Jméno: _____ Datum: _____ Body: _____

Nejlepší VPN pro příkazový řádek Linuxu Rozhraní (CLI)

Správa zabezpečených relací VPN a řešení potíží s připojením pomocí nástrojů CLI v Linuxu.

NASTAVENÍ VPN V LINUXOVÉM CLI – PŘEHLED UČIVA

STUDENT
STUDENTSKÝ STATUS
Dráha obránce sítě

ZABEZPEČENÝ
STAV PŘIPOJENÍ
Stínění datových paketů

AKTIVNÍ
OCHRANA PROTI ÚNIKŮM
Ochrana proti únikům DNS a IPv6

Vítejte! Tento balíček aktivit vás provede konfigurací VPN v příkazové řádce Linuxu. Prozkoumáte rozhraní řádkových klientů, konfigurační soubory, unit služby systemd, soubory přihlašovacích údajů a nastavení DNS přes resolvectl.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte konfigurace VPN a zabezpečení sítě.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce nejlepšími VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/nejlepsi-vpn-pro-linux/rozhrani-prikazoveho-radku/

Váš studijní plán: VPN v linuxovém CLI

- Nakonfigurujte bezpečná VPN připojení pomocí nástrojů příkazové řádky.
- Vytvořte pravidla firewallu, která zabrání únikům nešifrovaného veřejného provozu.
- Diagnostikujte konflikty překladu DNS a vynuťte zabezpečené jmenné servery.

NASTAVENÍ VPN V LINUXOVÉM CLI – POKYNY

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na parametry příkazů CLI a konfigurační soubory. Zakončete bonusovou aktivitou Mysli rychle.

OVLÁDÁNÍ VPN Z TERMINÁLU A HANDSHAKY NA BÁZI KONFIGURACÍ (ÚVOD)

Správa VPN připojení přes rozhraní příkazového řádku (CLI) je na headless linuxových uzlech zásadní. Uživatelé využívají vyhrazené klientské příkazy, konfigurační soubory a služby systemd k navazování zabezpečených tunelů, prevenci úniků DNS a správě firewallových killswitchů.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jakou rychlost podle CLI průvodce VPN.com průměrně dosahuje WireGuard?**
   - A. 300–400 Mbps
   - B. 20–40 Mbps
   - C. 5–10 Mbps
   - D. 1–2 Mbps

2. **2. Který VPN klient podporuje připojení pomocí čísel serverů (např. us2435)?**
   - A. ExpressVPN
   - B. NordVPN
   - C. ProtonVPN
   - D. Mullvad

3. **3. Který poskytovatel má proprietární protokol jménem Lightway?**
   - A. ExpressVPN
   - B. NordVPN
   - C. Surfshark
   - D. ProtonVPN

4. **4. Která VPN zaměřená na soukromí nevyžaduje k registraci e-mailovou adresu ani jméno?**
   - A. NordVPN
   - B. Mullvad
   - C. ExpressVPN
   - D. Surfshark

5. **5. Kolik podle CLI průvodce VPN.com průměrně dosahuje OpenVPN na moderním hardwaru?**
   - A. 5–10 Mbps
   - B. 20–40 Mbps
   - C. 150–250 Mbps
   - D. 1–2 Mbps

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Linuxový klient NordVPN spouští démona na pozadí jménem nordvpnd.

○ Pravda ○ Nepravda

7 Otázka 7

7. ExpressVPN nenabízí žádnou aplikaci pro Linux.

○ Pravda ○ Nepravda

8 Otázka 8

8. Mullvad účtuje paušálně €5 měsíčně bez slev za délku předplatného.

○ Pravda ○ Nepravda

9 Otázka 9

9. Proton VPN zveřejňuje zdrojový kód své linuxové aplikace pod licencí GPL.

○ Pravda ○ Nepravda

10 Otázka 10

10. Surfshark umožňuje pouze 5 souběžných připojení zařízení.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Pro spouštění VPN tunelů přímo z konzole používají administrátoři _____ .
2. Parametry připojení a šifrovací klíče uchovává lokální _____ .
3. Správu připojení na pozadí automatizuje povolená _____ .
4. Uživatelské jméno a heslo, tedy _____ , by měly být bezpečně uloženy v samostatném souboru.
5. Pojistný kill switch se konfiguruje pravidly netfilter v místním nastavení nástroje _____ .
6. Parametry překladu DNS u konkrétního spojení se auditují nástrojem _____ .

