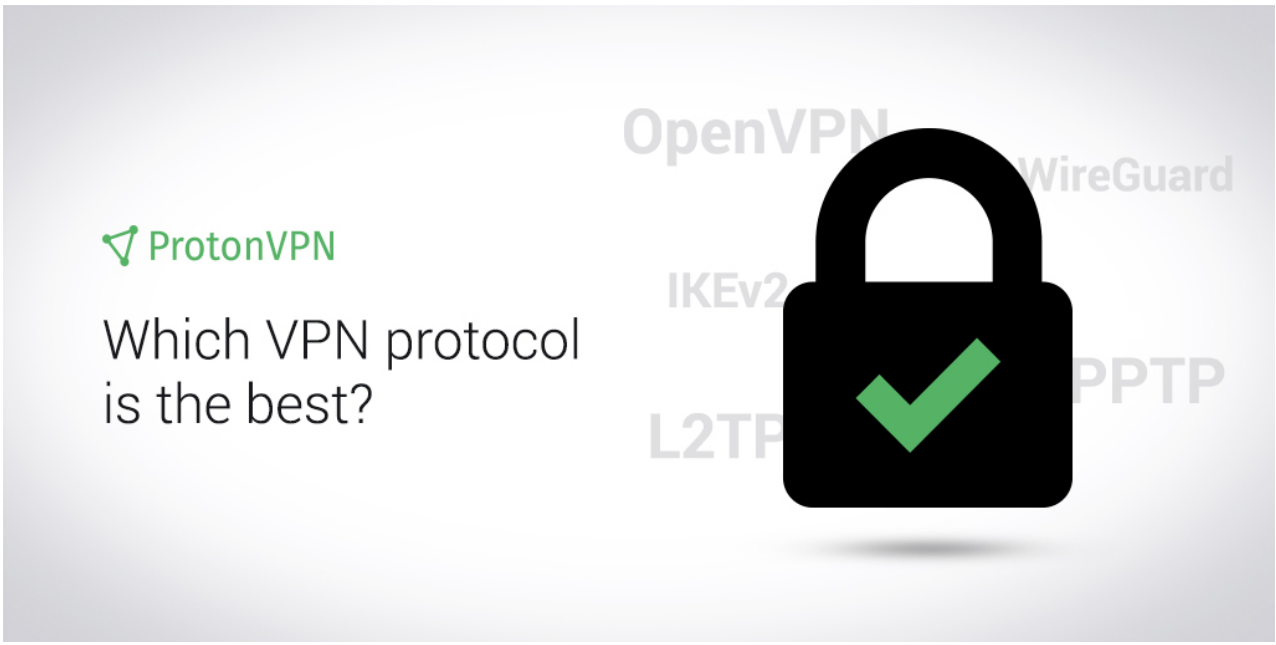
Který protokol VPN je nejlepší?

protonvpn.com/blog/whats-the-best-vpn-protocol

Richie Kochem, Richie Koch May 27, 2019



Tento článek byl aktualizován, aby zahrnoval protokoly WireGuard a Stealth VPN.

Vysvětlíme, co je protokol VPN a k čemu slouží. Porovnáváme také silné a slabé stránky nejběžnějších protokolů, včetně OpenVPN, WireGuard, IKEv2, PPTP a L2TP.

Než důvěřujete VPN, že chrání vaši internetovou aktivitu, musíte se ujistit, že zavedla nezbytná ochranná opatření. Vyhodnocení techničtějších aspektů VPN může být obtížné. Často to znamená, že se snažíte porozumět abecední polévce různých zkratek.

Zahájili jsme sérii příspěvků, ve kterých vysvětlujeme některá naše bezpečnostní opatření, aby lidé mohli činit informovanější rozhodnutí. Náš první příspěvek vysvětlil, co znamená HMAC SHA-384 . Tento příspěvek prozkoumá protokoly VPN, co dělají, jak fungují a co to znamená, pokud služba VPN používá například OpenVPN přes L2TP.

