Streisand: Vlastní VPN server pro vyšší bezpečnost i obcházení cenzury Internetu

Michal Altair Valášek

michal.valasek@altairis.cz
@ridercz

Obsah

Datum vydání: 30.7.2017
Verze: 5

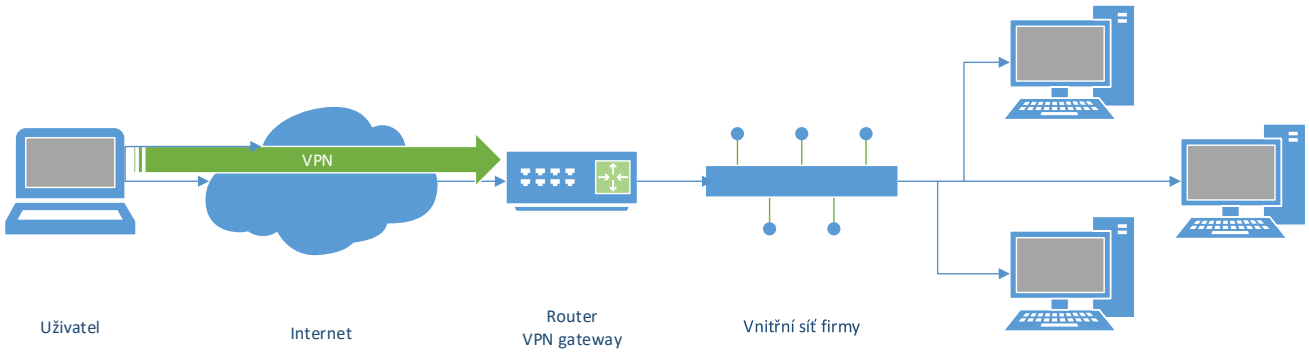
Aktuální verzi této příručky najdete vždy ke stažení na https://altair.is/streisand

[1] https://creativecommons.org/licenses/by-sa/4.0/

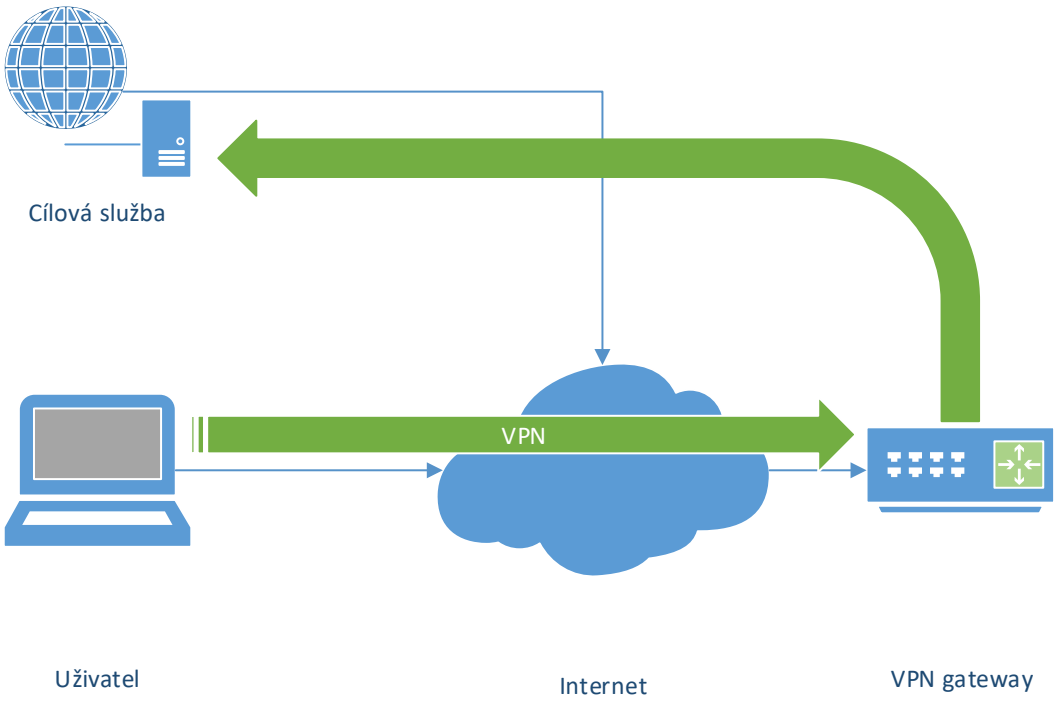
Co je VPN a proč ji chcete používat

Virtuální privátní síť

VPN znamená Virtual Private Network, tedy virtuální privátní síť. Můžete si ji představit jako virtuální kabel, který je natažen mezi dvěma body Internetu, skrze různé jiné sítě. Jako tunel, skrz který tečou data.



Typické použití VPN je ve firemní sféře, kde se mohou uživatelé z vnější sítě (Internetu, třeba zaměstnanci z domova nebo z hotelu na služební cestě) připojit do vnitřní sítě firmy a tváří se, jako kdyby byli fyzicky přítomni. Skrze VPN se ovšem můžete připojit i do dalších sítí a do Internetu. Pokud máte „vytočeno“ VPN spojení, jde (resp. může jít v závislosti na nastavení) veškerý provoz do Internetu nejdříve skrz VPN a poté z tamní sítě „zpět“ do Internetu. Pro zbytek světa to přitom vypadá, jako by se uživatel připojoval z místa, kde VPN končí. Lze tak „schovat“ fyzické i síťové umístění uživatele.



VPN jsou navíc typicky šifrované. Provozovatelé sítí, skrz které provoz teče, do něj na rozdíl od obvyklého stavu nemohou nijak zasahovat a nedokáží jej ani přečíst. Poznají sice, že je ustaveno VPN spojení a že jsou přes něj přenášena nějaká data (a jejich objem), ale to je zhruba všechno.

Proč používat VPN?

Bezpečí na cestách

Právě tato vlastnost virtuálních privátních sítí vede k tomu, že se používají i v případě, že chceme přistupovat k Internetu, ne do nějaké konkrétní vnitřní sítě. V praxi se často k Internetu připojujeme do sítí, jimž zcela nedůvěřujeme. Například do veřejných sítí v restauracích, hotelech a na letištích a podobně. Provozovatele těchto sítí zpravidla neznáme a nevíme, zda jim můžeme důvěřovat. Zabezpečení těchto sítí navíc nebývá na moc vysoké úrovni, takže i pokud nepodezíráme ze zlých úmyslů přímo provozovatele, musíme se mít na pozoru před nekalými úmysly ostatních uživatelů.

Některé protokoly – například HTTPS a další protokoly zabezpečené pomocí TLS – jsou sice proti útokům tohoto typu do jisté míry chráněny, ale stoprocentně spolehnout se na to zpravidla nemůžeme, potenciál k útokům je příliš velký.

Takovou nedůvěryhodnou síť můžeme přesto bezpečně využívat – pokud ji použijeme jenom jako cestu k ustavení tunelu – VPN – do nějakého důvěryhodného bodu, odkud pak přistupujeme dále do Internetu.

Ochrana před blokováním a cenzurou

Použití VPN nás také může ochránit před cenzurou Internetu nebo blokováním „nevhodných“ stránek. Jednoduše se z cenzurované sítě připojíme někam, kde omezení již neplatí.

Provoz VPN jako takové samozřejmě lze blokovat také. Ovšem pouze jako celek, nelze zabránit pouze určitému druhu provozu nebo dalšímu spojení. A ačkoliv je to technicky možné – a celkem snadné – zpravidla se tak neděje. Jak již bylo popsáno výše, VPN se rutinně využívají v profesionální praxi. Používají se ve firemním prostředí, používají se pro správu serverů a sítí (na řadu serverů není z bezpečnostních důvodů možný přístup z Internetu, ale jenom z vnitřní sítě, do níž se lze dostat VPNkou).

Pokud tedy budete chtít přistupovat k webu, který je z rozhodnutí ministerstva financí blokován v ČR, stačí vytočit VPN kamkoliv za hranice, kde je Internet ještě svobodný, a připojit se odtamtud.

VPN jako služba a proč ji nepoužívat

Poslední dobou se roztrhl pytel s komerčními i bezplatnými službami, které nabízejí VPN nebo se tak přinejmenším tváří. Zdánlivě se jedná o nejjednodušší řešení – stačí využívat příslušnou službu a je hotovo. Nicméně tento postup obecně nedoporučuji.

Použitím VPN se bezpečnostní problémy neřeší, jenom se přesunou – na provozovatele VPN, do jehož rukou svěřujete svou bezpečnost a své soukromí. Protože on vidí a obecně může modifikovat váš provoz. Ukazuje se, že všichni provozovatelé VPN (zejména těch bezplatných nebo levných) nejsou až tak důvěryhodní. Někteří modifikují váš provoz a vkládají do webových stránek svou reklamu. Většinou si musíte nainstalovat speciální klientský program, který může nainstalovat pokud ne přímo malware, tak přibalené další programy, bez kterých byste se obešli. Bezpečnost samotných VPN také není vždy dobrá, nedávné studie prokázaly, že mnoho poskytovatelů má své servery nastavené špatně a provoz lze dešifrovat nebo na něj úspěšně útočit jinak.

Vlastní brána v oblacích

Pokud toho jsme technicky a organizačně schopni, je samozřejmě nejlepší si provozovat vlastní VPN server (také se mu někdy říká VPN gateway, brána) v prostředí, kterému důvěřujeme. Odkudkoliv se pak můžeme připojit na server pod naší kontrolou a pak z něj dále.

Tento postup je výhodný i v případě, že se nacházíme v síti (nebo zemi), která si nepřeje, aby její uživatelé VPN obecně používali, třeba k obcházení vynucené cenzury. Jak již bylo řečeno, není obvykle žádoucí blokovat VPN jako takové. Ale je snadné blokovat konkrétní populární poskytovatele VPN služeb – to dělají například v Číně.

Technologií pro provoz VPN je navíc celá řada a některé z nich jsou navržené tak, že při pohledu zvenčí nevypadají jako VPN, ale jako běžný provoz, např. HTTPS.

VPN gateway můžeme rozběhnout například u sebe doma nebo ve firmě, pokud k tomu máme vhodné připojení a server, ale jednodušší a výhodnější může být umístit ji k některému poskytovateli cloudových služeb. A to hned z několika důvodů:

- Je to snadné a levné; v návodu popisované řešení jste schopni provozovat s nákladem v desetikorunách měsíčně.
- Cloudové služby nabízejí dostatečné rychlosti připojení, aby nás VPN příliš nezpomalovala.
- Na připojení k cloudovým serverům není nic nestandardního ani podezřelého. Běží tam statisíce různých webů a různých služeb.
- Je snadné změnit IP adresu cloudového serveru, pokud to potřebujeme.
- Lze si vybírat z mnoha datacenter po celém světě. Můžeme se tvářit jako uživatel z jiné země a obejít tak například různá regionální omezení.

Streisand Effect a Streisand server

Streisand Effect je název pro situaci, kdy snaha skrýt nějakou informaci nebo zabránit jejímu šíření vede k opačnému efektu, zvýšení zájmu o ni. Je pojmenován podle případu, kdy se herečka Barbra Streisand snažila soudně zakázat šíření fotografie svého domu. Před podáním žaloby byl snímek ze stránky fotografa stažen pouze šestkrát, z toho dvakrát hereččinými právníky. Měsíc po podání žaloby si jej prohlédlo přes 420 000 lidí.

Streisand je název projektu pro snadné a automatizované vytvoření serveru pro VPN gateway. Vytvořit a zkonfigurovat VPN server ručně není triviální. Streisand tento proces automatizuje. Jedná se o sadu skriptů, které umí po zadání přístupových údajů k poskytovateli cloudových služeb (podporováni jsou Amazon EC2, Digital Ocean, Google Compute Engine, Linode a Rackspace) vytvořit cloudový server a na dálku na něm zkonfigurovat VPN gateway.

Podporuje přitom několik různých protokolů a typů VPN. Nejpoužívanější je nejspíše standardní L2TP/IPSec, pro který je podpora ve všech běžných operačních systémech. Streisand ale umožňuje i připojení přes OpenConnect, Cisco AnyConnect, OpenVPN, Shadowsocks, Stunnel, Tor nebo WireGuard.

Streisand je zároveň navržen jako bezúdržbový, resp. server se udržuje a aktualizuje sám, je-li v provozu.

Tento princip, tedy vytváření na dálku, je však poněkud těžkopádný pro běžné uživatele, kteří nemají k dispozici další server, na kterému by si rozjeli příslušnou instrumentaci. Naštěstí však existuje návod, jak vše zkonfigurovat na cloudovém serveru přímo. Článek **The VPN You Should Be Using**[2], jehož autorem je **Jerry Gamblin**, se stal základem tohoto návodu.

[2] https://jerrygamblin.com/2016/07/10/the-vpn-you-should-be-using/

Návod k použití návodu

Tato příručka obsahuje několik návodů, pomocí kterých můžete nainstalovat a zkonfigurovat vlastní VPN server v cloudu. Návody nemusíte realizovat všechny, vyberte si ty, které budete potřebovat.

