

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

Michal Altair Valášek

michal.valasek@altairis.cz @ridercz

Obsah

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 V PN jako služba a proč ji nepoužívat 6 V PN jako služba a proč ji nepoužívat 6 V PN jako služba a proč ji nepoužívat 6 V Vatví provanov oblacích 6 Streisand Effect a Streisand server 7 Vávoť k použití návodu 9 Typografické konvence 9 Vytvoření vírtuálního počítače u Digital Ocean 11 Vytvoření vírtuálního počítače u Digital Ocean 12 Vytvoření dropletu (virtuálního serveru) 11 První přihlášení 12 20. Nastavení dynamického DNS 15 31. Instalace streisand serveru 17 34. Instalace certifikátu CA Streisand serveru 19 95. Ziskání přihlašovacích údajů pro L2TP/IPSec VPN 21 96. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 97 hýprava připojení 27 97 hýpava připojení 27 98. Instalace a konfigurace OpenVPN 32 99. Zitvoření nového VPN připojení <	Obsah	
Virtuální privátní síť5Proč používat VPN?6VPN jako služba a proč ji nepoužívat6Vlastní brána v oblačích6Streisand Effect a Streisand server7Vávod k použití návodu9Typografické konvence9901. Vytvoření virtuálního počítače u Digital Ocean11Vytvoření dropletu (virtuálního serveru)11Prvín jřihlášení12202. Nastavení dynamického DNS1533. Instalace Streisand serveru1724. Instalace certifikátu CA Streisand serveru1725. Získání přihlašovacích údajů pro L2TP/IPSec VPN2126. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.123Příprava připojení23Vytvoření nového VPN připojení23Odpojení od VPN a opětovné připojení27Vytvoření nového VPN připojení27Odpojení od VPN a opětovné připojení27Odpojení od VPN a opětovné připojení3038. Instalace OpenVPN31Získání konfigurače OpenVPN32Připrava připojení32Připrava připojení32Připojení a odpojení VPN32Připojení a o	Co je VPN a proč ji chcete používat	5
Proč používat VPN?	Virtuální privátní síť	5
VPN jako služba a proč ji nepoužívat6Vlastní brána v oblacích6Streisand Effect a Streisand server7Vávod k použití návodu9Typografické konvence9D1. Vytvoření virtuálního počítače u Digital Ocean11Vytvoření virtuálního počítače u Digital Ocean11Vytvoření virtuálního počítače u Digital Ocean11První přihlášení12D2. Nastavení dynamického DNS15D3. Instalace Streisand serveru17J4. Instalace certifikátu CA Streisand serveru19D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN21D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.123Příprava připojení23Odpojení od VPN a opětovné připojení26J7. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení27Vytvoření nového VPN připojení27Odpojení od VPN a opětovné připojení30D8. Instalace a konfiguračního souboru31Získání konfiguračního souboru31Získání konfigurač OpenVPN32Příprava připojení30D331Získání konfigurač OpenVPN32Konfigurač OpenVPN32Připojení a odpojení VPN32Připojení a odpojení VPN32Připojení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení a popiotné zřízení dropletu u Digital Ocean36Poznámky k používání snapshotů36Poznámky k používání snapshotů<	Proč používat VPN?	6
Vlastní brána v oblacích6Streisand Effect a Streisand server7Vávod k použití návodu9Typografické konvence911. Vytvoření virtuálního počítače u Digital Ocean11Vytvoření virtuálního počítače u Digital Ocean11První přihlášení1212. Nastavení dynamického DNS1503. Instalace Streisand serveru1714. Instalace certifikátu CA Streisand serveru1915. Získání přihlašovacích údajů pro L2TP/IPSec VPN2116. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.123Příprava připojení23Odpojení od VPN a opětovné připojení2617. Nastavení L2TP/IPSec VPN na Windows 727Vytvoření nového VPN připojení2308. Instalace de konfigurace OpenVPN3127. Vytvoření nového VPN připojení3008. Instalace a konfigurace OpenVPN3128. Konfigurace OpenVPN32Připojení a odpojení volboru3127. Vytvoření nového VPN připojení32Vytvoření nového VPN připojení32Připojení a odpojení volboru3127. Vytvoření nového VPN připojení3227. Vytvoření nového VPN apětovné připojení3239. Zrušení a opětovné připojení3339. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu ze snapshotu36Poznámky k používání snapshotů36Poznámky k používání snapshotů36	VPN jako služba a proč ji nepoužívat	6
Streisand Effect a Streisand server 7 Vávod k použítí návodu 9 Typografické konvence 9 D1. Vytvoření virtuálního počítače u Digital Ocean 11 Vytvoření virtuálního počítače u Digital Ocean 11 První přihlášení 12 D2. Nastavení dynamického DNS 15 D3. Instalace Streisand serveru 17 D4. Instalace certifikátu CA Streisand serveru 19 D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN 21 D6. Nastavení L2TP/IPSec VPN na Windows 8.1 23 Příprava připojení 23 Odpojení od VPN a opětovné připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Příprava připojení 30 D8. Instalace a konfigurace OpenVPN 31 Instalace a konfigurace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a opětovné připojení 32 Připojení a opětovné připojení 33 D9. Zrušení a opětovné zízení dropletu u Digital Ocean <	Vlastní brána v oblacích	6
Návod k použití návodu9Typografické konvence9D1. Vytvoření virtuálního počítače u Digital Ocean11Vytvoření dropletu (virtuálního serveru)11První přihlášení1220. Nastavení dynamického DNS1531. Instalace Streisand serveru17D4. Instalace Streisand serveru19D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN21D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.123Příprava připojení23Odpojení od VPN a opětovné připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Odpojení od VPN a opětovné připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Vytvoření nového VPN připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Výtvoření nového VPN připojení27Odpojení od VPN a opětovné připojení30D8. Instalace a konfigurace OpenVPN31Získání konfiguračního souboru31Instalace OpenVPN32Připojení a odpojení VPN32Připojení a odpojení VPN32Připojení a odpojení VPN33D9. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu36Opětovné zřízení dropletu ze snapshotu36Poznámky k používání snapshotů36 <td>Streisand Effect a Streisand server</td> <td>7</td>	Streisand Effect a Streisand server	7
Typografické konvence9D1. Vytvoření virtuálního počítače u Digital Ocean11Vytvoření virtuálního serveru)11První přihlášení12D2. Nastavení dynamického DNS15J3. Instalace Streisand serveru17J4. Instalace Streisand serveru19D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN21D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.123Příprava připojení23Vytvoření nového VPN připojení23Odpojení od VPN a opětovné připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení30D8. Instalace a konfigurace OpenVPN31Získání konfigurace OpenVPN32Konfigurace OpenVPN32Připojení a dopojení VPN32Připojení a dopojení VPN33D9. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu36Opětovné zřízení dropletu z snapshotu36Poznámky k používání snapshotů36	Návod k použití návodu	9
D1. Vytvoření virtuálního počítače u Digital Ocean 11 Vytvoření dropletu (virtuálního serveru) 11 První přihlášení 12 D2. Nastavení dynamického DNS 15 D3. Instalace Streisand serveru 17 D4. Instalace certifikátu CA Streisand serveru 19 D5. Získání přihlášovacích údajů pro L2TP/IPSec VPN 21 D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Připojení a odpojení VPN souboru 33 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean 35 Vytvoření	Typografické konvence	9
