Dnešní debata však zcela ignoruje fakt, že virtuální privátní sítě nejsou pouze potrubím spoujícím vzdálené zaměstnance s centrálními pracovními servery.

A to je ohromnná škoda, protože VPN mohou být užitečnými nástroji pro ochranu online soukromí, a nemusíte ani nosit bílý límeček, abyste mohli využít jejich výhod.

VPN, jak jejich jméno napovídá, jsou prostě virtuální verzí bezpečných, fyzických sítí – pavučin počítačů navzájem spojených kvůli sdílení souborů a dalších zdrojů. Ovšem VPN spojují s vnějším světem prostřednictvím internetu a mohou sloužit k zajištění obecného internetového provozu jakožto "doplňku" k podnikovým zdrojům. V reále je drtivá většina moderních VPN šifrovaná, takže se k nim počítače, zařízení a další sítě připojují skrze šifrované tunely.

## Proč byste měli chtít VPN

Jsou minimálně čtyři hlavní důvody, proč začít používat VPN. Zaprvé – můžete ji použít pro bezpečné připojení ke vzdálené síti přes internet. Většina společností využívá VPN k tomu, aby se zaměstnanci mohli připojit k souborům, aplikacím, tiskárnám a dalším zdrojům na kancelářské síti, aniž by ohrozili bezpečnost. I vy ale můžete nakonfigurovat svou vlastní VPN, abyste jejím prostřednictvím mohli bezpečně vzdáleně přistupovat k vaší domácí síti.

Zadruhé, VPN jsou velmi užitečné pro bezpečné propojení více sítí. Z tohoto důvodu se většina menších i větších firem spoléhá na VPN také pro sdílení serverů a dalších síťových zdrojů napříč více kancelářemi nebo obchodními jednotkami na celém světě. Ale dokonce i v případě, že se nemusíte starat o řetězec obchodů nebo kanceláří, můžete stejný trik použít pro propojení více domácích sítí nebo jiných sítí pro osobní potřebu.

Zatřetí, jestliže vám dělá starosti vaše online soukromí, je připojení k šifrované VPN ve chvíli, kdy jste na veřejné či nedůvěryhodné síti (například na Wi-Fi hotspotu v hotelu nebo kavárně), chytrou a jednoduchou bezpečnostní praktikou. Protože VPN šifruje váš internetový provoz, zabraňuje ostatním, kteří by se potenciálně mohli snažit špehovat vaše surfování na Wi-Fi, v krádeži vašich hesel či jiných údajů.

A konečně začtvrté, jedním z nejlepších důvodů pro používání VPN je obejití regionálních omezení – známých jako geoblocking – na konkrétních webech. Novináři a političtí disidenti používají VPN k tomu, aby obešli státem zřízenou cenzuru. Vy však můžete VPN využít také pro oddechové účely, jako je připojení k britské VPN, abyste mohli sledovat BBC iPlayer mimo Velkou Británii. Protože váš internetový provoz směřuje skrze VPN, vypadá to, jako byste byli britský návštěvník.

### Vyberte si svůj protokol

Při výběru síťového protokolu pro vaši VPN máte v podstatě jen čtyři možnosti. V krátkosti se na ně podívejme a zhodnoťme jejich silné a slabé stránky.

**Point-to-Point Tunneling Protocol (PPTP)** je nejméně bezpečná VPN metoda; tento protokol je nicméně vhodný pro vaši první VPN, protože jej podporuje téměř každý operační systém – Windows, Mac OS a dokonce i mobilní operační systémy.

**Layer 2 Tunneling Protocol (L2TP)** a **Internet Protocol Security (IPsec)** jsou bezpečnější než PPTP a jsou téměř stejně široce podporovány, mají však komplikovanější nastavení a jsou náchylné ke stejným problémům s připojením jako PPTP.

Secure Sockets Layer (SSL) VPN systémy poskytují stejnou úroveň bezpečnosti, které věříte, když se přihlašujete na internetové bankovnictví a další citlivé domény. Většina SSL VPN se označuje jako "bezklientová", protože už nepotřebujete dedikovaný VPN klient, abyste se k nějaké připojili. Jsou oblíbeným typem VPN, protože spojení se děje přes webový prohlížeč a proto jsou intuitivnější a spolehlivější než PPTP, L2TP nebo IPsec.

**OpenVPN** je přesně tím, co bychom si pod jejím názvem představovali. Jde o open-source VPN systém, který je založen na SSL kódu. Je bezplatný a bezpečný a netrpí problémy s připojením, avšak pro OpenVPN od vás bude požadována instalace klienta, protože Windows, Mac OS X ani mobilní zařízení ji nativně nepodporují.