- Návod **01. Vytvoření virtuálního počítače u Digital Ocean** vás seznamuje s poskytovatelem cloudových služeb Digital Ocean. Ukáže vám, jak si tam můžete zřídit účet a vytvořit virtuální server.
- Návod **02. Nastavení dynamického DNS** se bude hodit, pokud nechcete svůj VPN server nechat běžet trvale. V takovém případě se totiž bude měnit jeho IP adresa. V tomto návodu si ukážeme, jak můžete pomocí služby FreeMyIP změny IP adres sledovat a mít server dostupný vždy pod stejnou IP adresou.
- Návod **03. Instalace Streisand serveru** je jádrem této příručky. Popisuje postup pro vytvoření VPN serveru Streisand. Zde by návod v zásadě mohl skončit, protože Streisand vám dává instrukce, jak se připojit pomocí různých metod. Tyto instrukce jsou bohužel místy zastaralé a místy poněkud matoucí, proto jsem připravil další návody, které jsou podrobnější a aktuální.
- Návod **04. Instalace certifikátu CA Streisand serveru** nejspíš nebudete potřebovat. Popisuje, jak můžete certifikační autoritu Streisand serveru přidat mezi důvěryhodné, bez čehož se ovšem nejspíš obejdete – potřebuejete to jenom pro stažení přístupových informací.
- Návody **05. Získání přihlašovacích údajů pro L2TP/IPSec VPN**, **06. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1** a **07. Nastavení L2TP/IPSec VPN na Windows 7** se zabývají možností připojení pomocí L2TP/IPSec. Výhodou této technologie je, že ji podporuje naprostá většina platforem. Tento návod se zabývá pouze Windows, ale pokud napíšete obdobné instrukce pro jiné systémy, zejména Mac OS, iOS a Android, rád je přidám do další verze. Nevýhodou je, že tato technologie nefunguje vždy a v některých sítích je (záměrně nebo špatnou konfigurací) blokována.
- Návod **08. Instalace a konfigurace OpenVPN** proto popisuje jiný způsob připojení, OpenVPN. To sice vyžaduje instalaci příslušného software, ale je jednodušší na konfiguraci a funguje spolehlivěji i v různě divně nastavených sítích. Opět platí, že ačkoliv popisuji pouze instalaci pod Windows, OpenVPN klient je dostupný pro většinu běžných platforem.
- Poslední návod **09. Zrušení a opětovné zřízení dropletu u Digital Ocean** vám může ušetřit peníze, protože ukazuje, jak můžete virtuální server spustit (a platit za něj) jenom když ho používáte.

Typografické konvence

Jednotlivé návody jsou prezentovány formou tabulky s po sobě následujícími očíslovanými kroky. Při práci na si **jednotlivé body odškrtávejte tužkou**. Přeskočení jednoho bodu může znamenat problém, který se ale projeví až o mnoho kroků později a může být obtížné ho odhalit.

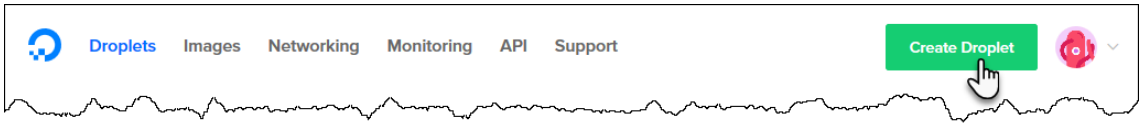
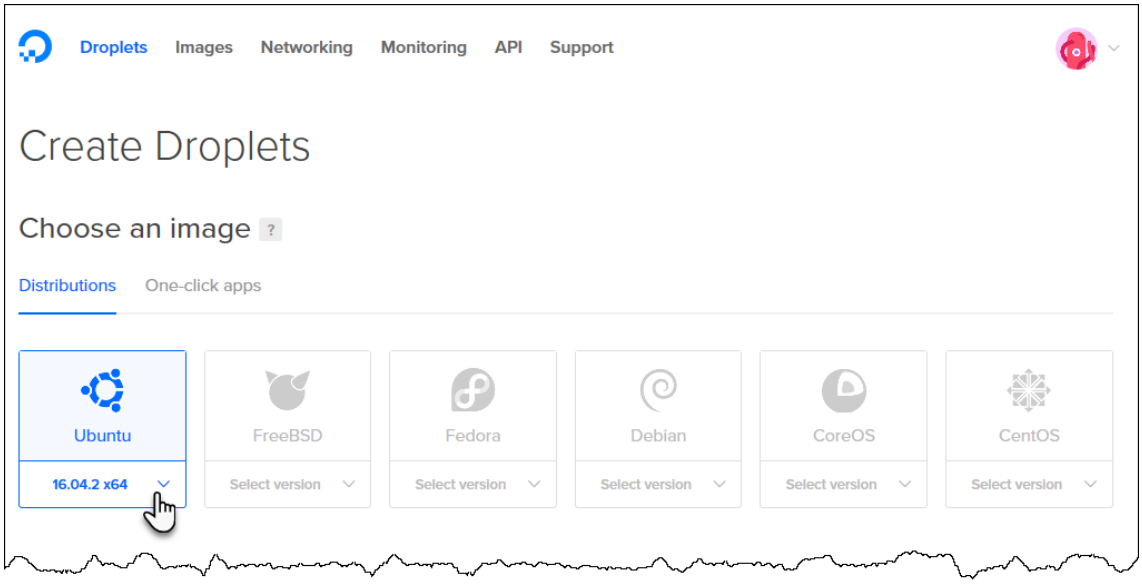
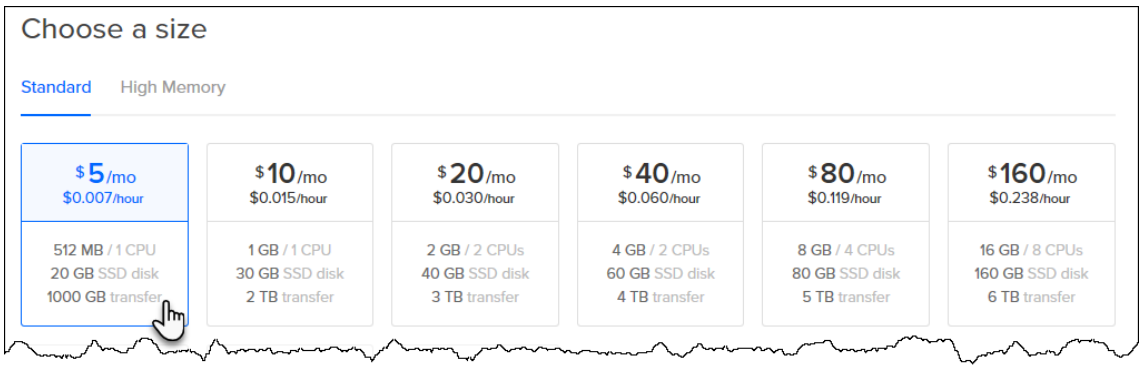
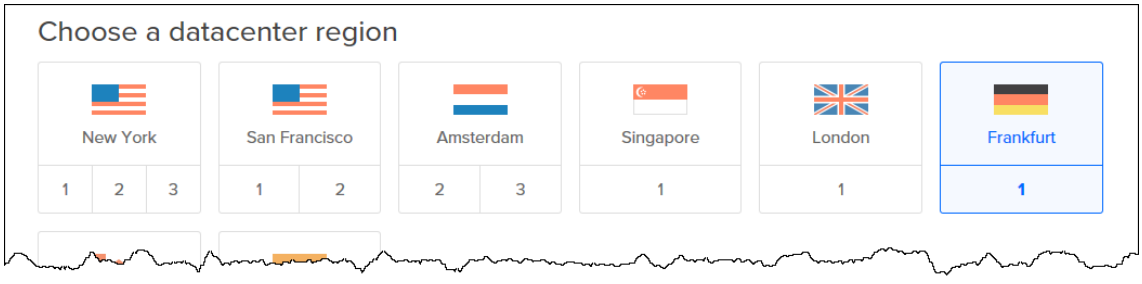
1.	Jednotlivé kroky jsou uvedeny v tabulce a očíslovány.
2.	Názvy příkazy a URL jsou psány `tímto neproporcionálním písmem`.
3.	Názvy prvků uživatelského rozhraní programů, menu a podobně jsou psány kurzívou. Pro ukázku hierarchie v menu se používá šipka: *File → Open*.
ⓘ	*Kontextové poznámky a doplňující informace jsou psány takto, v samostatných buňkách.*

4.	Delší sekvence příkazů jsou zapsány takto:
	`root@server:~$ passwd`
	`Changing password for root.`
	`(current) UNIX password: stareheslo`
	`Enter new UNIX password: noveheslo`
	`Retype new UNIX password: noveheslo`
	Příkazy, které máte zadat jsou zobrazeny tučně. Pokud text nebude při zadávání vidět (typicky hesla) je zobrazen přeškrtnutý.

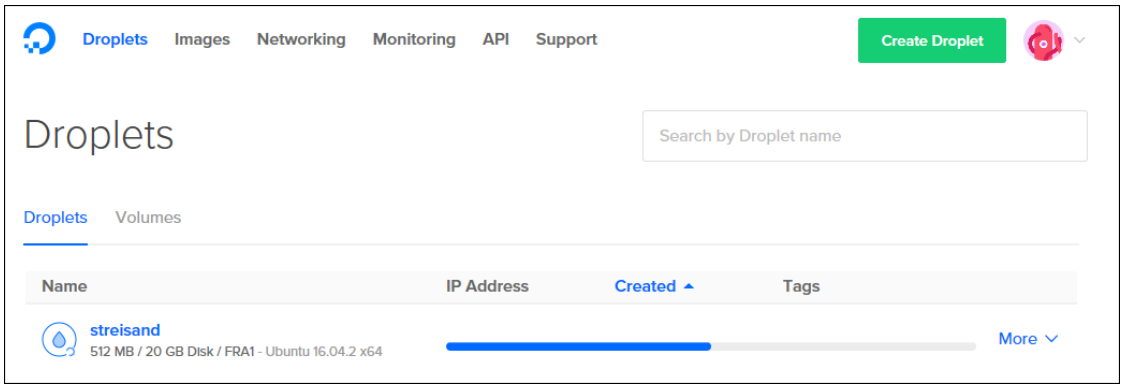
01. Vytvoření virtuálního počítače u Digital Ocean

1.	Otevřete v prohlížeči adresu `https://www.digitalocean.com/`.
2.	Klepněte na tlačítko *Sign Up*.
3.	Vytvořte si nový uživatelský účet. To předpokládá i ověření e-mailové adresy a zadání informací o platební kartě.

Vytvoření dropletu (virtuálního serveru)

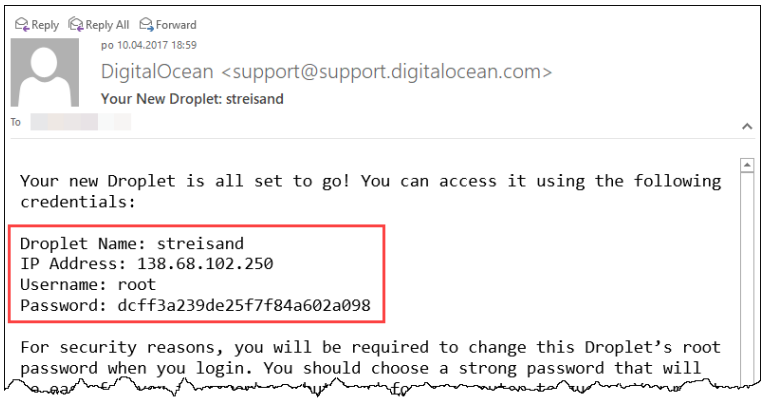
4.	Po přihlášení klepněte na zelené tlačítko *Create Droplet*: 
5.	V sekci *Choose an image* vyberte *Ubuntu 16.04 x64*: 
6.	V sekci *Choose a size* zvolte nejmenší velikost za $ 5 měsíčně: 
7.	Sekci *Add block storage* ponechte beze změny.
8.	V sekci *Choose a datacenter region* si zvolte místo, kde se má váš server nacházet: 

ⓘ	*Pro všechny, k nimž se poté z VPN připojíte, to bude vypadat jako kdybyste se nacházeli v zemi, kterou si teď zvolíte. To může být užitečné pro obcházení různých regionálních blokování a podobně. Já jsem v příkladu výše zvolil Frankfurt, protože je k nám z hlediska síťové topologie obvykle nejblíže a spojení tedy bude nejrychlejší.*
9.	Sekci *Select additional options* ponechte beze změny.
10.	Sekci *Add your SSH keys* ponechte beze změny.
ⓘ	*Pokud umíte používat SSH a autentizaci klíči, můžete je samozřejmě použít a ušetřit si práci s opisováním hesla a ještě zvýšit bezpečnost.*
11.	V sekci *Finalize and create* dejte svému serveru jméno (např. `streisand`) a klepnutím na velké tlačítko *Create* jej vytvořte.
12.	Čekejte, bude to nějakou dobu trvat, přibližně minutu až dvě.

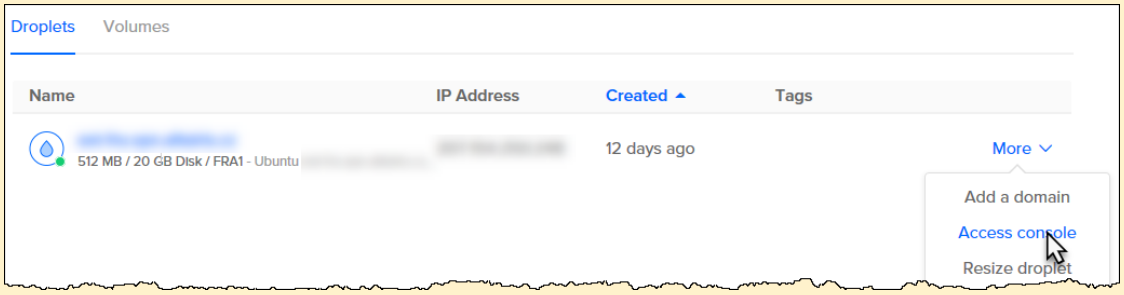


První přihlášení

13.	O vytvoření serveru budete informováni e-mailem. Součástí zprávy je též IP adresa, uživatelské jméno (`root`) a jednorázové heslo, které použijete pro první připojení:



14.	Pro připojení použijte SSH klienta. V následujícím příkladu používám standardní SSH, které je součástí *Bash on Ubuntu on Windows*, tedy linuxového subsystému ve Windows 10. Můžete nicméně použít například populární PuTTY[3] nebo cokoliv jiného.
ⓘ	*Pokud žádného SSH klienta nemáte a nechcete si ho instalovat, můžete použít i webové rozhraní DigitalOcean. U dropletu klepněte na* More *v pravé části a z rozbalovacího seznamu zvolte* Access Console.