Vytvoření dropletu (virtuálního serveru)11První přihlášení1222. Nastavení dynamického DNS1533. Instalace Streisand serveru1774. Instalace Streisand serveru1995. Získání přihlašovacích údajů pro L2TP/IPSec VPN2196. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.12397 říprava připojení2304 opjení od VPN a opětovné připojení2304 opjení od VPN a opětovné připojení2677. Nastavení L2TP/IPSec VPN na Windows 72797 říprava připojení2670. Nastavení L2TP/IPSec VPN na Windows 72797 říprava připojení2670. Nastavení L2TP/IPSec VPN na Windows 72797 říprava připojení2677. Nastavení L2TP/IPSec VPN na Windows 72797 říprava připojení270dpojení od VPN a opětovné připojení3008. Instalace a konfigurace OpenVPN.3121. Získání konfiguračního souboru.3111. Instalace OpenVPN3280. Konfigurace OpenVPN3299. Zrušení a opětovné zřízení dropletu u Digital Ocean3591. Zrušení a opětovné zřízení dropletu u Digital Ocean3592. Zrušení dropletu ze snapshotu3693. Opětovné zřízení dropletu ze snapshotu3694. Poznámky k používání snapshotů36	01. Vytvoření virtuálního počítače u Digital Ocean	
První přihlášení12První přihlášení15D2. Nastavení dynamického DNS15D3. Instalace Streisand serveru17D4. Instalace certifikátu CA Streisand serveru19D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN21D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.123Příprava připojení23Odpojení od VPN a opětovné připojení23Odpojení od VPN a opětovné připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení27Odpojení od VPN a opětovné připojení27Vytvoření nového VPN připojení27Vytvoření nového VPN připojení27Odpojení od VPN a opětovné připojení27Vytvoření nového VPN připojení30D8. Instalace a konfiguračního souboru.31Instalace OpenVPN.32Konfiguračního souboru.33D9. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu.35Zrušení dropletu36Opětovné zřízení dropletu ze snapshotu.36Poznámky k používání snapshotů36	Vytvoření dropletu (virtuálního serveru)	
D2. Nastavení dynamického DNS 15 D3. Instalace Streisand serveru 17 D4. Instalace certifikátu CA Streisand serveru 19 D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN 21 D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfiguračního souboru 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Připojení a odpojení VPN 32 Připojení a odpojení VPN 33 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean </td <td>První přihlášení</td> <td></td>	První přihlášení	
D3. Instalace Streisand serveru 17 D4. Instalace certifikátu CA Streisand serveru 19 D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN 21 D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Příprava připojení 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytorění nového VPN připojení 27 Odpojení od VPN a opětovné připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 33 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean 35 Vytoření snapshotu 36 Opětovné zřízení dropletu ze snapshotu 36 </td <td>02. Nastavení dynamického DNS</td> <td></td>	02. Nastavení dynamického DNS	
04. Instalace certifikátu CA Streisand serveru 19 05. Získání přihlašovacích údajů pro L2TP/IPSec VPN 21 06. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 23 Odpojení od VPN a opětovné připojení 26 07. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 27 Odpojení od VPN a opětovné připojení 30 08. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 33 09. Zrušení a opětovné zřízení dropletu u Digital Ocean 35 Vytvoření snapshotu 36 Opětovné zřízení dropletu ze snapshotu 36 Opětovné zřízení dropletu ze snapshotu 36 Poznámky k používání snapsh	03. Instalace Streisand serveru	
D5. Získání přihlašovacích údajů pro L2TP/IPSec VPN 21 D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 27 Odpojení od VPN a opětovné připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 32 Připojení a opětovné zřízení dropletu u Digital Ocean 35 Zyušení dropletu 36 Opětovné zřízení dropletu ze snapshotu 36 Poznámky k používání snapshotů 36	04. Instalace certifikátu CA Streisand serveru	
D6. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1 23 Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 32 Připojení a opětovné zřízení dropletu u Digital Ocean 35 Vytvoření snapshotu 35 Zrušení dropletu 36 Opětovné zřízení dropletu ze snapshotu 36 Poznámky k používání snapshotů 36	05. Získání přihlašovacích údajů pro L2TP/IPSec VPN	
Příprava připojení 23 Vytvoření nového VPN připojení 23 Odpojení od VPN a opětovné připojení 26 D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 32 Připojení a odpojení VPN 32 Připojení a odpojení VPN 33 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean 35 Vytvoření snapshotu 35 Zrušení dropletu 36 Opětovné zřízení dropletu ze snapshotu 36 Poznámky k používání snapshotů 36	06. Nastavení L2TP/IPSec VPN na Windows 10 a Windows 8.1	
Vytvoření nového VPN připojení23Odpojení od VPN a opětovné připojení26D7. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení27Vytvoření nového VPN připojení27Odpojení od VPN a opětovné připojení30D8. Instalace a konfigurace OpenVPN31Získání konfiguračního souboru31Instalace OpenVPN32Konfigurace OpenVPN32Připojení a odpojení VPN32Vytvoření a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu36Opětovné zřízení dropletu z snapshotu36Poznámky k používání snapshotů36	Příprava připojení	
Odpojení od VPN a opětovné připojení2607. Nastavení L2TP/IPSec VPN na Windows 727Příprava připojení27Vytvoření nového VPN připojení27Odpojení od VPN a opětovné připojení3008. Instalace a konfigurace OpenVPN31Získání konfiguračního souboru31Instalace OpenVPN32Konfigurace OpenVPN32Připojení a odpojení VPN32Připojení a odpojení VPN3309. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu36Opětovné zřízení dropletu ze snapshotu36Poznámky k používání snapshotů36	Vytvoření nového VPN připojení	
D7. Nastavení L2TP/IPSec VPN na Windows 7 27 Příprava připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 32 Připojení a odpojení VPN 33 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean 35 Vytvoření snapshotu 35 Zrušení dropletu 36 Opětovné zřízení dropletu ze snapshotu 36 Poznámky k používání snapshotů 36	Odpojení od VPN a opětovné připojení	
Příprava připojení 27 Vytvoření nového VPN připojení 27 Odpojení od VPN a opětovné připojení 30 D8. Instalace a konfigurace OpenVPN 31 Získání konfiguračního souboru 31 Instalace OpenVPN 32 Konfigurace OpenVPN 32 Připojení a odpojení VPN 32 Připojení a odpojení VPN 33 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean 35 Vytvoření snapshotu 35 Zrušení dropletu 36 Opětovné zřízení dropletu ze snapshotu 36 Poznámky k používání snapshotů 36	07. Nastavení L2TP/IPSec VPN na Windows 7	
Vytvoření nového VPN připojení27Odpojení od VPN a opětovné připojení30D8. Instalace a konfigurace OpenVPN31Získání konfiguračního souboru31Instalace OpenVPN32Konfigurace OpenVPN32Připojení a odpojení VPN32Připojení a odpojení VPN33D9. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu36Opětovné zřízení dropletu ze snapshotu36Poznámky k používání snapshotů36	Příprava připojení	
Odpojení od VPN a opětovné připojení	Vytvoření nového VPN připojení	
 D8. Instalace a konfigurace OpenVPN	Odpojení od VPN a opětovné připojení	
Získání konfiguračního souboru.31Instalace OpenVPN32Konfigurace OpenVPN32Připojení a odpojení VPN33D9. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu36Opětovné zřízení dropletu ze snapshotu36Poznámky k používání snapshotů36	08. Instalace a konfigurace OpenVPN	
Instalace OpenVPN32Konfigurace OpenVPN32Připojení a odpojení VPN3309. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu36Opětovné zřízení dropletu ze snapshotu36Poznámky k používání snapshotů36	Získání konfiguračního souboru	
Konfigurace OpenVPN32Připojení a odpojení VPN33D9. Zrušení a opětovné zřízení dropletu u Digital Ocean35Vytvoření snapshotu35Zrušení dropletu36Opětovné zřízení dropletu ze snapshotu36Poznámky k používání snapshotů36	Instalace OpenVPN	
Připojení a odpojení VPN	Konfigurace OpenVPN	
 D9. Zrušení a opětovné zřízení dropletu u Digital Ocean	Připojení a odpojení VPN	
Vytvoření snapshotu	09. Zrušení a opětovné zřízení dropletu u Digital Ocean	
Zrušení dropletu	Vytvoření snapshotu	
Opětovné zřízení dropletu ze snapshotu	Zrušení dropletu	
Poznámky k používání snapshotů	Opětovné zřízení dropletu ze snapshotu	
	Poznámky k používání snapshotů	

