



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

Michal Altair Valášek

michal.valasek@altairis.cz
@ridercz

Obsah

Obsah	3
Co je VPN a proč ji chcete používat	5
Virtuální privátní síť	5
Proč používat VPN?	6
VPN jako služba a proč ji nepoužívat	6
Vlastní brána v oblacích	6
Streisand Effect a Streisand server	7
Návod k použití návodu	9
Typografické konvence	9
01. Vytvoření virtuálního počítače u Digital Ocean	11
Vytvoření dropletu (virtuálního serveru)	11
První přihlášení	12
02. Vytvoření virtuálního počítače v Microsoft Azure	15
Vytvoření Azure Cloud Shellu	15
Vytvoření SSH klíčů	16
Vytvoření VM pomocí skriptu	16
První připojení přes SSH	18
03. Nastavení dynamického DNS	19
04. Instalace Streisand serveru	21
05. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1	27
Získání přihlašovacích údajů	27
Příprava připojení	28
Vytvoření nového VPN připojení	28
Odpojení od VPN a opětovné připojení	30
06. Nastavení L2TP/IPSec VPN na Windows 7	31
Získání přihlašovacích údajů	31
Příprava připojení	32
Vytvoření nového VPN připojení	32
Odpojení od VPN a opětovné připojení	35
07. Nastavení L2TP/IPSec VPN na Androidu 6.0	37
08. Instalace a konfigurace OpenVPN na Windows	39
Získání konfiguračního souboru	39
Příprava OVPN souboru	39
Instalace OpenVPN	40
Konfigurace OpenVPN	40
Připojení a odpojení VPN	40
09. Zrušení a opětovné zřízení dropletu u Digital Ocean	41
Vytvoření snapshotu	41
Zrušení dropletu	42
Opětovné zřízení dropletu ze snapshotu	42
Poznámky k používání snapshot	42

Datum vydání: 5.12.2017

Verze: 11

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



Toto dílo je šířeno pod licencí CC BY-SA 4.0 – **Creative Commons Attribution-ShareAlike 4.0 International**¹. Můžete ho nadále šířit a upravovat za předpokladu, že uvedete původního autora a budete-li jej šířit pod stejnou licencí.

Za spolupráci při tvorbě české verze děkuji následujícím lidem (a jiným druhům, vy víte co jste zač):

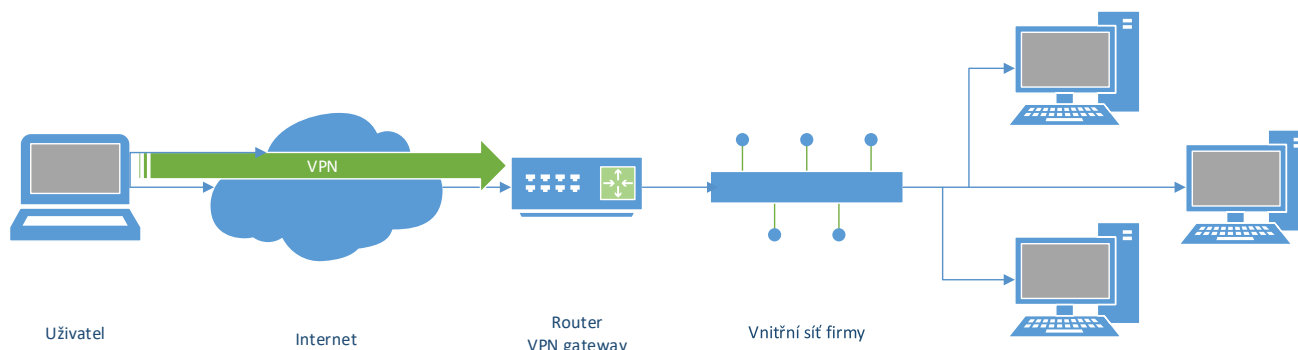
- Richard Torhan
- Kamil Roman
- Jakub Čermák

¹<https://creativecommons.org/licenses/by-sa/4.0/>

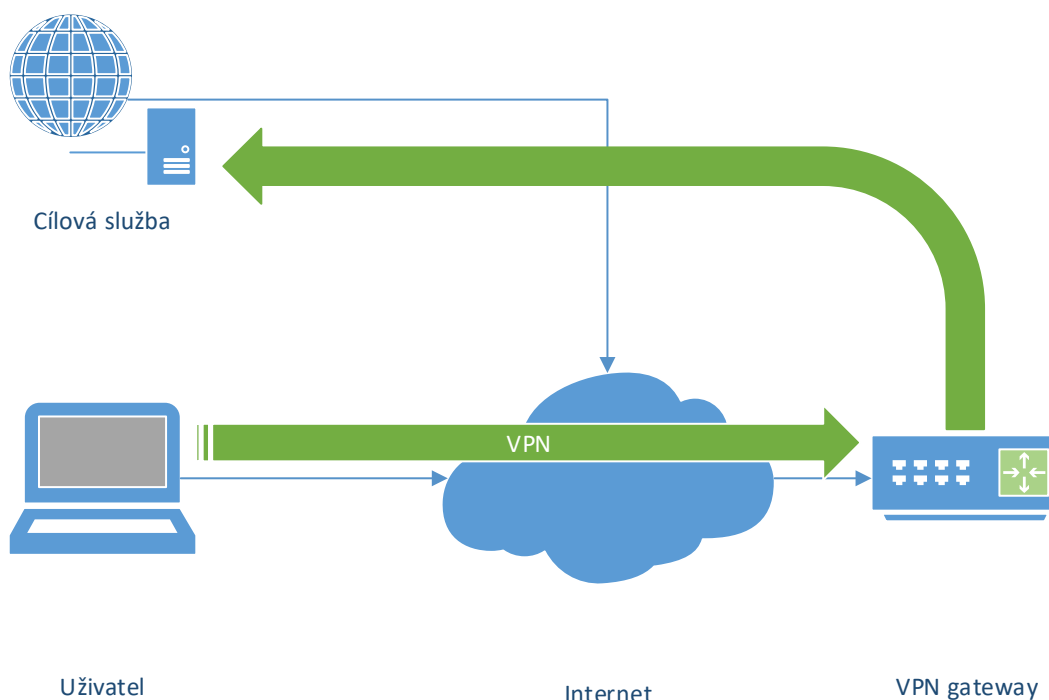
Co je VPN a proč ji chcete používat

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 využít 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 navrženy 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 kterém 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. Návodů 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. V návodu **02. Vytvoření virtuálního počítače v Microsoft Azure** najdete tento postup pro cloudovou službu od Microsoftu, která nyní nabízí VM na rok zdarma.
- **Návod 03. 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 04. 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.
- **Návody 05. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1, 06. Nastavení L2TP/IPSec VPN na Windows 7 a 07. Nastavení L2TP/IPSec VPN na Androidu 6.0** se zabývají možností připojení pomocí L2TP/IPSec. Výhodou této technologie je, že ji podporuje naprostá většina platform. Tento návod se zabývá platformami Windows a Android, na návodech pro Mac OS a iOS se pracuje. Nevýhodou je, že tato technologie nefunguje vždy a v některých sítích je (záměrně nebo špatnou konfigurací) blokována.
- **Návod 08. Instalace a konfigurace OpenVPN na Windows** 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 popisují pouze instalaci pod Windows, OpenVPN klient je dostupný pro většinu běžných platform.
- 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

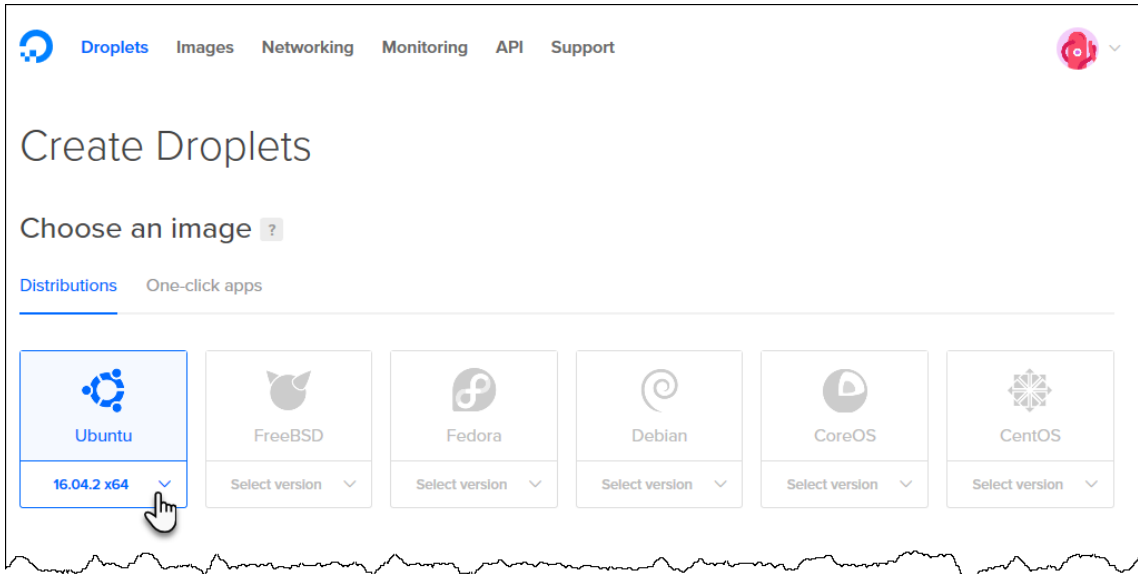
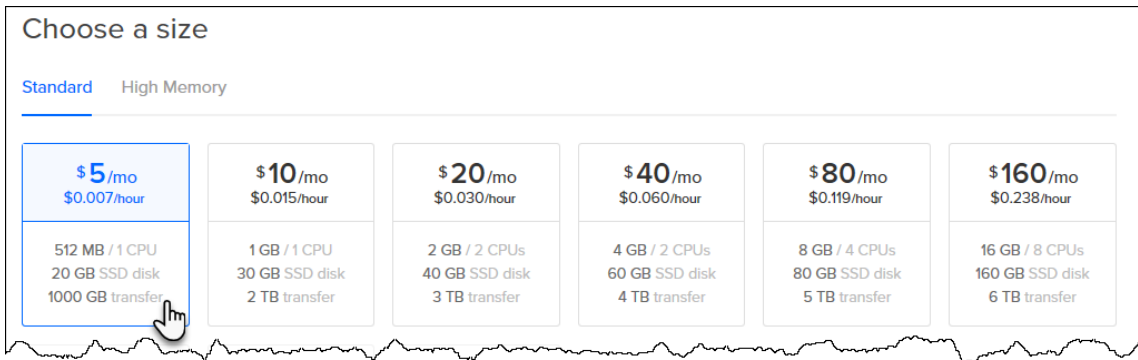
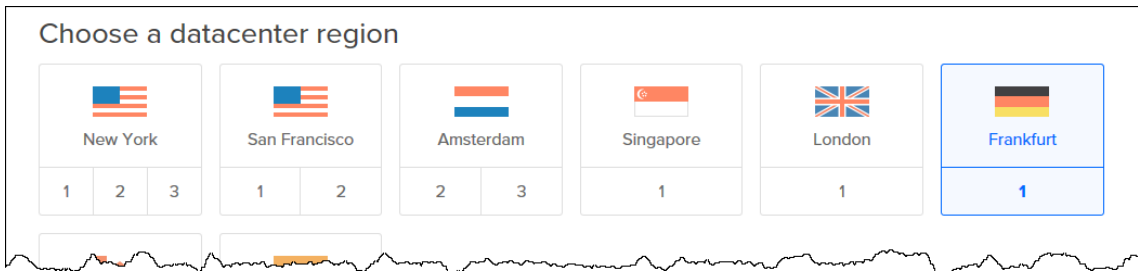
Jednotlivé návody jsou prezentovány formou tabulky s po sobě následujícími očíslovanými kroky. Při práci na si **jednotlivé body odškrtněte tužkou**. Přeskočení jednoho bodu může znamenat problém, který se ale projeví až o mnoho kroků později a může být obtížné ho odhalit.

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 ukázkou hierarchie v menu se používá šipka: <i>File → Open</i> .
①	<i>Kontextové poznámky a doplňující informace jsou psány takto, v samostatných buňkách.</i>
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.

