# Jak funguje VPN?

protonvpn.com/blog/how-does-a-vpn-work

Douglasem Crawfordem, Douglas Crawford November 4, 2020

Virtuální privátní síť (VPN) poskytuje soukromí a řadu dalších výhod při připojení k internetu. Náš příspěvek na blogu Co je to VPN? vysvětluje, co tato technologie dělá, a některé důvody, proč by mohlo být užitečné nainstalovat si do zařízení vlastní VPN.

V tomto článku půjdeme hlouběji a vysvětlíme techničtější aspekty fungování VPN způsobem, který snadno pochopí každý.

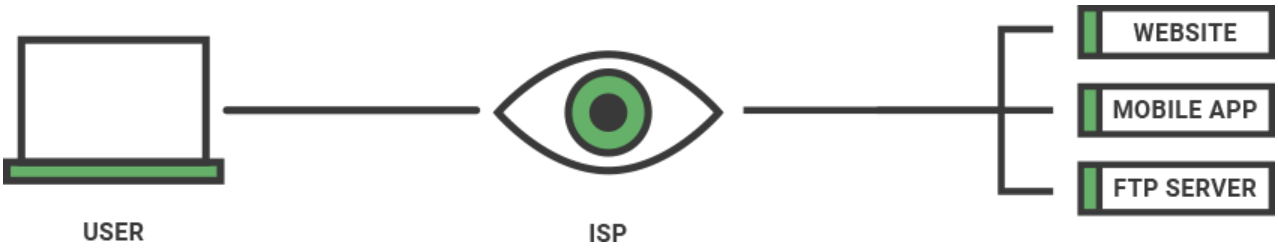
Začneme některými základy internetu a pak si povíme, jak VPN zapadá do obrázku, a na konci bude následovat sekce otázek a odpovědí.

## Jak funguje internet (bez VPN)

Váš poskytovatel internetových služeb (ISP) připojí vaše zařízení k internetu, takže veškerá data mezi vaším zařízením a servery (např. weby), ke kterým se na internetu připojujete, proudí přes servery vašeho poskytovatele internetu. Každému zařízení na internetu je přiděleno jedinečné číslo známé jako IP adresa.

Když do adresního řádku prohlížeče zadáte adresu URL webové stránky, váš prohlížeč odešle vašemu poskytovateli internetových služeb požadavek známý jako DNS dotaz, ve kterém vás požádá o správnou IP adresu pro počítač, ke které se chcete připojit.

DNS je podobný velkému telefonnímu seznamu, který mapuje adresy URL jako „protonvpn.com“ na jejich odpovídající IP adresy. Jakmile váš prohlížeč získá správnou IP adresu od vašeho ISP, zahájí spojení s webovou stránkou (nebo jiným internetovým zdrojem).



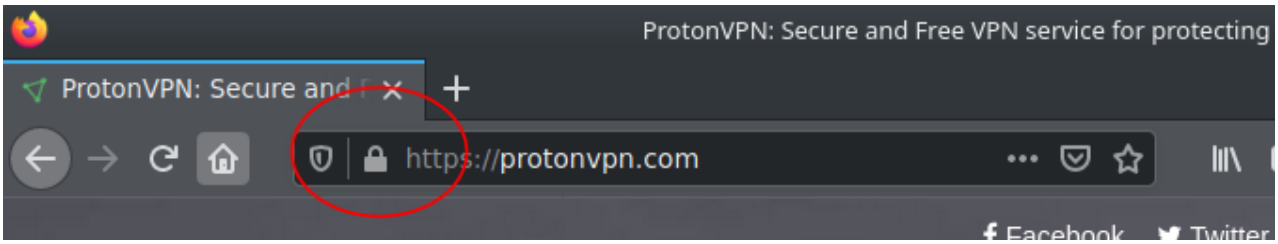

## Co vidí váš ISP

Váš ISP (jako je Verizon, Vodafone nebo Comcast) zná IP adresu routeru, který používáte, a čí účet patří. Také ví, které webové stránky jste navštívili, protože téměř každý ISP na světě zaznamenává dotazy DNS, které zpracovává (spolu s časovým razítkem, kdy dotaz zadáváte).

I když váš ISP neprovádí vyhledávání DNS (například pokud jste ručně zadali IP adresu nebo použili službu DNS třetí strany), stále vidí požadavek DNS, protože obvykle nejsou šifrovány.

