



TECHNICKÁ UNIVERZITA V LIBERCI  
Ekonomická fakulta

Obrázek 1: Logo EF TUL

Zdroj: <https://gaudeamus.cz/fakulty/detail-fakulty/facultyHash:0174f7ab9e3323106b9b3fdb0b14516e>

# Co je VPN a proč ji používat?

Vojtěch Macko

Podniková ekonomika – Management služeb

Kombinované studium

Akademický rok 2024/2025

06. 03. 2025

## Obsah

ÚVOD .....	1
Co je to VPN?.....	1
Typy připojení VPN .....	1
Historie VPN .....	2
Využití VPN .....	3
Proč používat VPN a jaké jsou její výhody? .....	3
Jaké jsou nevýhody VPN?.....	4
Na co se dívat při výběru VPN .....	4
Nejpopulárnější VPN poskytovatelé .....	6
ZÁVĚR .....	7
ZDROJE .....	7

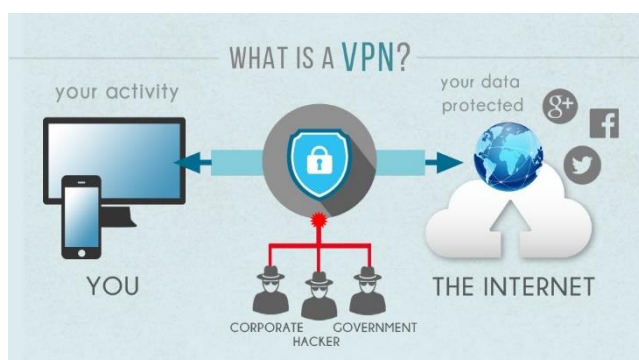
## Seznam obrázků

Obrázek 1: Logo EF TUL.....	1
Obrázek 2: Schéma fungování VPN .....	1
Obrázek 3: Typy VPN .....	1
Obrázek 4: Aplikace NordVPN .....	6
Obrázek 5: Aplikace Surfshark VPN.....	6

# ÚVOD

## Co je to VPN?

VPN (Virtual Private Network – virtuální privátní síť) je technologie, která umožňuje bezpečné a šifrované připojení k internetu. Funguje tak, že vytváří šifrovaný tunel mezi zařízením uživatele a vzdáleným serverem provozovaným poskytovatelem VPN. Tímto způsobem dochází ke skrytí skutečné IP adresy uživatele a zajištění vyšší úrovně soukromí a bezpečnosti.



Obrázek 2: Schéma fungování VPN

Zdroj: <https://www.alza.cz/slovník/co-je-vpn>

## Typy připojení VPN

Typ VPN	Popis	Příklad použití	Běžné protokoly
Vzdálený přístup (Remote Access VPN)	Připojení jednotlivých uživatelů k firemní síti nebo k internetu přes šifrované spojení.	Home office, přístup k firemním datům.	OpenVPN, IKEv2, L2TP/IPsec
Síťová VPN (Site-to-Site VPN)	Spojuje dvě nebo více celých sítí do jedné privátní sítě.	Firemní pobočky propojené přes VPN.	IPsec, MPLS VPN
Softwarová VPN	VPN běží jako aplikace na zařízení (PC, mobil, router).	Osobní VPN pro soukromí a bezpečnost.	OpenVPN, WireGuard, IKEv2
Hardwarová VPN	Dedikované zařízení (router, firewall) spravuje VPN spojení.	Firemní síť s vysokými požadavky na bezpečnost.	IPsec, OpenVPN
OpenVPN	Open-source, velmi bezpečný a flexibilní.	VPN poskytovatelé, podnikové sítě.	OpenVPN
IPsec (IKEv2, L2TP/IPsec)	Často používaný v podnikových sítích, stabilní.	Firemní VPN, mobilní zařízení.	IKEv2, L2TP/IPsec
WireGuard	Moderní, rychlý a bezpečný protokol s jednoduchým designem.	Mobilní zařízení, osobní VPN.	WireGuard
PPTP (zastaralý)	Rychlý, ale má slabé zabezpečení.	Starší zařízení, kde není jiná možnost.	PPTP

Obrázek 3: Typy VPN

Zdroj: <https://chatgpt.com> přes výstřižky

## Historie VPN

VPN technologie vznikla v 90. letech, kdy firmy hledaly bezpečný způsob připojení zaměstnanců k firemním sítím přes internet. Internet se tehdy rychle rozšiřoval, ale zároveň přinášel bezpečnostní rizika – nešifrované připojení znamenalo, že data mohla být snadno zachycena hackery.

V roce 1996 vytvořil Microsoft protokol PPTP (Point-to-Point Tunneling Protocol), který umožňoval vytvoření prvních VPN spojení. PPTP sice nebyl příliš bezpečný, ale byl první široce používanou VPN technologií.

## 2000–2010: rozvoj VPN pro osobní použití

S rostoucím počtem kybernetických útoků a sledování ze strany poskytovatelů internetu začali lidé využívat VPN i pro osobní soukromí.