Datum vydání:	30.7.2017
Verze:	5

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 International¹. Můžete ho nadále šířit a upravovat za předpokladu, že uvedete původního autora a budete-li jej šířit pod stejnou licencí.

¹https://creativecommons.org/licenses/by-sa/4.0/
3

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.
Û	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)



٦	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 <i>Add your SSH keys</i> ponechte beze změny.
٦	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
	<i>Create</i> jej vytvořte.
12.	Čekejte, bude to nějakou dobu trvat, přibližně minutu až dvě.
	Droplets Images Networking Monitoring API Support Create Droplet O Search by Droplet name
	Droplets Volumes Name IP Address Created Tags Image: Streisand Size MB / 20 GB Disk / FRA1 - Ubuntu 16.04.2 x64 More More

První přihlášení

13.	O vytvo	oření serveru b	oudete informová	ni e-mailem. Sou	učástí zprávy je	e též IP adres	a, uživatelské jméno	
	(root)	a jednorázové	e heslo, které pou	žijete pro první j	ořipojení:			
			Carley Carly All Converd po 10.04.2017 18:59 DigitalOcea Your New Drop	an <support@support let: streisand</support@support 	.digitalocean.com>		^	
			Your new Droplet i credentials:	s all set to go! You	ı can access it us	ing the followir	ng A	
			Droplet Name: stre IP Address: 138.68 Username: root Password: dcff3a23	isand .102.250 9de25f7f84a602a098				
			For security reason password when you Angel Angel Ange	ns, you will be requ login. You should ch	uired to change th noose a strong pas	is Droplet's roc sword that will)t	
14.	Pro při	pojení použijte	e SSH klienta. V ná	sledujícím příkla	adu používám	standardní S	SH, které je součástí <i>Bas</i>	h
	on Ubu	ntu on Windo	ws, tedy linuxovél	no subsystému v	ve Windows 10). Můžete nic	méně použít například	
	populá	rní PuTTY ³ neb	o cokoliv jiného.					
	Pokud : Digital	žádného SSH k Ocean. U drop Droplets Volumes	lienta nemáte a n letu klepněte na N	echcete si ho ins Aore v pravé čás	stalovat, může sti a z rozbalov	te použít i we acího seznan	bové rozhraní v zvolte Access Console	2.
(î)		Name		IP Address	Created	Tags		
		512 MB / 20 GB	B Disk / FRA1 - Ubuntu		12 days ago		More V	
							Add a domain	
							Access concole Resize droplet	
		have a second			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			