[3] `http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html`

15. Připojte se jako uživatel root k IP adrese vašeho serveru (zde `138.68.102.250`):

```
altair@akhal-teke:~$ ssh root@138.68.102.250
```

Budete vyzváni k ověření pravosti klíče serveru (zobrazený fingerprint bude jiný než v příkladu). Odpovězte `yes` a stiskněte *Enter*.

```
The authenticity of host '138.68.102.250 (138.68.102.250)' can't be established.
ECDSA key fingerprint is b5:ec:b8:cb:9e:b0:fc:7b:3e:2a:54:8a:88:22:91:3e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '138.68.102.250' (ECDSA) to the list of known hosts.
```

Zadejte jednorázové heslo, které jste obdrželi e-mailem.

```
root@138.68.102.250's password: dcff3a239de25f7f84a602a098
You are required to change your password immediately (root enforced)
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Po prvním přihlášení si musíte změnit heslo. Zadejte ještě jednou heslo, které jste dostali e-mailem a pak dvakrát nové heslo. To již po prvotní konfiguraci nebudete k připojování k VPN potřebovat.

```
Changing password for root.
(current) UNIX password: dcff3a239de25f7f84a602a098
Enter new UNIX password: noveheslo
Retype new UNIX password: noveheslo
```

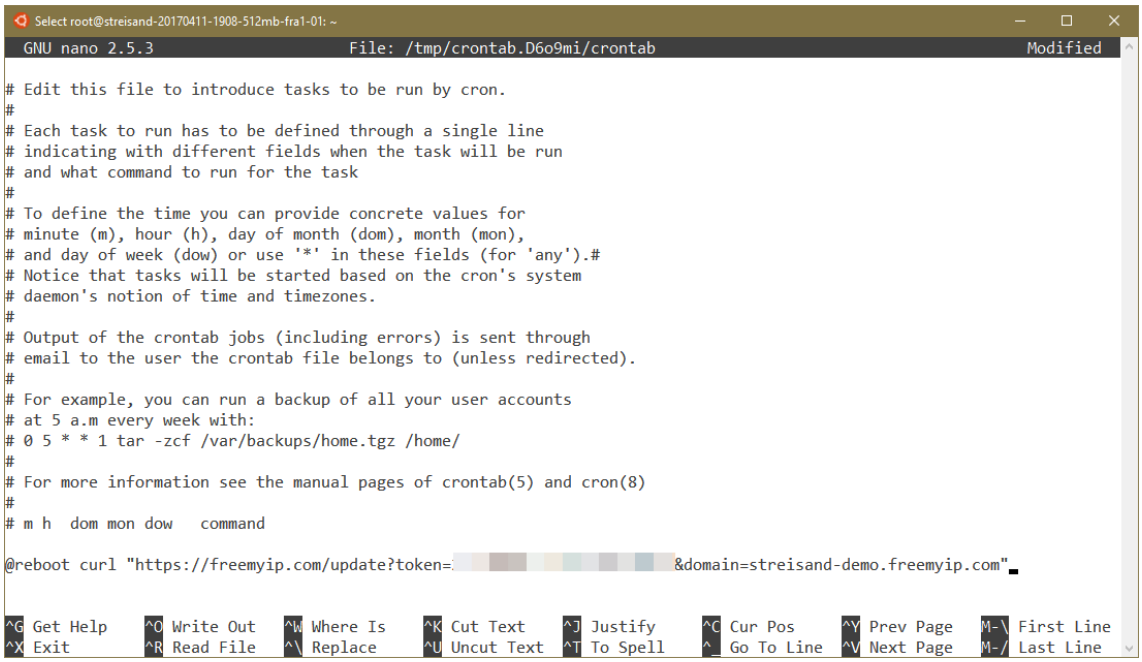
Jakmile uvidíte text v následujícím tvaru, jste úspěšně přihlášeni.

```
root@streisand:~#
```

02. Nastavení dynamického DNS

Náš server má dynamicky přidělenou IP adresu, která se může měnit, pokud ho budete používat jenom občas. Proto použijeme službu FreeMyIP, která umožní přidělit tomuto serveru logické jméno, které bude stálé.

1.	Otevřete v prohlížeči adresu `https://www.freemyip.com/`.
2.	Do pole *Domain name* zadejte název, který chcete používat. Musí být unikátní. V příkladech dále používám hostname `streisand-demo.freemyip.com`, ale vy si zvolte jiný. Poté klepněte na *Check Availability*.
3.	Pokud daný hostname není volný, zkuste to znovu. Pokud je, klepněte na *Submit*.
4.	Služba vám vygeneruje URL zhruba v následujícím formátu (skutečná adresa se bude lišit): `https://freemyip.com/update?token=xxxxxxxxxxxxxxxxxx&domain=streisand-demo.freemyip.com`
ⓘ	*Pokud uděláte HTTP request na tuto adresu, nasměruje se hostname (zde* `streisand-demo.freemyip.com`*) na tu IP adresu, z níž požadavek přišel. Potřebujeme tedy zařídit, aby po každém restartu server poslal tento HTTP request pomocí příkazu* `curl`*. To zařídíme pomocí služby* Cron*, což je plánovač událostí.*
5.	Připojte se pomocí SSH na server. Pro přihlášení použijte nové heslo, nastavené v kroku 15 návodu ***Error! Not a valid result for table.***.

6.	Na serveru spusťte příkaz `crontab -e`, kterým spustíte editaci tabulky plánovače událostí. Když se vás zeptá, jaký editor chcete používat, zvolte možnost 2, tedy `/bin/nano`:
	`root@streisand:~# crontab -e`
	`no crontab for root - using an empty one`
	
	`Select an editor.  To change later, run 'select-editor'.`
	`  1. /bin/ed`
	`  2. /bin/nano        <---- easiest`
	`  3. /usr/bin/vim.basic`
	`  4. /usr/bin/vim.tiny`
	
	`Choose 1-4 [2]: 2`
	 

7.	Ukáže se vám rozhraní textového editoru *GNU Nano*. Pomocí šipek dojděte na konec souboru (za řádky začínající znakem #, což znamená komentář.
8.	Přidejte nový řádek, který bude obsahovat `@reboot curl` a adresu získanou v bodu 4 v uvozovkách: `@reboot curl "https://freemyip.com/update?token=xxxxxxxxxxxxx&domain=streisand-demo.freemyip.com"`
9.	Vyskočte z editoru stiskem kláves `Ctrl`+X (označeno jako ^X).
10.	Na otázku *Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?* odpovězte Y.
11.	Název souboru nechte beze změny (stiskněte pouze `Enter`).
12.	Následujícím příkazem restartujte server, čímž vyzkoušíte, že se aktualizace DNS provede: `reboot now`

03. Instalace Streisand serveru

1. Připojte se pomocí SSH na server (nyní již nemusíte používat IP adresu, ale můžete použít DNS jméno, které jste nastavili v předchozím příkladu *02. Nastavení dynamického DNS*). Na serveru zadejte následující příkaz, kterým aktualizujete seznam dostupných balíčků. To bude trvat několik minut.

```
root@streisand:~# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Hit:2 http://ams2.mirrors.digitalocean.com/ubuntu xenial InRelease
…
Fetched 11.5 MB in 4s (2,418 kB/s)
Reading package lists... Done
root@streisand:~#
```

2. Zadejte následující příkaz, kterým nainstalujete komponenty, které Streisand potřebuje. Opět to bude nějakou dobu trvat:

```
root@streisand:~# apt-get install -y git python-paramiko python-pip python-pycurl python-dev
build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
…
Setting up python-wheel (0.29.0-1) ...
Setting up python-pycurl (7.43.0-1ubuntu1) ...
Processing triggers for libc-bin (2.23-0ubuntu7) ...
root@streisand:~#
```

3. Zadejte následující příkaz, kterým nainstalujete Ansible, který Streisand využívá pro konfiguraci:

```
root@streisand:~# pip install ansible markupsafe dopy==0.3.5
Collecting ansible
  Downloading ansible-2.2.2.0.tar.gz (2.5MB)
    100% |████████████████████████████████| 2.5MB 353kB/s
…
Successfully installed PyYAML-3.12 ansible-2.2.2.0 dopy-0.3.5 jinja2-2.9.6 markupsafe-1.0
requests-2.13.0
root@streisand:~#
```

4. Zadejte následující příkaz, kterým stáhnete aktuální verzi Streisand z Githubu:

```
root@streisand:~# git clone https://github.com/jlund/streisand.git && cd streisand/playbooks
Cloning into 'streisand'...
remote: Counting objects: 6470, done.
remote: Compressing objects: 100% (58/58), done.
remote: Total 6470 (delta 27), reused 0 (delta 0), pack-reused 6409
Receiving objects: 100% (6470/6470), 1.11 MiB | 0 bytes/s, done.
Resolving deltas: 100% (3793/3793), done.
Checking connectivity... done.
root@streisand:~/streisand/playbooks#
```

5. Zadejte následující příkaz, kterým modifikujete řídící soubor tak, aby se odkazoval na váš server (místo `streisand-demo.freemyip.com` zadejte váš název serveru):

```
root@streisand:~/streisand/playbooks# sed -i 's/streisand-host/streisand-demo.freemyip.com/g'
streisand.yml
```

6. Následujícím příkazem otevřete k editaci soubor group_vars/all:

```
root@streisand:~/streisand/playbooks# nano group_vars/all
```

7. Soubor upravte tak, aby měl následující obsah (přidané řádky jsou vyznačeny tučně):

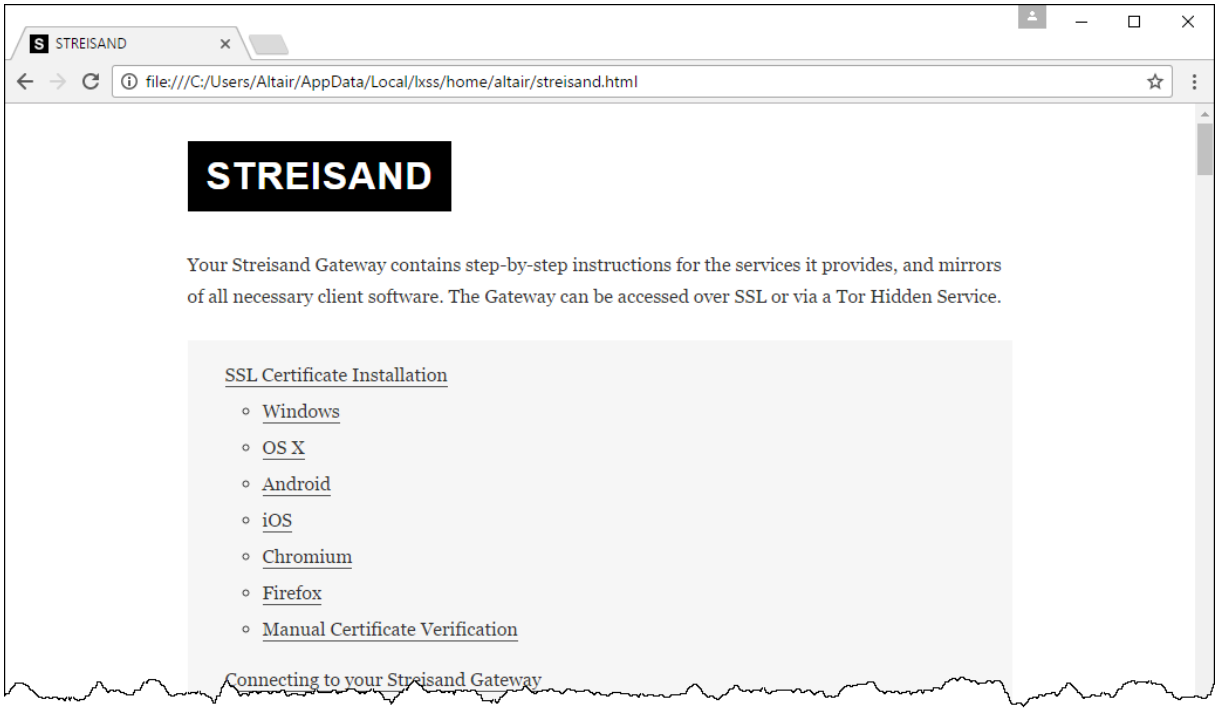
```
---
upstream_dns_servers:
  - 8.8.8.8
  - 208.67.222.222

streisand_ci: no
streisand_noninteractive: no
streisand_client_test: no
streisand_shadowsocks_enabled: yes
streisand_wireguard_enabled: yes
streisand_openvpn_enabled: yes
streisand_stunnel_enabled: yes
streisand_tor_enabled: no
streisand_openconnect_enabled: yes