Shrnuto a podtrženo: Jestliže si nejste jisti, používejte SSL nebo OpenVPN. Vezměte ale na vědomí, že některé ze služeb uvedených v další sekci tyto protokoly nevyužívají. Namísto toho využívají své vlastní VPN technologie.

Jestliže byste prostřednictvím VPN rádi rychle propojili více počítačů do jedné sítě, zvažte instalaci speciálního serverového VPN softwaru.

Potřebujete-li spolehlivější a robustnější nastavení (takové, které podporuje spojování více kanceláří po celém světě), možná byste mohli použít dedikovaný VPN router. Pokud ale chcete VPN používat jen k zabezpečení internetového provozu na veřejných Wi-Fi hotspotech a dalších nedůvěryhodných sítích – nebo přistupovat na regionálně zakázané stránky – potom se vyplatí zaregistrovat se k poskytovateli externí hostované VPN.

### Nastavte si jednoduchou VPN ve Windows

Windows standardně obsahuje VPN klienta, který podporuje protokoly PPTP a L2TP/IPsec. Proces nastavení je jednoduchý: jestliže používáte Windows 8, běžte v šému na vyhledávání, do vyhledávacího řádku napište **VPN** a spusťte průvodce VPN kliknutím na *Nastavit připojení virtuální privátní sítě (VPN)*.

Tohoto klienta můžete využít pro bezpečné připojení k jiným počítačům s Windows nebo jiným VPN serverům, které podporují protokoly PPTP a L2TP/IPsec – stačí jen dodat IP adresu nebo doménové jméno VPN serveru, ke

kterému se chcete připojit. Jestliže se připojujete ke korporátní nebo komerční VPN, můžete pro zjištění správné IP adresy kontaktovat administrátora. Jestliže si ve Windows vytvoříte svůj vlastní VPN server, můžete IP adresu tohoto serveru zjistit tak, že do vyhledávacího řádku napíšete **CMD**, čímž spustíte příkazový řádek, do něhož napíšete **ipconfig**. Tento jednoduchý trik je praktický, jestliže nastavujete svůj počítač s Windows jako VPN server, a potom se k němu připojujete tak, abyste mohli odkudkoliv bezpečně vzdáleně přistupovat k vašim souborům.

Malá poznámka: Při nastavování příchozích PPTP VPN připojení ve Windows musíte nakonfigurovat svůj síťový router tak, aby přesměrovat VPN provoz na počítač s Windows, na nějž chcete vzdáleně přistupovat. To uděláte tak, že se přihlásíte do ovládacího panelu routeru (jak to udělat, to by vám měl poradit manuál výrobce) a nakonfigurujete přesměrování portů či nastavení virtuálního serveru na přesměrovací port 1723 na IT adresu počítače, na nějž chcete přistoupit. Navíc musejí být aktivovány možnosti PPTP nebo VPN pass through v nastavení firewallu, ty však bývají zapnuty standardně.

# Krok za krokem: jak se připojit k VPN ve Windows 7 (odchozí)

**1. krok** Klikněte na tlačítko Start. Do vyhledávacího proužku vepište **VPN** a potom vyberte možnost *Nastavit připojení virtuální privátní sítě (VPN)*.

**2. krok** Vložte do následujícího dialogu IP adresu nebo doménové jméno serveru, k němuž se chcete připojit. Jestliže se připojujete k pracovní síti, poskytne vám adresu váš IT administrátor.

**3. krok** Jestliže chcete nastavit připojení, ale zatím se nepřipojovat, vyberte možnost *Nepřipojovat nyní*. V opačném případě pole nechte neodškrtnuté a klikněte na *Další*.

**4. krok** Na další obrazovce můžete buďto vložit vaše uživatelské jméno a heslo, nebo daná pole nechat nevyplněná. Uživatelské údaje po vás následně budou vyžadovány ve chvíli, kdy se budete reálně připojovat

**5. krok** Pro připojení klikněte vpravo dole na oznamovací oblasti na možnosti připojení (většinou jde o ikonu ve formě zobrazení dostupného signálu Wi-Fi sítě). Zde narazíte na možnost *Telefonická připojení a sítě VPN*.

6. krok Objeví se přihlašovací okno, do nějž zadáte své uživatelské údaje. Potom kliknete na Připojit.

**7. krok** Jestliže se nemůžete připojit, může být problém v konfiguraci serveru (kvůli výše zmíněným různým typům VPN.) Zeptejte se svého síťového administrátora, jaký typ VPN využívá. Na obrazovce *Připojit pomocí VPN připojení* vyberte *Vlastnosti*.

8. krok Běžte do panelu *Bezpečnost* a zde vyberte konkrétní typ VPN z vyskakovacího menu.