³ http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html 12

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 <i>Enter</i> .
	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 jednorazové heslo, které jste obdrželi e-mailem.
	root@138.68.102.250's password: dc++3a239dc25+7+84a602a098
	You are required to change your password immediately (root enforced)
	<pre>* Documentation: https://help.ubuntu.com</pre>
	<pre>* Management: https://landscape.canonical.com</pre>
	* Support: https://ubuntu.com/advantage
	Cat cloud support with Ukuntu Advantage Cloud Guest
	bttp://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;
	individual files in /usr/share/doc/*/convright
	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 <i>Domain name</i> 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=xxxxxxxxxxxxx&domain=streisand-demo.freemyip.com
	Pokud uděláte HTTP request na tuto adresu, nasměruje se hostname (zde streisand-
$(\mathbf{\hat{U}})$	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 cur1. To zařídíme pomocí služby Cron, což je
	plánovač události.
5.	Připojte se pomocí SSH na server. Pro přihlášení použíjte nové heslo, nastavené v kroku 15 návodu <i>Error! N</i>
	ot a valid result for table.
6.	Na serveru spustte příkaz chontabili – e, kterým spustite editáci tabulky plánovače události. Když se vás
	zepta, jaky editor chcete pouzivat, zvolte moznost 2, tedy / bin/hano:
	no crontab for root - using an empty one
	Select an editor. To change later, run 'select-editor'.
	2. /bin/nano < easiest
	3. /usr/bin/vim.basic
	4. /usr/bin/vim.tiny
	Choose 1-4 [2]: 2
	GNU nano 2.5.3 File: /tmp/crontab.D6o9mi/crontab Modified
	# Edit this file to introduce tasks to be run by cron.
	# # Each task to run has to be defined through a single line
	<pre># indicating with different fields when the task will be run # and what command to run for the task</pre>
	# # To define the time you can provide concrete values for
	<pre># minute (m), hour (h), day of month (dom), month (mon), # and day of week (dow) or use '*' in these fields (for 'any') #</pre>
	# Notice that tasks will be started based on the cron's system
	# daemon's notion of time and timezones. #
	# Output of the crontab jobs (including errors) is sent through # email to the user the crontab file belongs to (unless redirected).
	# # For example, you can run a backup of all your user accounts
	<pre># at 5 a.m every week with: # 0.5 * * 1 tar -zcf /var/backuns/home tgz /home/</pre>
	# For more information see the moreal ranges of emortab/(5) and ener(9)
	# For more information see the manual pages of crontab(5) and cron(8)
	# m h dom mon dow command
	@reboot curl "https://freemyip.com/update?token=: & & & & & & & & & & & & & & & & & & &
	^G Get Help ↑0 Write Out ↑₩ Where Is ↑K Cut Text ↑J Justify ↑C Cur Pos ↑Y Prev Page M-\ First Line
	^X Exit^R Read File _^\ Replace^U Uncut Text _^T To Spell Go To LineV Next PageM-/ Last Line
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 @reboot curl a adresu získanou v bodu 4 v uvozovkách:
	<pre>@reboot curl "https://treemyip.com/update?token=xxxxxxxx&domain=streisand-demo.freemyip.com" </pre>
9.	vyskocte z editoru stiskem klaves UTP1+X (oznaceno jako ^X).
10.	Na otazku save moaijiea bujjer (ANSWERING "NO" WILL DESTRUY CHANGES) ? Odpovezte Y.
11.	Nazev soudoru nechte deze zmeny (stisknete pouze Enter).
12.	ivasiedujicim prikazem restartujte server, cimz vyzkousite, ze se aktualizace DNS provede:

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 predchozim prikladu U2. Nastaveni dynamickeho DNS). Na serveru zadejte nasledujici prikaz, 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]
	Fetched 11.5 MB in 4s (2,418 kB/s)
	root@streisand:~#
2.	Zadejte následující příkaz, kterým nainstalujete komponenty, které Streisand potřebuje. Opět to bude
	nejakou dobu trvat:
	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-lubuntul)
	Processing triggers for libc-bin (2.23-0ubuntu7)
3.	Zadejte následující příkaz, kterým nainstalujete Ansible, který Streisand využívá pro konfiguraci:
	<pre>root@streisand:~# pip install ansible markupsafe dopy==0.3.5</pre>
	Collecting ansible Downloading ansible-2.2.2.0.tar.gz (2.5MB)
	100% 100% 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
Δ	root@stre1sand:~# Zadejte následující příkaz, kterým stábnete aktuální verzi Strejsand z Githubu:
	root@streisand:~# git clone https://github.com/jlund/streisand.git && cd streisand/playbooks
	Cloning into 'streisand'
	remote: Counting objects: 64/0, 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#
J.	streisand-demo, freemvip, com zadeite váš název serveru):
	<pre>root@streisand:~/streisand/playbooks# sed -i 's/streisand-host/streisand-demo.freemyip.com/g'</pre>
6	streisand.yml
0.	root@streisand:~/streisand/playbooks# nano group vars/all
7.	Soubor upravte tak, aby měl následující obsah (přidané řádky jsou vyznačeny tučně):
	- 8.8.8.8
	- 208.67.222.222
	streisand_ci: no
	streisand_noninteractive: no
	streisand_shadowsocks_enabled: yes
	streisand_wireguard_enabled: yes
	streisand_stunnel_enabled: yes
	streisand_tor_enabled: no
	streisand_openconnect_enabled: yes
	<pre>gpg_key_server_address: "x-hkp://pool.sks-keyservers.net"</pre>