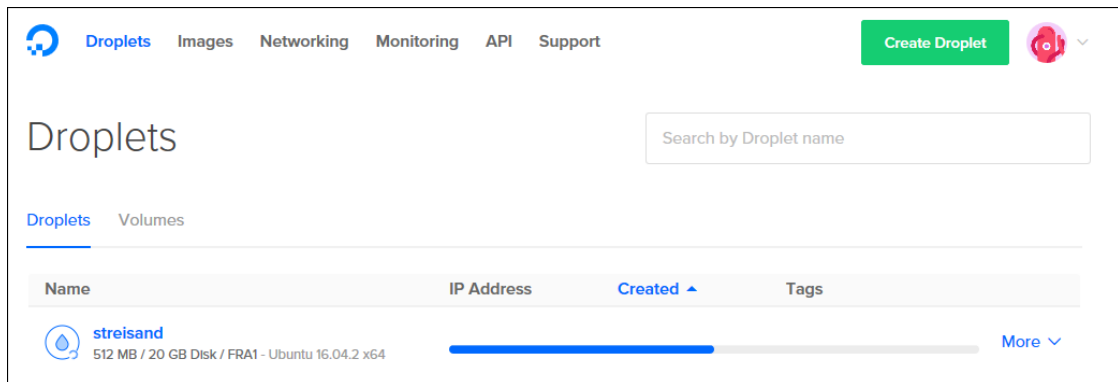
01. Vytvoření virtuálního počítače u Digital Ocean

1.	Otevřete v prohlížeči adresu https://www.digitalocean.com/ .
①	Můžete se též registrovat přes tuto adresu: https://m.do.co/c/121847281617 . To je můj referral link a pokud se přes něj přihlásíte, dostanete do začátku kredit 10 USD a já dostanu provizi, když něco utratíte.
2.	Klepněte na tlačítko <i>Sign Up</i> .
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 <i>Create Droplet</i> v pravé horní části stránky.
5.	V sekci <i>Choose an image</i> vyberte <i>Ubuntu 16.04 x64</i> : 
6.	V sekci <i>Choose a size</i> zvolte nejmenší velikost za \$ 5 měsíčně: 
7.	Sekci <i>Add block storage</i> ponechte beze změny.
8.	V sekci <i>Choose a datacenter region</i> si zvolte místo, kde se má váš server nacházet: 
①	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

	<i>výše zvolil Frankfurt, protože je k nám z hlediska síťové topologie obvykle nejbližší a spojení tedy bude nejrychlejší.</i>
9.	Sekci <i>Select additional options</i> ponechte beze změny.
10.	Sekci <i>Add your SSH keys</i> ponechte beze změny.
①	<i>Pokud umíte používat SSH a autentizaci klíči, můžete je samozřejmě použít a ušetřit si práci s opisováním hesla a ještě zvýšit bezpečnost.</i>
11.	V sekci <i>Finalize and create</i> dejte svému serveru jméno (např. streisand) a klepnutím na velké tlačítko <i>Create</i> jej vytvořte.
12.	Čekajte, 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 <i>Bash on Ubuntu on Windows</i> , tedy linuxového subsystému ve Windows 10. Můžete nicméně použít například populární PuTTY ³ nebo cokoliv jiného.
①	<i>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.</i>
15.	Připojte se jako uživatel root k IP adrese vašeho serveru (zde v příkladu uvádím 198.51.100.1): altair@akhal-teke:~\$ ssh root@198.51.100.1

³ <http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

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

```
The authenticity of host '198.51.100.1 (198.51.100.1)' 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 '198.51.100.1' (ECDSA) to the list of known hosts.
```

Zadejte jednorázové heslo, které jste obdrželi e-mailem.

```
root@198.51.100.1'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 přihlášení.

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

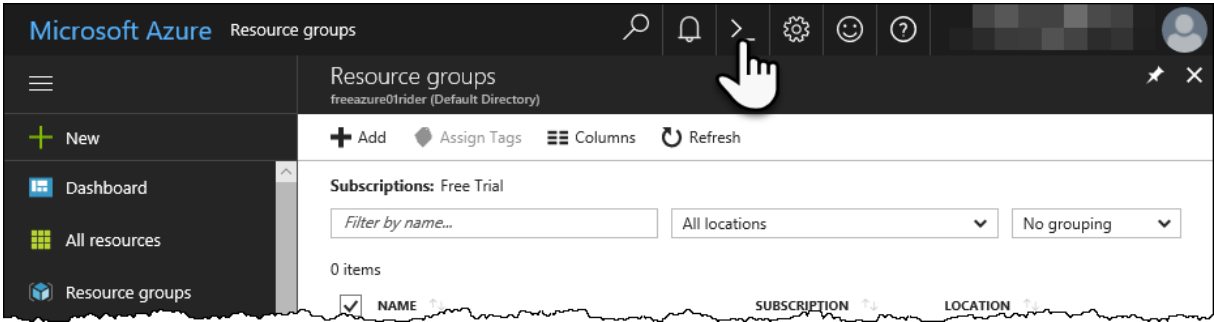
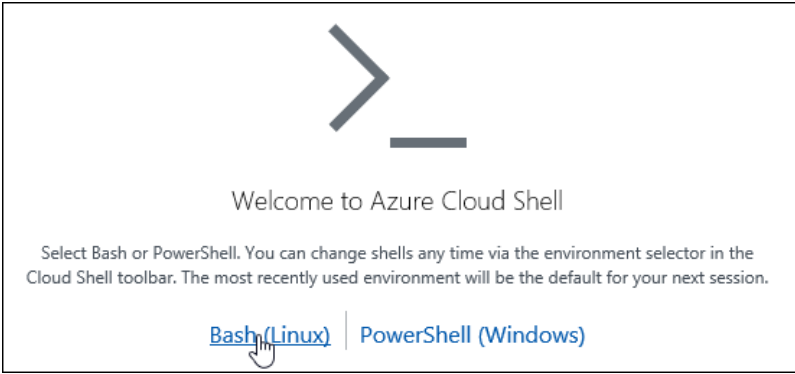
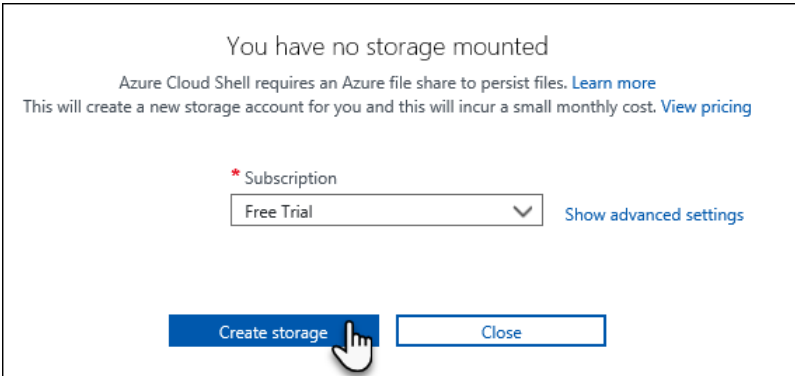

02. Vytvoření virtuálního počítače v Microsoft Azure

Jiným cloudovým poskytovatelem je Microsoft Azure. V době psaní tohoto článku nabízí na 12 měsíců zdarma virtuální server velikosti B1S (1 CPU core, 1 GB RAM), jinak stojí \$4.46 měsíčně. Pro prvních 30 dnů máte k dispozici navíc kredit \$200 na využití ostatních služeb. Po uplynutí těchto 30 dnů je nutné přejít na Pay-as-you-go program, kdy za služby, které nejsou zdarma, platíte standardní sazbu.

1.	Otevřete v prohlížeči adresu https://www.azure.com/ .
2.	Klepněte na odkaz <i>Start Free</i> a přihlašte se svým Microsoft účtem nebo si vytvořte nový. V průběhu registrace budete muset ověřit své telefonní číslo a zadat číslo platební karty (nebudete ale nic platit, pokud to v Azure explicitně nepovolíte).

Vytvoření Azure Cloud Shellu

Potřebná VM se dá v Azure „naklikat“ přes webové rozhraní, ale rychlejší je využít funkci Azure Cloud Shell, což je příkazová řádka v prohlížeči. Pomocí ní se také dá celý proces dobře automatizovat. Další výhodou Azure Cloud Shellu je, že se pomocí něj můžete na vytvořený server připojit přes SSH rovnou z prohlížeče, bez nutnosti cokoli instalovat na svůj lokální počítač.

3.	Po přihlášení v pravém horním rohu klepněte na symbol >_: 
4.	Ve spodní části okna prohlížeče se zobrazí okno, kde si budete moci vybrat, zda chcete používat Bash nebo PowerShell. V tomto návodu budeme používat Bash, proto na něj klepněte: 
5.	V následujícím dialogu klepněte na <i>Create storage</i> : 

6.	Vyčkejte, dokud neproběhne vytvoření Azure Cloud Shellu. Že je vše dokončeno poznáte tak, že se vám zobrazí prompt v následujícím tvaru: uzivatel@Azure:~\$
7.	Kdykoliv budete chtít v Azure používat příkazový řádek, stačí klepnout na ikonku >_ na vrchu stránky.

Vytvoření SSH klíčů

Pro přihlašování k vašemu cloudovému serveru budeme používat místo hesla SSH klíč. Je to bezpečnější a pohodlnější.

8.	Pár SSH klíčů vytvořte následujícím příkazem: <pre>username@Azure:~\$ ssh-keygen Generating public/private rsa key pair. Enter file in which to save the key (/home/username/.ssh/id_rsa): (stiskněte ENTER) Created directory '/home/username/.ssh'. Enter passphrase (empty for no passphrase): (stiskněte ENTER) Enter same passphrase again: (stiskněte ENTER) Your identification has been saved in /home/username/.ssh/id_rsa. Your public key has been saved in /home/username/.ssh/id_rsa.pub. The key fingerprint is: SHA256:8xafXuWck0rI4PLhZx35TE8sVApjXp9Ey1eTA+L46UA username@cc-5b9d-ba50de7d-459161135-226p4 The key's randomart image is: +---[RSA 2048]---+ . .ooo o = o+= E + +.*+ . . o o.o So.oo=O.+.= . oo++.*+ +..+.o.oo oo .. +---[SHA256]-----+</pre>
①	<i>Pokud si chcete vygenerované klíče lokálně zazálohovat, což je dobrý nápad, můžete si je vypsát následujícími příkazy:</i> • Veřejný klíč: <code>cat .ssh/id_rsa.pub</code> • Tajný klíč: <code>cat .ssh/id_rsa</code> <i>Vypsané hodnoty si přes schránku uložte a zazálohujte</i>

Vytvoření VM pomocí skriptu

Proces vytváření a konfigurace VM jsem pro vás naskriptoval. Skript vytvoří Azure Resource Group jménem Streisand. RG je organizační jednotka, skupina různých služeb, které lze jednotně spravovat a případně smazat. Dále pak vytvoří Network Security Group a v ní pravidla pro firewall, která povolí porty potřebné pro různé služby, které Streisand poskytuje. Jako poslední vytvoří vlastní VM.

9.	Následujícím příkazem stáhněte skript pro vytvoření VM (celý příkaz musí být na jednom řádku): <pre>username@Azure:~\$ wget https://raw.githubusercontent.com/ridercz/Scripts/master/StreisandAzure/streisand-create-vm.sh --2017-10-22 16:34:04-- https://raw.githubusercontent.com/ridercz/Scripts/master/StreisandAzure/streisand-create-vm.sh Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.36.133 Connecting to raw.githubusercontent.com (raw.githubusercontent.com) 151.101.36.133 :443... connected. HTTP request sent, awaiting response... 200 OK Length: 3435 (3.4K) [text/plain] Saving to: 'streisand-create-vm.sh' streisand-create-vm.sh 100%[=====] 3.35K --.-KB/s in 0s 2017-10-22 16:34:04 (55.7 MB/s) - 'streisand-create-vm.sh' saved [3435/3435]</pre>
10.	Následujícím příkazem nastavte soubor streisand-create-vm.sh jako spustitelný: <pre>username@Azure:~\$ chmod +x streisand-create-vm.sh</pre>

11.	Následujícím příkazem skript spustíte: username@Azure:~\$./streisand-create-vm.sh																								
①	Skript se nastavuje pomocí následujících proměnných prostředí:																								