Tento příspěvek se ponoří do některých vnitřních funkcí VPN. I když se snažíme pojmy jasně vysvětlit, tento příspěvek bude užitečnější, pokud přijdete s některými základními technickými znalostmi. Pokud si nejste jisti, jak VPN funguje, může být užitečné přečíst si níže odkazovaný článek, než budete pokračovat.

Přečtěte si, jak funguje VPN

Protokoly VPN

VPN spoléhají na to, co se nazývá „tunelování“ k vytvoření privátní sítě mezi dvěma počítači přes internet. Protokol VPN, také známý jako „protokol tunelování“, jsou pokyny, které vaše zařízení používá k vyjednávání zabezpečeného šifrovaného připojení, které tvoří síť mezi vaším počítačem a jiným počítačem.

Protokol VPN se obvykle skládá ze dvou kanálů: datového kanálu a řídicího kanálu. Řídicí kanál je zodpovědný za výměnu klíčů, ověřování a výměny parametrů (jako je poskytování IP nebo tras a serverů DNS). Datový kanál, jak jste možná uhodli, je zodpovědný za přenos vašich dat o internetovém provozu. Tyto dva kanály společně vytvářejí a udržují bezpečný tunel VPN. Aby však vaše data prošla tímto bezpečným tunelem, musí být zapouzdřena.

Zapouzdření je, když protokol VPN odebírá bity dat, známé jako datové pakety, z vašeho internetového provozu a umísťuje je do jiného paketu. Tato další vrstva je nezbytná, protože konfigurace protokolů, které vaše VPN používá v datovém kanálu, nemusí být nutně stejné jako běžné internetové použití. Dodatečná vrstva umožňuje vašim informacím cestovat tunelem VPN a dostat se na správné místo určení.

To vše je trochu technické, takže široký přehled: Když se připojíte k serveru VPN, VPN použije svůj řídicí kanál k vytvoření sdílených klíčů a připojení mezi vaším zařízením a serverem. Jakmile je toto spojení navázáno, datový kanál začne přenášet váš internetový provoz. Když VPN diskutuje o silných a slabých stránkách svého

výkonu nebo mluví o „zabezpečeném VPN tunelu“, mluví o svém datovém kanálu. Po vytvoření tunelu VPN má řídicí kanál za úkol udržovat stabilitu připojení.

PPTP

Point-to-Point Tunneling Protocol (PPTP) je jedním ze starších protokolů VPN. Původně byl vyvinut s podporou společnosti Microsoft, a proto všechny verze Windows a většina ostatních operačních systémů mají nativní podporu pro PPTP.

PPTP používá protokol Point-to-Point Protocol (PPP), který je sám o sobě jako proto-VPN. Navzdory tomu, že je PPP poměrně starý, může autentizovat uživatele (obvykle pomocí MS-CHAP v2) a zapouzdřit samotná data, což mu umožňuje zvládnout povinnosti řídicího kanálu i datového kanálu. PPP však nelze směrovat; nelze jej samostatně odeslat přes internet. PPTP tedy znovu zapouzdří data zapouzdřená PPP pomocí generického zapouzdření směrování (GRE), aby vytvořil svůj datový kanál.

Bohužel PPTP nemá žádné vlastní šifrovací nebo autentizační funkce. Při implementaci těchto funkcí spoléhá na PPP – což je problematické, protože autentizační systém PPP a šifrování, které do něj Microsoft přidal, MPPE, jsou slabé.

Šifrování: protokol Microsoft Point-to-Point Encryption (MPPE), který používá algoritmus RSA RC4. Maximální síla MPPE je 128bitové klíče.

Rychlost: Protože jeho šifrovací protokoly nevyžadují velký výpočetní výkon (RC4 a pouze 128bitové klíče), PPTP udržuje vysoké rychlosti připojení.

Známá zranitelnost: PPTP má od roku 1998 řadu známých zranitelností. Jedna z nejzávažnějších zranitelností využívá nezapouzdřenou autentizaci MS-CHAP v2 k provedení útoku typu man-in-the-middle (MITM).