Q	
0.	Vyskočte z editoru stiskem klaves Ctr1+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 tile in the generated-docs tolder is ready to give to friends, family members, and fellow activists. Press Enter to continue :
13	Stiskněte <i>Enter</i> . Nenechte se zaskočit tím, že počítač vypíše chybu, že se mu nepodačilo otevřít HTMI
_0.	soubor. To je za těchto okolností normální.
14.	Instalace ie nyní dokončena. V souboru ~/streisand/generated-docs/streisand.html naidete
	instrukce pro připojení.
_	Instrukce zkopírujte na svůj počítač. Pokud máte na svém počítači SCP pokračujte podle následujícího
(j)	návodu. Nemáte-li, pokračujte bodem 14.
15.	Ukončete spojení se serverem pomocí příkazu exit:
	root@streisand:~# exit
	logout
16	Následujícím příkazem (spuštěným pa lokálním počítači, pe pa vzdáleném serveru) zkonírujte soubor
10.	streisand html na svůj počítač Místo streisand-demo freemvin com opět zadejte váš název
	serveru:
	<pre>scr root@streisand-demo.freemyip.com:/root/streisand/generated-docs/streisand.html streisand.html</pre>
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
	uložitjako streisand.html.
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: Streisand market i str
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: Streisand in the streisand in
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND × × \leftrightarrow C () file:///C:/Users/Altair/AppData/Local/kxss/home/altair/streisand.html \Rightarrow :
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND $\leftarrow \rightarrow \mathbb{C}$ () file:///C:/Users/Altair/AppData/Local/Ixss/home/altair/streisand.html STREISAND
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND × C ③ file:///C:/Users/Altair/AppData/Local/lxss/home/altair/streisand.html ☆ :: STREISAND
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: Streisand Description Image: Streisand Description Image: Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: Streisand micros Image: Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service.
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND STREISAND STREISAND Your Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service. SSL Certificate Installation • Windows • OS X
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND STREISAND Your Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service. SSL Certificate Installation • Windows • OSX • Android
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND STREISAND STREISAND Your Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service. SSL Certificate Installation
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND STREISAND STREISAND Your Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service.
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: STREISAND STREISAND STREISAND STREISAND Your Streisand Gateway contains step-by-step instructions for the services it provides, and mirrors of all necessary client software. The Gateway can be accessed over SSL or via a Tor Hidden Service.
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto:
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: tak
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: StressAnd Ima
18.	uložit jako streisand.html. Výsledný soubor bude vypadat přibližně takto: Image: StressAND interview interv

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.
U	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:
	Certificate Information
	This CA Root certificate is not trusted. To enable trust,
	install this certificate in the Trusted Root Certification Authorities store.
	Issued to: Streisand Effect Department
	Yound has Stational Effect Developed
	Issued by: Sueband Elect Department
	Valid from 10.04.2017 to 09.04.2022
	Install Certificate Issuer Statement
	NS IN
	ОК
<u>р</u> .	V dalžím kraku klapněta na Dlaca all certificatos in the following store a nak na Drewse. V dialogu wherte
/.	Trusted Poot Cartification Authorities a noté kloppěto pa Next:
	Tusted Nool Certification Authonities a pole Riephete na Wext.
	×
	Certificate Import Wizard
	Certificate Store Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate.
	Automatically select the certificate store based on the type of certificate
	O Place all certificates in the following store Certificate store:
	Trusted Root Certification Authorities
	3 Next Cancel
8.	Klepněte na <i>Finish</i> .
9.	V okně <i>Security Warning</i> klepněte na <i>Yes</i> .
10.	Ukáže se zpráva <i>The import was successful.</i> 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.

(zjistěte postupem dle následujícího návodu)

- Uživatelské jméno: streisand
- Heslo:
- Sdílený klíč (pre-shared key): ______ (zjistěte postupem dle následujícího návodu)



6.	Klepněte na odkaz <i>Windows</i> .
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.
	≜ _ п х
	S STREISAND ×
	← → C Image: Secure https://streisand-demo.freemyip.com/l2tp-ipsec/#windows ★ Image: Secure https://streisand-demo.freemyip.com/l2tp-ipsec/#windows
	8. Enter streisand in the Destination name held.
	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 <i>Password</i> field.
	13. Check the <i>Remember this password</i> checkbox.
	have a second a secon
0	Najděta v saznamu krak řísla 12. Hodnota na čodém pozadí je váč pro sharod kov (na obrázku píže
ο.	i Najuele v sezilalnu krok cisio 12. Hounola na seueni pozaŭi je vas pre-snareu key (na obrazku nize
0.	anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte.
0.	anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte.
0.	anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte.
0.	anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. S STREISAND × C Secure https://streisand-demo.freemyip.com/l2tp-ipsec/#windows ☆ :
0.	anthelices-barrettes-peptized, váš bude jiný). Tento klíč si poznamenejte. S STREISAND × C Secure https://streisand-demo.freemyip.com/l2tp-ipsec/#windows ☆: Type of VPN drop-down menu.
0.	anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. S STREISAND × ← → C Secure https://streisand-demo.freemyip.com/l2tp-ipsec/#windows ☆: Type of VPN drop-down menu. 19. Click the Advanced settings button.
0.	Najuete v seznamu krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: streisand key for authentication and enter anthelices-barrettes-peptized for the Key.
0.	Najuete v seznamu krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: Streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: Streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: Streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized krok na sedem pozadi je vas pre-snared key (na obrazku nize anthelices - barrettes - peptized key (na obrazku nize anthelices - barrettes - peptized key (na obrazku nize anthelices - barrettes - peptized for the Key. Image: Streisand key for authentication and enter anthelices - barrettes - peptized for the Key. Image: Streisand key for obrazku settings.
0.	Najuete v seznamu krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices -barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices -barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: streisand krok cisio 12. Hodnota na sedem pozadi je vas pre-snared key (na obrazku nize anthelices -barrettes - peptized, váš bude jiný). Tento klíč si poznamenejte. Image: streisand 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.