	<table><tr><th>Název</th><th>Popis</th><th>Výchozí hodnota</th></tr><tr><td>REGION</td><td>Azure region (umístění serveru)</td><td>WestEurope</td></tr><tr><td>RG_NAME</td><td>Název resource group</td><td>Streisand</td></tr><tr><td>NSG_NAME</td><td>Název network security group</td><td>StreisandNSG-\$REGION</td></tr><tr><td>VM_NAME</td><td>Název virtuálního serveru</td><td>Streisand-\$REGION</td></tr><tr><td>VM_SIZE</td><td>Velikost virtuálního serveru</td><td>Standard_B1s</td></tr><tr><td>VM_SSH_KEY</td><td>Cesta k použitému SSH klíči</td><td>~/.ssh/id_rsa.pub</td></tr><tr><td>LOGFILE</td><td>Cesta k vytvářenému log souboru</td><td>streisand-create-vm-*.log</td></tr></table>	Název	Popis	Výchozí hodnota	REGION	Azure region (umístění serveru)	WestEurope	RG_NAME	Název resource group	Streisand	NSG_NAME	Název network security group	StreisandNSG-\$REGION	VM_NAME	Název virtuálního serveru	Streisand-\$REGION	VM_SIZE	Velikost virtuálního serveru	Standard_B1s	VM_SSH_KEY	Cesta k použitému SSH klíči	~/.ssh/id_rsa.pub	LOGFILE	Cesta k vytvářenému log souboru	streisand-create-vm-*.log
	Název	Popis	Výchozí hodnota																						
	REGION	Azure region (umístění serveru)	WestEurope																						
	RG_NAME	Název resource group	Streisand																						
	NSG_NAME	Název network security group	StreisandNSG-\$REGION																						
	VM_NAME	Název virtuálního serveru	Streisand-\$REGION																						
	VM_SIZE	Velikost virtuálního serveru	Standard_B1s																						
	VM_SSH_KEY	Cesta k použitému SSH klíči	~/.ssh/id_rsa.pub																						
	LOGFILE	Cesta k vytvářenému log souboru	streisand-create-vm-*.log																						
Proměnné prostředí se nastavují před spuštěním skriptu příkazem export NÁZEV=hodnota. Záleží na velikosti velkých a malých písmen. Tj. např. budete-li chtít VM umístit do regionu EastUS, zadejte před spuštěním následující příkaz:																									
username@Azure:~\$ export REGION=EastUS																									
V době psaní tohoto textu byla bezplatná velikost B1S dostupná v regionech EastUS, WestUS2, WestEurope a SoutheastAsia. ⁴																									
12.	Skript vypíše seznam nastavení: Configured options for a Streisand VM: Region: WestEurope Resource Group: Streisand Network Security Group: StreisandNSG-WestEurope VM Name: Streisand-WestEurope VM Size: Standard_B1s VM SSH Key: /home/username/.ssh/id_rsa.pub Log file name: streisand-create-vm-20171204-214627.log This script will take about 10-15 minutes to complete. Are you sure you want to continue? (y/N) Pokud s hodnotami souhlasíte, zadejte y a stiskněte ENTER. Pokud chcete něco změnit, stiskněte naprázdno ENTER a upravte proměnné jak bylo napsáno výše.																								
13.	Výkejte, dokud neproběhnou všechny operace. To bude trvat cca. 10-15 minut. Na konci skript vypíše výsledek podobný následujícímu: Creating Azure Resource Group Streisand... Creating Network Security Group StreisandNSG-WestEurope... Adding firewall rules to StreisandNSG-WestEurope: SSH... IPSec-IKE... IPSec-L2TP... IPSec-NATT... HTTPS... HTTP... OpenConnect-TCP... OpenConnect-UDP... OpenVPN-TCP... OpenVPN-UDP... ... Creating VM... Migrating disk to cheaper Standard tier: Deallocating current VM... Updating disk... Starting VM... Done, the following VMs are available in the Streisand resource group: <table><tr><th>Name</th><th>IP</th><th>Location</th><th>Size</th><th>Provisioning</th><th>State</th></tr><tr><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>Streisand-WestEurope</td><td>198.51.100.1</td><td>westeurope</td><td>Standard_B1s</td><td>Succeeded</td><td>VM running</td></tr></table> It took 12 min, 10 sec. Log file is available: streisand-create-vm-20171204-214627.log	Name	IP	Location	Size	Provisioning	State	-----	-----	-----	-----	-----	-----	Streisand-WestEurope	198.51.100.1	westeurope	Standard_B1s	Succeeded	VM running						
Name	IP	Location	Size	Provisioning	State																				
-----	-----	-----	-----	-----	-----																				
Streisand-WestEurope	198.51.100.1	westeurope	Standard_B1s	Succeeded	VM running																				
14.	IP adresa nově vytvořené VM se nachází ve sloupci IP, zde 198.51.100.1.																								

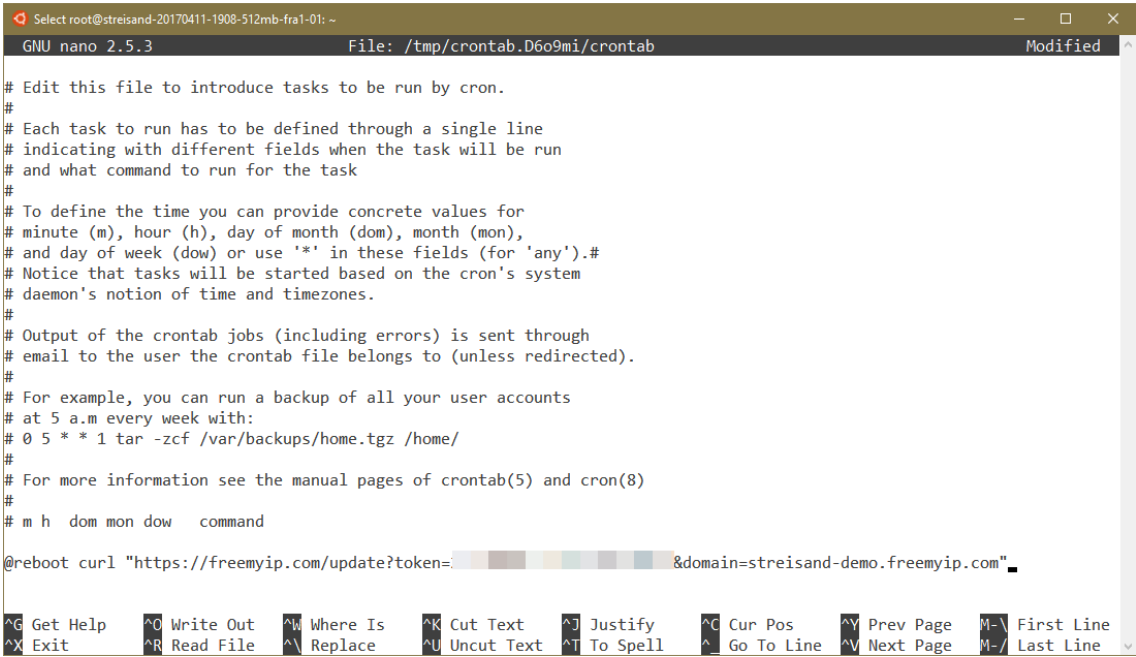
⁴ Dostupnost služeb v jednotlivých regionech najdete na <https://azure.microsoft.com/en-us/regions/services/>

První připojení přes SSH

15.	Na server se připojte následujícím příkazem (IP adresu nahradíte dle předchozího kroku): <code>username@Azure:~\$ ssh 198.51.100.1</code>
①	<i>Nemusíte zadávat žádné jméno a heslo, autentizujete se pomocí SSH klíče vytvořeného v kroku 8.</i>
16.	Při prvním přihlášení budete vyzváni k potvrzení správnosti SSH klíče serveru. Zadejte yes: The authenticity of host '198.51.100.1 (198.51.100.1)' can't be established. ECDSA key fingerprint is SHA256:xx. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '198.51.100.1' (ECDSA) to the list of known hosts.
17.	Jakmile uvidíte následující text, jste přihlášení: Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.11.0-1013-azure x86_64) ... <code>username@Streisand-WestEurope:~\$</code>

03. 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 <i>Domain name</i> zadejte název, který chcete používat. Musí být unikátní. V příkladech dále používám hostname <code>streisand-demo.freemyip.com</code> , ale vy si zvolte jiný. Poté klepněte na <i>Check Availability</i> .
3.	Pokud daný hostname není volný, zkuste to znovu. Pokud je, klepněte na <i>Submit</i> .
4.	Služba vám vygeneruje URL zhruba v následujícím formátu (skutečná adresa se bude lišit): <code>https://freemyip.com/update?token=xxxxxxxxxxxxxxxx&domain=streisand-demo.freemyip.com</code>
①	<i>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.</i>
5.	Připojte se pomocí SSH na server.
6.	Na serveru spusťte příkaz <code>sudo crontab -e</code> , kterým spustíte editaci tabulky plánovače událostí. Když se vás zeptá, jaký editor chcete používat, zvolte možnost 2, tedy <code>/bin/nano</code> : <pre>user@streisand:~\$ sudo 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</pre> 
7.	Ukáže se vám rozhraní textového editoru <i>GNU Nano</i> . Pomocí šipek dojděte na konec souboru (za řádky začínající znakem #, což znamená komentář).
8.	Přidejte nový řádek, který bude obsahovat <code>@reboot curl</code> a adresu získanou v bodu 4 v uvozovkách: <code>@reboot curl "https://freemyip.com/update?token=xxxxxxxxxxxxxxxx&domain=streisand-demo.freemyip.com"</code>
9.	Vyskočte z editoru stiskem kláves <code>Ctrl+X</code> (označeno jako <code>^X</code>).
10.	Na otázku <i>Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?</i> odpovězte <code>Y</code> .
11.	Název souboru nechte beze změny (stiskněte pouze <code>Enter</code>).
12.	Následujícím příkazem restartujte server, čímž vyzkoušíte, že se aktualizace DNS provede: <code>user@streisand:~\$ sudo reboot now</code>

04. Instalace Streisand serveru

Důležitá poznámka: Následující příklad předpokládá, že jste na serveru přihlášení jako root (administrátor). Tak funguje například DigitalOcean. V případě Windows Azure jste přihlášení jako jiný uživatel.

Pokud je poslední znak promptu # (např. root@streisand:~#), nemusíte nic dělat, máte práva roota. Pokud je poslední znak promptu \$ (např. user@streisand:~\$), zadejte před vykonáním příkazů v tomto příkladu následující příkazy:

```
username@Streisand-WestEurope:~$ sudo su
root@streisand:/home/username# cd ~
root@streisand:~#
```

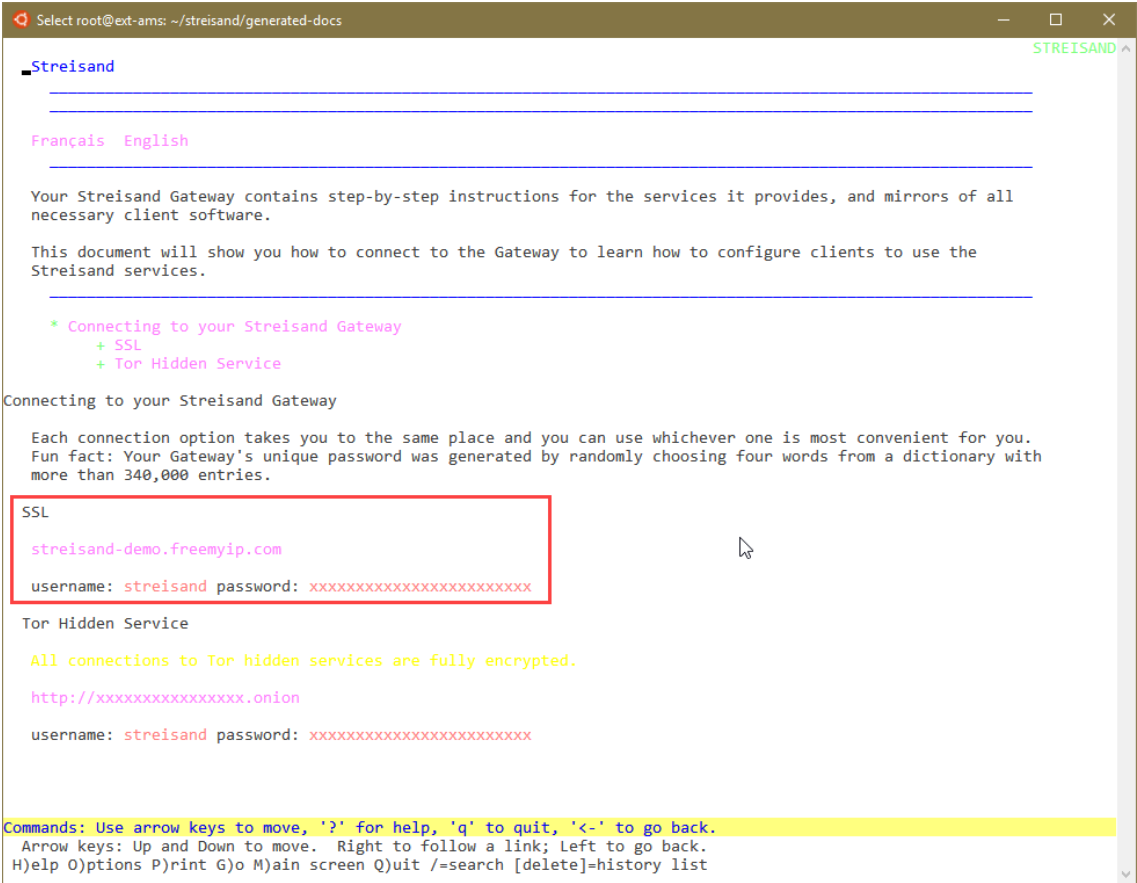
Povšimněte si přitom, že po zadání sudo su se změnil poslední znak z \$ na #, protože jste tímto příkazem získali práva roota. Příkaz sudo se dá s jistou mírou tolerance přirovnat k UAC promptu z Windows.

1.	Připojte se pomocí SSH na server (nyní již nemusíte používat IP adresu, ale můžete použít DNS jméno, které jste nastavili v předchozím příkladu 03. <i>Nastavení dynamického DNS</i>).
2.	Vytvořte pár klíčů pro ssh připojení následujícím příkazem: <pre>root@streisand:~/streisand# ssh-keygen Generating public/private rsa key pair. Enter passphrase (empty for no passphrase): (zadejte heslo nebo jen ENTER) Enter same passphrase again: (zadejte heslo nebo jen ENTER) Your identification has been saved in /root/.ssh/id_rsa. Your public key has been saved in /root/.ssh/id_rsa.pub. The key fingerprint is: SHA256:HA7NBCPRWdn0+Cy1ztU0pXj4DTmYcNONk78Vy6qCwQ4 root@streisand The key's randomart image is: +---[RSA 2048]-----+ ooo+o+o o. +. .o=. . = *+=o . + . B B++ + . + + O+ . S . + + = E o + o . o o + o . . . +---[SHA256]-----+</pre>
①	<i>Tyto klíče nebudeme sami k ničemu používat, ale potřebuje je instalace Streisand.</i>
3.	Připravil jsem skript, který řadu následujících kroků provede automaticky. Pokud jej chcete použít, pokračujte následujícím krokem. Pokud mi nevěříte (což je docela správné) a chcete celý proces udělat sami, pokračujte krokem číslo 8.
4.	Následujícím příkazem stáhněte skript pro vytvoření VM (celý příkaz musí být na jednom řádku): <pre>username@Azure:~\$ wget https://raw.githubusercontent.com/ridercz/Scripts/master/StreisandAzure/streisand-setup.sh --2017-10-22 16:34:04-- https://raw.githubusercontent.com/ridercz/Scripts/master/StreisandAzure/streisand-setup.sh Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.36.133 Connecting to raw.githubusercontent.com (raw.githubusercontent.com) 151.101.36.133 :443... connected. HTTP request sent, awaiting response... 200 OK Length: 3435 (3.4K) [text/plain] Saving to: 'streisand-setup.sh' streisand-setup.sh 100%[=====] 3.35K --.-KB/s in 0s 2017-10-22 16:34:04 (55.7 MB/s) - 'streisand-setup.sh' saved [3435/3435]</pre>
5.	Následujícím příkazem nastavte soubor streisand-setup.sh jako spustitelný:
6.	Následujícím příkazem skript spusťte:

7.	Poračujte krokem číslo 14 – několik kroků můžete přeskočit, udělal je za vás skript.
8.	Na serveru zadejte následující příkaz, kterým aktualizujete seznam dostupných balíčků a nainstalované balíčky samotné. To bude trvat několik minut. <pre> root@streisand:~# apt-get update && apt-get upgrade -y 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:~#</pre>
9.	Zadejte následující příkaz, kterým nainstalujete komponenty, které Streisand potřebuje. Opět to bude nějakou dobu trvat: <pre> 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:~#</pre>
10.	Zadejte následující příkaz, kterým nainstalujete Ansible, který Streisand využívá pro konfiguraci: <pre> root@streisand:~# pip install ansible markupsafe 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:~#</pre>
11.	Zadejte následující příkaz, kterým stáhnete aktuální verzi Streisand z Githubu: <pre> root@streisand:~# git clone https://github.com/jlund/streisand.git 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#</pre>
12.	Přejděte do nově vytvořeného adresáře streisand následujícím příkazem: <pre> root@streisand:~# cd streisand</pre>
13.	Spustíte instalaci následujícím příkazem: <pre> root@streisand:~/streisand# ./streisand</pre>
14.	Spustí se průvodce, kde jako první zvolte volbu 7 (instalace na lokální server) a potvrďte zadáním slova streisand. Nechcete instalaci customizovat, takže na příslušnou otázku jenom naprázdno odešlete ENTERem. <pre> S T R E I S A N D Created new Streisand home directory: /root/.streisand Created new Streisand site vars file: /root/.streisand/site.yml Which provider are you using? 1. Amazon 2. Azure 3. DigitalOcean 4. Google 5. Linode 6. Rackspace 7. Localhost (Advanced) 8. Existing Server (Advanced) :7 LOCAL PROVISIONING WILL OVERWRITE CONFIGURATION ON **THIS** MACHINE.</pre>

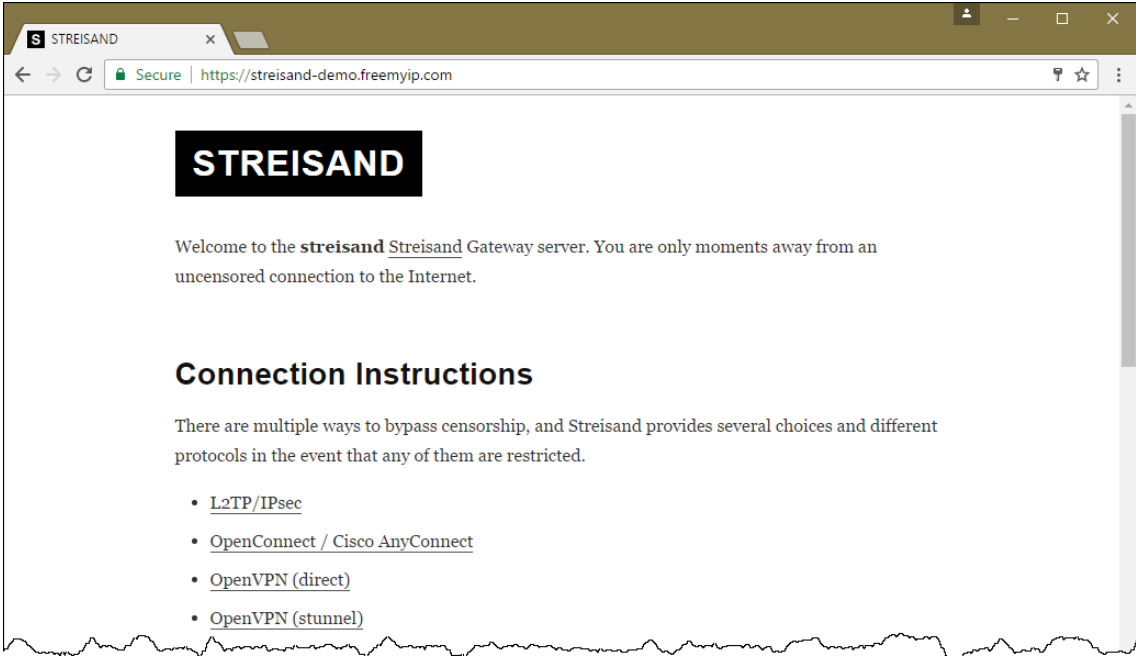
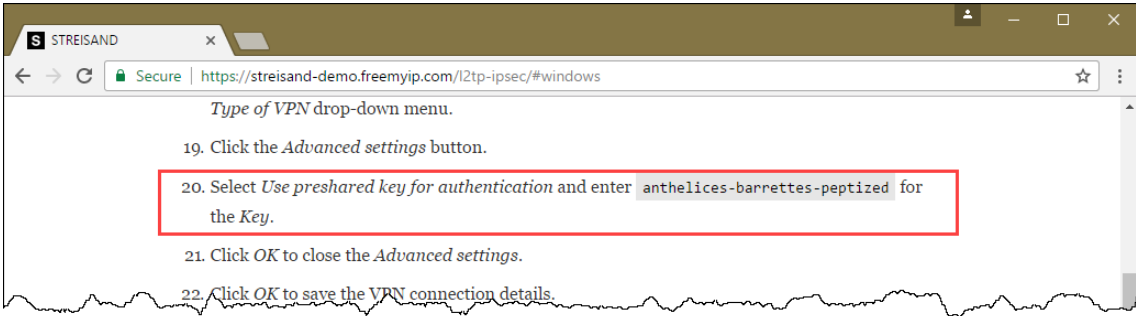
	THE MACHINE YOU ARE CURRENTLY EXECUTING THIS SHELL SCRIPT ON. ARE YOU 100% SURE THAT YOU WISH TO CONTINUE? Please enter the word 'streisand' to continue: streisand Confirmed. Continuing Do you wish to customize which services Streisand will install? Please enter the word 'yes' or hit enter to continue: (stiskněte ENTER) Installing Streisand services specified in /root/.streisand/site.yml ...
15.	Nyní proběhne řada akcí, může to trvat i několik minut.