- Vznikají silnější protokoly jako OpenVPN (2001) – poskytuje lepší šifrování a větší bezpečnost než PPTP.
- VPN se stává populární pro obcházení geografických blokáží (např. sledování amerického Netflixu z jiných zemí).

## 2010–současnost: masové rozšíření VPN

S rostoucími obavami o soukromí a bezpečnost se VPN stává běžnou součástí internetu. Mezi hlavní důvody nárůstu používání patří:

- **Zvýšené sledování vlád a ISP (Edward Snowden, 2013)** – lidé si začali více chránit své soukromí.
- **Cenzura internetu v některých zemích (Čína, Rusko)** – VPN pomáhá obcházet blokace.
- **Rozvoj streamovacích služeb** – VPN umožňuje přístup k obsahu omezenému na určité regiony.
- **Nové protokoly (WireGuard, IKEv2)** – zvyšují bezpečnost a rychlost VPN připojení.

Dnes se VPN používá nejen pro firemní bezpečnost, ale i pro osobní anonymitu, streaming a ochranu na veřejných sítích.

Zdroj: <https://chatgpt.com>

## Využití VPN

VPN je často využívána k ochraně osobních údajů při připojení k veřejným Wi-Fi sítím, k anonymnímu prohlížení internetu a k obcházení geografických omezení. Technologie VPN je dostupná na různých platformách, včetně počítačů, chytrých telefonů a tabletů.

## Proč používat VPN a jaké jsou její výhody?

- **Ochrana soukromí** – VPN skrývá skutečnou IP adresu uživatele a šifruje jeho internetový provoz. Díky tomu se snižuje možnost sledování online aktivit třetími stranami, jako jsou poskytovatelé internetu, inzerenti nebo vládní organizace.
- **Bezpečnost při používání veřejných Wi-Fi sítí** – veřejné Wi-Fi sítě, například v kavárnách nebo na letištích, mohou být snadným cílem pro hackery. VPN šifruje komunikaci, čímž chrání osobní a citlivé údaje, jako jsou hesla, bankovní údaje nebo e-maily.
- **Obcházení geografických omezení** – některý online obsah je dostupný pouze v určitých regionech. Pomocí VPN lze změnit IP adresu na jinou zemi a získat tak přístup k blokovánému obsahu, například ke streamovacím službám nebo sociálním sítím.
- **Anonymní prohlížení internetu** – používáním VPN lze zabránit sledování internetové aktivity poskytovateli internetu a dalšími subjekty. To je užitečné zejména v zemích s omezenou internetovou svobodou.
- **Bezpečný vzdálený přístup** – firmy často využívají VPN pro bezpečné připojení zaměstnanců k firemním sítím na dálku. To umožňuje efektivní práci odkudkoli bez rizika úniku citlivých dat.
- **Ochrana před cenzurou a vládním dohledem** – v některých zemích je internet přísně cenzurován a monitorován. VPN pomáhá obejít cenzuru a poskytuje přístup k necenzurovanému obsahu.

- **Šetření peněz při online nákupech** – ceny některých produktů a služeb (například letenek, hotelů nebo streamovacích služeb) se mohou lišit v závislosti na geografické poloze uživatele. Změnou IP adresy pomocí VPN lze získat lepší nabídky.

## **Jaké jsou nevýhody VPN?**

- **Snížení rychlosti internetu** – kvůli šifrování a přesměrování provozu přes servery může dojít ke zpomalení připojení.
- **Důvěra ve poskytovatele VPN** – některé VPN (hlavně zdarma) mohou zaznamenávat uživatelská data a prodávat je třetím stranám.
- **Kompatibilita s některými službami** – některé weby a streamovací služby blokují VPN servery, což může ztížit přístup.
- **Cena kvalitní VPN** – dobré VPN nejsou zdarma a jejich předplatné může být pro některé uživatele nákladné.
- **Možné legální problémy** – použití VPN je v některých zemích regulováno nebo zakázáno.

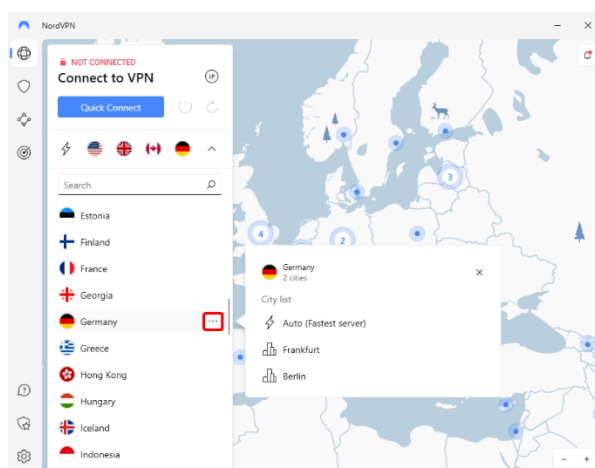
## **Na co se dívat při výběru VPN**

- **Bezpečnost a šifrování** – zjistěte, jaká šifrování VPN poskytuje. Doporučuje se vybrat službu se sofistikovanými šifrovacími algoritmy, jako je například 256bitové šifrování AES-256, které patří v současnosti mezi nejbezpečnější.
- **Protokoly** – VPN aplikace obvykle podporuje různé protokoly, jako je např. OpenVPN, WireGuard, IKEv2/IPSec nebo SSTP. Každý z protokolů má své výhody a nevýhody v rychlosti a bezpečnosti. Protokol OpenVPN je obecně považován za nejlepší dostupný protokol.