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

Příprava připojení

Spusťte příkazovou řádku jako správce. Stiskněte klávesy Win+X a z menu zvolte Command prompt (Admin), 1. případně PowerShell (Admin): ee, and dille Computer Management Command Prompt Command Prompt (Admin) 3 Task Manager Setti<u>ng</u>s File <u>E</u>xplorer <u>S</u>earch Run Sh<u>u</u>t down or sign out > <u>D</u>esktop 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 1 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						
5.	5. Klepněte na Set up a new connection or network:						
	🛱 Network and Sharing Center – 🗆 X						
A Search Control Panel > Network and Internet > Network and Sharing Center Search Control Panel Search Co							
	Control Panel Home Change adapter settings						
	Change advanced sharing settings Hotel_Omega_1 Access type: Internet Public network Connections: Image: Wi-Fi (Hotel_Omega_1)						
	Change your networking settings See also HomeGroup Troubleshoot problems Automatic and the set of						

6.	Klepněte na Connect to a workplace a poté na Next.
	Set Up a Connection or Network
	Choose a connection option
	Connect to the Internet Set up a broadband or dial-up connection to the Internet. Set up a new network Set up a new router or access point. Manually connect to a wireless network Connect to a hidden network or create a new wireless profile. Connect to a workplace Set up a dial-up or VPN connection to your workplace.
	2 Next Cancel
7.	Klepněte na Use my Internet connection (VPN).
8.	Zadejte IP adresu vašeho Streisand serveru do pole <i>Internet address</i> . Spojení můžete pojmenovat
	(Destination name). Pote Repriete na Create.
	— — X 🗧 🦕 Connect to a Workplace
	Type the Internet address to connect to
	Your network administrator can give you this address.
	Internet address: streisand-demo.freemyip.com
	Destination name: Streisand 2
	Use a <u>s</u> mart card
	Remember my credentials
	Allow other people to use this connection This option allows anyone with access to this computer to use this connection.
	3 <u>Create</u> Cancel
9.	V okně Network and Sharing Center klepněte na Change adapter settings:
	🛱 Network and Sharing Center — 🗆 🗙
	← → × ↑ 🔛 > Control Panel > Network and Internet > Network and Sharing Center v & Search Control Panel P
	Control Panel Home View your basic network information and set up connections
	View your active networks
	Change advanced s Hotel_Omega_1 Access type: Internet settings Public network Connections: all Wi-Fi (Hotel Omega 1)
10.	Klepněte na název připojení (určený v kroku 8, zde Streisand) pravým tlačítkem a z kontextového menu
	zvolte Properties.



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				
(I)	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*.

	and a second and a second and a second and a second a sec						
Programs (1)							
	Open Image: Second state Image: Second state <						
	See more results cmd × Log off >						
	A = A = A						
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						
٦	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

1	Poté klepněte provým tločítkem polikopu síťového přinciení po hlovním popelu o z kontextového menu							
4.	role Repliete plavyin tlacticem ha konu sitoveno pripojem na mavium panetu a 2 kontextoveno menu							
	zvoite Open Network and Sharing Center.							
5.	5. Klepněte na <i>Set up a new connection or network</i> :							
	Control Panel 🕨	Network and Internet Network and Sharing Center	r 👻 😽 Search Control Panel 🔎					
	Control Panel Home	View your basis notwork information s	e e e e e e e e e e e e e e e e e e e					
		view your basic network information a	and set up connections					
	Change adapter settings	📃 🔍 ——— 🚑	F See full map					
	Change advanced sharing settings	CRYPTODEMO class.skc (This computer)	ola.cz Internet					
		View your active networks	Connect or disconnect					
		class.skola.cz	Access type: Internet					
		Public network	Connections: 📱 Local Area Connection					
Change your networking settings								
		Set up a new connection or network						
		Set up a wireless, broadband, dial-up, ad	I hoc, or VPN connection; or set up a router or access point.					
		Connect to a network						
		Connect or reconnect to a wireless, wire	d, dial-up, or VPN network connection.					
		Choose homegroup and sharing options						
	- marine and a							

6.	Klepněte na <i>Connect to a workplace</i> a poté na <i>Next</i> .							
	😡 🐏 Set Up a Connection or Network							
	Choose a connection option							
	Connect to the Internet							
	Set up a wireless, broadband, or dial-up connection to the Internet.							
	Set up a new network Configure a new router or access point.							
	Connect to a workplace							
	Set up a dial-up connection							
	Connect to the Internet using a dial-up connection.							
	Next Cancel							
7.	Klepněte na Use my Internet connection (VPN).							
8.	Zadejte IP adresu vašeho Streisand serveru do pole <i>Internet address</i> . Spojení můžete pojmenovat							
	tlačítko Next.							
	Connect to a Workplace							
	Type the Internet address to connect to							
	Your network administrator can give you this address.							
	Internet address: streisand-demo.freemyip.com							
	Destination name: Streisand 2							
	Use a <u>s</u> mart card							
	😵 🔲 Allow other people to use this connection This option allows anyone with access to this computer to use this connection.							
	3 Don't connect now; just set it up so I can connect later							
	4 Next Cancel							
0	V dalším kroku průvodce zadejte uživatelské iméno (st pej s and) a beslo zijičtěné v předchozím pávodu (05							
9.	Získání přihlašovacích údajů pro L2TP/IPSec VPN). Zaškrtněte Remember this password a klepněte na							
	tlačítko <i>Create</i> .							
	Connect to a Workplace							
	Type your user name and password							
	User name: streisand							
	Password extremism-remades							
	Show characters							
	Remember this password							
	Domain (optional):							
	Create Cancel							
10.	Spojení je vytvořeno. Klepněte na tlačítko <i>Close</i> .							

