Virtual Private Networks (VPN’s)

Homework

Leonardo Hügens, 31/10/2024

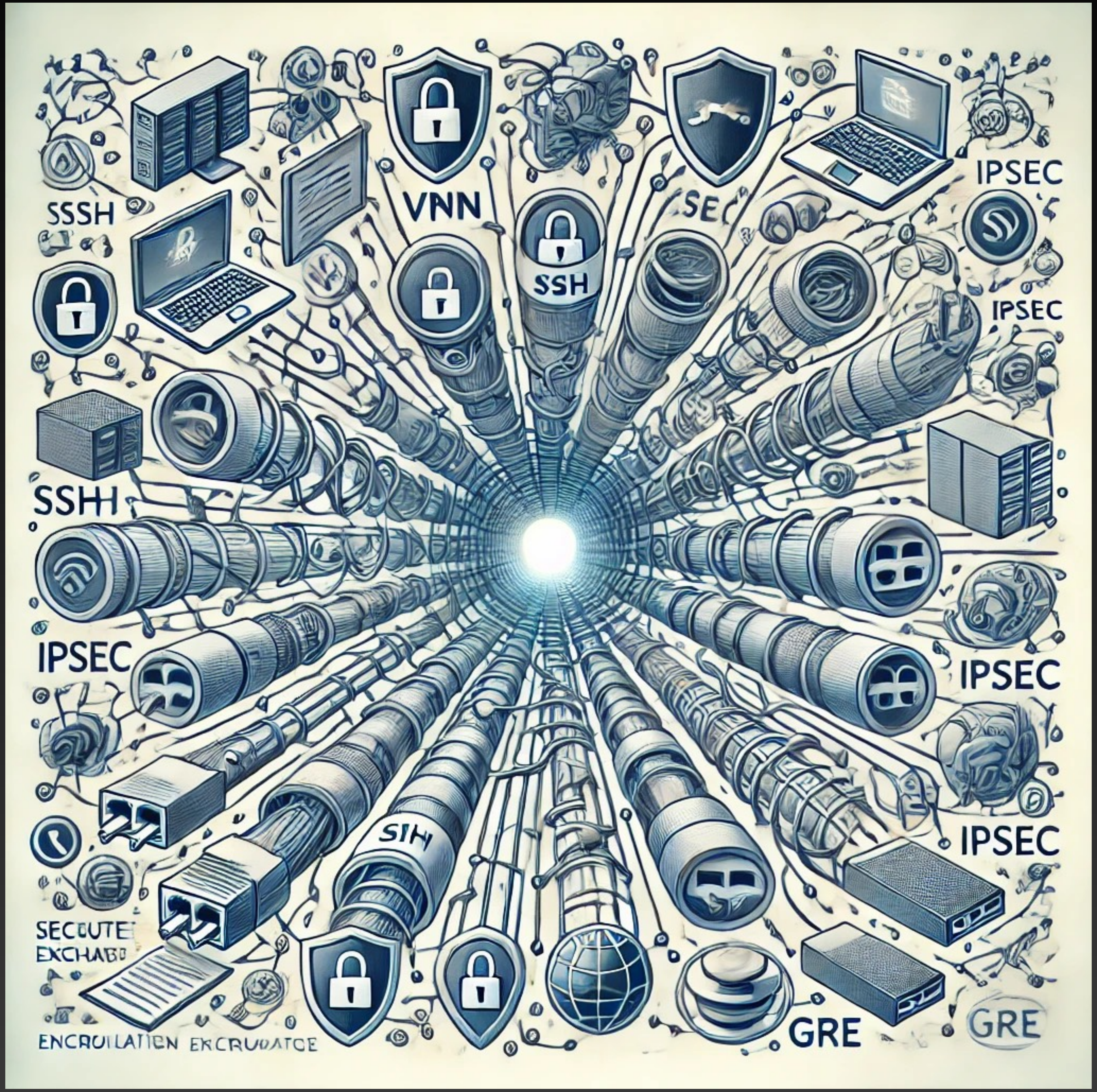
Definition

- A **Virtual Private Network** is a network architecture for virtually extending a private network across one or multiple other networks which are either untrusted (as they are not controlled by the entity aiming to implement the VPN) or need to be isolated (thus making the lower network invisible or not directly usable).

- VPN’s can extend access to a private network to users who do not have direct access to it, such as an office network allowing secure access from off-site over the internet.

- This is achieved by creating a link between computing devices and computer networks by the use of network *tunnelling protocols*.