16.	Na následující výzvu zadejte DNS název vašeho Streisand serveru, vytvořený v předchozím návodu 03. <i>Nastavení dynamického DNS</i>. Také zadejte e-mailovou adresu, na kterou vám mají být zasílány zprávy při problémech s certifikátem. Which domain do you want to use to host Streisand server? This is an optional question. If you have a domain that points to your Streisand server, the installation scripts can request Let's Encrypt HTTPS certificates for you automatically. If you do not provide one or the request fails, self-signed certificates will be used instead. If you have just created a new cloud server in previous steps, it is good time to point your domain to your server's public address, as DNS changes take time to propagate. Please type your domain below. Press enter to skip. : streisand-demo.freemyip.com Which email address do you want to use as contact of Streisand server? This is an optional question. The email is only used as contact method of your Let's Encrypt account. Please type your email below. Press enter to skip. : hostmaster@example.com
17.	Vyčkejte. Nyní se vše instaluje a konfiguruje a bude to trvat docela dlouho, několik desítek minut.
18.	Po úspěšném dokončení instalace se zobrazí následující zpráva: <pre>TASK [streisand-gateway : Success!] ***** [streisand-gateway : Success!] 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.: Stiskněte ENTER a nenechte se zaskočit zobrazenou chybou, že není možné otevřít HTML soubor.</pre>
19.	Informace potřebné pro připojení k vašemu novému Streisand serveru se nacházejí ve složce generated-docs. Název souboru je odvozen od názvu vašeho serveru. Seznam souborů si můžete vypsát pomocí následujícího příkazu: <pre>root@streisand:~/streisand# ls -l generated-docs/ total 32 -rw-r--r-- 1 root root 7363 Oct 21 23:07 streisand-firewall-information-fr.html -rw-r--r-- 1 root root 7351 Oct 21 23:07 streisand-firewall-information.html -rw-r--r-- 1 root root 7431 Oct 21 23:07 streisand-fr.html -rw-r--r-- 1 root root 7280 Oct 21 23:07 streisand.html</pre> Nejdůležitější soubor se základními informacemi se v tomto případě jmenuje streisand.html. V něm se nacházejí důležité informace a je nutné ho zobrazit.
①	<i>Instrukce zkopírujte na svůj počítač. Pokud máte na svém počítači SCP a umíte jej používat, pokračujte následujícím krokem. Pokud nemáte, pokračujte krokem 22.</i>
20.	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 a místo streisand.html název souboru. Uživatelské jméno root před zavináčem nahraďte svým uživatelským jménem (v Microsoft Azure je odvozeno od vaší e-mailové adresy a vidíte ho v rámci promptu před zavináčem, případně jej můžete zjistit pomocí příkazu whoami). <pre>scp root@streisand-demo.freemyip.com:~/streisand/generated-docs/streisand.html streisand.html</pre>

21.	Lokálně stažený soubor otevřete v prohlížeči a opište si přihlašovací údaje: STREISAND Français English Your Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. This document will show you how to connect to the Gateway to learn how to configure clients to use the Streisand services. Connecting to your Streisand Gateway ◦ SSL ◦ Tor Hidden Service Connecting to your Streisand Gateway Each connection option takes you to the same place and you can use whichever one is most convenient for you. Fun fact: Your Gateway's unique password was generated by randomly choosing four words from a dictionary with more than 340,000 entries. SSL streisand-demo.freemyip.com username: <code>streisand</code> password: <code>xx</code> Tor Hidden Service <i>All connections to Tor hidden services are fully encrypted.</i> http://xxxxxxxxxxxxxxxxxx.onion username: <code>streisand</code> password: <code>xx</code>
22.	Pokračujte krokem 26. Nemáte-li SCP, můžete si na server nainstalovat textový prohlížeč Lynx následujícím příkazem: <pre> root@streisand:~# apt-get install -y lynx Reading package lists... Done Building dependency tree Reading state information... Done The following additional packages will be installed: lynx-common The following NEW packages will be installed: lynx lynx-common 0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded. Need to get 1,035 kB of archives. After this operation, 2,761 kB of additional disk space will be used. Get:1 http://mirrors.digitalocean.com/ubuntu xenial/universe amd64 lynx-common all 2.8.9dev8-4ubuntu1 [411 kB] ... Setting up lynx (2.8.9dev8-4ubuntu1) ... update-alternatives: using /usr/bin/lynx to provide /usr/bin/www-browser (www-browser) in auto mode root@streisand:~# </pre>
23.	Prohlížení souboru spustíte následujícím příkazem (název souboru upravte dle skutečnosti): <pre> root@streisand:~# lynx ~/streisand/generated-docs/streisand.html </pre>

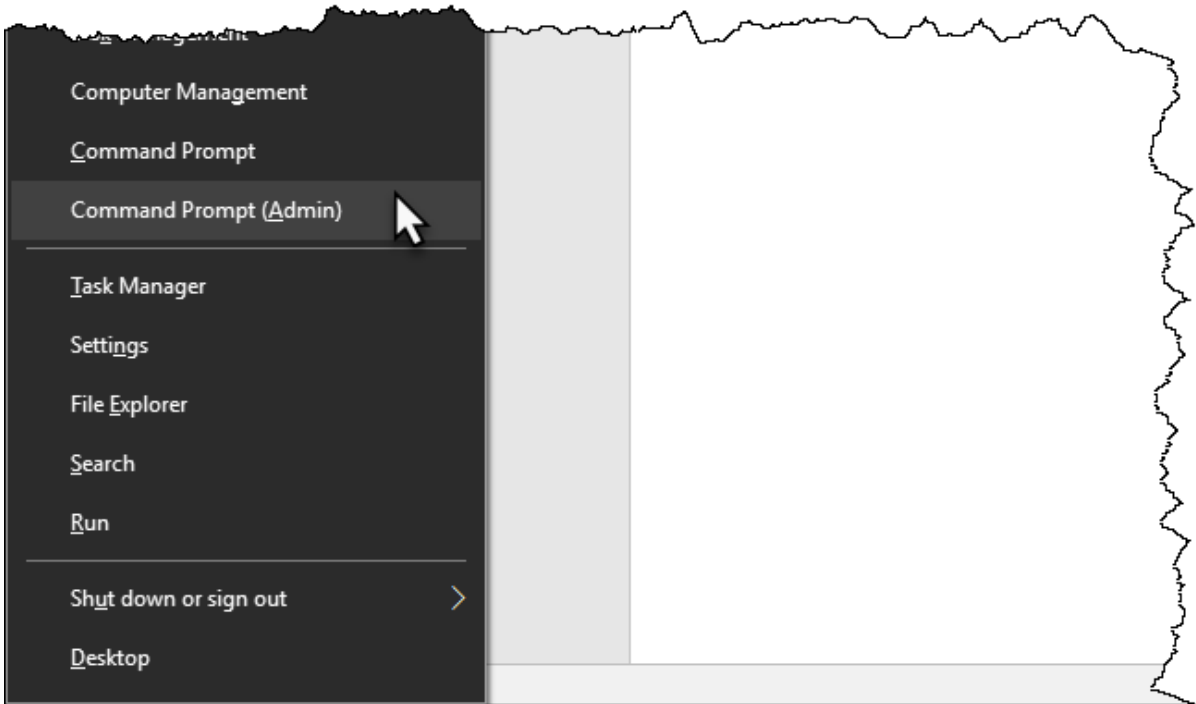
24.	Zobrazí se vám informační soubor – opište si přihlašovací údaje: 
25.	Z prohlížeče vyskočíte klávesou Q a potvrdíte ENTER.
26.	Zadejte do prohlížeče adresu uvedenou v instrukčním souboru (zde https://streisand-demo.freemyip.com). Pro přihlášení uveďte uživatelské jméno streisand a heslo uvedené v instrukčním souboru.