- **Placené služby vs. VPN zdarma** – obezřetnost je na místě při používání bezplatných služeb, jelikož některé z nich mohou sbírat vaše osobní údaje a prodávat je třetím stranám. Placené služby obvykle nabízejí lepší zabezpečení a rychlost než bezplatné VPN.
- **Rychlost a výkon** – podívejte se na rychlost a výkon VPN serverů, zejména pokud plánujete streamovat videa nebo hrát online hry.
- **Počet serverů a umístění** – zkontrolujte, kolik serverů má VPN a ve kterých zemích jsou umístěny. Čím více serverů a rozmanitější geografické pokrytí síť nabízí, tím větší máte flexibilitu IP adres.
- **Bezplatné zkušební období nebo záruka vrácení peněz** – ujistěte se, že VPN nabízí zkušební období nebo záruku vrácení peněz, abyste mohli otestovat službu a případně ji vrátit, pokud vás neuspokojí.
- **Uživatelská přívětivost a technická podpora** – služba by měla být snadno použitelná a měla by mít uživatelsky přívětivé rozhraní. Recenze snadno najdete na internetu v počítačových online magazínech. Také se ujistěte, že služba poskytuje dostatečnou technickou podporu v případě potřeby.
- **Záznamy dat** – zjistěte, jaká data poskytovatel ukládá o vaší činnosti na internetu. Pokud preferujete co největší anonymitu, hledejte službu, která neuchovává žádné záznamy o online aktivitách svých uživatelů.
- **Reputace** – Chcete-li získat dostatečné povědomí o tom, jak konkrétní VPN funguje, přečtěte si spotřebitelské i profesionální recenze. Při výběru si dávejte bedlivý pozor, protože se v současnosti na internetu vyskytuje řada produktů, které se jako VPN pouze tváří.
- **Sdílené IP adresy**– Zvolte si VPN, která nabízí sdílené IP adresy. Když se přes jednu IP adresu budete připojovat společně s více anonymními uživateli, vaše soukromí bude chráněno lépe.

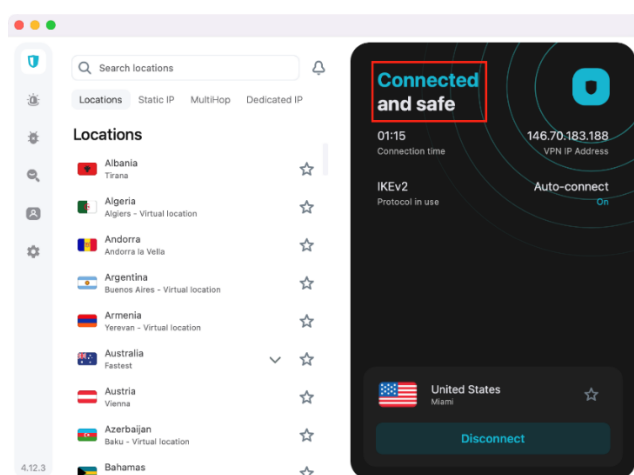
## Nejpopulárnější VPN poskytovatelé

- NordVPN
- Surfshark
- Express VPN
- CyberGhost
- Private Internet Access
- Proton VPN
- Atlas VPN
- ESET a Avast VPN



Obrázek 4: Aplikace NordVPN

Zdroj: <https://support.nordvpn.com/hc/en-us/articles/19472023025169-Installing-and-using-NordVPN-on-Windows-10-and-11>



Obrázek 5: Aplikace Surfshark VPN

Zdroj: <https://support.surfshark.com/hc/en-us/articles/360003089093-How-to-make-sure-if-Surfshark-VPN-is-working>



## ZÁVĚR

Osobní zkušenost s používáním VPN nemám, protože jsem zatím neměl potřebu a důvod VPN využívat, ale to se může kdykoliv změnit. I když s VPN nemám zkušenost, i tak jsem si toto téma vybral, protože je extrémně zajímavé a vědět o něm něco více považuji za důležité, hlavně v dnešní době, kdy je důležité chránit svoje osobní údaje a zajistit jim jejich bezpečnost, před jakýmkoliv kybernetickými útoky.

## ZDROJE

Informace:

- <https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-vpn>
- <https://www.mozilla.org/cs/products/vpn/more/what-is-a-vpn>
- <https://www.eset.com/cz/vpn/>
- <https://www.webhostingcentrum.cz/vpn>
- <https://blog.avast.com/cs/co-je-vpn-a-jak-funguje>
- <https://chatgpt.com>

Ostatní zdroje:

- Google obrázky