gpg_key_server_address: "x-hkp://pool.sks-keyservers.net"
```

8.	Vyskočte z editoru stiskem kláves `Ctrl`+X (označeno jako ^X).
9.	Na otázku *Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?* odpovězte Y.
10.	Název souboru nechte beze změny (stiskněte pouze `Enter`).
11.	Zadejte následující příkaz, kterým Streisand nainstalujete. Místo `streisand-demo.freemyip.com` opět zadejte váš název serveru: `root@streisand:~/streisand/playbooks# ansible-playbook -i "streisand-demo.freemyip.com," -c local streisand.yml`
12.	Čekejte. Tento proces bude nějakou dobu trvat, přibližně 10-20 minut. Že je dokončen poznáte podle následující zprávy: `Server setup is complete. The `streisand.html` instructions file in the generated-docs folder is ready to give to friends, family members, and fellow activists. Press Enter to continue.:`
13.	Stiskněte *Enter*. Nenechte se zaskočit tím, že počítač vypíše chybu, že se mu nepodařilo otevřít HTML soubor. To je za těchto okolností normální.
14.	Instalace je nyní dokončena. V souboru `~/streisand/generated-docs/streisand.html` najdete instrukce pro připojení.
ⓘ	*Instrukce zkopírujte na svůj počítač. Pokud máte na svém počítači SCP pokračujte podle následujícího návodu. Nemáte-li, pokračujte bodem 14.*

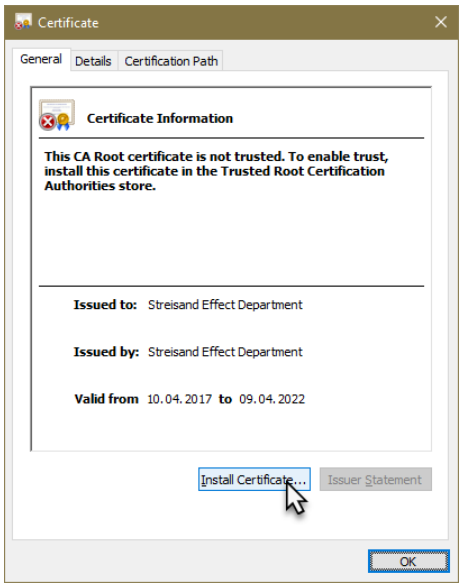
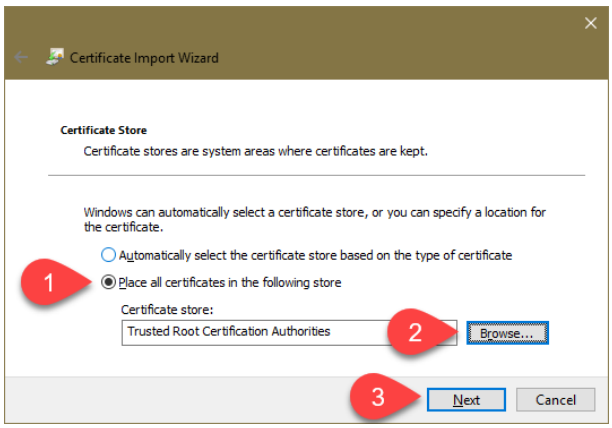
15.	Ukončete spojení se serverem pomocí příkazu `exit`:
	`root@streisand:~# exit`
	`logout`
	`Connection to streisand-demo.freemyip.com closed.`

16.	Následujícím příkazem (spuštěným na lokálním počítači, ne na vzdáleném serveru) zkopírujte soubor `streisand.html` na svůj počítač. Místo `streisand-demo.freemyip.com` opět zadejte váš název serveru: `scp root@streisand-demo.freemyip.com:/root/streisand/generated-docs/streisand.html streisand.html`
17.	Pokud nemáte SCP, můžete si soubor nechat (na serveru) vypsat na konzoli pomocí následujícího příkazu: `cat /root/streisand/generated-docs/streisand.html` Zdrojový kód HTML pak můžete zkopírovat přes schránku a na svém počítači vložit do textového editoru a uložit jako `streisand.html`.
18.	Výsledný soubor bude vypadat přibližně takto:  Tento soubor obsahuje instrukce pro použití vašeho VPN serveru a potřebné přihlašovací údaje. Uložte si ho a můžete jej sdílet s dalšími lidmi, kteří mají váš VPN server využívat. Následující návody jsou pouze rozšířením a aktualizací instrukcí, které najdete v tomto souboru. Instalace Streisand serveru jako takového je nyní hotová.

04. Instalace certifikátu CA Streisand serveru

Streisand server má vlastní certifikační autoritu, kterou musíte přidat mezi důvěryhodné. Postup pro přidání certifikátu na různých operačních systémech najdete v soboru `streisand.html`, který jste stáhli v předchozím kroku. Následující postup je platný na Windows 7-10.

Přidání certifikátu CA mezi důvěryhodné není naprosto nezbytné. Pouze v následujících návodechpro získání přihlašovacích údajů budete muset potvrdit, že se chcete připojit k web serveru i když nemá platný serverový certifikát.

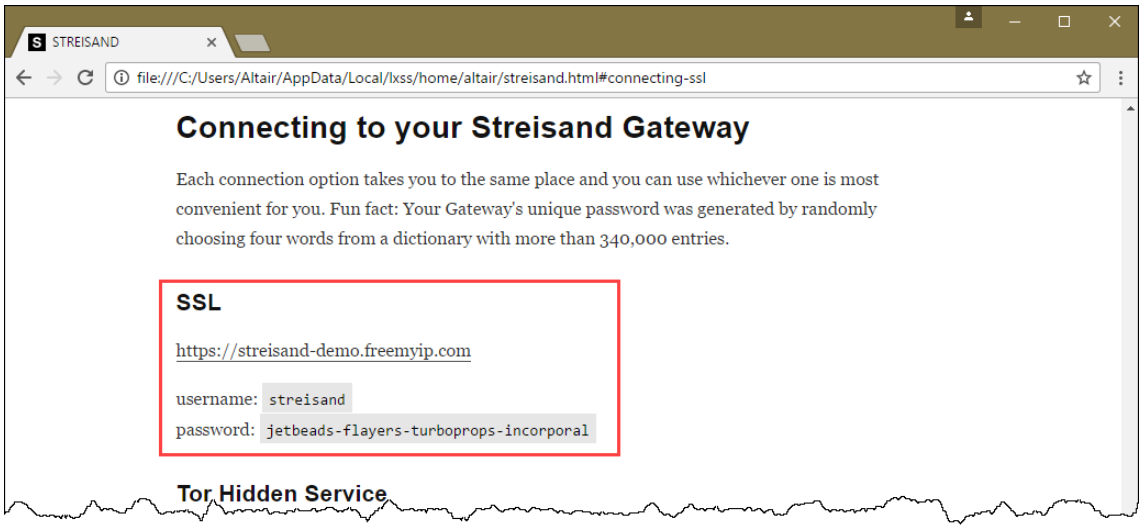
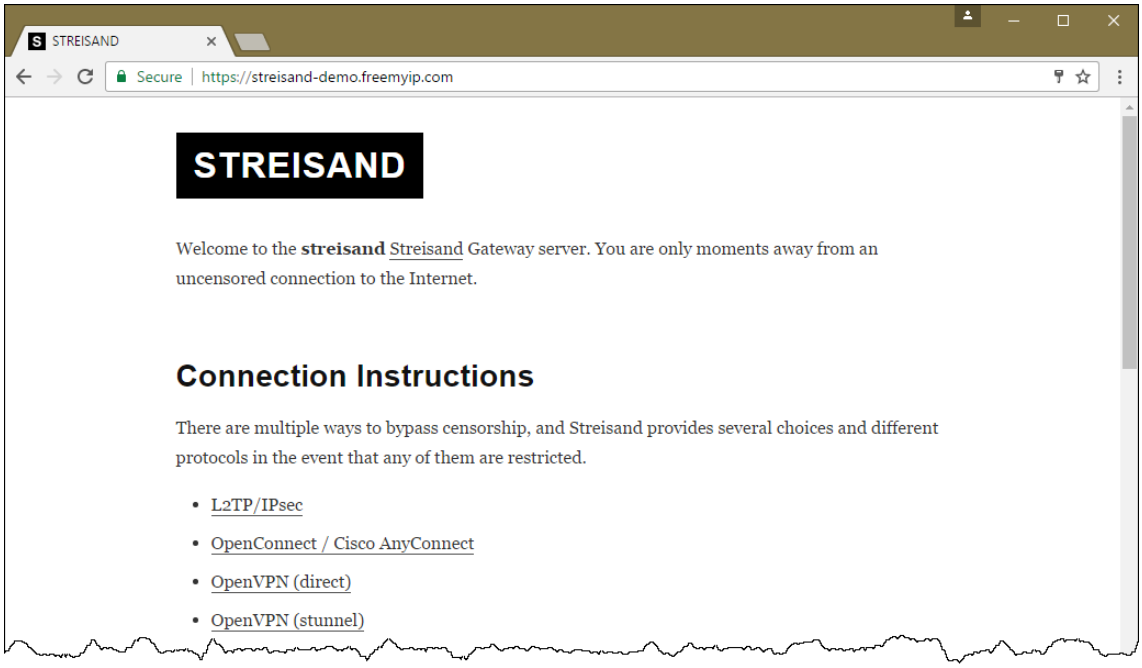
1.	Otevřete soubor `streisand.html`.
ⓘ	*Způsob vkládání certifikátu v HTML souboru není kompatibilní s Internet Explorerem a Edge na Windows 10. Použijte proto jiný prohlížeč – Firefox, Chrome nebo Operu.*
2.	Klepněte na odkaz *SSL Certificate Installation*.
3.	Klepněte na tlačítko *Download Certificate*.
4.	Otevřete stažený soubor.
5.	Klepněte na tlačítko *Install certificate*: 
6.	V průvodci zvolte *Current User* a klepněte na *Next*.
7.	V dalším kroku klepněte na *Place all certificates in the following store* a pak na *Browse*. V dialogu vyberte *Trusted Root Certification Authorities* a poté klepněte na *Next*: 