11.	V okně Network and Sharing Center klepněte na Change adapter settings:						
	🕢 😳 🗢 😟 🕨 Control Panel 🕨 Network and Internet 🕨 Network and Sharing Center 🔹 🍫 Search Control Panel 🔎						
Control Panel Home View your basic network information and set up connections							
	Change adapter settings See full map						
	Change advanced shaving CRYPTODEMO class.skola.cz Internet						
	(Ihis computed and the second						
12.	Klepněte na název připojení (určený v kroku 8, zde <i>Streisand</i>) pravým tlačítkem a z kontextového menu zvolte <i>Propertie</i> s						
13.	Nastavte podrobnější parametry připojení:						
	Na záložce Security nastavte jako Type of VPN hodnotu Layer 2 Tunneling Protocol with IPSec						
	(L2TP/IPSec).						
	 Klepnete na tracitko Advanced Settings a zadejte hodnotu presnared key (viz predchozi navod 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 <i>Microsoft CHAP version 2 (MS-CHAP v2)</i> .						
	Pote kiepnete na <i>OK</i> .						
	Streisand Properties						
	General Options Security Networking Sharing						
	1 Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec) 3 Image: Second secon						
	Data encryption:						
	Require encryption (disconnect if server declines)						
	Authentication Use Extensible Authentication Protocol (EAP)						
	Properties 5 OK Cancel						
	Unencrypted password (PAP)						
	Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2)						
	Automatically use my Windows logon name and password (and domain, if any)						
	8 OK Cancel						
14.	Klepnete na ikonu sitových pripojení na hlavním panelu. V seznamu pripojení klepnete na nazev nove vytvořeného připojení (<i>Streisand</i>) a poté na tlačítko <i>Connect</i> .						
	Currently connected to:						
	Tass.skola.cz Internet access						
	Dial-up and VPN						
	Streisand						
	Open Network and Sharing Center						
	CS 🚎 🛅 🎦 📂 😭						

15.	V dalším okně klepněte na <i>Connect</i> .					
	Second Streisand					
	User name: Istreisand					
	Password: [To change the saved password, click here]					
	Domain:					
	Save this user name and password for the following users:					
	Me only					
	Connect Cancel Properties Help					
١	Pokud toto okno nechcete v budoucnu zobrazovat, klepnėte na Properties a potom zrušte zaškrtnuti Prompt					
16	for name and password, certificate, etc.					
16.	Zobrazi se okno s informacemi o prubehu pripojovani, které se posléze samo zavre.					
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					
Inebo poskytovatel připojení. V takovém případě je nutné buďto změnit konfiguraci nebo použít něl						
	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