ZÁSOBNÍK SLOV

IPTABLES KONFIGURAČNÍ SOUBOR PŘIHLAŠOVACÍ ÚDAJE RESOLVECTL
ROZHRANÍ CLI SLUŽBA SYSTEMD SMĚROVACÍ TABULKA TUNEL

Sem napište své odpovědi:

1.
2.
3.
4.
5.
6.

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

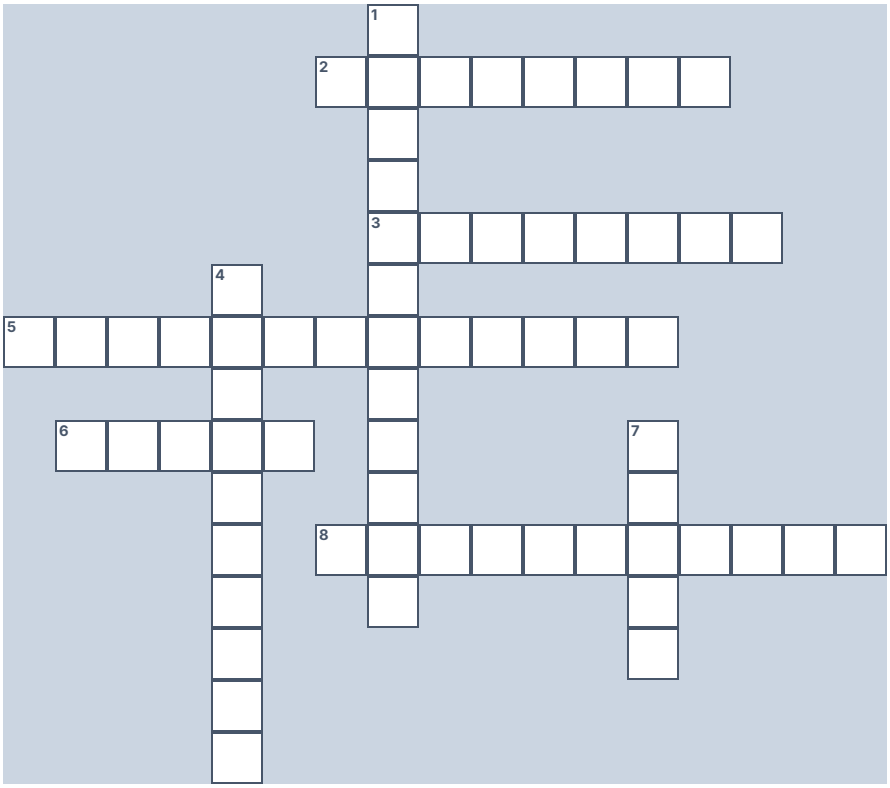
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. ROZHRANÍ CLI	A	Virtuální rozhraní point-to-point předávající šifrované síťové pakety.
☐	2. KONFIGURAČNÍ SOUBOR	B	Nástroj příkazové řádky dotazující rozsahy DNS serverů pro jednotlivá rozhraní.
☐	3. SLUŽBA SYSTEMD	C	Soubor na místním disku obsahující koncové body připojení a klíče.
☐	4. PŘIHLAŠOVACÍ ÚDAJE	D	Proces programu běžící nezávisle na pozadí a spravující služby.
☐	5. IPTABLES	E	Jednotka systemd spravující životní cyklus klienta běžícího na pozadí.
☐	6. RESOLVECTL	F	Prostředí příkazové řádky používané k přímému spouštění klientských příkazů.
☐	7. TUNEL	G	Chráněné soubory tokenů obsahující ověřovací hodnoty uživatele.
☐	8. DÉMON	H	Framework Netfilter spravující pravidla zahazování a povolování paketů.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