8.	Klepněte na *Finish*.
9.	V okně *Security Warning* klepněte na *Yes*.
10.	Ukáže se zpráva *The import was successful.* Tím je import certifikátu dokončen.

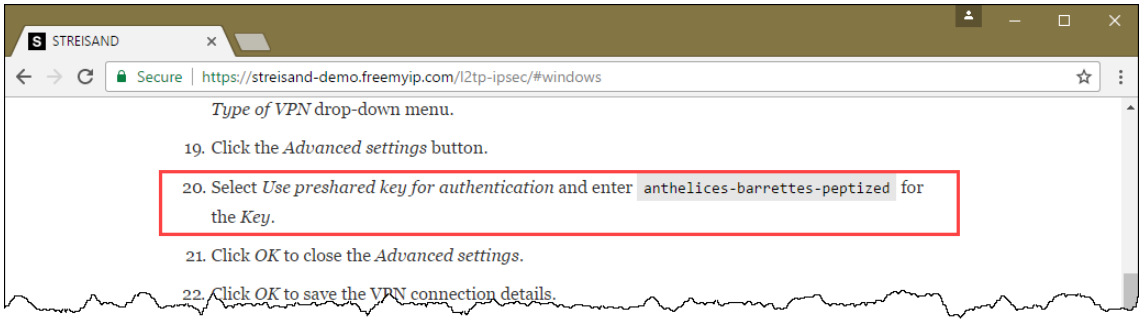
05. Získání přihlašovacích údajů pro L2TP/IPSec VPN

Soubor `streisand.html` a z něj odkazovaný web na našem serveru obsahuje instrukce, které potřebujete pro nastavení různých typů VPN. Bohužel, tyto instrukce jsou v některých ohledech neúplné a nevedou k požadovanému výsledku. Proto následující příklady obsahují podrobnější instrukce, jak zkonfigurovat VPN.

K tomu potřebujete znát následující údaje:

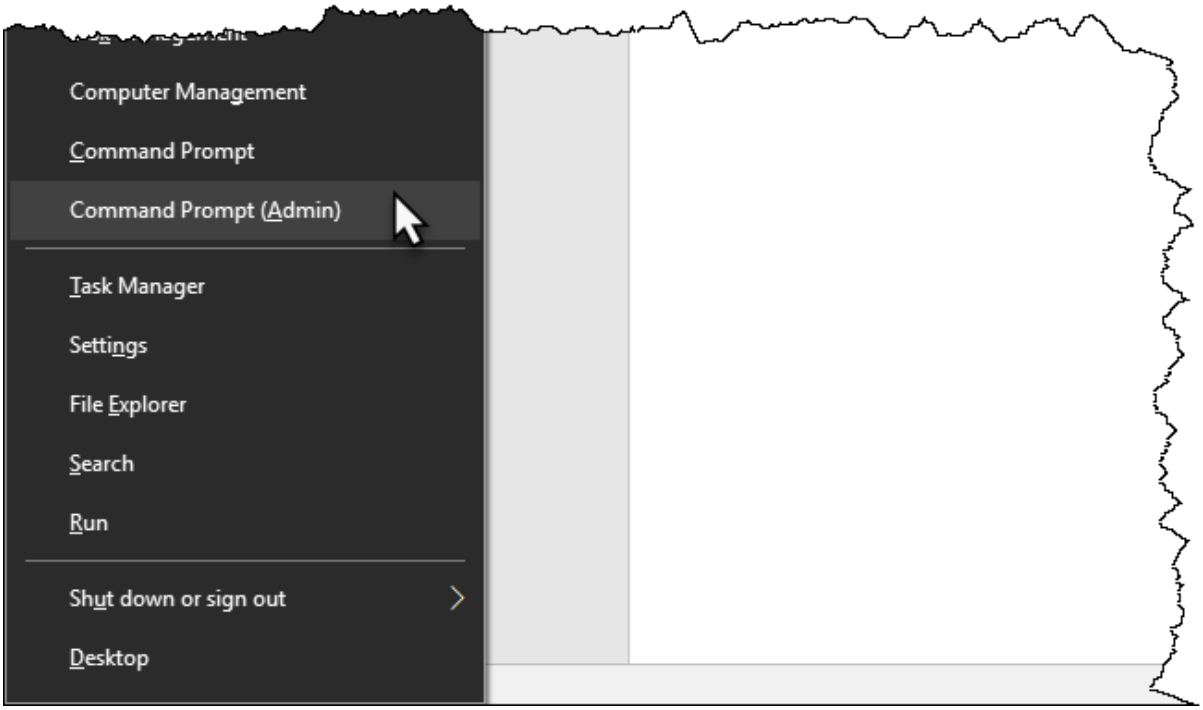
- Název serveru: název vašeho Streisand serveru. Zde `streisand-demo.freemyip.com`.
- Uživatelské jméno: `streisand`
- Heslo: _____ *(zjistěte postupem dle následujícího návodu)*
- Sdílený klíč (pre-shared key): _____ *(zjistěte postupem dle následujícího návodu)*

1.	Otevřete soubor `streisand.html`.
2.	Klepněte na odkaz *Connecting to your Streisand Gateway – SSL*.
3.	Přejděte na zde uvedenou adresu a přihlašte se uvedeným uživatelským jménem a heslem. To ještě neslouží k připojení k VPN, ale pouze k získání přihlašovacích údajů. 
4.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN: 
5.	Klepněte na odkaz *L2TP/IPsec*.

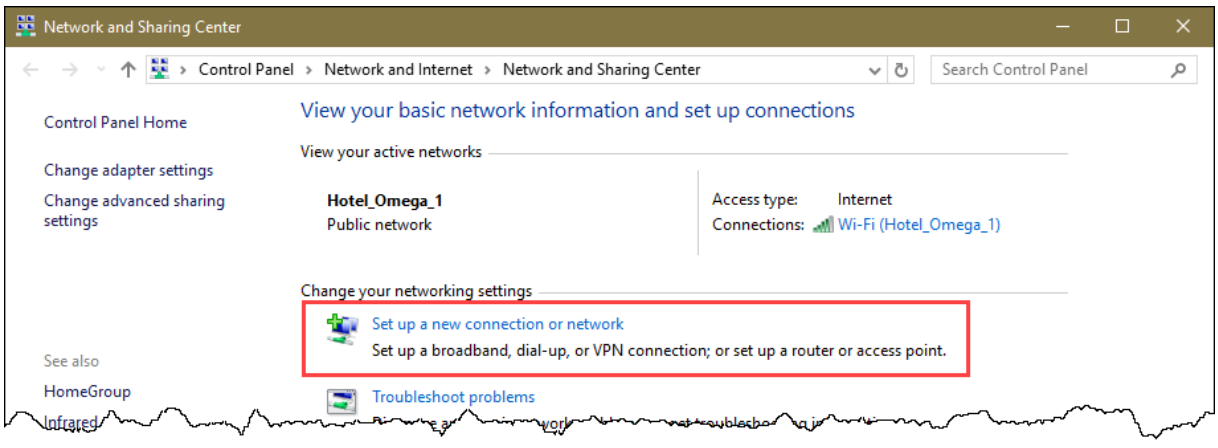
6.	Klepněte na odkaz *Windows*.
7.	Najděte v seznamu krok číslo 12. Hodnota na šedém pozadí je vaše heslo (na obrázku níže `extremism-remades`, vaše bude jiné). Toto heslo si poznamenejte. 
8.	Najděte v seznamu krok číslo 12. Hodnota na šedém pozadí je váš pre-shared key (na obrázku níže `anthelices-barrettes-peptized`, váš bude jiný). Tento klíč si poznamenejte. 

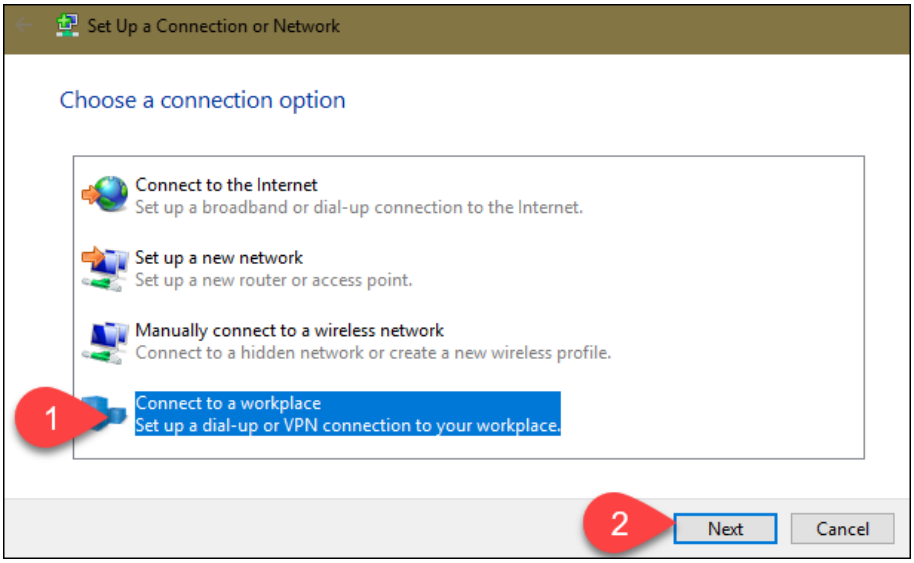
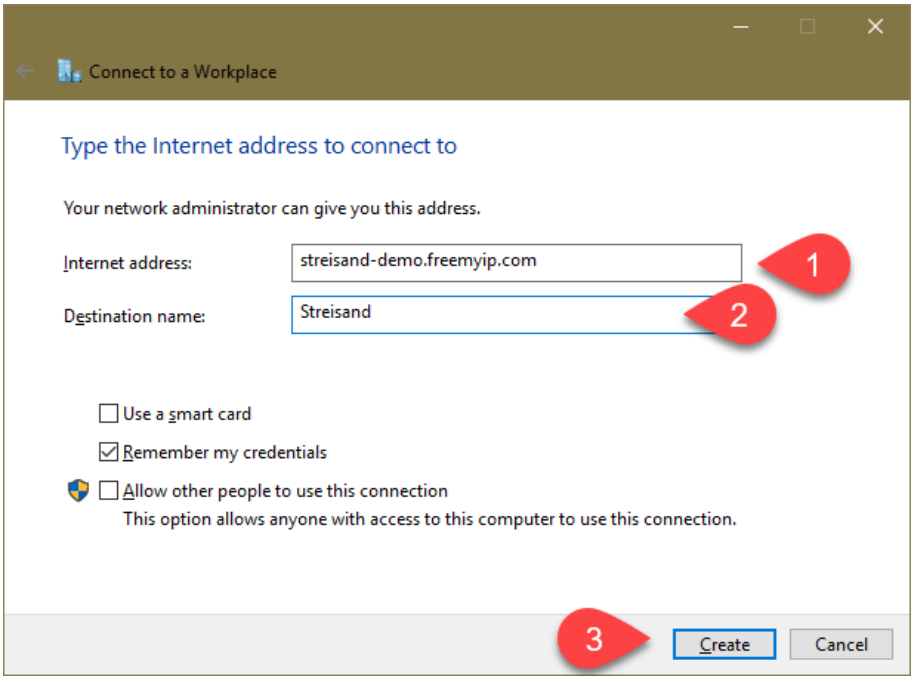
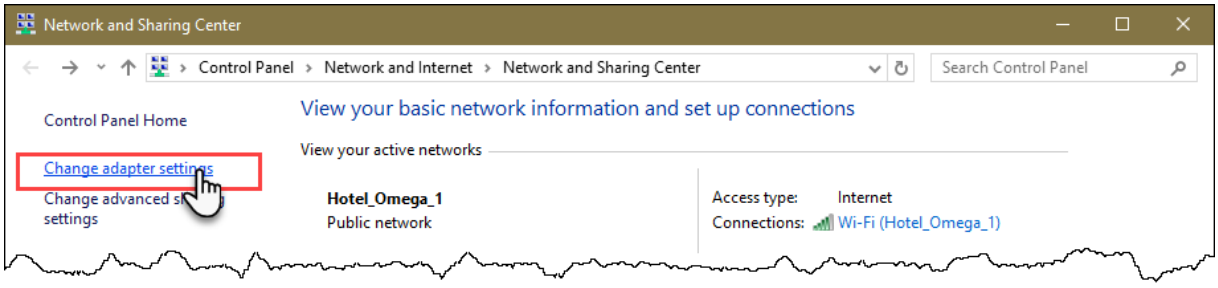
06. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1

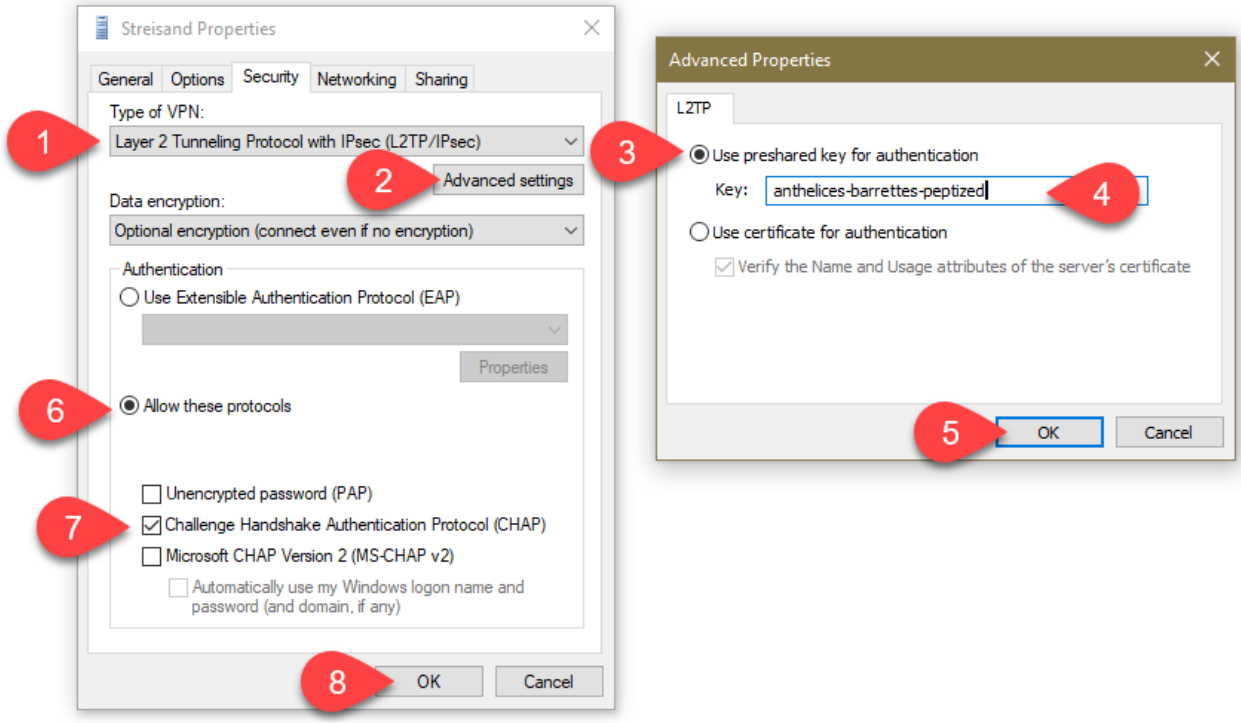
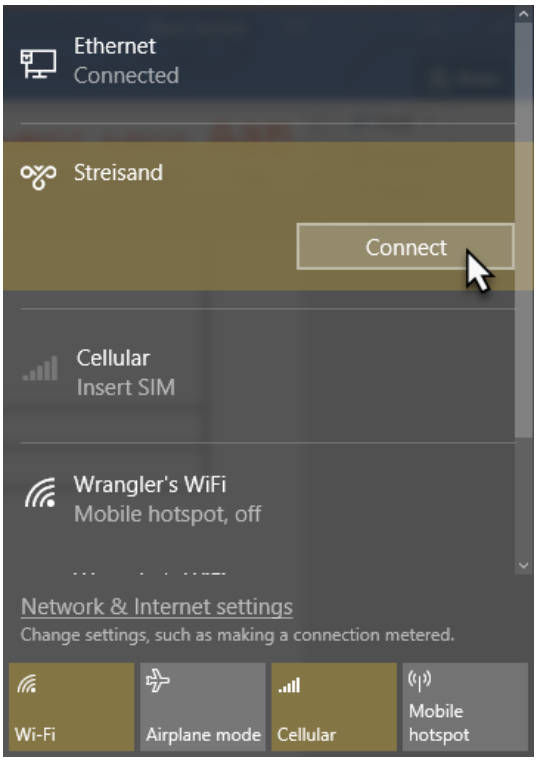
Příprava připojení

1.	Spusťte příkazovou řádku jako správce. Stiskněte klávesy *Win+X* a z menu zvolte *Command prompt (Admin)*, případně *PowerShell (Admin)*: 
2.	Zadejte do příkazové řádky následující příkaz (celý musí být na jednom řádku): `REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 2`
ⓘ	*Novější verze Windows mají ve výchozím nastavení problém ustavit VPN, pokud jsou za NAT bránou či routerem, což bývá obvyklé. Výše uvedený příkaz toto nastavení změní.*
3.	Aby se změny projevily, restartujte počítač.

Vytvoření nového VPN připojení

4.	Poté klepněte pravým tlačítkem na ikonu síťového připojení na hlavním panelu a z kontextového menu zvolte *Open Network and Sharing Center*.
5.	Klepněte na *Set up a new connection or network*: 

6.	Klepněte na *Connect to a workplace* a poté na *Next*. 
7.	Klepněte na *Use my Internet connection (VPN)*.
8.	Zadejte IP adresu vašeho Streisand serveru do pole *Internet address*. Spojení můžete pojmenovat (*Destination name*). Poté klepněte na *Create*. 
9.	V okně *Network and Sharing Center* klepněte na *Change adapter settings*: 
10.	Klepněte na název připojení (určený v kroku 8, zde *Streisand*) pravým tlačítkem a z kontextového menu zvolte *Properties*.

11.	Nastavte podrobnější parametry připojení: • Na záložce *Security* nastavte jako *Type of VPN* hodnotu *Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)*. • Klepněte na tlačítko *Advanced Settings* a zadejte hodnotu *preshared key* (viz předchozí návod *05. Získání přihlašovacích údajů pro L2TP/IPSec VPN*) a potvrďte klepnutím na *OK*. • V části *Authentication* povolte jako protokol *Challenge Handshake Authentication Protocol (CHAP)* a zrušte zaškrtnutí *Microsoft CHAP version 2 (MS-CHAP v2)*. • Poté klepněte na *OK*. 