Porty firewallu: TCP port 1723. Použití GRE v PPTP znamená, že nemůže procházet firewallem pro překlad síťových adres a je jedním z nejjednodušších protokolů VPN k blokování. (NAT firewall umožňuje několika lidem sdílet jednu veřejnou IP adresu současně. To je důležité, protože většina jednotlivých uživatelů nemá svou vlastní IP adresu.)

Stabilita: PPTP není tak spolehlivý a ani se neobnovuje tak rychle jako OpenVPN přes nestabilní síťová připojení.

Závěr: Pokud máte obavy o zabezpečení svých dat, není důvod používat PPTP. Dokonce i Microsoft doporučil svým uživatelům, aby upgradovali na jiné protokoly VPN, aby ochránili svá data.

L2TP/IPSec

Protokol tunelování druhé vrstvy (L2TP) měl nahradit PPTP. L2TP zvládne autentizaci samostatně a provádí zapouzdření UDP, takže svým způsobem může tvořit jak řídicí, tak datový kanál. Podobně jako PPTP však sám o sobě žádné šifrování nepřidává. I když L2TP může odesílat PPP, aby se předešlo inherentním slabostem PPP, L2TP je obvykle spárován se sadou zabezpečení internetového protokolu (IPSec), aby zvládl jeho šifrování a autentizaci.

IPSec je flexibilní rámec, který lze použít pro VPN a také pro směrování a zabezpečení na úrovni aplikací. Když se připojíte k serveru VPN pomocí L2TP/IPSec, IPSec vyjedná sdílené klíče a ověří připojení zabezpečeného řídicího kanálu mezi vaším zařízením a serverem.

IPSec pak data zapouzdří. Když IPSec provede toto zapouzdření, použije ověřovací hlavičku a použije Encapsulation Security Payload (ESP). Tyto speciální hlavičky přidávají digitální podpis ke každému paketu, takže útočníci nemohou manipulovat s vašimi daty, aniž by upozornili server VPN.

ESP šifruje zapouzdřené datové pakety, aby je nemohl přečíst žádný útočník (a v závislosti na nastavení VPN datový paket i ověřuje). Jakmile IPSec data zapouzdří, L2TP tato data znovu zapouzdří pomocí UDP, aby mohla procházet datovým kanálem.

Několik protokolů VPN, včetně IKEv2, používá šifrování IPSec. Přestože je IPSec obecně bezpečný, je velmi složitý, což může vést ke špatné implementaci. L2TP/IPSec je podporován na většině hlavních operačních systémů.

Šifrování: L2TP/IPSec může používat šifrování 3DES nebo AES, ačkoli vzhledem k tomu, že 3DES je nyní považováno za slabou šifru, používá se jen zřídka.

Rychlost: L2TP/IPSec je obecně pomalejší než OpenVPN při použití stejné síly šifrování. Je to způsobeno především tím, že šifrování AES používané OpenVPN je na většině běžných procesorů hardwarově akcelerované.

Známá zranitelnost: L2TP/IPSec je pokročilý protokol VPN, ale uniklá prezentace NSA naznačuje, že zpravodajská agentura již našla způsoby, jak s ním manipulovat. Navíc kvůli složitosti IPSec mnoho poskytovatelů VPN k nastavení L2TP/IPSec používalo předsdílené klíče .

Porty brány firewall: Port UDP 500 se používá pro počáteční výměnu klíčů, port UDP 5500 pro průchod NAT a port UDP 1701 pro umožnění provozu L2TP. Protože používá tyto pevné porty, L2TP/IPSec se snáze blokuje než některé jiné protokoly.

Stabilita: L2TP/IPSec není tak stabilní jako některé pokročilejší protokoly VPN. Jeho složitost může vést k častým výpadkům sítě.

Závěr: Zabezpečení L2TP/IPSec je nepochybně lepší než PPTP, ale nemusí chránit vaše data před pokročilými útočníky. Jeho nižší rychlosti a nestabilita také znamenají, že uživatelé by měli zvážit

použití L2TP/IPSec pouze v případě, že neexistují žádné jiné možnosti.