27.	Na tomto webu najdete personalizované informace potřebné pro připojení pomocí různých typů VPN (pozor, jsou jiné než výše uvedené jméno a heslo, to slouží pouze k připojení na informační server). Můžete se jimi řídit, případně můžete použít další návody v této příručce, které jsou podrobnější a aktualizované.

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

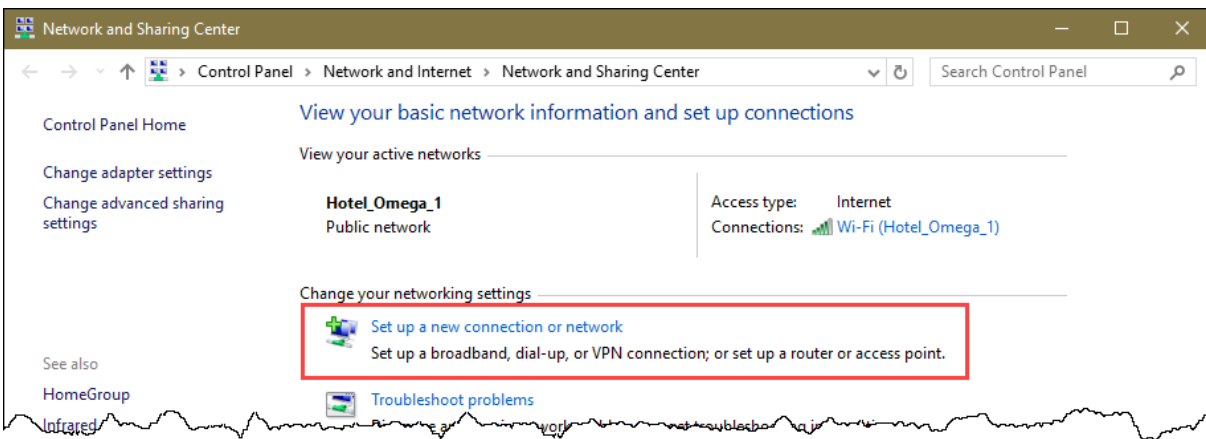
Získání přihlašovacích údajů

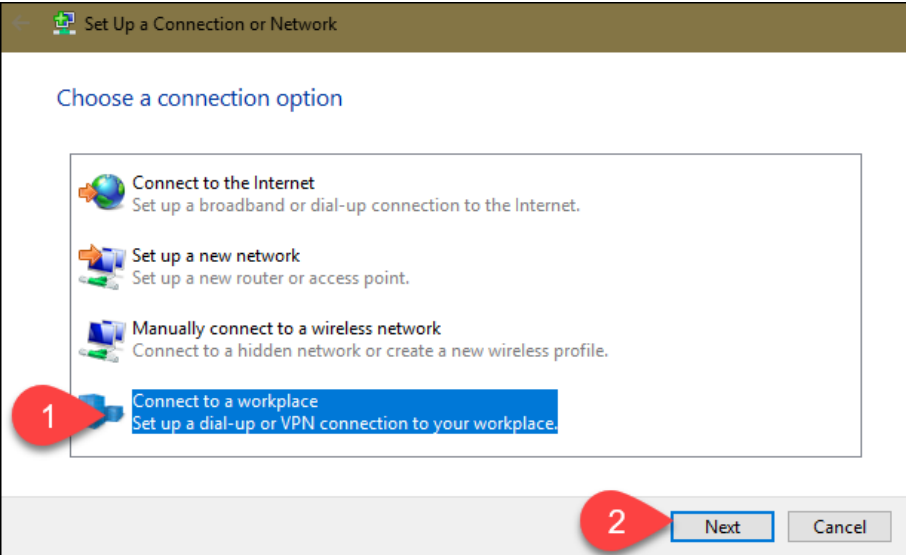
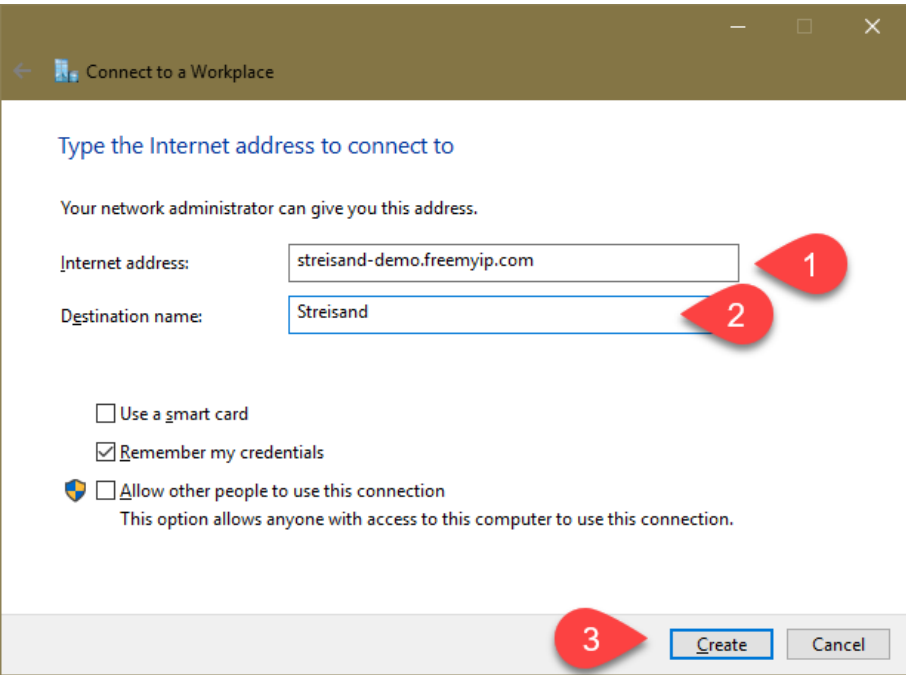
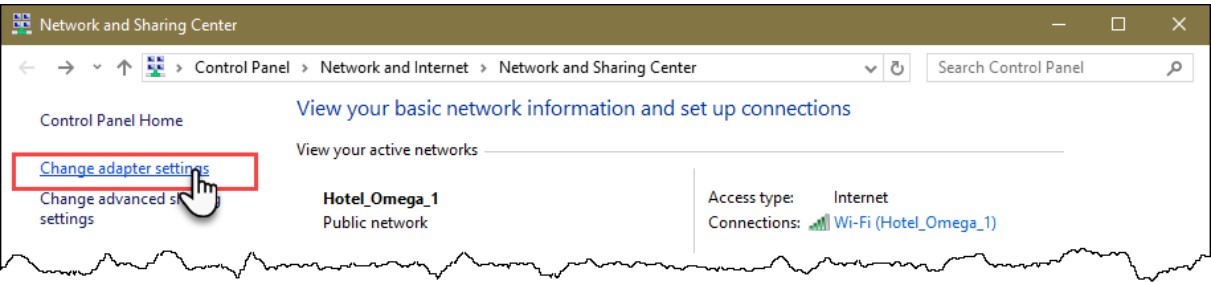
1.	Zadejte do prohlížeče adresu svého Streisand serveru a přihlaste se jménem a heslem, viz konec předchozího příkladu 04. <i>Instalace Streisand serveru</i> .
2.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN:  The screenshot shows the Streisand website in a web browser. The URL is https://streisand-demo.freemyip.com. The page has a black header with the word 'STREISAND' in white. Below the header, it says 'Welcome to the streisand Streisand Gateway server. You are only moments away from an uncensored connection to the Internet.' Under the heading 'Connection Instructions', it lists four options: L2TP/IPsec, OpenConnect / Cisco AnyConnect, OpenVPN (direct), and OpenVPN (stunnel). STREISAND Welcome to the streisand Streisand Gateway server. You are only moments away from an uncensored connection to the Internet. Connection Instructions There are multiple ways to bypass censorship, and Streisand provides several choices and different protocols in the event that any of them are restricted. • L2TP/IPsec • OpenConnect / Cisco AnyConnect • OpenVPN (direct) • OpenVPN (stunnel)
3.	Klepněte na odkaz <i>L2TP/IPsec</i> .
4.	Klepněte na odkaz <i>Windows</i> a poté <i>Manual VPN configuration</i> .
5.	Najděte v seznamu bod číslo 12. Hodnota na šedém pozadí je vaše heslo (na obrázku níže extremism-remades, vaše bude jiné). Toto heslo si poznamenejte.  The screenshot shows the Streisand website with the URL https://streisand-demo.freemyip.com/l2tp-ipsec/#windows. It lists steps 8 through 13. Step 12 is highlighted with a red box: '12. Enter extremism-remades in the Password field.' The text 'extremism-remades' is on a grey background. 8. Enter streisand in the Destination name field. 9. Check the Don't connect now; just set it up so I can connect later checkbox. 10. Click Next. 11. Enter streisand in the User name field. 12. Enter extremism-remades in the Password field. 13. Check the Remember this password checkbox.
6.	Najděte v seznamu krok číslo 20. Hodnota na šedém pozadí je váš pre-shared key (na obrázku níže anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte.  The screenshot shows the Streisand website with the URL https://streisand-demo.freemyip.com/l2tp-ipsec/#windows. It lists steps 19 through 22. Step 20 is highlighted with a red box: '20. Select Use preshared key for authentication and enter anthelices-barrettes-peptized for the Key.' The text 'anthelices-barrettes-peptized' is on a grey background. Type of VPN drop-down menu. 19. Click the Advanced settings button. 20. Select Use preshared key for authentication and enter anthelices-barrettes-peptized for the Key. 21. Click OK to close the Advanced settings. 22. Click OK to save the VPN connection details.

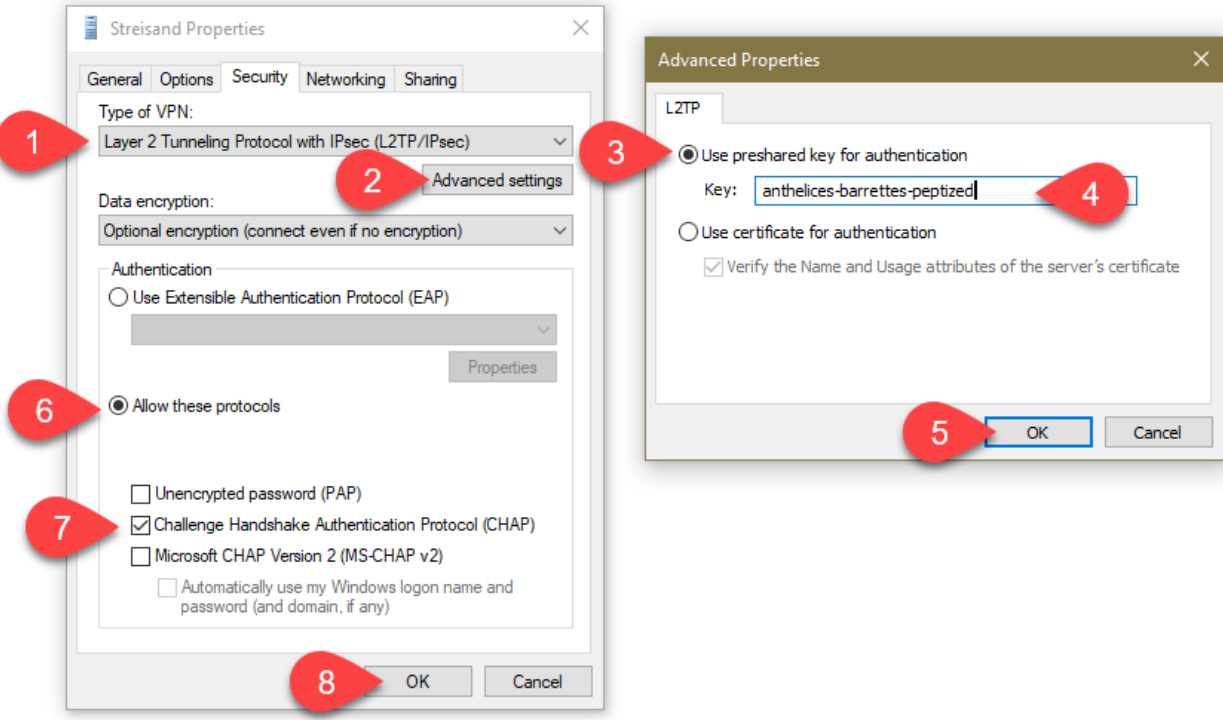
Příprava připojení

7.	Spustíte příkazovou řádku jako správce. Stiskněte klávesy <i>Win+X</i> a z menu zvolte <i>Command prompt (Admin)</i> , případně <i>PowerShell (Admin)</i> :
	
8.	Zadejte do příkazové řádky následující příkaz (celý musí být na jednom řádku): <pre>REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 2</pre>
①	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.
9.	Aby se změny projevily, restartujte počítač.

Vytvoření nového VPN připojení

10.	Poté klepněte pravým tlačítkem na ikonu síťového připojení na hlavním panelu a z kontextového menu zvolte <i>Open Network and Sharing Center</i> .
11.	Klepněte na <i>Set up a new connection or network</i> : 

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

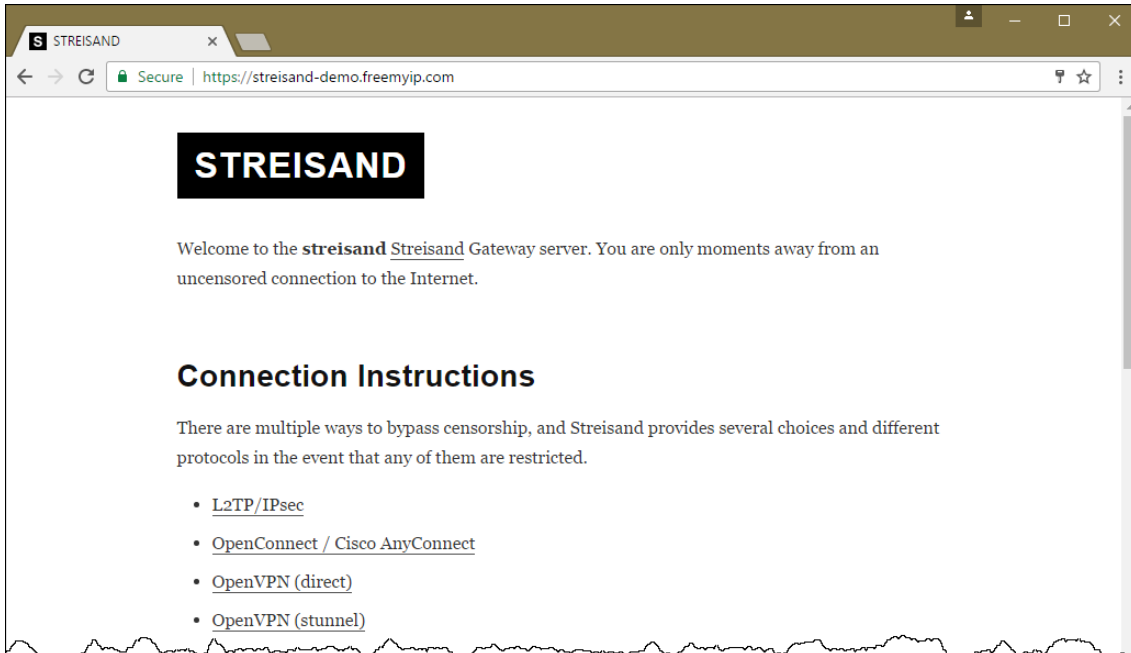
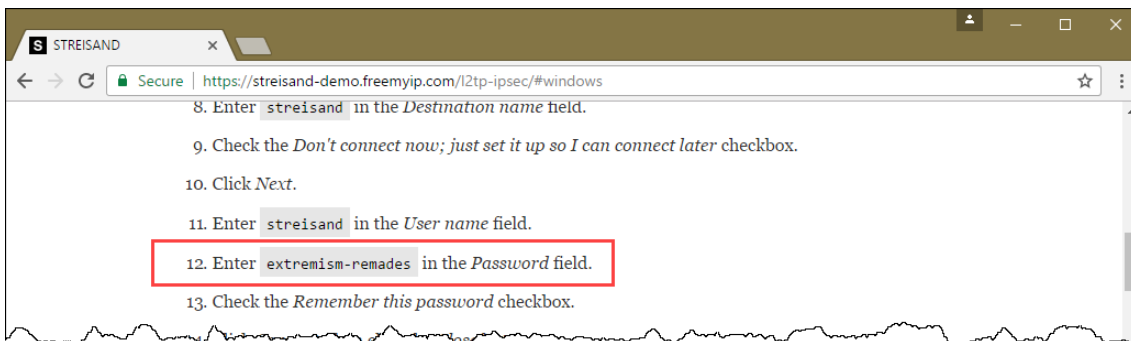
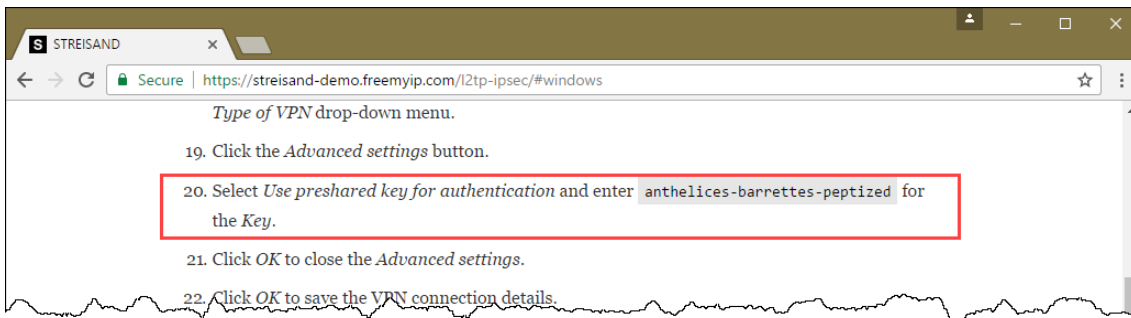
17.	Nastavte podrobnější parametry připojení: - Na záložce <i>Security</i> nastavte jako <i>Type of VPN</i> hodnotu <i>Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)</i>. - Klepněte na tlačítko <i>Advanced Settings</i> a zadejte hodnotu <i>preshared key</i> zjištěnou v kroku 6 a potvrďte klepnutím na <i>OK</i>. - V části <i>Authentication</i> povolte jako protokol <i>Challenge Handshake Authentication Protocol (CHAP)</i> a zrušte zaškrtnutí <i>Microsoft CHAP version 2 (MS-CHAP v2)</i>. - Poté klepněte na <i>OK</i>. 
18.	Klepněte na ikonu síťových připojení na hlavním panelu.