12.	Klepněte na ikonu síťových připojení na hlavním panelu.
13.	V seznamu připojení klepněte na název nově vytvořeného připojení (*Streisand*) a poté na tlačítko *Connect* 

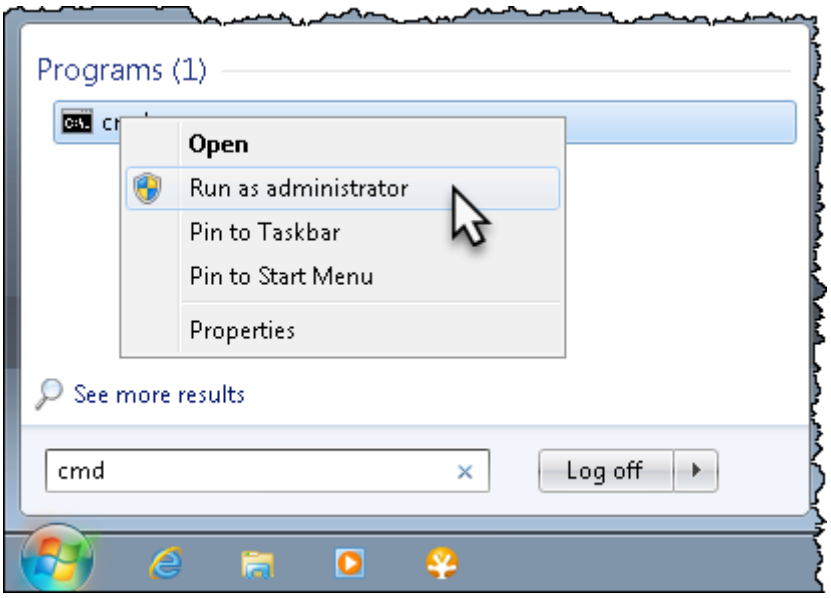
14.	Zadejte uživatelské jméno `streisand` a heslo zjištěné v předchozím návodu (*05. Získání přihlašovacích údajů pro L2TP/IPSec VPN*) a klepněte na OK.
15.	Váš počítač se nyní připojí k VPN a bude do Internetu přistupovat jejím prostřednictvím
ⓘ	*Pokud by vám připojení nefungovalo, je možné, že jej blokuje (záměrně nebo technickou chybou) váš router nebo poskytovatel připojení. V takovém případě je nutné buďto změnit konfiguraci nebo použít některou z jiných metod připojení, které Streisand podporuje.*

Odpojení od VPN a opětovné připojení

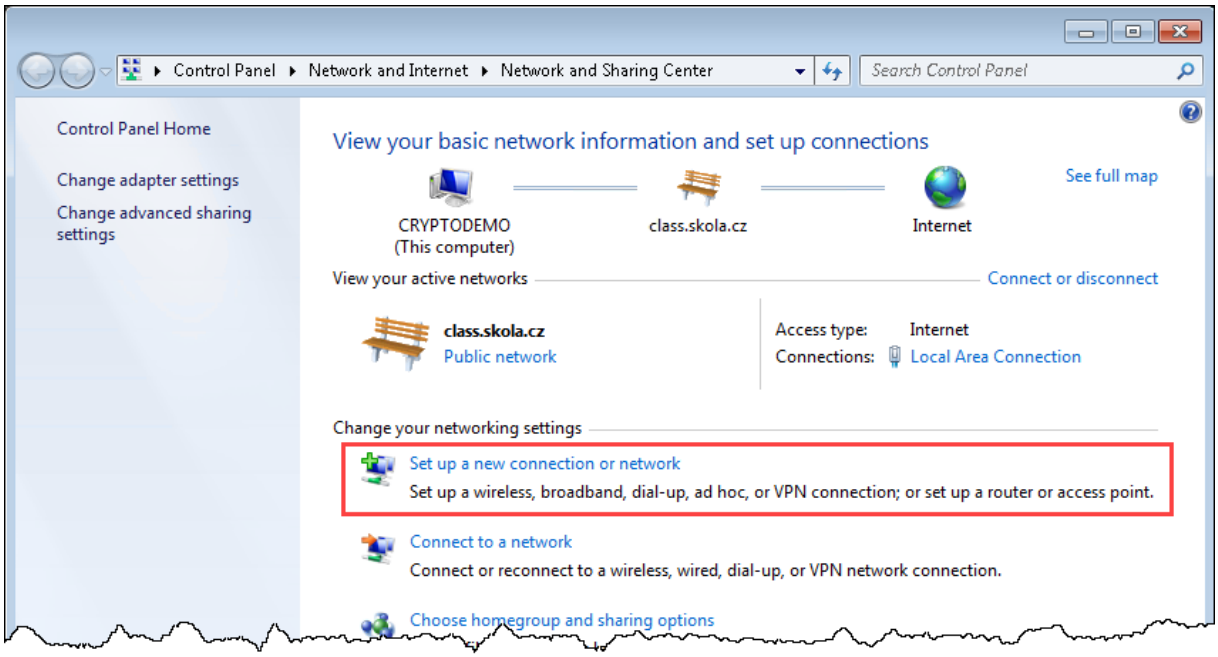
16.	Pokud se chcete od VPN odpojit, klepněte na ikonu síťových připojení na hlavním panelu, v seznamu zvolte název svého připojení (*Streisand*) a poté klepněte na tlačítko *Disconnect*.
17.	Budete-li se chtít znovu připojit, stačí opět klepnout na ikonu síťových připojení, v seznamu zvolit připojení *Streisand* a klepnout na *Connect*.

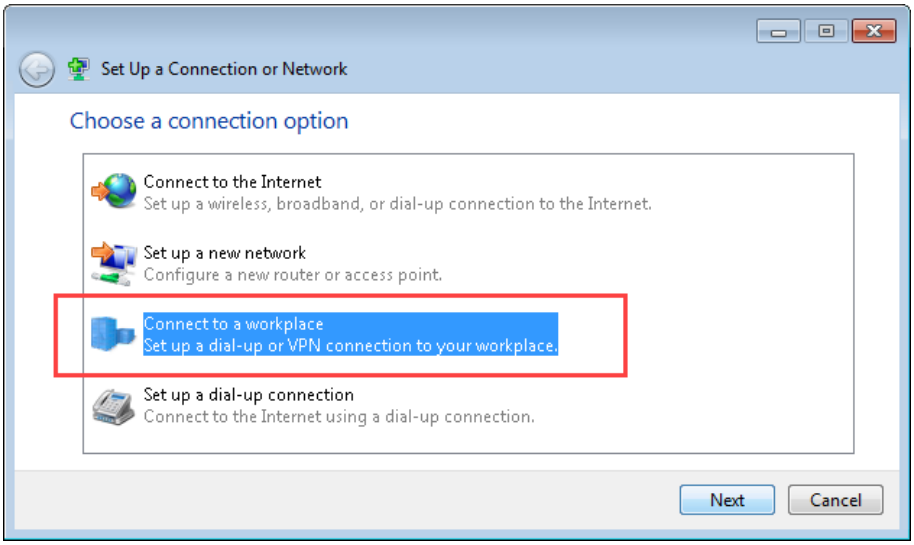
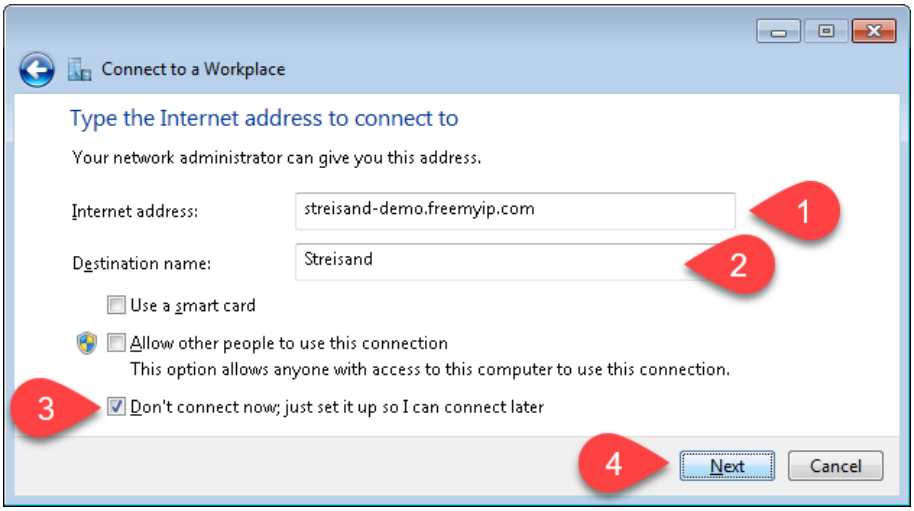
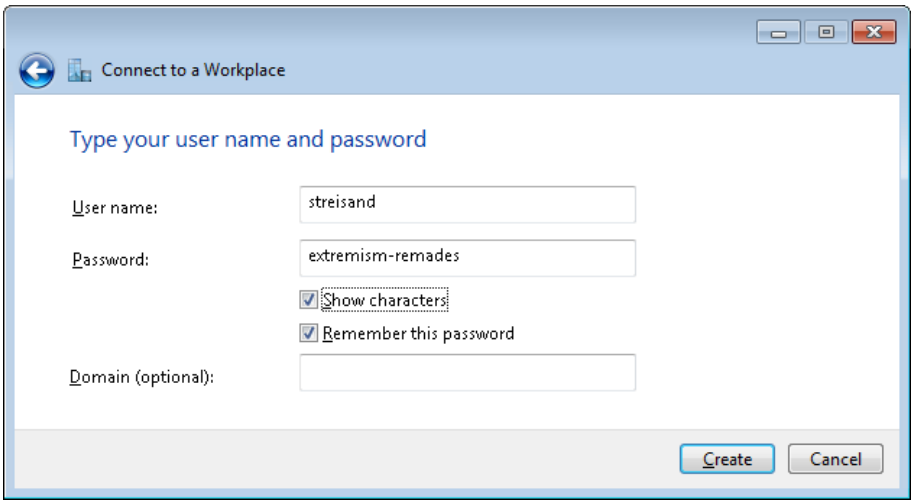
07. Nastavení L2TP/IPSec VPN na Windows 7

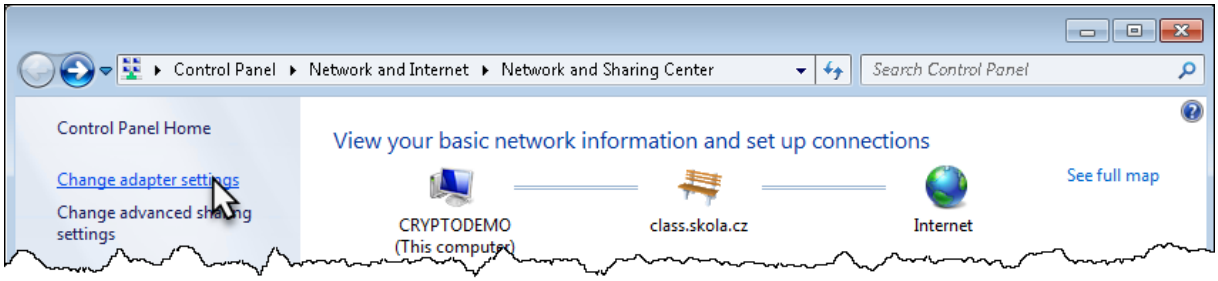
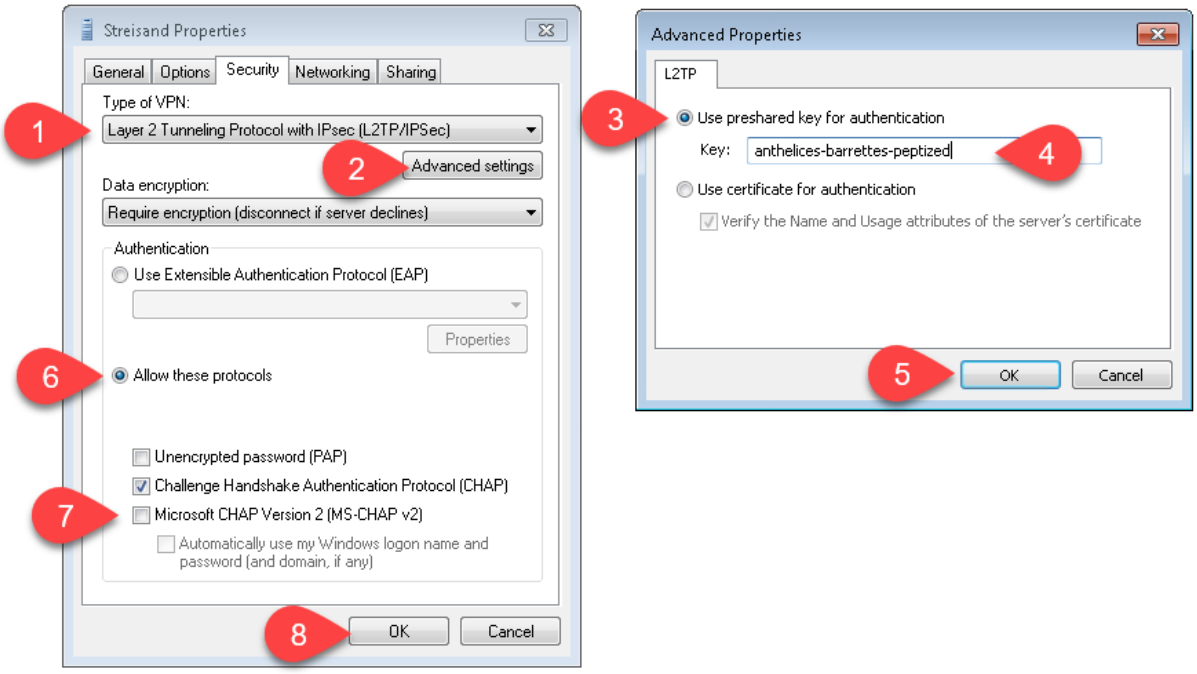
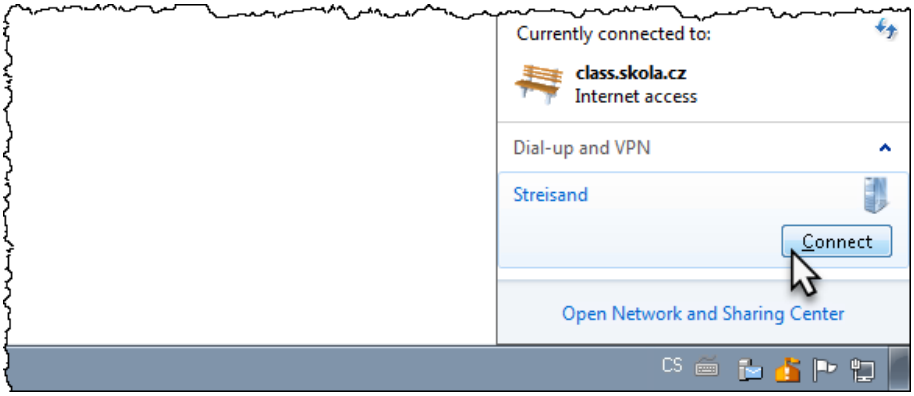
Příprava připojení

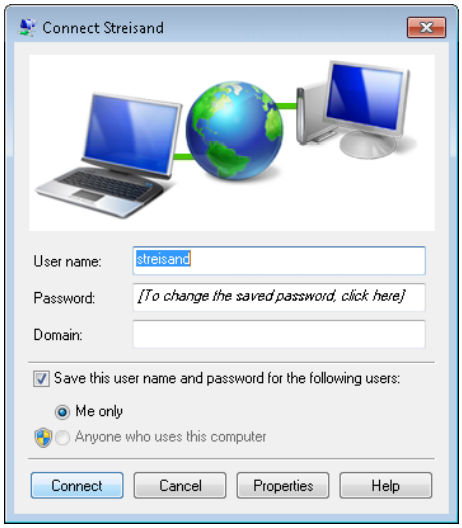
1.	Spusťte příkazovou řádku jako správce. Do vyhledávání v nabídce Start zadejte `cmd`. Poté co bude nalezen program `cmd.exe` na něj klepněte pravým tlačítkem a z kontextového menu zvolte *Run as administrator*. 
2.	Zadejte do příkazové řádky následující příkaz (celý musí být na jednom řádku): `REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 2`
ⓘ	*Novější verze Windows mají ve výchozím nastavení problém ustavit VPN, pokud jsou za NAT bránou či routerem, což bývá obvyklé. Výše uvedený příkaz toto nastavení změní.*
3.	Aby se změny projevily, restartujte počítač.

Vytvoření nového VPN připojení

4.	Poté klepněte pravým tlačítkem na ikonu síťového připojení na hlavním panelu a z kontextového menu zvolte *Open Network and Sharing Center*.
5.	Klepněte na *Set up a new connection or network*: 

6.	Klepněte na *Connect to a workplace* a poté na *Next*. 
7.	Klepněte na *Use my Internet connection (VPN)*.
8.	Zadejte IP adresu vašeho Streisand serveru do pole *Internet address*. Spojení můžete pojmenovat (*Destination name*). Zaškrtněte *Don't connect now; just set it up so I can connect later.* Poté klepněte na tlačítko *Next*. 
9.	V dalším kroku průvodce zadejte uživatelské jméno (`streisand`) a heslo zjištěné v předchozím návodu (*05. Získání přihlašovacích údajů pro L2TP/IPSec VPN*). Zaškrtněte *Remember this password* a klepněte na tlačítko *Create*. 
10.	Spojení je vytvořeno. Klepněte na tlačítko *Close*.

11.	V okně *Network and Sharing Center* klepněte na *Change adapter settings*: 
12.	Klepněte na název připojení (určený v kroku 8, zde *Streisand*) pravým tlačítkem a z kontextového menu zvolte *Properties*.
13.	Nastavte podrobnější parametry připojení: • Na záložce *Security* nastavte jako *Type of VPN* hodnotu *Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)*. • Klepněte na tlačítko *Advanced Settings* a zadejte hodnotu *preshared key* (viz předchozí návod *05. Získání přihlašovacích údajů pro L2TP/IPSec VPN*) a potvrďte klepnutím na *OK*. • V části *Authentication* povolte jako protokol *Challenge Handshake Authentication Protocol (CHAP)* a zrušte zaškrtnutí *Microsoft CHAP version 2 (MS-CHAP v2)*. • Poté klepněte na *OK*. 
