Virtual Private Networks
VPNs

Characteristics of VPN

Encryption

- Packets between the beginning of the VPN tunnel and the termination point are encrypted to prevent packet sniffing.
- Security protocol depends on intended use. For example, WAN implementation may require TLS while many others use IPSEC.

User Authentication

- Prevents unauthorized access

Message Integrity

- Checks if message has been changed (Can provide User Integrity)

Encapsulation

IP Protocol Header

Encapsulation Protocol

Embedded protocol

- Ethernet Frame
- IPX
- Etc

Characteristics of VPN

IPSEC

- Allows full integrity checking
- Applicable for IP (Layer 3) tunneling
- Does not handle TCP (Layer 4) tunneling well (e.g. TCP Meltdown)

SSL/TLS

- Overcomes TCP meltdown effects.

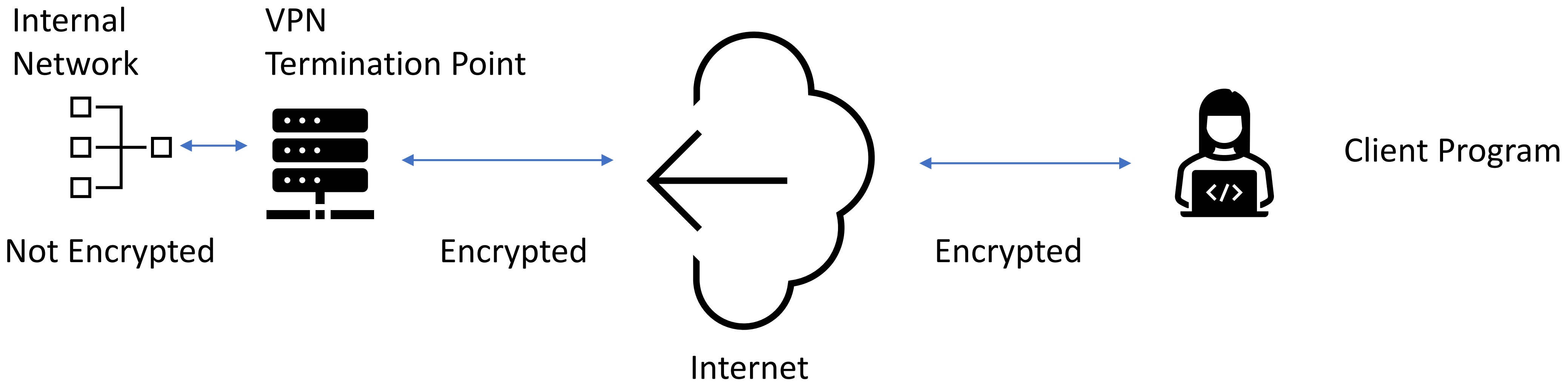
Data Link (Layer 2) Tunneling

- Encapsulates multiple protocols (i.e. IPX)
- Supports VLAN tags for trunking

Types of VPN

Remote Access

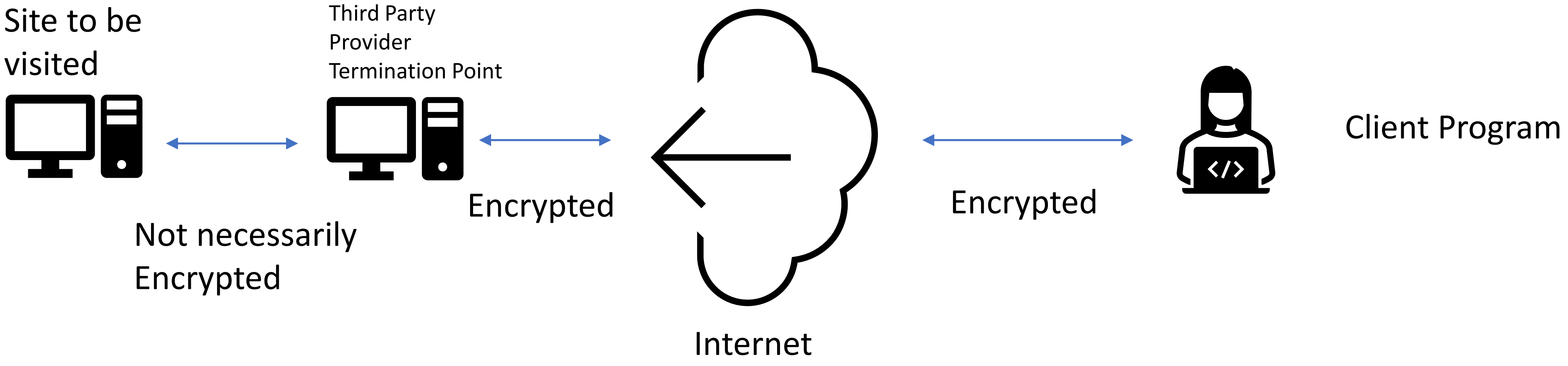
- Usually provided by an organization to give users remote access.
- Service often is housed in the router/firewall
- Client installs a local program to initiate the connection