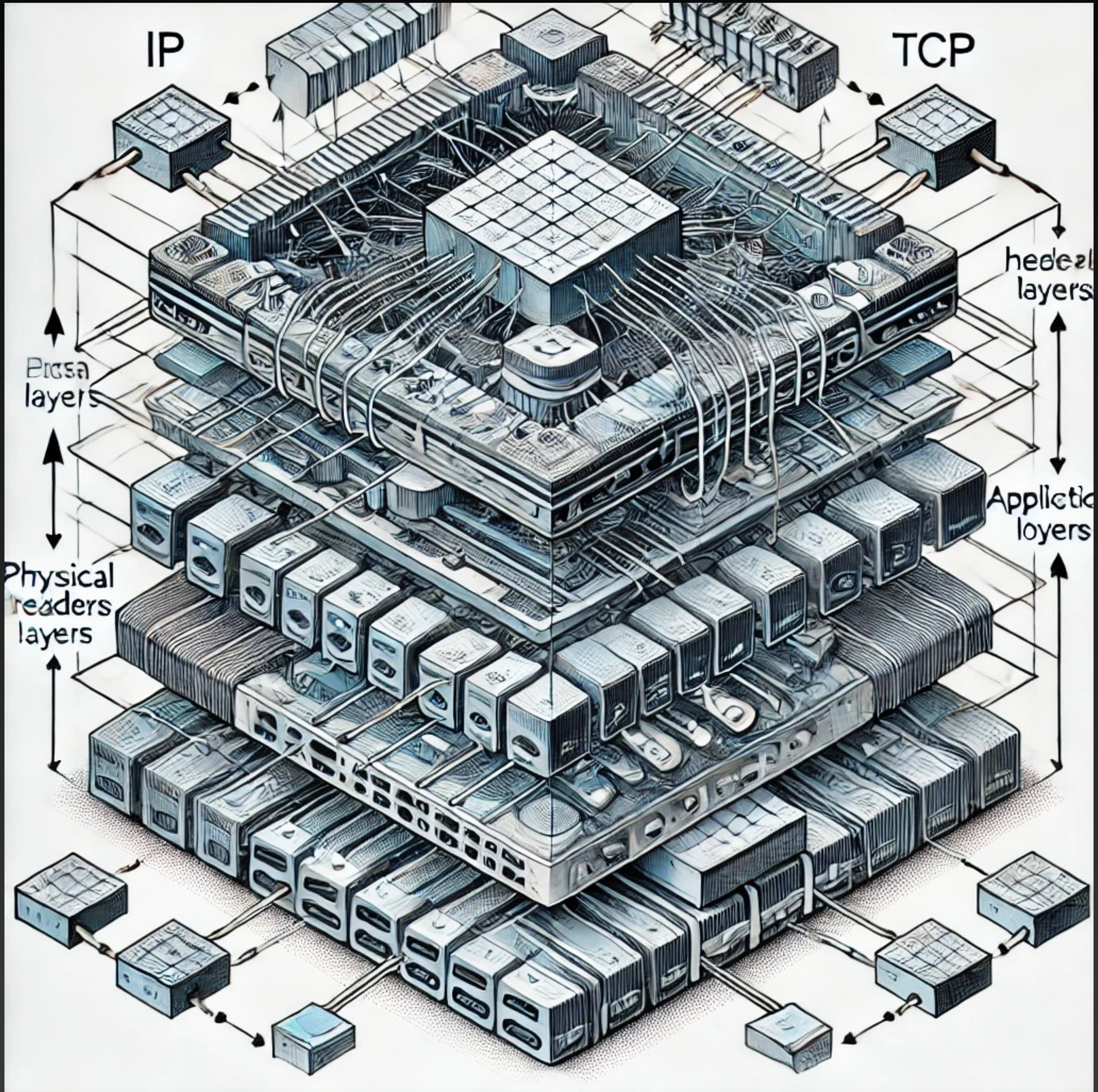
Tunneling Protocols



Tunnelling Protocols

- A **Tunneling Protocol** is a communication protocol which allows for the movement of data from one network to another.
- It can, for example, allow private network communications to be sent across a public network (such as the Internet), or for one network protocol to be carried over an incompatible network, ….. through a process called……..

Encapsulation



Encapsulation (in networking)