2. Chráněné soubory tokenů obsahující ověřovací údaje uživatele (8)

3. Rámec netfilter spravující pravidla zahazování a povolování paketů (8)

5. Jednotka systemd řídící běh klienta na pozadí (13)

6. Program běžící nezávisle na pozadí a spravující služby (5)

8. Prostředí příkazové řádky pro přímé spouštění klientských příkazů (11)

SVISLÉ NÁPOVĚDY

1. Soubor na disku obsahující koncové body připojení a klíče (12)

4. Nástroj příkazové řádky pro dotazy na DNS servery jednotlivých rozhraní (10)

7. Virtuální point-to-point rozhraní přeposílající šifrované síťové pakety (5)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

2 vodorovně: Chráněné soubory tokenů obsahující ověřovací údaje uživatele (8 písmen):

3 vodorovně: Rámec netfilter spravující pravidla zahazování a povolování paketů (8 písmen):

5 vodorovně: Jednotka systemd řídící běh klienta na pozadí (13 písmen):

6 vodorovně: Program běžící nezávisle na pozadí a spravující služby (5 písmen):

8 vodorovně: Prostředí příkazové řádky pro přímé spouštění klientských příkazů (11 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Soubor na disku obsahující koncové body připojení a klíče (12 písmen):

4 svisle: Nástroj příkazové řádky pro dotazy na DNS servery jednotlivých rozhraní (10 písmen):

7 svisle: Virtuální point-to-point rozhraní přeposílající šifrované síťové pakety (5 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

R O Z H R A N Í C L I A Ď Ó Ď
O É G I D S Ř L E N U T N E I
B Š N O M É D Ž T É Ř Ů E A Á
U Ř P O Q U Y R J S U Š Č Ň Ý
O L T C E V L O S E R B Ě Š X
S W Í A S Ž Ý Ý L F I N S J N
G M Ť P G R Ř G Ž Á Ó Ů Ě Ú C
I Ý Š Ý B G M Ž F J Ó Q S O X
F C N Ž Z Ě Ý P W Ú L Ů E Q B
N Ó V Ť N F Ů Č Ý Ú K S L Á X
O S Y S T E M D S L U Ž B A Ž
K Y N Š R X H P D Á Č J A Ř V
W X P O V Ě Ř E N Í L Í T H U
H Ě B E I K Ť Š V Ř Z E P H E
Š C A M R C Ž N K V Š Ú I Á Š

SEZNAM SLOV

ROZHRANÍCLI KONFIGSOUBOR SYSTEMDSLUŽBA POVĚŘENÍ IPTABLES
RESOLVECTL TUNEL DÉMON

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. ROZHRANÍCLI**
- **B. KONFIGSOUBOR**
- **C. SYSTEMDSLUŽBA**
- **D. POVĚŘENÍ**
- **E. IPTABLES**
- **F. RESOLVECTL**
- **G. TUNEL**
- **H. DÉMON**

DEFINICE A POLE K PŘIŘAZENÍ

1. Soubor na disku obsahující koncové body připojení a klíče.
2. Program běžící nezávisle na pozadí a spravující služby.
3. Chráněné soubory tokenů obsahující ověřovací údaje uživatele.
4. Prostředí příkazové řádky pro přímé spouštění klientských příkazů.
5. Virtuální point-to-point rozhraní přeposílající šifrované síťové pakety.
6. Jednotka systemd řídící běh klienta na pozadí.
7. Nástroj příkazové řádky pro dotazy na DNS servery jednotlivých rozhraní.
8. Rámec netfilter spravující pravidla zahazování a povolování paketů.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny virtuální privátní sítě (VPN). Odpovědi pište do připravených polí.