Types of VPN

Point to Point

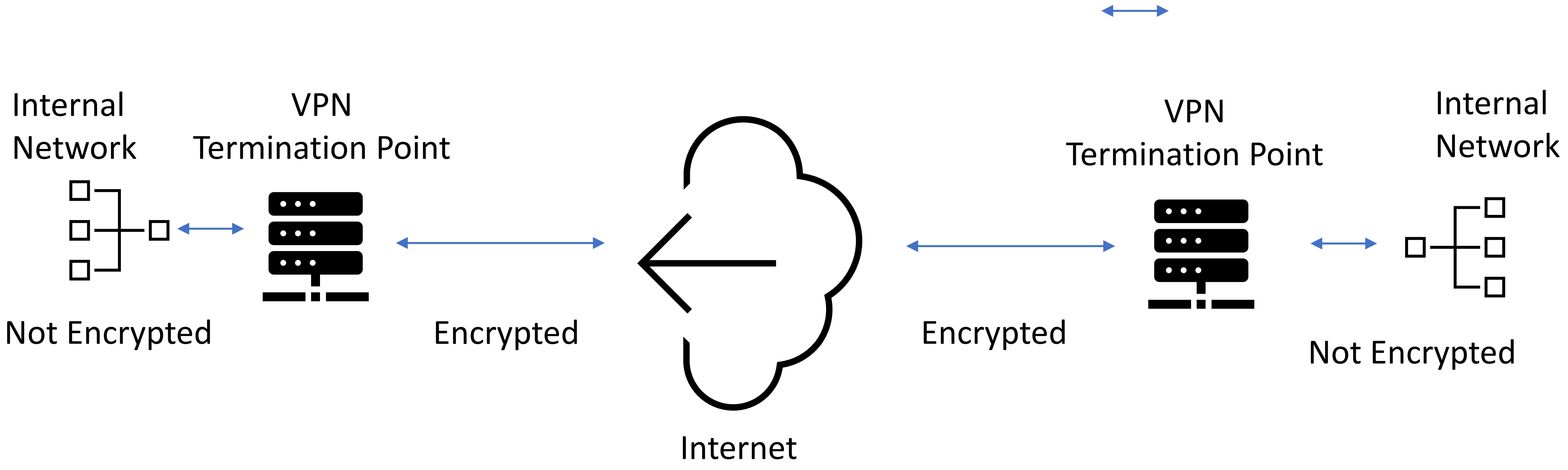
- Usually provided by a third party provider.
- Used to give the person anonymity of location and IP
- Client installs a local program to initiate the connection


Site to be visited
Third Party Provider Termination Point
Not necessarily Encrypted
Encrypted
Internet
Encrypted
Client Program

Types of VPN

Site to Site

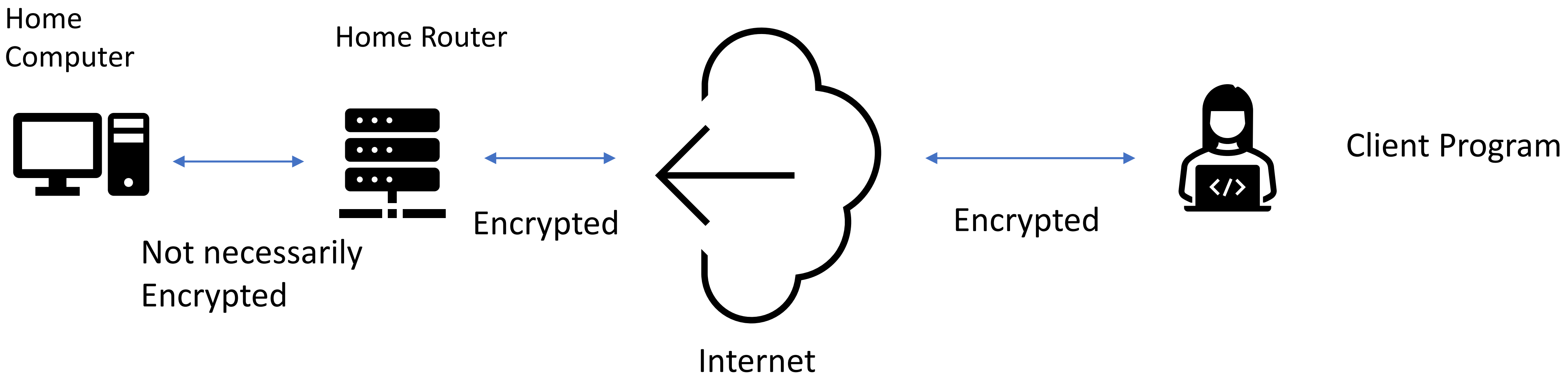
- Usually provided by an organization to extend network connections
- Service often is housed in the router/firewall



Types of VPN

Home VPN

- Used to provide you VPN access to your home computer.
- Setup VPN accounts on you computer
- Forward a port on your router to the ***private*** address of your computer.


Home Computer
Home Router
Not necessarily Encrypted
Encrypted
Internet
Encrypted
Client Program