IKEv2/IPSec

Internet key exchange verze 2 (IKEv2) je relativně nový tunelovací protokol, který je ve skutečnosti součástí samotné sady IPSec. Microsoft a Cisco spolupracovaly na vývoji původního protokolu IKEv2/IPSec, ale nyní existuje mnoho open-source iterací.

IKEv2 nastaví řídicí kanál ověřením zabezpečeného komunikačního kanálu mezi vaším zařízením a serverem VPN pomocí algoritmu výměny klíčů Diffie–Hellman . IKEv2 pak použije tento zabezpečený komunikační kanál k vytvoření toho, co se nazývá přidružení zabezpečení, což jednoduše znamená, že vaše zařízení a server VPN používají ke komunikaci stejné šifrovací klíče a algoritmy.

Jakmile je přidružení zabezpečení na místě, může IPSec vytvořit tunel, aplikovat ověřené hlavičky na vaše datové pakety a zapouzdřit je pomocí ESP. (Opět platí, že v závislosti na tom, která šifra je použita, by ESP mohl zpracovat autentizaci zprávy.) Zapouzdřené datové pakety jsou pak znovu zapouzdřeny v UDP, aby mohly projít tunelem.

IKEv2/IPSec je podporován ve Windows 7 a novějších verzích, macOS 10.11 a novějších verzích a také ve většině mobilních operačních systémů.

Šifrování: IKEv2/IPSec může používat řadu různých kryptografických algoritmů, včetně AES, Blowfish a Camellia. Podporuje 256bitové šifrování.

Rychlost: IKEv2/IPSec je rychlý protokol VPN, i když obvykle není tak rychlý jako hardwarově akcelerovaný OpenVPN nebo WireGuard.

Známá zranitelnost: IKEv2 / IPSec nemá žádné známé slabiny a téměř všichni experti na IT bezpečnost jej považují za bezpečný, pokud je správně implementován pomocí Perfect Forward Secrecy.

Porty brány firewall: Port UDP 500 se používá pro počáteční výměnu klíčů a port UDP 4500 pro průchod NAT. Protože vždy používá tyto porty, je IKEv2/IPSec jednodušší zablokovat než některé jiné protokoly.

Stabilita: IKEv2/IPSec podporuje protokol Mobility a Multihoming, díky čemuž je spolehlivější než většina ostatních protokolů VPN, zejména pro uživatele, kteří často přepínají mezi různými sítěmi WiFi.

Závěr: Se silným zabezpečením, vysokými rychlostmi a zvýšenou stabilitou je IKEv2/IPSec dobrý protokol VPN. Nedávné představení WireGuard však znamená, že existuje jen málo důvodů, proč jej zvolit před novějším protokolem VPN.

OpenVPN

OpenVPN je open-source tunelovací protokol. Na rozdíl od protokolů VPN, které se spoléhají na sadu IPSec, OpenVPN používá SSL/TLS pro výměnu klíčů a nastavení řídicího kanálu a jedinečný protokol OpenVPN pro zpracování zapouzdření a datového kanálu.

To znamená, že jeho datový kanál i řídicí kanál jsou šifrovány, což jej činí poněkud jedinečným ve srovnání s jinými protokoly VPN. Je podporován na všech hlavních operačních systémech prostřednictvím softwaru třetích stran.

Šifrování: OpenVPN může použít jakýkoli z různých kryptografických algoritmů obsažených v knihovně OpenSSL k šifrování svých dat, včetně AES, RC5 a Blowfish.

Další informace o šifrování AES

Rychlost: Při použití UDP udržuje OpenVPN rychlá připojení, ačkoli IKEv2/IPSec a WireGuard jsou obecně přijímány jako rychlejší.

Známá zranitelnost: OpenVPN nemá žádné známé zranitelnosti, pokud je implementován s dostatečně silným šifrovacím algoritmem a Perfect Forward Secrecy. Je to průmyslový standard pro VPN, které se zabývají bezpečností dat.