19.	V seznamu připojení klepněte na název nově vytvořeného připojení (<i>Streisand</i>) a poté na tlačítko <i>Connect</i> .
20.	Zadejte uživatelské jméno <i>streisand</i> a heslo zjištěné v kroku 5 a klepněte na <i>OK</i> .
21.	Váš počítač se nyní připojí k VPN a bude do Internetu přistupovat jejím prostřednictvím
①	<i>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.</i>

Odpojení od VPN a opětovné připojení

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

06. Nastavení L2TP/IPSec VPN na Windows 7

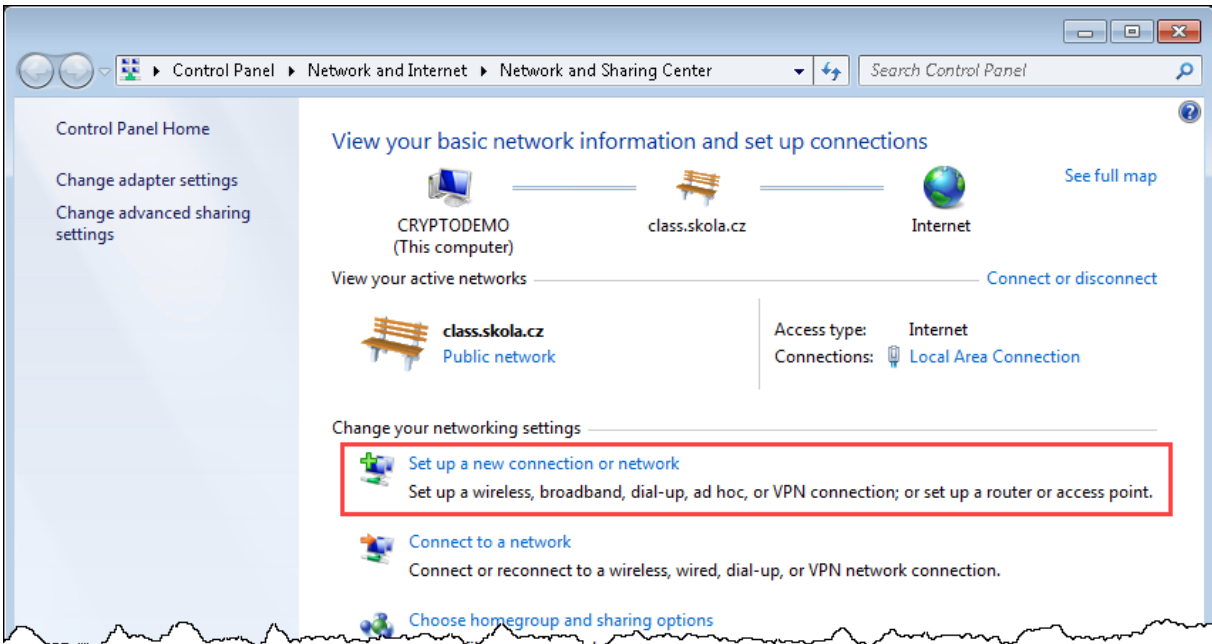
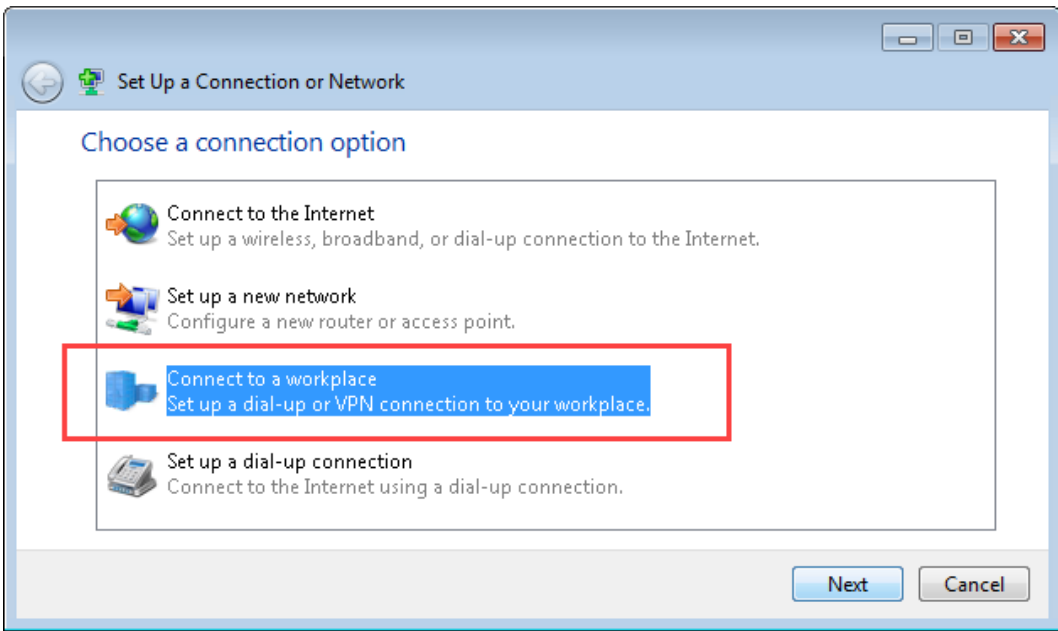
Získání přihlašovacích údajů

1.	Zadejte do prohlížeče adresu svého Streisand serveru a přihlaste se jménem a heslem, viz konec příkladu 04. <i>Instalace Streisand serveru.</i>
2.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN: 
3.	Klepněte na odkaz <i>L2TP/IPsec.</i>
4.	Klepněte na odkaz <i>Windows.</i>
5.	Najděte v seznamu bod číslo 12. Hodnota na šedém pozadí je vaše heslo (na obrázku níže extremism-remades, vaše bude jiné). Toto heslo si poznamenejte. 
6.	Najděte v seznamu bod číslo 20. Hodnota na šedém pozadí je váš pre-shared key (na obrázku níže anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte. 

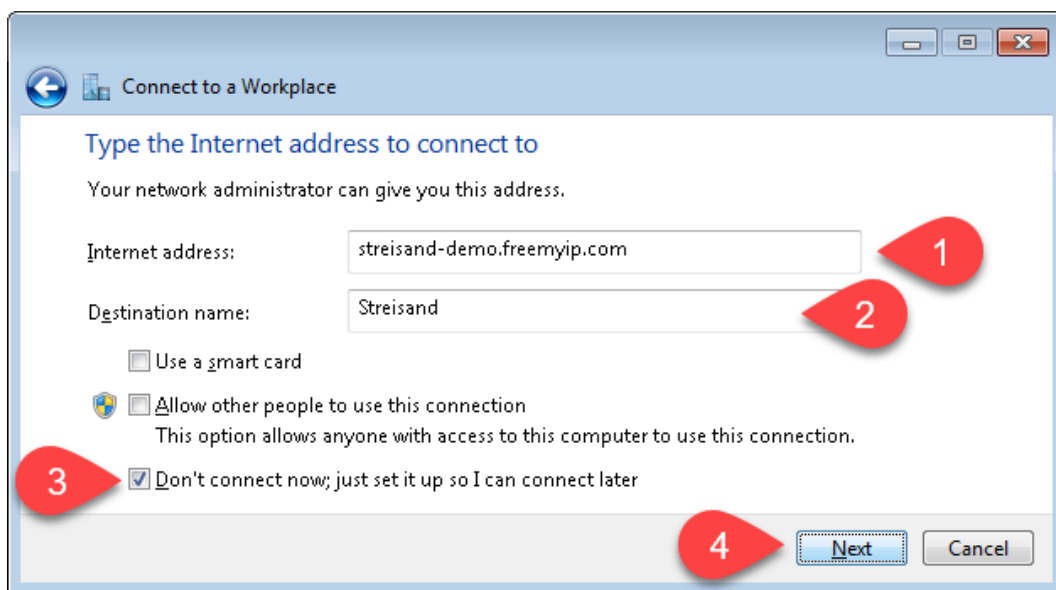
Příprava připojení

7.	Spustíte 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 <i>Run as administrator</i> .
8.	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
①	<i>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.</i>
9.	Aby se změny projevily, restartujte počítač.

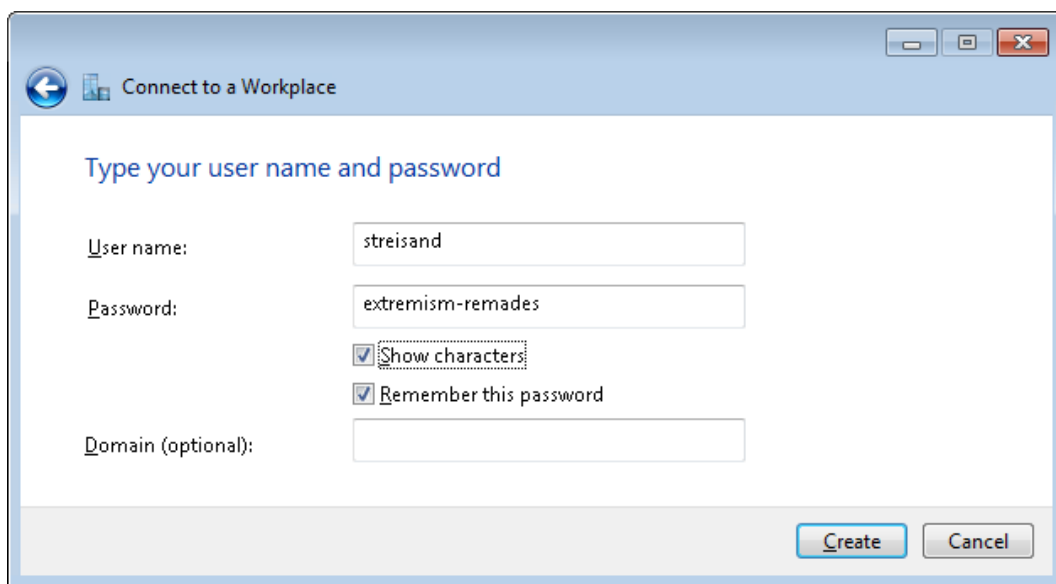
Vytvoření nového VPN připojení

10.	Poté klepněte pravým tlačítkem na ikonu síťového připojení na hlavním panelu a z kontextového menu zvolte <i>Open Network and Sharing Center</i> .
11.	Klepněte na <i>Set up a new connection or network</i>: 
12.	Klepněte na <i>Connect to a workplace</i> a poté na <i>Next</i>. 
13.	Klepněte na <i>Use my Internet connection (VPN)</i> .

14. 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*.

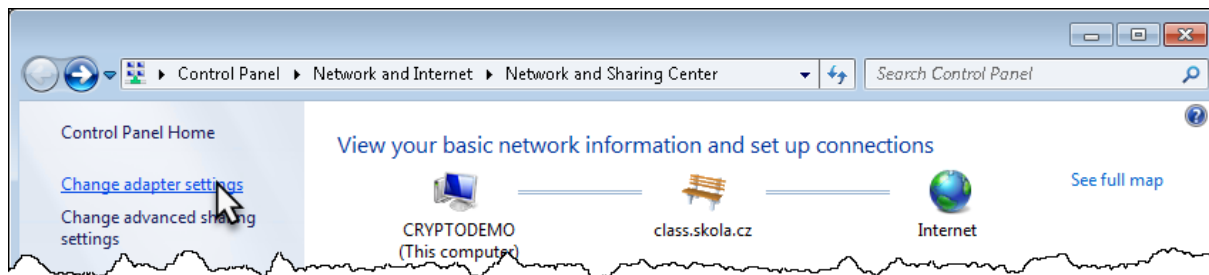


15. V dalším kroku průvodce zadejte uživatelské jméno (*streisand*) a heslo zjištěné v kroku 5. Zaškrtněte *Remember this password* a klepněte na tlačítko *Create*.



16. Spojení je vytvořeno. Klepněte na tlačítko *Close*.

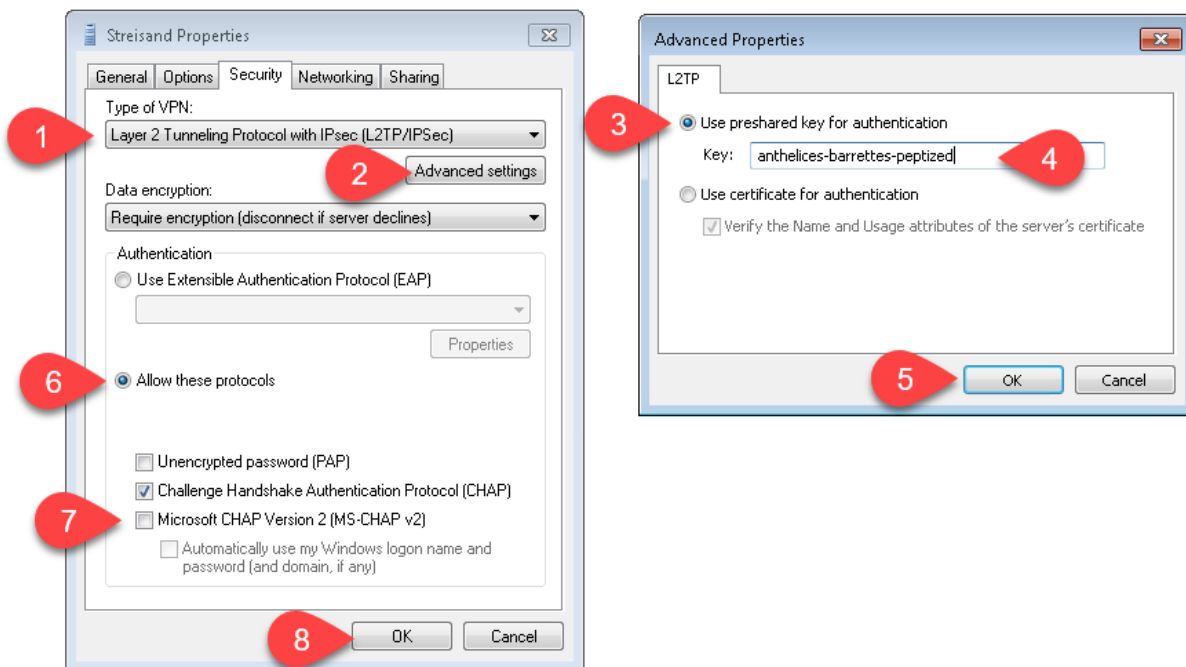
17. V okně *Network and Sharing Center* klepněte na *Change adapter settings*:



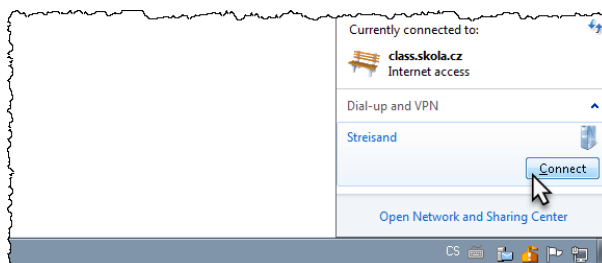
18. Klepněte na název připojení (určený v kroku 8, zde *Streisand*) pravým tlačítkem a z kontextového menu zvolte *Properties*.

19. 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* zjištěnou v kroku 6 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*.



20. Klepněte na ikonu síťových připojení na hlavním panelu. V seznamu připojení klepněte na název nově vytvořeného připojení (*Streisand*) a poté na tlačítko *Connect*.



21. V dalším okně klepněte na *Connect*.

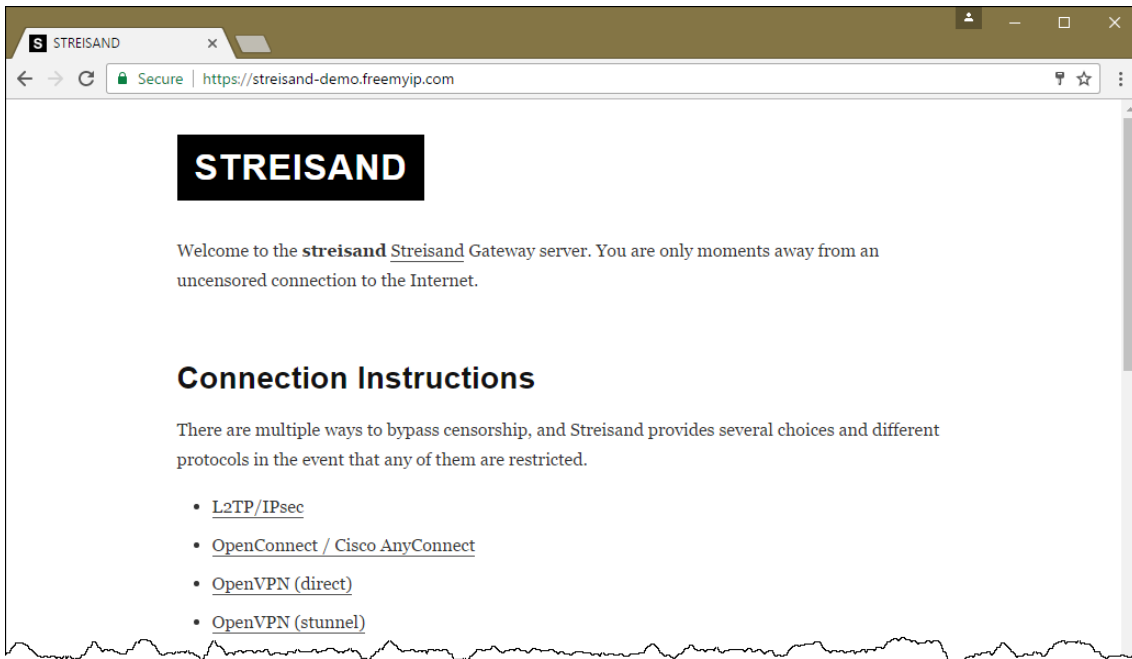
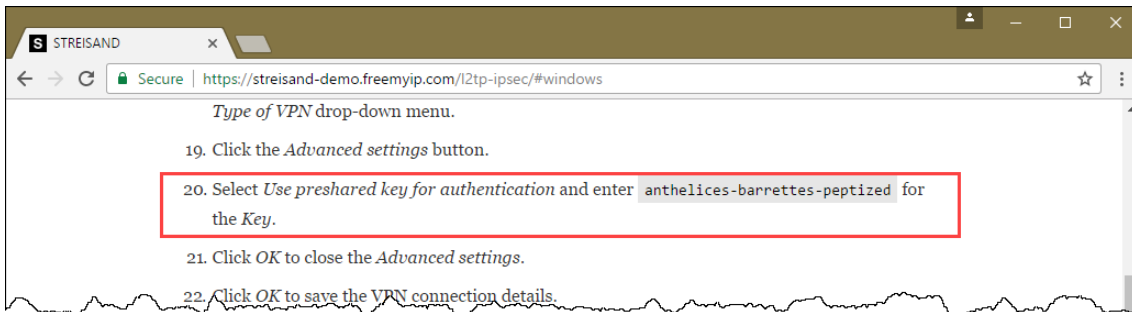


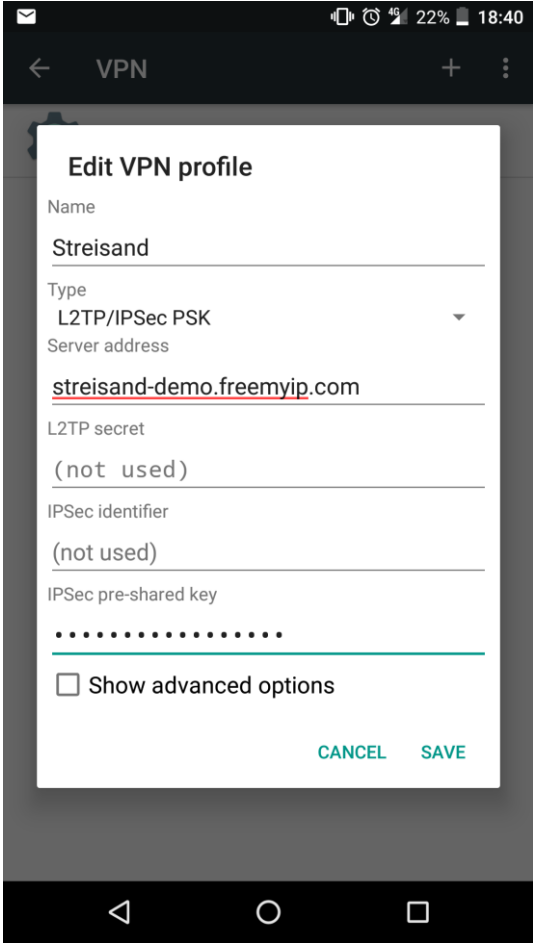
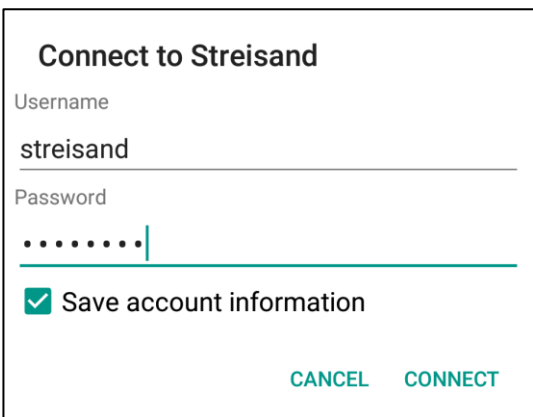
①	<i>Pokud toto okno nechcete v budoucnu zobrazovat, klepněte na Properties a potom zrušte zaškrtnutí Prompt for name and password, certificate, etc.</i>
22.	Zobrazí se okno s informacemi o průběhu připojování, které se posléze samo zavře.
23.	Váš počítač se nyní připojil k VPN a bude do Internetu přistupovat jejím prostřednictvím
①	<i>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.</i>

Odpojení od VPN a opětovné připojení

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

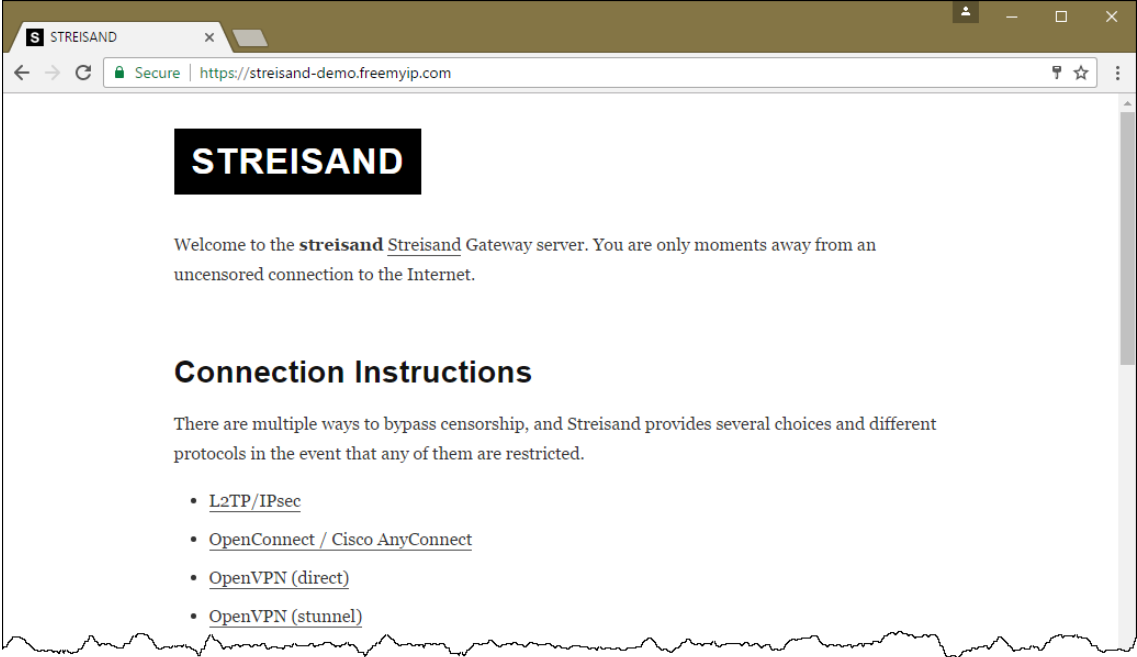
07. Nastavení L2TP/IPSec VPN na Androidu 6.0

1.	Zadejte do prohlížeče adresu svého Streisand serveru a přihlaste se jménem a heslem, viz konec předchozího příkladu 04. <i>Instalace Streisand serveru.</i>
2.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN: 
3.	Klepněte na odkaz <i>L2TP/IPsec</i> .
4.	Klepněte na odkaz <i>Android</i> . Můžete postupovat podle návodu na webu (pouze jako název serveru zadejte DNS jméno vašeho serveru, ne IP adresu), nebo postupovat dalšími kroky zde.
5.	Najděte v seznamu bod číslo 8. Hodnota na šedém pozadí je váš pre-shared key (na obrázku níže anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte. 
6.	Najděte v seznamu bod číslo 12. Hodnota na šedém pozadí je vaše heslo (na obrázku níže extremism-remades, vaše bude jiné). Toto heslo si poznamenejte. 
7.	Spustíte na svém zařízení s Androidem aplikaci <i>Settings</i> .
8.	V sekci <i>Wireless & Networks</i> klepněte na <i>More....</i>
9.	Klepněte na <i>VPN</i> .

10.	Klepněte na tlačítko + v pravém horním rohu.
11.	V následném dialogu vyplňte parametry: - Název: Streisand (případně jaký chcete) - Type: L2TP/IPSec PSK - Server address: název serveru, zde streisand-demo.freemyip.com - IPSec pre-shared key: Hodnota zjištěná v kroku 5. Poté klepněte na <i>Save</i>. 