1. RNLOAÍRCZIH
2. BEYMSSŽDAL UST
3. APIBLSET
4. NLETU
5. OBOSRNIUGK OF
6. NÍĚEPŘOV
7. EOREVCTLLS
8. NDMOÉ

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Firewallové nástroje, které znáte			
2	Způsoby instalace softwaru na Linuxu			
3	Zařízení, která mohou používat VPN			
4	Slova, která popisují open source			
5	Příkazy, které můžete použít v Linux			
6	Programy, které byste nainstalovali na Linux			
7	Soubory nebo složky, které může VPN používat			
8	Zařízení, na kterých může běžet Linux			
9	Co zkontrolovat, když se VPN nepřipojí			
10	Zvířata nebo maskoti ze světa počítačů			
11	Linuxové distribuce, které znáte			
12	Slova z tohoto pracovního listu, která si chcete zapamatovat			
13	VPN služby, které znáte			
14	Věci, které lze nastavit v terminálu			
15	Důvody, proč používat Linux			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: OCHRANA HEADLESS SERVERU



Scénář: Správce Linuxu potřebuje zabezpečit vzdálené zálohy souborů z headless koncového uzlu umístěného v datacentru sdíleného hostingu.

Otázka k diskusi: Jaké nástroje a příkazy použít ke spuštění tunelu a ke kontrole překladů DNS daného spojení?

PŘÍPADOVÁ STUDIE 2: AUTOMATIZACE ODCHOZÍHO KILL SWITCHE



Scénář: Administrátor chce zajistit, aby headless terminálové spojení přerušilo veškerý veřejný provoz, pokud tunel VPN vypadne.

Otázka k diskusi: Jaká konkrétní pravidla firewallu je třeba přidat k vytvoření této pojistné hranice?

Kontrolní bod 9: Dešifrování šifry

Síťový inženýr zabezpečuje směrovací kanály a klientské tunely. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

4	18	14		30	32	20	8	18	38		4	13	26	2	20	15

18	14	20	32	37		28	8	26	35	8	26	38		3	8	40

19	22	20	14	30	22	26	32

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky k VPN (část A)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q1: Co je CLI VPN klient?

Program příkazového řádku, který vytváří zabezpečené tunely VPN bez potřeby grafického desktopového prostředí.

Q2: Jak zkontroluji stav VPN v systemd?

Spusťte systemctl status openvpn-client@profile a ověřte, že démoni připojení běží na pozadí.

Q3: Kde se ukládají konfigurace VPN?

Obvykle v adresářích /etc/openvpn/ nebo /etc/wireguard/ na standardních distribucích.

Q4: Co je rozhraní tun0?

Virtuální síťové tunelové rozhraní vytvořené jádrem systému při inicializaci připojení VPN.

Q5: Jak zkontroluji logy VPN připojení?

Pomocí journalctl -u openvpn-client sledujte logování v reálném čase a laďte selhání připojení. [10]

Kontrolní bod 10: Základní časté otázky k VPN (část B)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q6: K čemu se používá resolvectl?

Je to nástroj, který dotazuje stav DNS systemd-resolved a pravidla směrování na aktivních síťových spojích. [9]

Q7: Jak spustím VPN přes CLI?

Spusťte sudo openvpn --config client.ovpn nebo wg-quick up wg0 podle protokolu.

Q8: Co je headless server?

Server, který funguje bez monitoru, klávesnice nebo místního grafického rozhraní a je spravován vzdáleně.

Q9: Jaký je formát konfiguračního souboru WireGuardu?

WireGuard používá jednoduché konfigurační profily ve stylu ini, obvykle pojmenované wg0.conf.

Q10: Mohu spustit více CLI VPN současně?

Ano, konfigurací oddělených směrovacích tabulek a virtuálních tunelových rozhraní pro každého klienta.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část C)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q1: Jak automatizuji přihlášení k VPN při bootu bez monitoru?

V konfiguraci .ovpn odkažte na textový soubor s přihlašovacími údaji pomocí direktivy auth-user-pass. [11]

Q2: Jak nastavím směrování dle pravidel přes CLI?