V posledních letech došlo k nárůstu služeb DNS třetích stran, které ve skutečnosti šifrují dotazy DNS na ně. To je dobré, ale váš ISP stejně vidí, kterou webovou stránku navštěvujete, a to díky skutečnosti, že i když je dotaz DNS zašifrován, informace o cíli IP potřebné pro správné směrování vašich dat nikoli.

HTTPS je šifrovací protokol, který zabezpečuje spojení mezi webem a vaším zařízením. Z velké části díky hrdinskému úsilí kampaně Let's Encrypt se používání HTTPS stále více stává normou, spíše než výjimkou, jakou tomu bylo ještě před několika málo lety.




Zavřený visací zámek v adresním řádku vašeho prohlížeče znamená, že se používá HTTPS.

Bez HTTPS může váš ISP vidět vše, co na webu děláte. To zahrnuje jednotlivé stránky, které navštěvujete, veškeré platební údaje, které zadáte, a údaje z formuláře, které odešlete. HTTPS tomu brání. I když se používá HTTPS, váš ISP může stále vidět a zaznamenávat, které webové stránky navštěvujete (jen ne to, co na nich děláte).

A co vidí váš ISP, může vidět i vaše vláda.

### Co mohou weby vidět

Webové stránky mohou vidět poslední IP adresu v řetězci spojení mezi vaším zařízením a webovým serverem. Bez VPN se jedná o jedinečnou IP adresu, kterou váš ISP přidělil vašemu routeru.

Webové stránky tyto informace běžně zaznamenávají spolu s časovými razítky, frekvencí a délkou návštěv, aby porozuměly tomu, jak je webová stránka používána a jak funguje. Pokud by policie potřebovala identifikovat konkrétního uživatele těchto webových stránek, stačí požádat poskytovatele internetových služeb, aby identifikoval zákazníka, kterému přidělila tuto IP adresu.

Identifikovat jedince tímto způsobem je samozřejmě dost neobvyklé. Někdy to může dokonce vyžadovat právní nátlak, ačkoli většina ISP je ráda, že dobrovolně spolupracuje s legitimními požadavky vymáhání práva.

I když vás vaše IP adresa jednoznačně neidentifikuje, vaše IP adresa webům vždy sděluje, ve které zemi se nacházíte a pravděpodobně i ve kterém městě. Je to díky tomu, že ISP obvykle přidělují IP adresy

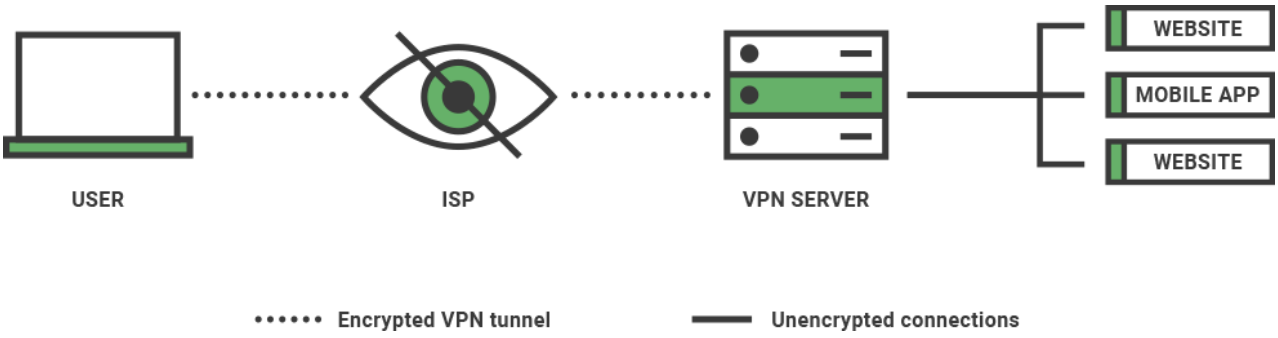
domácím uživatelům ve stejné geografické blízkosti v blocích a databáze, kde byly tyto bloky IP přiděleny, jsou veřejně dostupné.

**Stručně řečeno, internet nebyl stavěn pro soukromí, takže byste ho neměli očekávat, když jej používáte tak, jak je.**

## S VPN

Když na svém zařízení používáte aplikaci VPN, naváže šifrované připojení k serveru VPN. Toto připojení se provádí přes internet (takže stále potřebujete svého ISP) a často se nazývá „tunel VPN“.

Tento server VPN zpracovává všechny dotazy DNS a funguje jako prostředník, který sedí mezi vaším zařízením a internetem a směruje vaše data do správných cílů.