Porty brány firewall: OpenVPN lze nakonfigurovat tak, aby běželo na jakémkoli portu UDP nebo TCP, včetně portu TCP portu 443, který zpracovává veškerý provoz HTTPS a velmi obtížně blokuje.

Stabilita: OpenVPN je obecně velmi stabilní a má režim TCP pro potlačení cenzury.

Závěr: OpenVPN je bezpečný, spolehlivý a open source. Je to jeden z nejlepších protokolů VPN, které se v současné době používají, zejména pro uživatele, kteří se zajímají především o bezpečnost dat. Jeho schopnost směrovat spojení přes TCP (viz níže) z něj také dělá dobrou volbu pro vyhýbání se cenzuře. Nicméně, i když postrádá výhodu OpenVPN proti cenzuře, WireGuard je také bezpečný a je rychlejší než OpenVPN.

WireGuard®

WireGuard je open-source protokol VPN, který je bezpečný, rychlý a efektivní.

Šifrování: WireGuard používá ChaCha20 pro symetrické šifrování (RFC7539), Curve25519 pro anonymní výměnu klíčů, Poly1305 pro autentizaci dat a BLAKE2s pro hashování (RFC7693). Automaticky podporuje Perfect Forward Secrecy.

Rychlost: WireGuard používá nové, vysokorychlostní kryptografické algoritmy. Například ChaCha20 je mnohem jednodušší než šifry AES stejné síly a téměř stejně rychlé, i když většina zařízení nyní přichází s instrukcemi pro AES zabudovanými do jejich hardwaru. Výsledkem je, že WireGuard nabízí vysoké rychlosti připojení a má nízké nároky na procesor.

Známá zranitelnost: WireGuard prošel různými formálními ověřeními a aby mohl být začleněn do linuxového jádra, kódová základna WireGuard Linux byla nezávisle auditována třetí stranou.

Porty brány firewall: WireGuard lze nakonfigurovat tak, aby používal jakýkoli port a obvykle běží přes UDP. Proton VPN však také nabízí WireGuard TCP ve většině našich aplikací.

Stabilita: WireGuard je velmi stabilní protokol VPN a zavádí nové funkce, které jiné protokoly tunelování nemají, jako je udržování připojení VPN při změně serverů VPN nebo změně sítí WiFi.

Závěr: WireGuard, nejmodernější protokol VPN, je rychlý, efektivní a bezpečný. Není tak „testovaný“ jako OpenVPN a nenabízí anticenzurní schopnosti OpenVPN založené na TCP (viz níže), ale pro většinu lidí je to většinou protokol VPN, který doporučujeme používat.

Další informace o WireGuard

OpenVPN vs. WireGuard

Stealth

Stealth je nový protokol VPN vyvinutý společností Proton. S ním můžete přistupovat k cenzurovaným webům a komunikovat s lidmi na sociálních sítích, i když jsou běžné protokoly VPN blokovány vaší vládou nebo organizací.

Stealth je založen na WireGuard tunelovaném přes TLS. Používá proto stejné šifrování jako WireGuard s přidanou vrstvou šifrování TLS. Jinak je shodný s WireGuard (popsáno výše).

Zjistěte více o Stealth

Další důležité termíny

Při porovnávání různých protokolů VPN jste možná narazili na zkratky nebo technické termíny, které jste neznali. Vysvětlíme zde některé z nejdůležitějších.

TCP vs. UDP

Protokol řízení přenosu (TCP) a protokol uživatelských datagramů (UDP) jsou dva různé způsoby, kterými mohou zařízení mezi sebou komunikovat přes internet. Oba běží na internetovém protokolu, který je zodpovědný za odesílání datových paketů na az IP adres.

Když vidíte, že tunelovací protokol používá port TCP nebo port UDP, znamená to, že nastavuje spojení mezi vaším počítačem a serverem VPN pomocí jednoho z těchto dvou protokolů.