12.	Klepněte na název nově vytvořeného připojení.
13.	Zadejte uživatelské jméno streisand a heslo zjištěné v kroku 6 a klepněte na <i>Connect</i>. 
14.	Pro odpojení klepněte na název VPN a poté na <i>Disconnect</i> .

08. Instalace a konfigurace OpenVPN na Windows

Získání konfiguračního souboru

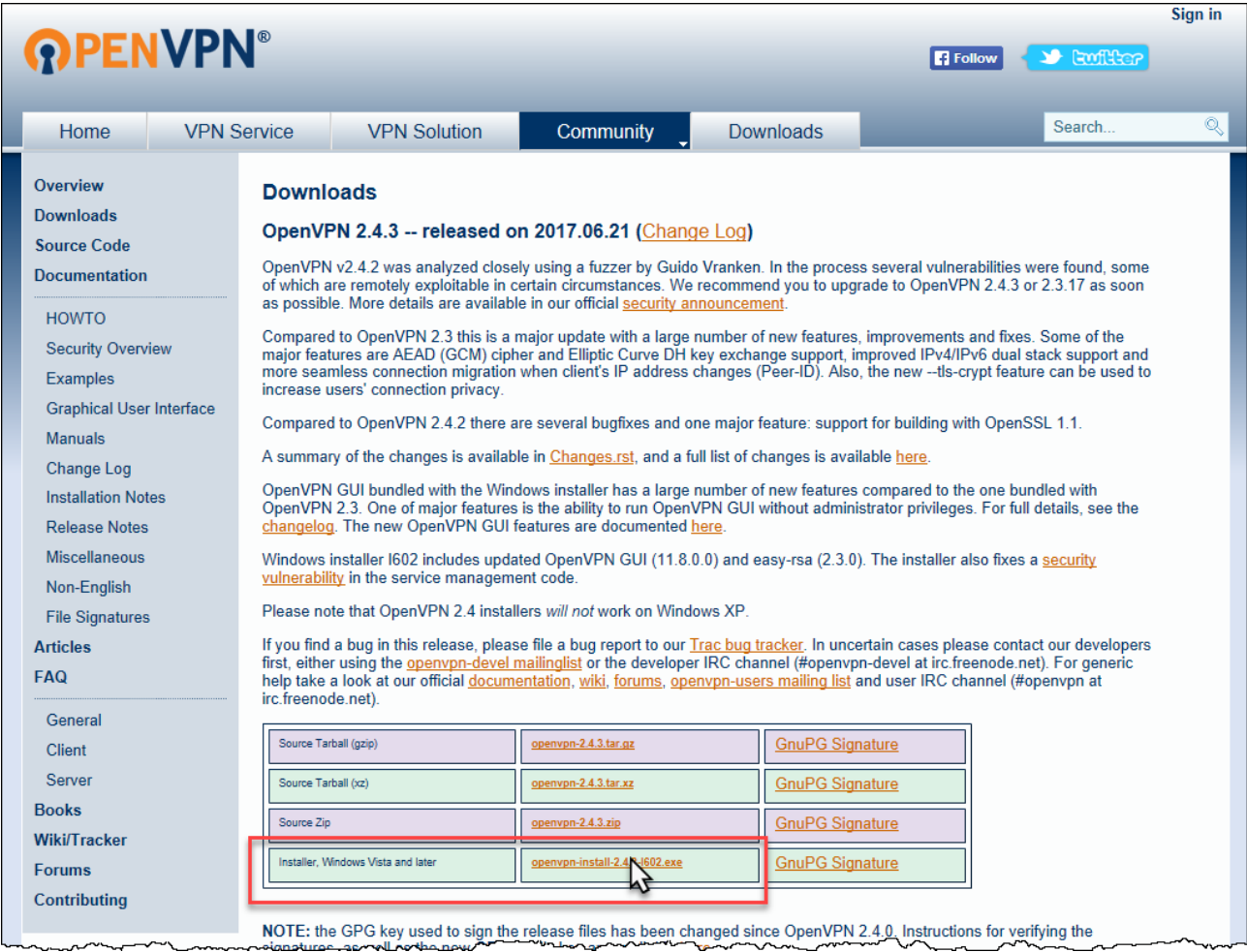
①	Soubory s nastavením si můžete stáhnout i přes scp, pokud ho máte a umíte používat. Použijte následující příkaz, upravený podle názvu vašeho serveru (celý musí být na jednom řádku): <pre>scp root@streisand-demo.freemyip.com:/var/www/streisand/openvpn/client-1/streisand-combined.ovpn streisand-combined.ovpn</pre> 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.	Zadejte do prohlížeče adresu svého Streisand serveru a přihlaste se jménem a heslem, viz konec příkladu 04. Instalace Streisand serveru.
2.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN: 
3.	Klepněte na odkaz <i>OpenVPN (direct)</i> .
4.	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.
5.	Stáhněte si soubor s příponou .ovpn. Na výběr máte z pěti variant s pěti různými náhodně vygenerovanými jmény, můžete použít kterýkoliv z nich (jde o pět různých profilů pro až pět různých uživatelů).

Příprava OVPN souboru

Stažený soubor má v názvu IP adresu, jmenuje se např. 198.51.100.1-combined.ovpn. I pro připojení se používá IP adresa, nikoliv DNS jméno. To je v pořádku v případě, že neplánujete adresu svého Streisand serveru nikdy měnit (poběží nepřetržitě). Pokud ale chcete server zapínat a vypínat dle potřeby (viz návod 09. Zrušení a opětovné zřízení dropletu u Digital Ocean), museli byste po každé změně IP adresy stahovat nový profil.

6.	Otevřete stažený soubor v textovém editoru, např. v Notepadu.
7.	Pomocí funkce <i>Edit → Replace</i> zaměňte v souboru všechny výskyty IP adresy (zde 198.51.100.1) za název vašeho serveru (v příkladu streisand-demo.freemyip.com)

Instalace OpenVPN

8.	Otevřete v prohlížeči adresu https://openvpn.net/ .
9.	Klepněte na odkaz <i>Community</i> .
10.	Klepněte na odkaz <i>Downloads</i> v levém menu.
11.	Stáhněte si instalátor pro Windows:
	
12.	Spustěte stažený instalátor OpenVPN.
13.	Klepněte na tlačítko <i>Next</i> .
14.	Klepnutím na <i>I Agree</i> odsouhlaste licenční podmínky.
15.	Ponechte výchozí nastavení komponent pro instalaci a klepněte na <i>Next</i> .
16.	Ponechte výchozí instalační adresář a klepněte na <i>Install</i> .
17.	Potvrďte instalaci ovladače pro TAP.
18.	Dokončete instalaci klepnutím na <i>Next</i> a <i>Finish</i> .

Konfigurace OpenVPN

19.	Spustěte program <i>OpenVPN GUI</i> .
20.	Zobrazí se varování, že nejsou definovány žádné profily. Zavřete ho klepnutím na <i>OK</i> .
21.	Na liště se objeví nová ikonka OpenVPN. Klepněte na ni pravým tlačítkem a z kontextového menu zvolte <i>Import file...</i>
22.	Vyberte soubor s příponou <i>.ovpn</i> , stažený v kroku číslo 5W.

Připojení a odpojení VPN

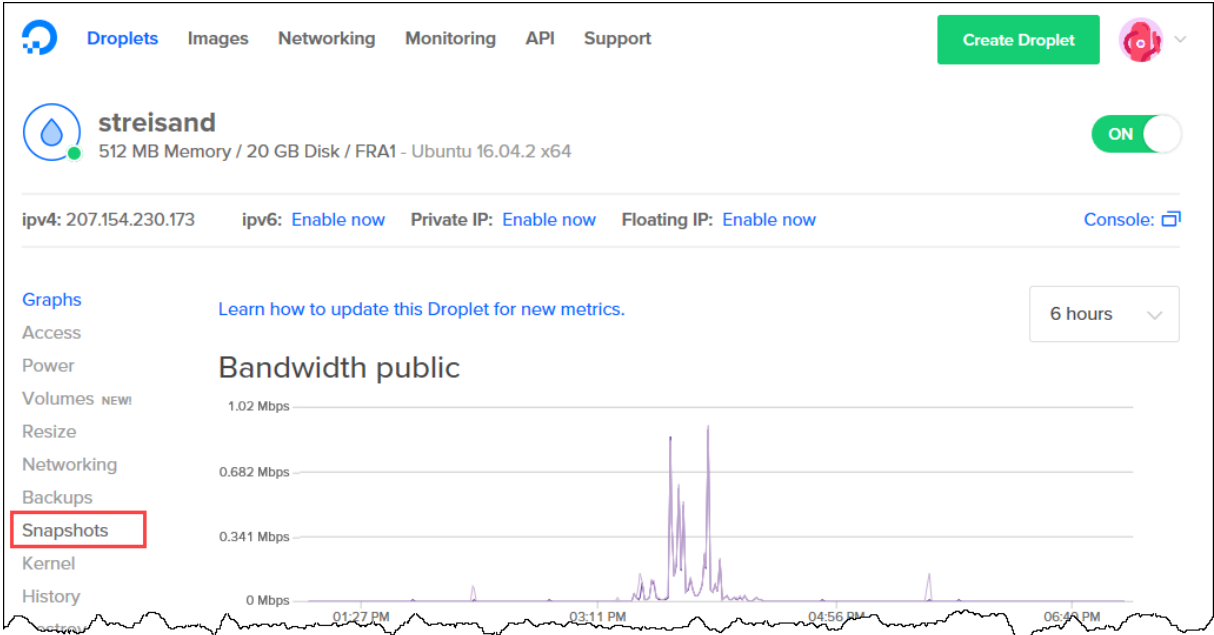
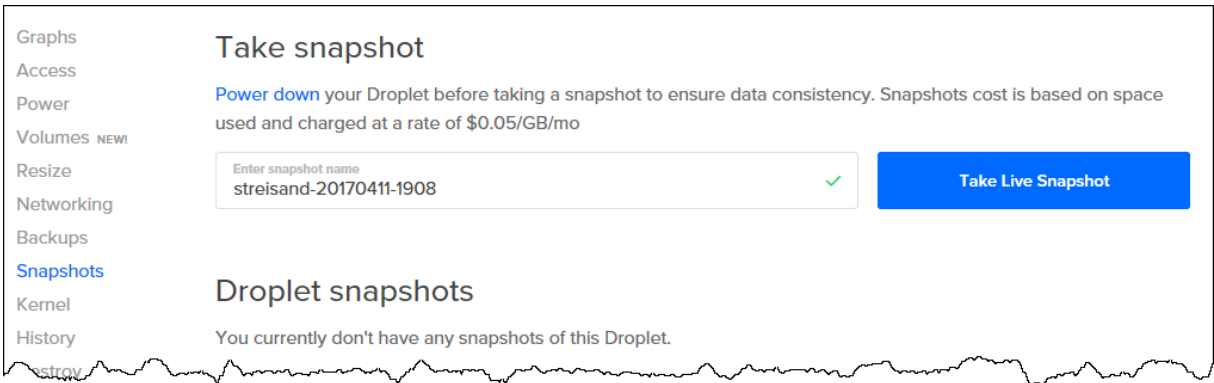
23.	Pro připojení do VPN klepněte na ikonku v liště pravým tlačítkem a zvolte <i>Connect</i> .
24.	Zobrazí se okno s popisem průběhu připojování. Když zmizí a ikonka v liště změní barvu na zelenou, jste připojeni.
25.	Pro odpojení klepněte na ikonku v liště pravým tlačítkem a zvolte <i>Disconnect</i>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

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.

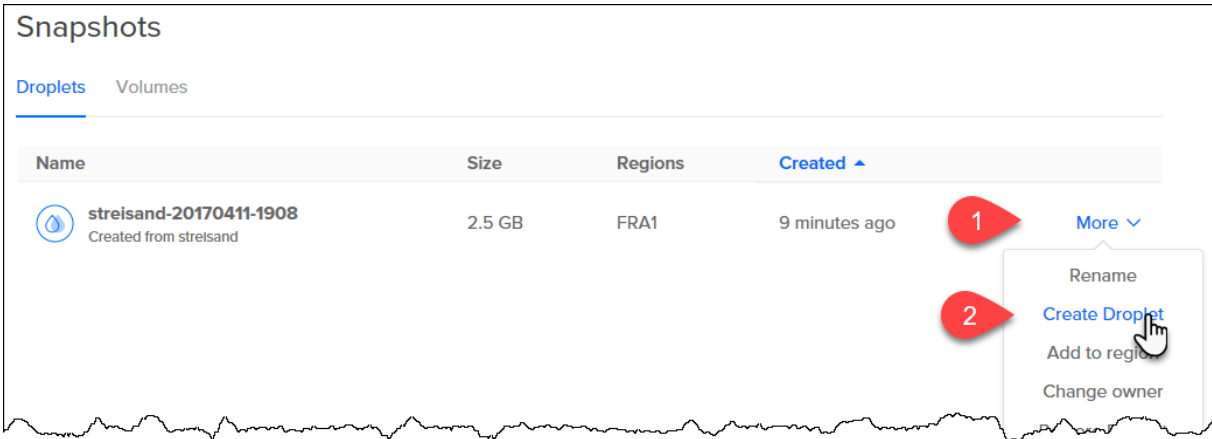
Vytvoření snapshotu

1.	Přihlašte se na svůj server pomocí SSH nebo webové konzole.
2.	Následujícím příkazem server vypněte: <pre>root@streisand:~# shutdown -hP now</pre> Connection to streisand-demo.freemyip.com closed by remote host. Connection to streisand-demo.freemyip.com closed.
①	<i>Vypnutí serveru není absolutně nezbytné, snapshot lze udělat i z běžícího počítače. Z důvodu konzistence dat se nicméně doporučuje server vypnout.</i>
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 <i>Take Live Snapshot</i> . 
7.	Vyčkejte, dokud se nevytvoří snapshot, což může nějakou trvat několik minut.
①	<i>I za snapshot se platí, ale méně. Za snapshot typického Streisand serveru zaplatíte přibližně 3 Kč měsíčně.</i>

Zrušení dropletu

8.	V levém menu klepněte na odkaz <i>Destroy</i> .
9.	Na stránce klepněte na velké tlačítko <i>Destroy</i> .
10.	V potvrzovacím dialogu klepněte na tlačítko <i>Confirm</i> .
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 <i>Images</i> v horní části stránky.
13.	V seznamu snapshotů vyberte ten správný a klepněte na odkaz <i>More</i> vpravo.
14.	Z menu zvolte <i>Create Droplet</i> . 
15.	Podobně jako při vytvoření nového dropletu můžete zvolit jeho velikost (a cenu) a pojmenovat ho.
16.	Klepnutím na tlačítko <i>Create</i> droplet vytvoříte a nainstalujete.

Poznámky k používání snapshot

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.