14.	Klepněte na ikonu síťových připojení na hlavním panelu. V seznamu připojení klepněte na název nově vytvořeného připojení (*Streisand*) a poté na tlačítko *Connect*. 

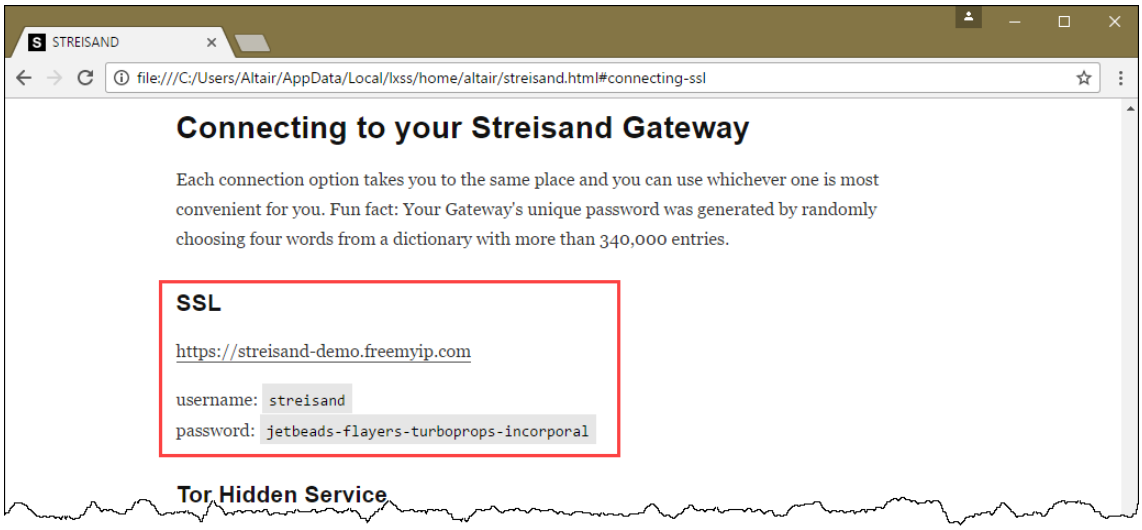
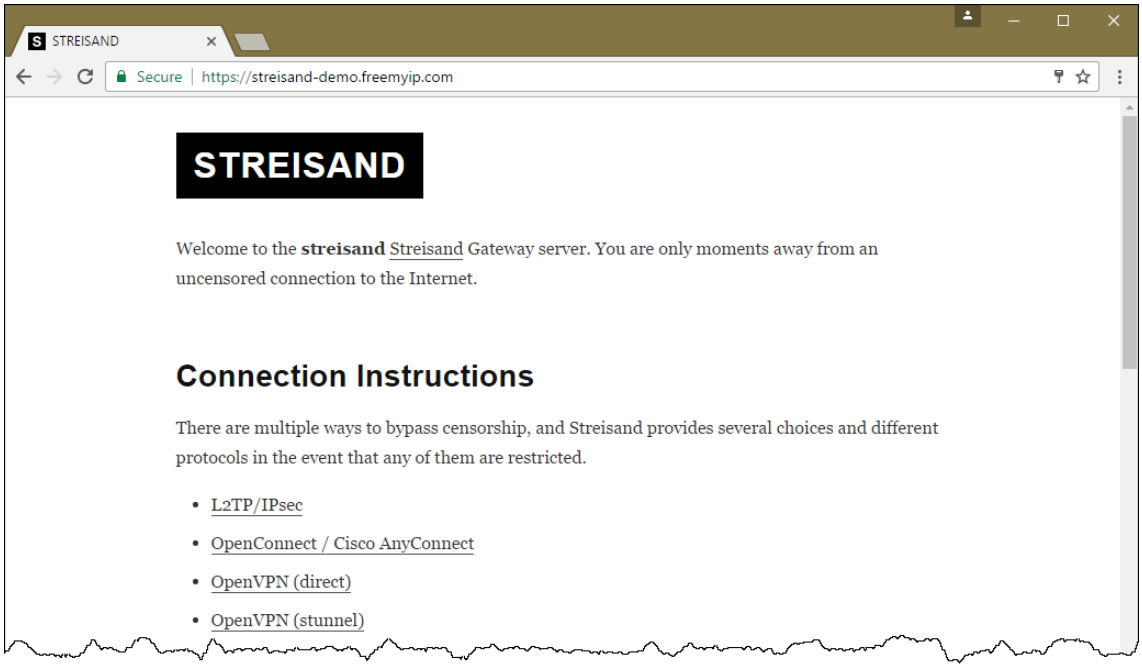
15.	V dalším okně klepněte na *Connect*. 
ⓘ	*Pokud toto okno nechcete v budoucnu zobrazovat, klepněte na* Properties *a potom zrušte zaškrtnutí* Prompt for name and password, certificate, etc.
16.	Zobrazí se okno s informacemi o průběhu připojování, které se posléze samo zavře.
17.	Váš počítač se nyní připojil k VPN a bude do Internetu přistupovat jejím prostřednictvím
ⓘ	*Pokud by vám připojení nefungovalo, je možné, že jej blokuje (záměrně nebo technickou chybou) váš router nebo poskytovatel připojení. V takovém případě je nutné buďto změnit konfiguraci nebo použít některou z jiných metod připojení, které Streisand podporuje.*

Odpojení od VPN a opětovné připojení

18.	Pokud se chcete od VPN odpojit, klepněte na ikonu síťových připojení na hlavním panelu, v seznamu zvolte název svého připojení (*Streisand*) a poté klepněte na tlačítko *Disconnect*.
19.	Budete-li se chtít znovu připojit, stačí opět klepnout na ikonu síťových připojení, v seznamu zvolit připojení *Streisand* a klepnout na *Connect*.

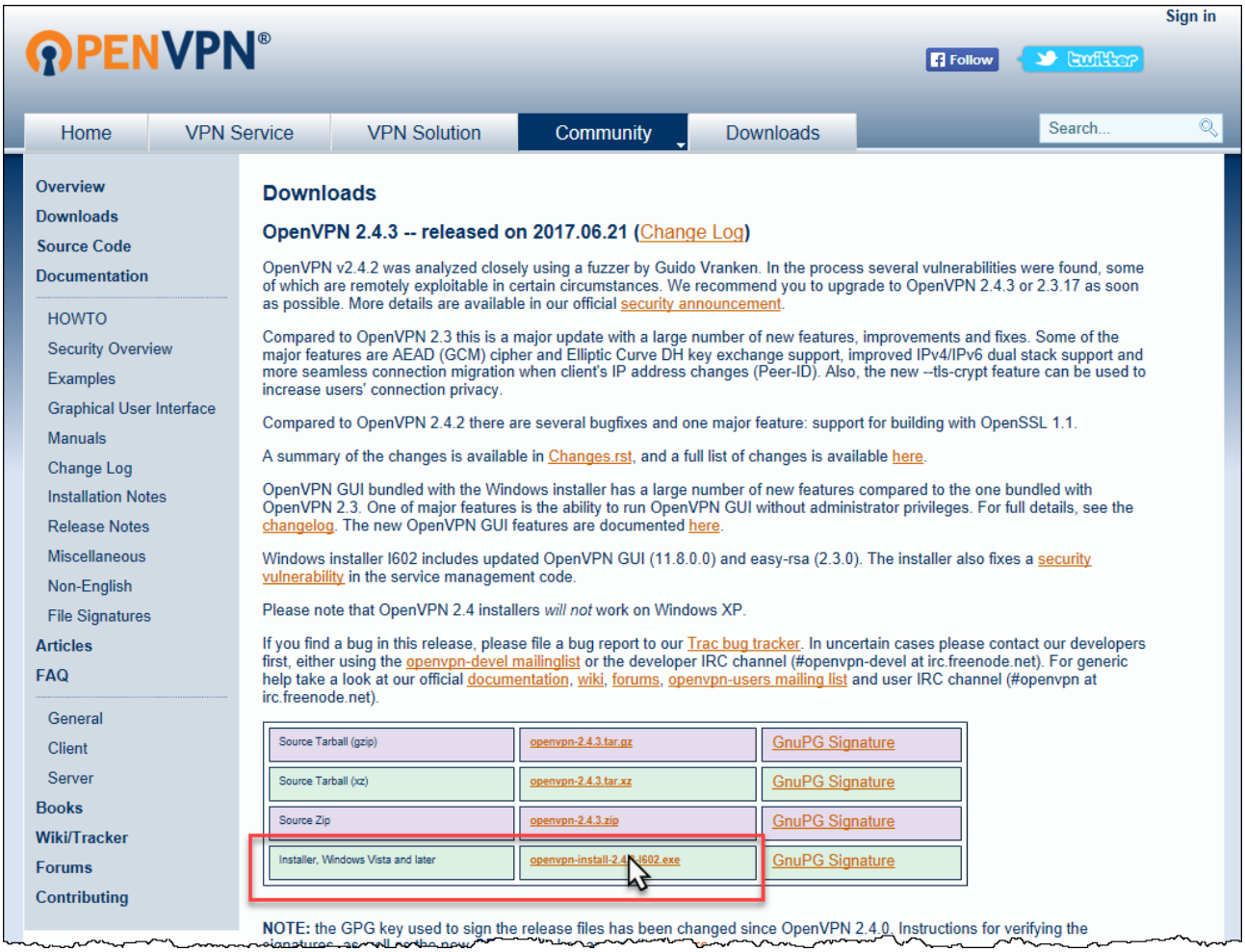
08. Instalace a konfigurace OpenVPN

Získání konfiguračního souboru

ⓘ	*Soubory s nastavením si můžete stáhnout i přes* scp*, pokud ho máte a umíte používat. Použijte následující příkaz, upravený podle názvu vašeho serveru (celý musí být na jednom řádku):* `scp root@streisand-demo.freemyip.com:/var/www/streisand/openvpn/client-1/streisand-combined.ovpn streisand-combined.ovpn` *V cestě můžete používat* `client-1` *až* `client-5`*, podle toho pro kterého uživatele chcete soubor získat. Pokud již soubor máte, pokračujte krokem číslo 8.*
1.	Otevřete soubor `streisand.html`.
2.	Klepněte na odkaz *Connecting to your Streisand Gateway – SSL*.
3.	Přejděte na zde uvedenou adresu a přihlašte se uvedeným uživatelským jménem a heslem. To ještě neslouží k připojení k VPN, ale pouze k získání přihlašovacích údajů. 
4.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN: 
5.	Klepněte na odkaz *OpenVPN (direct)*.
6.	Na samém konci stránky najdete profily ke stažení. Jsou tam tři sekce: • Alternate unified profiles for access via port 443 • Alternate unified profiles for access via UDP port 8757 • Alternate profile that will cycle through UDP port 8757, TCP port 636, and TCP port 443

	V různých sítích mohou být blokovány různé porty. Váš VPN server naslouchá na několika různých, aby zvýšil šanci, že budete úspěšní. Z tohoto pohledu je nejlepší profil v poslední sekci, který bude postupně zkoušet různé metody.
7.	Stáhněte si soubor s příponou `.ovpn`. Na výběr máte z odkazů *client-1* až *client-5*, můžete použít kterýkoliv z nich (jde o pět různých profilů pro až pět různých uživatelů).

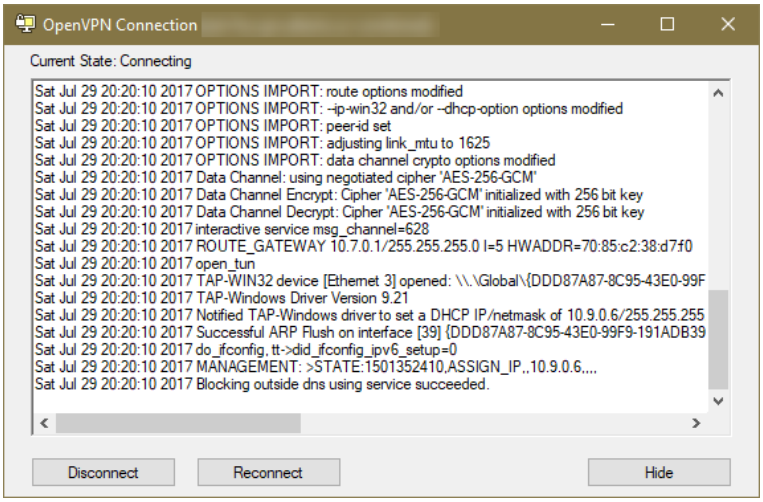
Instalace OpenVPN

8.	Otevřete v prohlížeči adresu `https://openvpn.net/`.
9.	Klepněte na odkaz *Community*.
10.	Klepněte na odkaz *Downloads* v levém menu.
11.	Stáhněte si instalátor pro Windows – v době psaní textu je aktuální verze 2.4.3: 
12.	Spusťte stažený instalátor OpenVPN.
13.	Klepněte na tlačítko *Next*.
14.	Klepnutím na *I Agree* odsouhlaste licenční podmínky.
15.	Ponechte výchozí nastavení komponent pro instalaci a klepněte na *Next*.