Zda protokol VPN používá TCP, UDP nebo obojí, může výrazně ovlivnit jeho výkon. TCP se primárně zaměřuje na přesné doručování dat prováděním dodatečných kontrol, aby se zajistilo, že data jsou ve správném pořadí, a pokud tomu tak není, opraví je.

Zní to jako dobrá funkce, ale provádění kontrol vyžaduje čas, což má za následek pomalejší výkon. Spuštění VPN přes TCP (TCP přes TCP) může zpomalit vaše připojení v takzvaném zhroucení TCP.

Pokud například provoz TCP prochází tunelem OpenVPN TCP a data TCP v tunelu detekují chybu, pokusí se kompenzovat, což by mohlo způsobit překompenzování tunelu TCP. Tento proces může způsobit vážné zpoždění v doručení vašich dat.

Je to však také dobré pro porážku cenzury. Je to proto, že provoz HTTPS používá port TCP 443, takže pokud směrujete připojení VPN přes stejný port, vypadá to jako běžný bezpečný provoz VPN.

Možnost provozovat provoz VPN přes port 443 je jednou z největších výhod používání OpenVPN (a WireGuard, pokud používáte vlastní TCP implementaci protokolu Proton VPN).

Další informace o TCP a UDP

Dokonalé dopředné utajení

Perfect Forward Secrecy je kritickou bezpečnostní složkou šifrované komunikace. Týká se operací, které řídí způsob generování vašich šifrovacích klíčů. Pokud vaše VPN podporuje Perfect Forward Secrecy, vytvoří jedinečnou sadu klíčů pro každou relaci (tj. pokaždé, když navážete nové připojení VPN).

To znamená, že i když útočník nějakým způsobem získá jeden z vašich klíčů, může jej použít pouze k přístupu k datům z této konkrétní relace VPN. Data ve zbývajících relacích zůstanou v bezpečí, protože je chrání různé jedinečné klíče. Znamená to také, že váš klíč relace zůstane zabezpečený, i když bude odhalen soukromý klíč vaší VPN.

Protokoly používané aplikacemi Proton VPN

Spustili jsme Proton VPN, abychom zajistili aktivistům, disidentům a novinářům bezpečný a soukromý přístup k internetu. Aby byla komunita Proton v bezpečí, používáme pouze důvěryhodné a prověřené protokoly VPN. Následující seznam ukazuje, které protokoly VPN jsou podporovány v našich různých aplikacích:

- Windows: OpenVPN, WireGuard®
- macOS: OpenVPN, IKEv2, WireGuard a Stealth
- Android: OpenVPN, WireGuard a Stealth
- iOS/iPadOS: OpenVPN, IKEv2, WireGuard a Stealth
- Linux: OpenVPN

OpenVPN a WireGuard můžete používat v režimech UDP nebo TCP.

Přečtěte si, jak změnit protokoly VPN

Naše aplikace pro Windows, macOS, Android a iOS/iPadOS podporují **Smart Protocol** . Tato anticenzurní funkce, která inteligentně testuje sítě, aby zjistila nejlepší konfiguraci protokolu VPN potřebnou pro optimální výkon nebo obcházela cenzuru.

Například může automaticky přepínat z IKEv2 na OpenVPN nebo OpenVPN UDP na OpenVPN TCP pomocí různých portů podle potřeby.

Další informace o Smart Protocol

Všechny naše aplikace používají nejsilnější nastavení zabezpečení podporované protokolem VPN. OpenVPN, WireGuard a IKEv2/IPSec jsou jediné protokoly, o kterých se drtivá většina odborníků na IT bezpečnost shoduje, že jsou bezpečné.

Odmítáme nabízet jakákoli připojení VPN pomocí PPTP nebo L2TP/IPSec (přestože jsou levnější na provoz a snadněji se konfigurují), protože jejich zabezpečení nesplňuje naše standardy.

Když se přihlásíte k Proton VPN, můžete si být jisti, že vaše připojení VPN používá nejnovější a nejsilnější protokoly tunelování.

S pozdravem,
The Proton VPN Team

ZÍSKEJTE PROTON 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