Ū	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						
	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.						
	S STREISAND ×						
	← → C ① file:///C:/Users/Altair/AppData/Local/lxss/home/altair/streisand.html#connecting-ssl ☆ :						
	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						
	https://streisand-demo.freemyip.com						
	username: streisand						
	password: jetbeads-flayers-turboprops-incorporal						
	Tor, Hidden Service						
	the second contraction of the second se						
4.	Zobrazí se vám stránka s konkrétním návodem na nastavení jednotlivých VPN:						
	S STREISAND ×						
	← → C Secure https://streisand-demo.freemyip.com ☆ ☆ 						
	STREISAND						
	Welcome to the streisand <u>Streisand</u> 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.						
	• <u>L2TP/IPsec</u>						
	OpenConnect / Cisco AnyConnect						
	• <u>OpenVPN (direct)</u>						
	· OpenVPN (stunnel)						
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 <i>client-1</i> až <i>client-5</i>, můžete použít kterýkoliv z nich (jde o pět různých profilů pro až pět různých uživatelů). 						
Insta	lace OpenVPN						
8.	Otevřete v prohlížeči	adresu https://ope	nvpn.net/.				
9.	Klepněte na odkaz Co	ommunity.	•				
10.	Klepněte na odkaz D	ownloads v levém men	u.				
11.	Stáhněte si instaláto	r pro Windows – v době	é psaní textu je al	ktuální verze 2.4.3:			
	PENVPN	N ®			Follow	Sign in	
	Home VPN S	Service VPN Solution	Community	Downloads	Search	Q	
	Overview	Downloads					
	Downloads Source Code	OpenVPN 2.4.3 released	on 2017.06.21 (Chang	<u>le Log</u>)			
	Documentation	OpenVPN v2.4.2 was analyzed clo of which are remotely exploitable in as possible. More details are availa	sely using a fuzzer by Guido o certain circumstances. We oble in our official security an	OVranken. In the process several recommend you to upgrade to C inouncement.	l vulnerabilities were found, some openVPN 2.4.3 or 2.3.17 as soon		
	HOWTO Security Overview Examples	Compared to OpenVPN 2.3 this is a major update with a large number of new features, improvements and fixes. Some of the major features are AEAD (GCM) cipher and Elliptic Curve DH key exchange support, improved IPv4/IPv6 dual stack support and more seamless connection migration when client's IP address changes (Peer-ID). Also, the newtts-crypt feature can be used to increase users' connection privacy.					
	Graphical User Interface	Compared to OpenVPN 2.4.2 there	are several bugfixes and o	ne major feature: support for buil	ding with OpenSSL 1.1.		
	Change Log	A summary of the changes is available in <u>Changes rst</u> , and a full list of changes is available <u>here</u> . OpenVPN GUI bundled with the Windows installer has a large number of new features compared to the one bundled with OpenVPN 2.3. One of major features is the ability to run OpenVPN GUI without administrator privileges. For full details, see the <u>changelog</u> . The new OpenVPN GUI features are documented <u>here</u> .					
	Installation Notes Release Notes						
	Miscellaneous Non-English	Windows installer I602 includes up vulnerability in the service manage	dated OpenVPN GUI (11.8.0 ment code.	0.0) and easy-rsa (2.3.0). The ins	staller also fixes a <u>security</u>		
	File Signatures	Please note that OpenVPN 2.4 inst	allers will not work on Windo	ows XP.			
	Articles FAQ	If you find a bug in this release, please file a bug report to our <u>Trac bug tracker</u> . In uncertain cases please contact our developers first, either using the <u>openvpn-devel mailinglist</u> or the developer IRC channel (#openvpn-devel at irc.freenode.net). For generic help take a look at our official <u>documentation</u> , <u>wiki</u> , <u>forums</u> , <u>openvpn-users mailing list</u> and user IRC channel (#openvpn at irc.freenode.net).					
	Client	Source Tarball (gzip)	openvpn-2.4.3.tar.gz	GnuPG Signature			
	Server	Source Tarball (xz)	openvpn-2.4.3.tar.xz	GnuPG Signature			
	Books	Source Zip	openvpn-2.4.3.zip	GnuPG Signature			
	Wiki/Tracker	Installer. Windows Vista and later	openyon-install-2.4 R-1602.exe	GnuPG Signature			
	Contributing		4				
	NOTE: the GPG key used to sign the release files has been changed since OpenVPN 2.4.0. Instructions for verifying the						
12.	Spusťte stažený insta	látor OpenVPN.					
13.	Klepněte na tlačítko	Next.					
14.	Klepnutím na <i>I Agree</i> odsouhlaste licenční podmínky.						
15.	Ponechte výchozí na:	stavení komponent pro	instalaci a klepn	ěte 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 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.
23. 24.	Pro připojení do VPN klepněte na ikonku v liště pravým tlačítkem a zvolte <i>Connect</i> . Zobrazí se okno s popisem průběhu připojování. Když zmizí a ikonka v liště změní barvu na zelenou, jste připojeni. Current State: Connection Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: route options modified Sat Jul 29 2020:10 2017 OPTIONS IMPORT: risk adjusting ink, mt to 1625 Sat Jul 29 2020:10 2017 OPTIONS IMPORT: risk adjusting ink, mt to 1625 Sat Jul 29 2020:10 2017 Data Channel: using negotiated cipher 'AES-256-GCM' Sat Jul 29 2020:10 2017 Data Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Data Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Data Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Data Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Data Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Tobat Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Tobat Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Tobat Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Tobat Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Tobat Channel Decrypt: Cipher 'AES-256-GCM' initialized with 256 bit key Sat Jul 29 2020:10 2017 Tobat Channel Decrypt: Cipher 'AES-255-255.255.01 = HWADDR=70:85:c2:38:d710 Sat Jul 29 2020:10 2017 TAP-WiNA
	Sat Jul 29 20:20:10 2017 do, ifconfig.ipv6 setup=0 Sat Jul 29 20:20:10 2017 MANAGEMENT: >STATE:1501352410,ASSIGN_IP.,10.9.0.6, Sat Jul 29 20:20:10 2017 Blocking outside dns using service succeeded.
	<
	Disconnect Reconnect Hide
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 s	erver pomocí SSH nebo webové konzole.			
2.	Následujícím příkazem server vypněte:				
	root@streisand:~# s	shutdown -hP now			
	Connection to stre	isand-demo.freemyip.com closed by remote host.			
	Connection to stre	isand-demo.freemyip.com closed.			
(i)	Vypnutí serveru neni	absolutně nezbytné, snapshot lze udělat i z běžícího počítače. Z důvo	du konzistence dat		
Ű	se nicméně doporuči	ije server vypnout.			
3.	Otevřete v prohlížeč	i adresu https://www.digitalocean.com/ a přihlašte se svým j	ménem a heslem.		
4.	V seznamu dropletů	klepněte na název vašeho Streisand serveru.			
5.	V levém menu klepn	ěte na odkaz Snapshot.			
	Droplets Im	ages Networking Monitoring API Support Create I	Droplet 💽 🗸		
	ipv4: 207.154.230.173	ipv6: Enable now Private IP: Enable now Floating IP: Enable now	Console: 🗇		
	Graphs Access	Learn how to update this Droplet for new metrics.	6 hours 🗸		
	Power	Bandwidth public			
	Volumes NEW!	102 Mbns			
	Resize				
	Networking	0.682 Mbps			
	Backups	0.002 mbps -			
	Snapshots	0.341 Mbps			
	Kernel				
	History	0 Mbps			
	Contract March	Ammen 2127 PM Ammen 23/11 PM	MG:4 PM		
6.	Zadejte název snaps	hotu (například ve formátu streisand-RRRRMMDD-hhmm) a klepněl	te na tlačítko <i>Take</i>		
	Live Snapshot.				
	Graphs	Take snapshot			
	Access	Power down your Draplat before taking a grapphat to answer data consistency. Chapabata cost is	based on onese		
	Power	used and charged at a rate of \$0.05/GB/mo.	based on space		
	Volumes NEW!				
	Resize	Enter snapshot name	e Snapshot		
	Networking	30613010-20170+11-1500			
	Backups				
	Snapshots				
	Kernel	Droplet snapshots			
	History	You currently don't have any snapshots of this Droplet.			
	stroy	American manufacture and the second s	m		
		- 7 77	~		
7.	Vyčkejte, dokud se n	evytvoří snapshot, což může nějakou trvat několik minut.			
1	I za snapshot se plat	í, ale méně. Za snapshot typického Streisand serveru zaplatíte přibližr	ně 3 Kč měsíčně.		

Zrušení dropletu

8.	V levém menu klepněte na odkaz Destroy.
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 Images v horní části	stránky.						
13.	V seznamu snapshotů vyberte ten správný a klepněte na odkaz <i>More</i> vpravo.							
14.	Z menu zvolte Create Droplet.							
	Snapshots							
	Droplets Volumes							
	Name	Size	Regions	Created A				
	Streisand-20170411-1908 Created from strelsand	2.5 GB	FRA1	9 minutes ago	1 More V Rename			
				•	Add to region			
	hand	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~				
15.	Podobně jako při vytvoření nového dropletu můžete zvolit jeho velikost (a cenu) a pojmenovat ho.							
16.	Klepnutím na tlačítko Create droplet vy	tvoříte a na	startujete.					

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.