16.	Ponechte výchozí instalační adresář a klepněte na *Install*.
17.	Potvrďte instalaci ovladače pro TAP.
18.	Dokončete instalaci klepnutím na Next a Finish.

Konfigurace OpenVPN

19.	Spusťte program *OpenVPN GUI*.
20.	Zobrazí se varování, že nejsou definovány žádné profily. Zavřete ho klepnutím na OK.
21.	Na liště se objeví nová ikonka OpenVPN. Klepněte na ni pravým tlačítkem a z kontextového menu zvolte *Import file...*
22.	Vyberte soubor s příponou `.ovpn`, stažený v kroku číslo 7.

Připojení a odpojení VPN

23.	Pro připojení do VPN klepněte na ikonku v liště pravým tlačítkem a zvolte *Connect*.
24.	Zobrazí se okno s popisem průběhu připojování. Když zmizí a ikonka v liště změní barvu na zelenou, jste připojeni. 
25.	Pro odpojení klepněte na ikonku v liště pravým tlačítkem a zvolte *Disconnect*.

09. Zrušení a opětovné zřízení dropletu u Digital Ocean

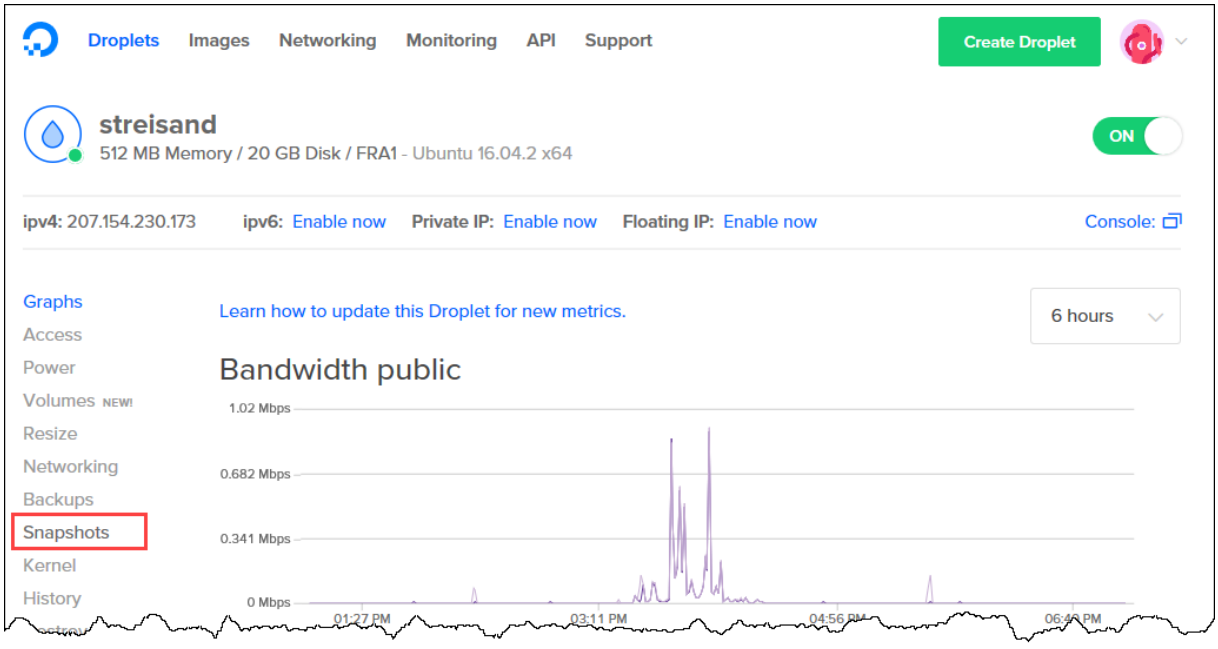
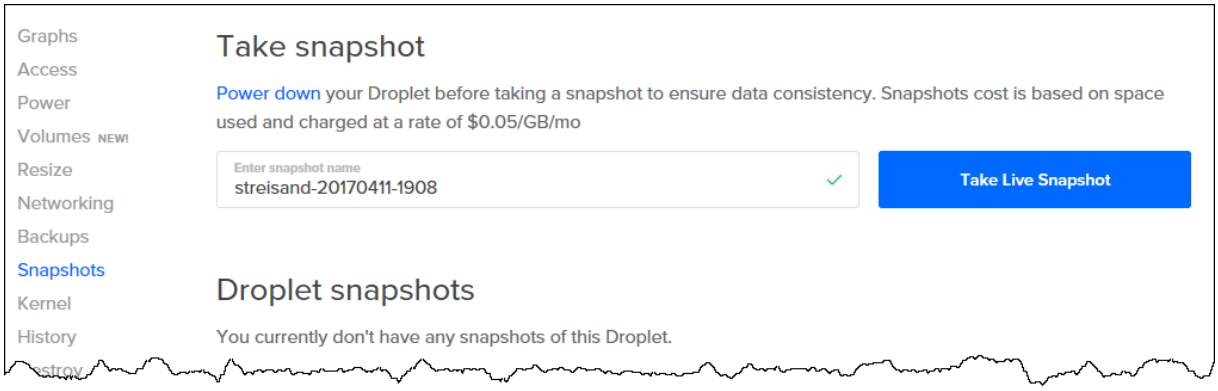
Provoz nejmenšího virtuálního serveru (dropletu) u Digital Ocean stojí $ 5 měsíčně. VPN ovšem nejspíš nebudete používat celou dobu, takže můžete ještě ušetřit a virtuální server mít spuštěný pouze ve chvíli, kdy jej chcete využít.

Aby se za něj neplatilo, nestačí ovšem virtuální počítač pouze vypnout. Musíte ho úplně zrušit a příště zřídit znovu. Ovšem abyste nemuseli začínat vždy od nuly, můžete si udělat takzvaný snapshot – obraz virtuálního počítače, který je možné kdykoliv proměnit na droplet.

Vytvoření snapshotu

1.	Přihlašte se na svůj server pomocí SSH nebo webové konzole.

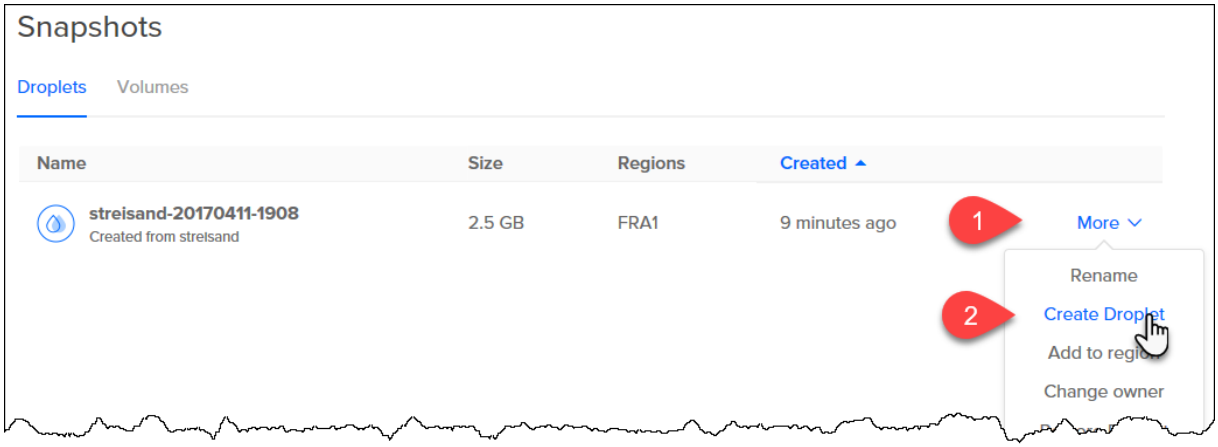
2.	Následujícím příkazem server vypněte:
	`root@streisand:~# shutdown -hP now`
	`Connection to streisand-demo.freemyip.com closed by remote host.`
	`Connection to streisand-demo.freemyip.com closed.`

ⓘ	*Vypnutí serveru není absolutně nezbytné, snapshot lze udělat i z běžícího počítače. Z důvodu konzistence dat se nicméně doporučuje server vypnout.*
3.	Otevřete v prohlížeči adresu `https://www.digitalocean.com/` a přihlašte se svým jménem a heslem.
4.	V seznamu dropletů klepněte na název vašeho Streisand serveru.
5.	V levém menu klepněte na odkaz Snapshot. 
6.	Zadejte název snapshotu (například ve formátu `streisand-RRRRMMDD-hhmm`) a klepněte na tlačítko *Take Live Snapshot*. 
7.	Vyčkejte, dokud se nevytvoří snapshot, což může nějakou trvat několik minut.
ⓘ	*I za snapshot se platí, ale méně. Za snapshot typického Streisand serveru zaplatíte přibližně 3 Kč měsíčně.*

Zrušení dropletu

8.	V levém menu klepněte na odkaz *Destroy*.
9.	Na stránce klepněte na velké tlačítko *Destroy*.
10.	V potvrzovacím dialogu klepněte na tlačítko *Confirm*.
11.	Nyní je droplet zničen a neplatíte za něj. Platíte pouze za diskový prostor zabraný snapshotem, což jsou minimální částky.

Opětovné zřízení dropletu ze snapshotu

12.	Klepněte na odkaz *Images* v horní části stránky.
13.	V seznamu snapshotů vyberte ten správný a klepněte na odkaz *More* vpravo.
14.	Z menu zvolte *Create Droplet*. 
15.	Podobně jako při vytvoření nového dropletu můžete zvolit jeho velikost (a cenu) a pojmenovat ho.
16.	Klepnutím na tlačítko *Create* droplet vytvoříte a nastartujete.

Poznámky k používání snapshotů

Procesem zrušení a nového vytvoření dropletu se **změní jeho IP adresa** a tím i IP adresa, pod kterou přistupujete do Internetu. To může být dobrou obranou proti případnému sledování.

Snapshot můžete používat opakovaně – stačí jej vytvořit jednou, nemusíte jej znovu vytvářet před každým zrušením dropletu. **Nicméně je třeba jej udržovat aktuální**, což Streisand za běhu dělá automaticky. Jednou za čas je tedy dobré vytvořit nový snapshot a ten starý smazat.