### Co vidí váš ISP

Váš ISP vidí, že jste připojeni k IP adrese patřící k serveru. Nebude automaticky vědět, že se jedná o VPN server, ale Sherlock Holmes by na to nemusel přijít, protože je to jediná IP adresa, ke které se zřejmě připojujete.

Nevidí žádné webové stránky nebo jiné internetové zdroje, ke kterým se připojujete prostřednictvím serveru VPN. Je to proto, že server VPN zpracovává dotazy DNS a směruje vaše data na správnou IP adresu.

Váš ISP také nevidí obsah vašich dat (včetně dat o cíli IP a požadavků na vyhledávání DNS), protože všechna data putující mezi vaším zařízením a serverem VPN jsou šifrována.

Když tedy používáte VPN, váš ISP nevidí, které webové stránky navštěvujete, a nemůže vidět obsah vašich dat (i když se nepoužívá HTTPS). Totéž platí pro hackery WiFi, provozovatele veřejných WiFi routerů nebo kohokoli jiného, kdo by za normálních okolností mohl vidět vaše data, když cestují mezi vaším zařízením a jeho cílem.

### Co vidí weby

Při použití VPN je poslední IP adresou v řetězci připojení mezi vaším zařízením a webovým serverem adresa VPN serveru. Server VPN proto chrání vaši skutečnou IP adresu před navštívenými weby, které uvidí pouze IP adresu serveru VPN.

Kromě jasných výhod ochrany soukromí je tato funkce VPN užitečná při zfalšování vaší geografické polohy, protože se zdá, že máte přístup k internetu odkudkoli, kde se nachází server VPN.

### Co vidí server VPN

Poskytovatel VPN v mnoha ohledech přebírá roli vašeho ISP. Zpracovává DNS dotazy a dokáže sledovat IP adresy, které navštěvujete.

Přestože je připojení mezi vaším zařízením a serverem VPN šifrováno sítí VPN, připojení mezi serverem VPN a navštívenými weby nikoli. To znamená, že (jako váš ISP obvykle může) server VPN zobrazit obsah provozu, který není chráněn protokolem HTTPS.

Je proto velmi důležité vybrat si službu VPN, která je důvěryhodná a bezpečná.

## Jak Proton VPN zajišťuje soukromí a transparentnost

Ve společnosti Proton je náš závazek k ochraně soukromí uživatelů dobře znám. Proton VPN a Proton Mail , největší poskytovatel šifrovaných služeb na světě, jsou důvěryhodnými novináři a aktivisty v této oblasti a podnikli jsme řadu kroků k posílení vaší bezpečnosti a soukromí:

- Na rozdíl od většiny ISP neuchováváme **žádné záznamy** , které by mohly ohrozit vaše soukromí. Uchovává se časové razítko vašeho posledního úspěšného pokusu o přihlášení, ale toto není spojeno s IP adresou, ze které se připojujete, ani s žádnou aktivitou při používání naší služby.
- Všechny naše aplikace jsou **plně auditované** a **mají otevřený zdrojový kód** , takže je může zkontrolovat každý.
- Sídlíme ve **Švýcarsku , zemi, která nemá žádné vazby na alianci pro hromadné sledování** Five Eyes pod vedením USA a která má jedny z nejpřísnějších zákonů na ochranu osobních údajů na světě.
- Používáme pouze nejbezpečnější **protokoly VPN** se **silným šifrováním** a **dopředným utajením** .
- Nabízíme speciálně odolnou **službu Secure Core VPN** pro ty, kteří ji potřebují.
- Naše aplikace nabízejí **ochranu proti úniku DNS** , aby bylo zajištěno, že vyhledávání DNS zpracovává výhradně Proton. **Ochrana proti úniku IPv6** zajišťuje, že žádná data nebudou nikdy směrována mimo tunel VPN.

## FAQ

### Co je šifrování?

Šifrování je matematický proces, který převádí data na nečitelné znaky, takže k nim nemá přístup nikdo bez správného klíče. Je to základní kámen pro udržení vašich dat v bezpečí na internetu. Proton VPN používá pouze ty nejsilnější šifrovací sady; Další informace naleznete v našem příspěvku o silném šifrování .