Pomocí příkazů ip route a ip rule směrujte provoz konkrétních aplikací přes rozhraní VPN brány.

Q3: Jak opravím úniky DNS na headless uzlu?

Nakonfigurujte systemd-resolved tak, aby upřednostňoval DNS VPN spoje nastavením výchozích domén v resolvectl.

Q4: Jaký je rozdíl mezi rozhraními tun a tap?

Tun pracuje na vrstvě 3 (směrování IP), zatímco tap pracuje na vrstvě 2 (ethernetové mosty) lokálních systémů.

Q5: Jak z konzole sleduji živou šířku pásma VPN?

Použijte řádkové monitory šířky pásma jako nload, vnstat nebo iftop zaměřené na rozhraní tun0.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část D)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q6: Jak nakonfiguruji nftables pro VPN killswitch?

Definujte pravidla, která zahazují odchozí pakety na rozhraních WAN, pokud cíl neodpovídá IP serveru VPN.

Q7: Jak ověřím, zda se má veřejná IP změnila?

Spusťte curl ifconfig.me nebo curl icanhazip.com z příkazové řádky pro zobrazení aktuální adresy brány.

Q8: Co je wg-quick?

Obalový skript příkazového řádku, který automatizuje vytváření, konfiguraci a spouštění rozhraní WireGuard. [8]

Q9: Jak ručně aktualizuji nastavení DNS přes shell?

Upravte symbolický odkaz /etc/resolv.conf nebo přidejte direktivy DNS přímo do konfigurací NetworkManageru.

Q10: Jak spustím vlastní skripty při připojení VPN?

Pomocí konfiguračních parametrů up a down v OpenVPN spouštějte skripty při změnách stavu.

Část 11: 10 faktů a poznatků o VPN z praxe

Projděte si fakta z praxe o rychlostech VPN šifrování, auditech protokolů, mobilní konektivitě a podnikové práci na dálku.

1. VPN POSTŘEH

VPN klienti pro příkazovou řádku běží bez grafického prostředí, což vyhovuje headless serverům.

2. VPN POSTŘEH

Tunely WireGuard se spravují přímo přes kernelové moduly jednoduchými shellovými příkazy.

3. VPN POSTŘEH

Služby jednotek systemd automatizují spuštění tunelu a zásady obnovy během startu systému.

4. VPN POSTŘEH

resolvectl zjišťuje aktivní konfigurace DNS na headless virtuálních síťových adaptérech.

5. VPN POSTŘEH

Headless uzly používají pravidla iptables k zahazování všech nešifrovaných odchozích síťových paketů.

6. VPN POSTŘEH

Zařízení tun0 směruje požadavky lokální virtuální podsítě přímo do aktivních tunelů.

7. POSTŘEH K VPN

Cesty k textovým souborům s přihlašovacími údaji umožňují bezobslužné nastavení serverů bez ručního zadávání hesel.

8. POSTŘEH K VPN

journalctl sleduje aktivní chyby připojení a časy handshaků v reálném čase.

9. POSTŘEH K VPN

Statistiky síťových rozhraní zobrazují přesné objemy odeslaných a stažených dat.

10. VPN POSTŘEH

Vlastní směrovací tabulky umožňují rozdělit provoz mezi místní sítě a zabezpečené tunely.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních technických standardů, specifikací a regulačních rámců.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] VPN.com. (2026). Best VPN for Command Line: CLI Tools for Sysadmins.
https://www.vpn.com/vpn/best-vpn-for-linux/command-line-interface/

[2] WireGuard. (n.d.). Installation.
https://www.wireguard.com/install/

[3] Kernel Newbies. (2020). Linux 5.6.
https://kernelnewbies.org/Linux_5.6

[4] Nord Security. (n.d.). nordvpn-linux: NordVPN Linux client.
https://github.com/NordSecurity/nordvpn-linux

[5] Proton AG. (n.d.). proton-vpn-gtk-app: Proton VPN GTK app.
https://github.com/ProtonVPN/proton-vpn-gtk-app

