

- VPN route all application traffic to VPN server.
- Proxy forward just configured app (Like browser) to proxy.
- Witch one is better?

Use case: Tor Proxy

- Tor app create socks server.
- Tor browser send browser traffic to Tor socks server.

Tor


Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor
network
Destination
Middle relay
Exit node

TOR

- Tor routing
- Toward privacy and security