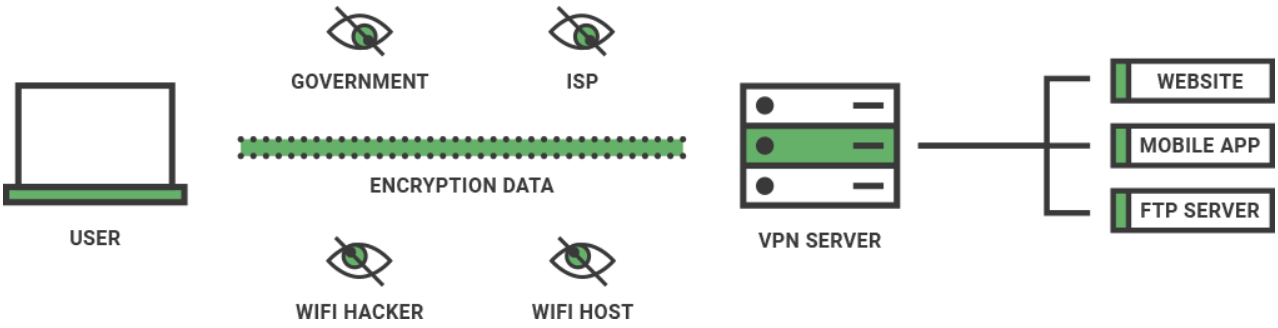
### Co je AES-256?

AES je šifrovací šifra se symetrickým klíčem používaná k zabezpečení velkých částí dat v klidu. AES-256 je implementován AES s 256bitovou velikostí klíče, což je jeho nejsilnější nastavení.

AES je schválen NIST a americká vláda zabezpečuje svá přísně tajná data pomocí AES-256. To vedlo mnoho služeb VPN, které používají AES-256 k popisu svého šifrování termíny jako „vojenská úroveň“. AES-256 je skutečně velmi bezpečný, ale je to pouze jedna z komponent potřebných k zajištění bezpečného připojení VPN.

## Co je šifrovací tunel nebo tunel VPN?

Síť VPN šifruje vaše data, když cestují mezi vaším zařízením a serverem VPN, a tak zabrání tomu, aby kdokoli, kdo by jinak měl k datům přístup (jako váš ISP nebo operátor veřejného routeru), viděl její obsah.




Jednotlivé „balíčky“ dat jsou zašifrovány na vašem zařízení a poté dešifrovány na serveru VPN. Analogie s tunelem je užitečný způsob, jak přemýšlet o tomto šifrovaném spojení.

## Co je protokol VPN?

Protokol VPN je sada pokynů používaných k vytvoření zabezpečeného spojení mezi dvěma počítači (vaším zařízením a serverem VPN). Existují různé protokoly VPN, ale Proton VPN podporuje **OpenVPN** , **IKEv2** a **WireGuard** .

**OpenVPN** – Bitvami testovaný protokol VPN, který je stále široce považován za poslední slovo, pokud jde o zabezpečení VPN.

**IKEv2** – Modernější protokol VPN, který je rychlý a zároveň je odborníky považován za velmi bezpečný.

**L2TP/IPsec** – Ačkoli se NSA domnívá, že je kompromitován, ve většině případů je tento protokol stále považován za bezpečný. Byl však nahrazen nadřazeným IKEv2.

**PPTP**– Vysoce nezabezpečený protokol, který někteří poskytovatelé nadále podporují z důvodů kompatibility.

**WireGuard** – Zcela nový protokol VPN, který je sice rychlý a bezpečný (alespoň teoreticky), ale stále je experimentální. Proton VPN s velkým zájmem sleduje vývoj WireGuard (nyní mimo beta fázi na Linuxu) a pomohla financovat jeho vývoj.

*Další informace o protokolech VPN.*

## Zpomalí VPN můj internet?

Ano, ale ne příliš. Šifrování a dešifrování vašich dat vyžaduje výpočetní výkon, který teoreticky může zpomalit vaše internetové připojení. V praxi zvládnou šifrování VPN bez znatelného zpomalení i moderní smartphony nižší třídy.

Větší problém je, jak daleko vaše data putují. Připojení k serveru VPN přidává další „nohu“ na jeho cestě, což jej nevyhnutelně zpomaluje. To platí zejména v případě, že se server VPN, ke kterému se připojujete, nachází na druhé straně světa než vy.

Pokud se však připojíte k serveru VPN poměrně blízko (například kdekoli v Evropě, pokud sídlíte v Evropě), je nepravděpodobné, že si všimnete jakéhokoli zpomalení. Kromě toho náš jedinečný **VPN Accelerator**Technologie může za určitých podmínek zvýšit rychlost o více než 400 % a je zvláště účinná při zmírňování ztráty rychlosti při připojování ke geograficky vzdáleným serverům.