[6] Debian. (n.d.). File list of package openvpn in trixie of architecture amd64.
https://packages.debian.org/trixie/amd64/openvpn/filelist

[7] The Linux Kernel documentation. (n.d.). Universal TUN/TAP device driver.
https://docs.kernel.org/networking/tuntap.html

[8] man7.org. (n.d.). wg-quick(8) — Linux manual page.
https://man7.org/linux/man-pages/man8/wg-quick.8.html

[9] man7.org. (n.d.). resolvectl(1) — Linux manual page.
https://man7.org/linux/man-pages/man1/resolvectl.1.html

[10] man7.org. (n.d.). journalctl(1) — Linux manual page.
https://man7.org/linux/man-pages/man1/journalctl.1.html

[11] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Otázka 1** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

CLI průvodce VPN.com uvádí, že WireGuard dosahuje průměrně 300–400 Mbps, rychleji než OpenVPN nebo IKEv2.

2 **Připojení k serveru** NORDVPN CLI **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

NordVPN umožňuje ve svém CLI přímá připojení ke konkrétním číslům serverů, například connect us2435.

3 **Protokol Lightway** EXPRESSVPN **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

ExpressVPN vyvinul Lightway, proprietární odlehčený protokol připojení postavený na vysokou rychlost.

4 **Anonymní účet** MULLVAD **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Mullvad přiděluje uživatelům náhodné 16místné číslo účtu a nevyžaduje e-mailovou adresu ani jméno.

5 **Otázka 5** **Správná odpověď: C**

POZNÁMKA PRO VYUČUJÍCÍ

CLI průvodce VPN.com uvádí, že OpenVPN dosahuje na moderním hardwaru průměrně 150–250 Mbps.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Linuxová aplikace NordVPN používá démona nordvpnd, se kterým komunikuje příkaz nordvpn.

7 **Otázka 7** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: ExpressVPN podporuje Linux, včetně Debianu, Ubuntu, Fedory a Archu.

8 **Otázka 8** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Mullvad účtuje paušálně €5 měsíčně, ať koupíte jakoukoli délku.

9 **Otázka 9** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Linuxová aplikace Proton VPN je open source, vydaná pod licencí GPL-3.0.

10 **Neomezená propojení** BEZ LIMITU ZAŘÍZENÍ — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Surfshark umožňuje neomezený počet souběžně připojených zařízení na jednom uživatelském účtu.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

F 1. ROZHRANÍ CLI	C 2. KONFIGURAČNÍ SOUBOR	E 3. SLUŽBA SYSTEMD	G 4. PŘIHLAŠOVACÍ ÚDAJE
H 5. IPTABLES	B 6. RESOLVECTL	A 7. TUNEL	D 8. DÉMON

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 ROZHRANÍ CLI	2 KONFIGURAČNÍ SOUBOR	3 SLUŽBA SYSTEMD	4 PŘIHLAŠOVACÍ ÚDAJE
5 IPTABLES	6 RESOLVECTL		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 B – KONFIGSOUBOR	2 H – DÉMON	3 D – POVĚŘENÍ	4 A – ROZHRANÍCLI
5 G – TUNEL	6 C – SYSTEMDSLUŽBA	7 F – RESOLVECTL	8 E – IPTABLES

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy ROZHRANÍ CLI, KONFIGURAČNÍ SOUBOR a SLUŽBA SYSTEMD a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

