<epam>

VPN and Proxy

TRAINING

CENTER

<epam>

What is VPN

A **virtual private network** (**VPN**) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.

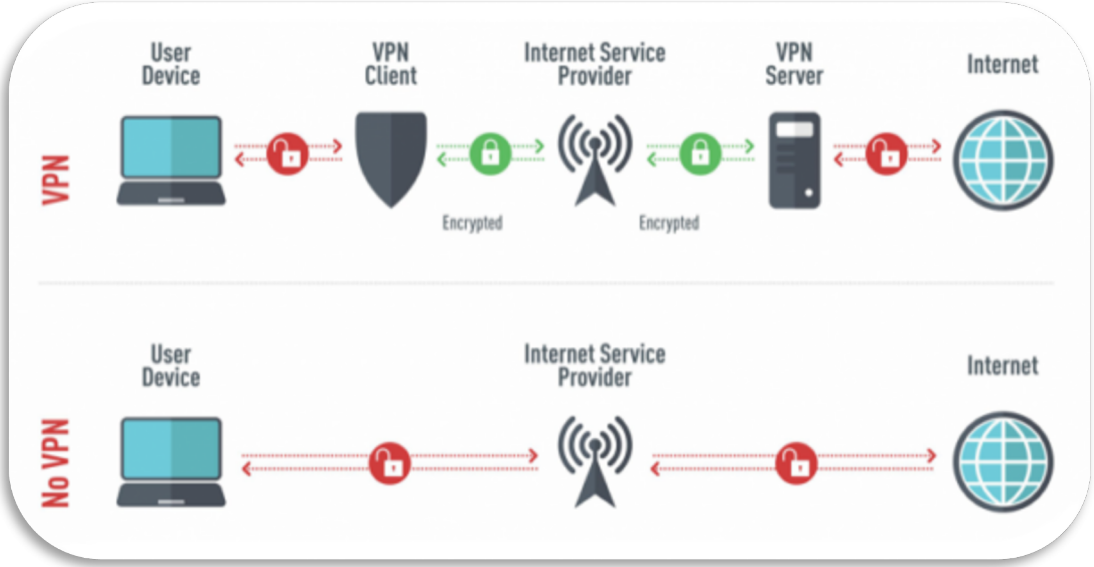
VPN privacy: What does a VPN hide?

A VPN can hide a lot of information that can put your privacy at risk.

Main of them:
- IP address and location
- Location for streaming
- Devices
- Web activity

How VPN works

A VPN can help protect against identity theft by helping protect your data. It creates an encrypted tunnel for the data you send and receive that's out of reach of cyberthieves.
A VPN can protect the information you share or access using your devices. That's especially important when using a public Wi-Fi network



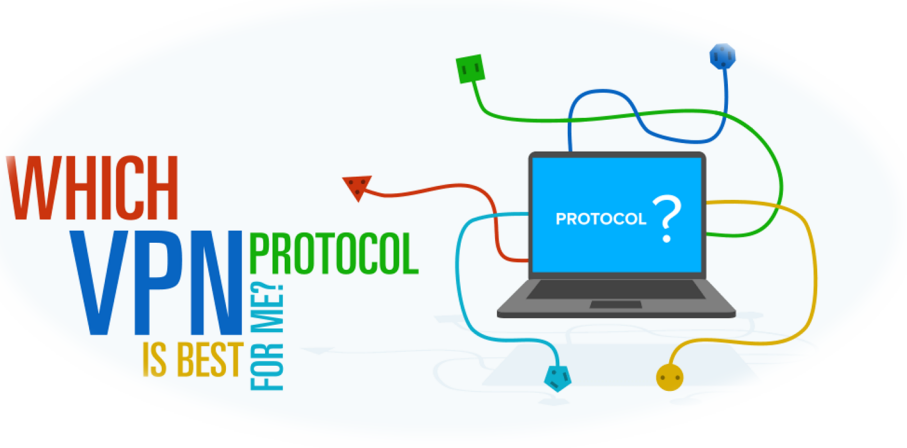
VPN types

VPNs can be characterized as **host-to-network** or ***remote access*** by connecting a single computer to a network or as *site-to-site* for connecting two networks.

VPN systems may be classified by:
- Tunneling protocol used to tunnel the traffic
- Tunnel's termination point location
- Type of topology of connections, such as site-to-site or network-to-network
- Levels of security provided
- Number of simultaneous connections

VPN protocols

A VPN protocol is basically the technology your VPN service uses to ensure you get the fastest and safest possible connection to the internet.
Combining encryption standards and transmission protocols, a VPN protocol determines how your data is transmitted between your device and the VPN server



Main of them:
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP/IPSec)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
- Internet Key Exchange, version 2 (IKEv2)
- OpenVPN
- SSH (Secure Shell)

Advantages and Disadvantages of VPN

Advantages:

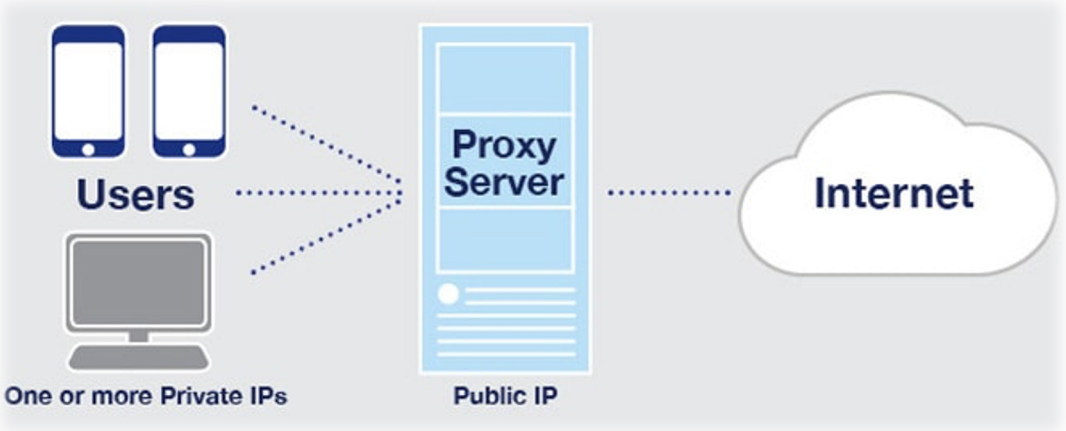
- Provides Anonymity
- Avoid Geo-restrictions
- Protection from Cyber attacks
- Prevent Bandwidth Throttling
- Improved Gaming Experience
- Bypass Firewall
- Helps you to save money

Disadvantages:

- Slowsdown the Internet Speed
- Costs more money
- Device Compatibility
- Privacy Issues
- Connection Droppings
- Configuration Difficulty
- Legality Issues

Proxy

Proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources. A proxy server potentially masking the true origin of the request to the resource server.



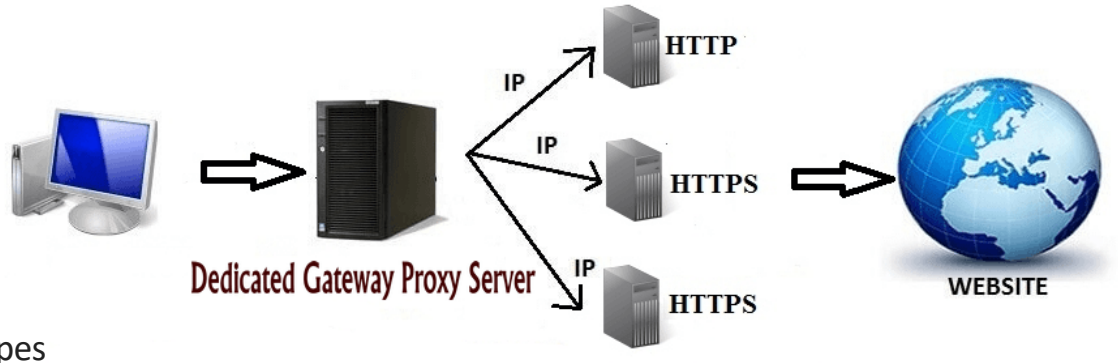
Use proxy server:
- Watching content that are restricted in certain regional areas.
- Bypassing content filters.
- To bypass restrictions to certain websites
- Hide your real IP and location.

Types and how it works

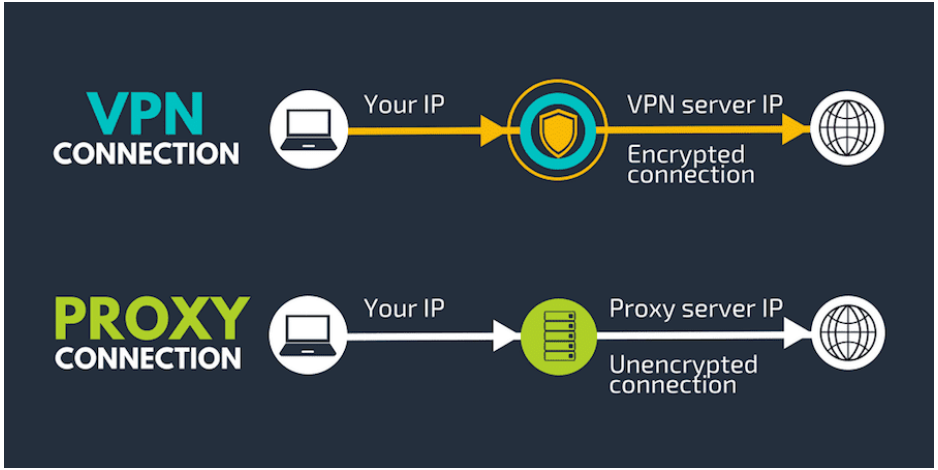
A **proxy server** acts as a middleman between your browser and the website you're accessing.

There are two main types of proxies
- **HTTP**: they can only support web traffic.
- **SOCKS**: they can support other traffic types

Unlike VPNs, when you set up a proxy connection, you don't redirect the whole internet connection.



Difference



VPN:
- Encrypts the whole internet connection
- Changes your IP
- Has its own software
- Encrypts the data being transferred
- Slower than a proxy
- More costly than a proxy

Proxy:
- Must be configured for each app
- Changes your IP
- Doesn’t have it own software
- Doesn’t encrypt the data being transferred
- Faster than a VPN
- Cheaper than a VPN