*Zjistěte více o VPN Accelerator*

Dalším faktorem, který je třeba zvážit, je „zatížení serveru“ VPN

serveru, který používáte. To znamená, kolik lidí jej používá ve stejnou dobu jako vy a tím klade nároky na jeho zdroje.

To je jediný důvod, proč naše bezplatné servery, které mohou být ve špičce trochu vytížené, ne vždy umožňují rychlosti, které jsou k dispozici při používání našich serverů Plus, které bývají méně vytížené.

## Co je ochrana proti úniku IPv6?

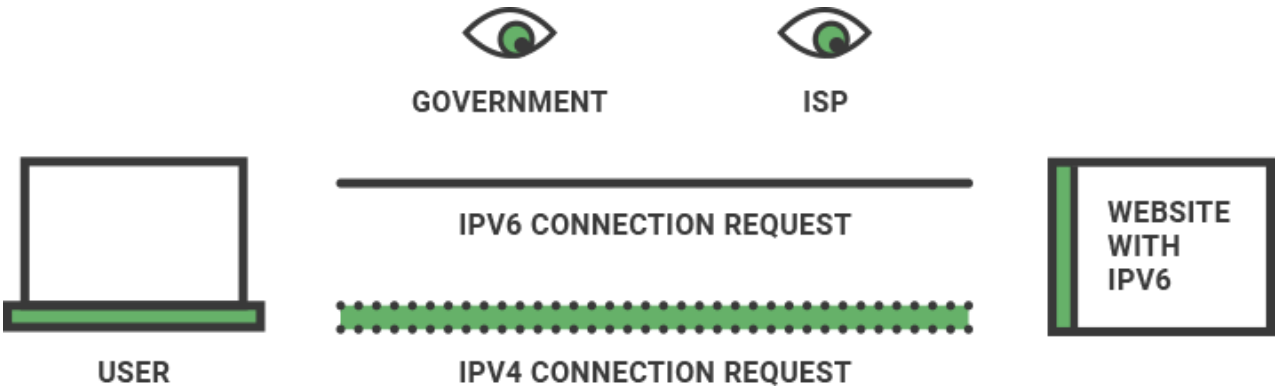
Každému zařízení připojenému k internetu je přiděleno jedinečné číslo pro jeho identifikaci. Obrovský rozmach internetu v posledních letech však znamená, že čísla přidělená pomocí starého systému IPv4 docházejí. Rychle.

IPv6 řeší tento problém pomocí 128bitových webových adres, čímž zpřístupňuje přibližně 2^128 ( kolem 340 miliard miliard miliard miliard) nových čísel, což by nás mělo udržet v chodu na nějakou dobu.

Všechny moderní operační systémy podporují IPv6, ale většina internetu stále používá IPv4. Jako hybridní kompromisní řešení tohoto problému bude vaše zařízení odesílat požadavky na připojení webům, které navštěvujete, pomocí jejich adres IPv4 i IPv6.

Pokud webová stránka podporuje IPv6, přijme připojení IPv6. Pokud podporuje pouze IPv4, nebude si ani uvědomovat pokus o připojení IPv6 a zahájí připojení IPv4.

Mnoho aplikací VPN z jiných služeb VPN je také pouze IPv4, a proto pouze směruje připojení IPv4 tunelem VPN. Když je navázáno připojení IPv6, aplikace VPN si toho není vědoma a připojení je tedy směrováno vaším operačním systémem mimo tunel VPN.




Web, ke kterému jste se připojili, tedy může vidět vaši skutečnou IPv6 adresu, i když používáte VPN. Toto je únik IPv6.

Aplikace Proton VPN ve výchozím nastavení blokují veškerý provoz IPv6, aby se tak nestalo. Na naši zkušenost s internetem to nemá žádný vliv.

## Co je ochrana proti úniku DNS?

Při použití VPN mají dotazy DNS procházet tunelem VPN, takže je může vidět a řešit pouze služba VPN. K úniku DNS dochází, když je požadavek DNS nějakým způsobem směrován mimo tunel VPN, takže jej může vidět (a obvykle také vyřešit) váš ISP.

Existuje řada důvodů, proč k tomu může dojít, a přestože Windows bývá nejhorším pachatelem, může se to stát na jakékoli platformě. Ochrana proti úniku DNS řeší problém pomocí pravidel brány firewall, aby zajistila, že žádný provoz nemůže opustit vaše zařízení mimo tunel VPN.

## Můžete nás sledovat na sociálních sítích, abyste měli přehled o nejnovějších verzích Proton VPN:

Chcete-li zdarma získat šifrovaný e-mailový účet Proton Mail, navštivte proton.me/mail