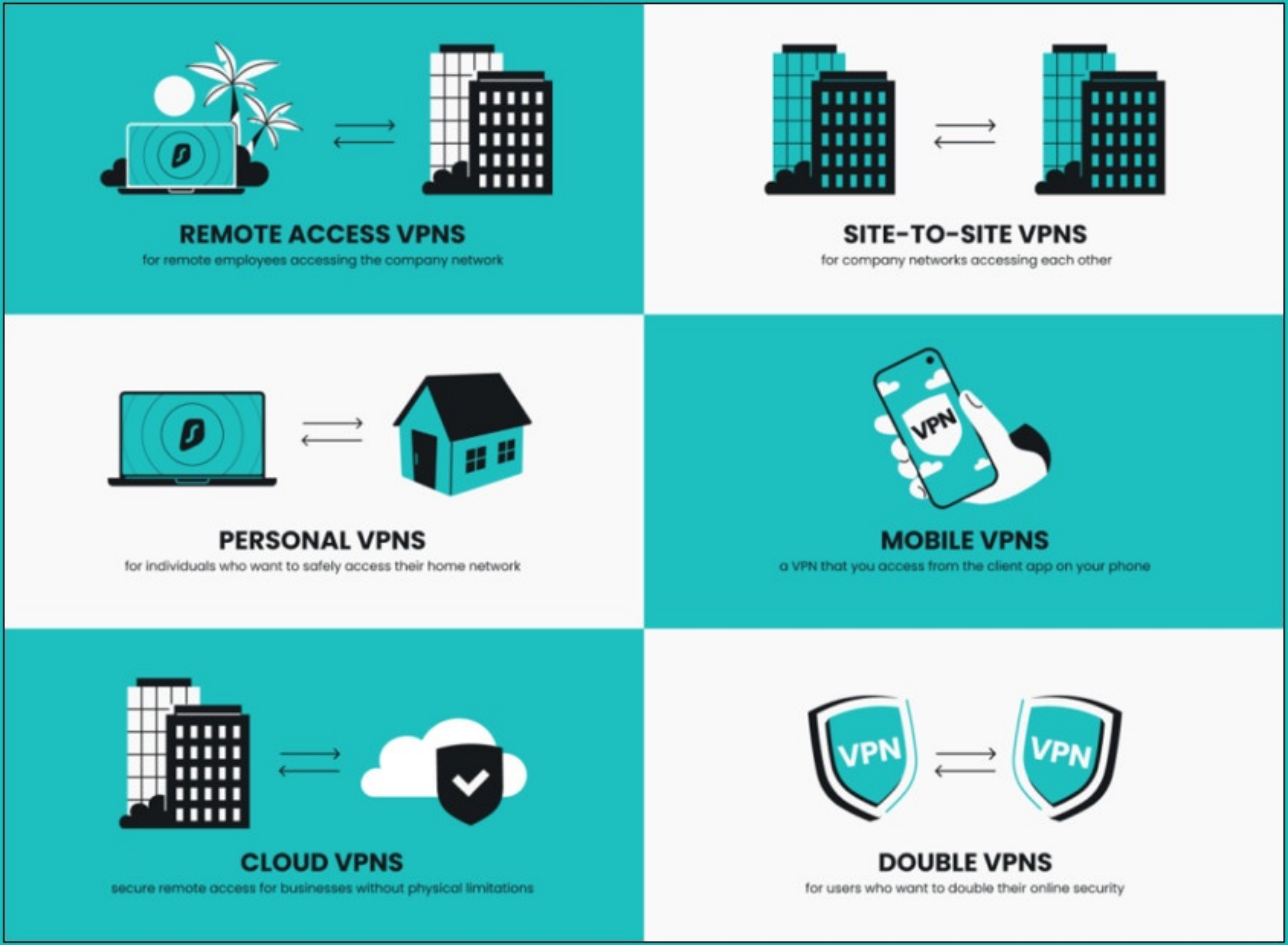
- In networking, **encapsulation** refers to the process of wrapping data with protocol-specific information as it moves down the layers. Each layer of the network stack adds its own header (and sometimes a footer) to the data, which contains control information like the source and destination addresses, error-checking details, or sequencing information.

Encryption

Encryption

- It is possible to make a VPN secure, to use on top of insecure communication medium (such as the public internet) by choosing a tunnelling protocol that implements encryption.
- Example: **Internet Protocol Security** (IPsec).
  - IPsec encapsulates an IP packet inside an IPsec packet.
  - De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

Different types of VPNs



REMOTE ACCESS VPNS
for remote employees accessing the company network

SITE-TO-SITE VPNS
for company networks accessing each other

PERSONAL VPNS
for individuals who want to safely access their home network

MOBILE VPNS
a VPN that you access from the client app on your phone

CLOUD VPNS
secure remote access for businesses without physical limitations

DOUBLE VPNS
for users who want to double their online security

Common Use Cases

- Remote work and accessing company resources.
- Privacy and security on public Wi-Fi.
- Bypassing geo-restrictions.
- Online privacy from ISPs.
- Secure online banking and shopping.

Security Benefits

- IP address masking.
- Data encryption.
- Protection agains man-in-the-middle attacks.
- Np-logs policies.
- Kill switches.

Potential Drawbacks

- Speed reduction.
- Cost considerations.
- Not all VPNs are equally secure.
- Some services block VPN access.
- Legal considerations in certain countries.

THANK YOU