#### Krok za krokem: Jak vytvořit VPN (příchozí)

**1. krok** Klikněte na tlačítko *Start* a do políčka vyhledávání napište **Sítě a sdílení**. Zvolte *Centrum síťových připojení a sdílení*.

2. krok Klikněte v levém menu na Změnit nastavení adaptéru.

- 3. krok Klikněte v horním menu na Soubor (jestli ho nevidíte, vyvolejte ho levým Altem) > Nové příchozí připojení.
- 4. krok Vyberte uživatele, kterým chcete poskytnout přístup a klikněte na Další.
- 5. krok Zaškrtněte *Prostřednictvím internetu* a opět klikněte na *Další*.
- 6. krok Zvolte internetový protokol, který byste chtěli použít. (Standardní TCP/IPv4 bude fungovat dobře.)
- 7. krok Nakonec klikněte na Povolit přístup. Gratulujeme, právě jste nastavili příchozí VPN připojení.

# Pro vytvoření VPN serveru využijte software externího vývojáře

Jestliže byste rádi vytvořili VPN připojení spojující více počítačů, mezi nimiž chcete sdílet zdroje, aniž byste museli konfigurovat router nebo obětovat jeden počítač a udělat z něj VPN server, stojí za zvážení VPN software externích vývojářů. Comodo Unite, Gbridge a TeamViewer jsou slušné, spolehlivé a bezplatné alternativy.

Chcete-li pracovat spěti nebo méně počítači, můžete používat také program LogMeln Hamachi. Tento program je ale natolik dobrý, že stojí za to koupit si plnou verzi, pokud chcete bezpečně propojit větší množství počítačů – dejme tomu pokud vlastníte malou, ale rostoucí firmu.

## Zvládněte to s vlastním VPN routerem

Jestliže chcete poskytovat robustní vzdálený přístup k celé síti nebo chcete propojit více různých geografických lokalit, zkuste si do sítě nakonfigurovat router s CPN serverem a klientem. Jestliže máte omezený rozpočet, je nejlevnějším způsobem nastavení vlastního dedikovaného VPN routeru je načíst zpětně open-source firmware, který umožňuje VPN funkcionalitu, jako <u>DD-WRT</u> či <u>Tomato</u>, na obyčejný levný router spotřebitelské úrovně. Drouhou možností je koupit si speciální router (běžně zvaný VPN router) s vestavěným VPN serverem. K modelům této kategorie patří ZyXel ZyWall 802.11n Wireless Internet Security Gigabit Firewall (USG20W), Cisco Wireless Network Security Firewall Router (RV220W) nebo Netgear ProSecure UTM Firewall with Wireless N (UTM9S).

Při výběru VPN routeru a externího firmwaru pro dosavadní router je třeba klást důraz na to, aby daná řešení podporovala síťový VPN protokol, který potřebujete pro vaše zařízení. Navíc zkontrolujte, kolik souběžných VPN uživatelů daný router podporuje.

# Ať se o to postará externí VPN poskytovatel

Jestliže pouze chcete VPN přístup, který by zakryl váš internetový provoz tehdy, když používáte veřejný Wi-Fi hotspot nebo jinou nedůvěryhodnou síť, či chcete mít přístup k regionálně blokovaným stránkám, je nejjednodušším řešením poskytovatel hostované VPN. K nejoblíbenějším patří <u>Hotspot Shield</u>, který nabízí jak bezplatné, tak i

placené VPN služby pro Windows, Mac, iOS a Android. Podobnými službami jsou HotSpotVPN, StrongVPN, a WiTopia.

Jestliže chcete být při vašem online počínání z jakéhokoliv důvodu anonymní a nechcete platit za VPN služby, můžete vyzkoušet Onion Router, síť serverů, které dokážou anonymizovat váš internetový provoz bezplatně. Navštivte <u>web TORu</u> a stáhněte si nejnovější balíček s prohlížečem. Potom už můžete začít surfovat s aktivovaným rozšířením TOR.

Síť Tor nabízí cestu k anonymnímu surfování. Když se připojíte k Toru, je všechen váš internetový provoz šifrovaný a je veden komplexní sítí anonymních uzlů, než se dostane do své cílové stanice. Jistě, není to stoprocentně bezpečné, ale které bezpečnostní řešení je? Tor funguje od roku 2002 a byl testován přímo v terénu – konkrétně v Egyptě a dalších zemích s represivními režimy, které omezují přístup k internetu. A osvědčil se.

O tom, jak Tor nastavit a jak vůbec funguje, si přečtěte zde.

Nezávisle na tom, jaký z výše uvedených postupů si vyberete, stojí za to začít používat VPN ještě dnes. Zabere to trochu času, ale je to jedno z nejchytřejších a nejjednodušších řešení, jak zvýšit bezpečnost svých online aktivit