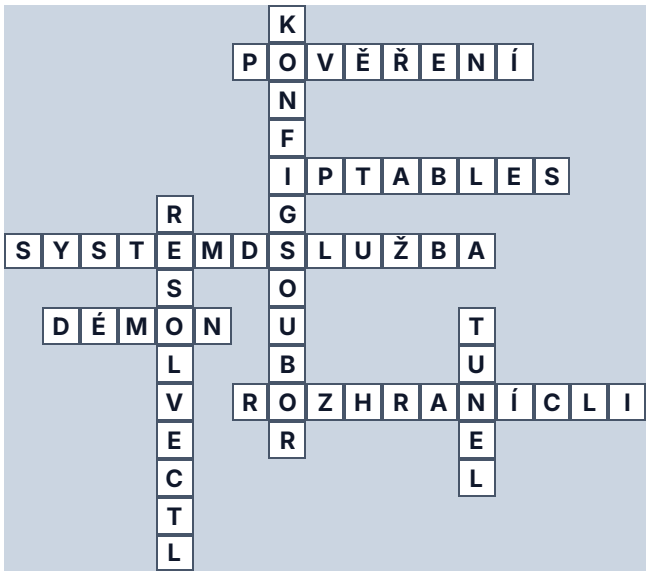
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

R	O	Z	H	R	A	N	Í	C	L	I	A	Ď	Ó	Ď
O	É	G	I	D	S	Ř	L	E	N	U	T	N	E	I
B	Š	N	O	M	É	D	Ž	T	É	Ř	Ů	E	A	Á
U	Ř	P	O	Q	U	Y	R	J	S	U	Š	Č	Ň	Ý
O	L	T	C	E	V	L	O	S	E	R	B	Ě	Š	X
S	W	Í	A	S	Ž	Ý	Ý	L	F	I	N	S	J	N
G	M	Ť	P	G	R	Ř	G	Ž	Á	Ó	Ů	Ě	Ú	C
I	Ý	Š	Ý	B	G	M	Ž	F	J	Ó	Q	S	O	X
F	C	N	Ž	Z	Ě	Ý	P	W	Ú	L	Ů	E	Q	B
N	Ó	V	Ť	N	F	Ů	Č	Ý	Ú	K	S	L	Á	X
O	S	Y	S	T	E	M	D	S	L	U	Ž	B	A	Ž
K	Y	N	Š	R	X	H	P	D	Á	Č	J	A	Ř	V
W	X	P	O	V	Ě	Ř	E	N	Í	L	Í	T	H	U
H	Ě	B	E	I	K	Ť	Š	V	Ř	Z	E	P	H	E
Š	C	A	M	R	C	Ž	N	K	V	Š	Ú	I	Á	Š

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: POVĚŘENÍ Chráněné soubory tokenů obsahující ověřovací údaje uživatele (8 písmen)

3 vodorovně: IPTABLES Rámec netfilter spravující pravidla zahazování a povolování paketů (8 písmen)

5 vodorovně: SYSTEMDSLUŽBA Jednotka systemd řídící běh klienta na pozadí (13 písmen)

6 vodorovně: DÉMON Program běžící nezávisle na pozadí a spravující služby (5 písmen)

8 vodorovně: ROZHRANÍCLI Prostředí příkazové řádky pro přímé spouštění klientských příkazů (11 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: KONFIGSOUBOR Soubor na disku obsahující koncové body připojení a klíče (12 písmen)

4 svisle: RESOLVECTL Nástroj příkazové řádky pro dotazy na DNS servery jednotlivých rozhraní (10 písmen)

7 svisle: TUNEL Virtuální point-to-point rozhraní přeposílající šifrované síťové pakety (5 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. RNLOAÍRCZIH — **ROZHRANÍCLI**
2. BEYMSSŽDALUST — **SYSTEMDSLUŽBA**
3. APIBLSET — **IPTABLES**
4. NLETU — **TUNEL**
5. OBOSRNIUGKOF — **KONFIGSOUBOR**
6. NÍĚEPŘOV — **POVĚŘENÍ**
7. EOREVCTLLS — **RESOLVECTL**
8. NDMOÉ — **DÉMON**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"CLI TUNELY CHRÁNÍ LINUX SERVERY BEZ MONITORU"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: OCHRANA HEADLESS SERVERU

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Linuxový administrátor potřebuje zabezpečit vzdálené zálohy souborů z headless terminálového uzlu umístěného ve sdíleném hostingovém datacentru.
- Doporučená strategie a řešení: Nakonfigurujte soubor nastavení klienta, spusťte službu přes systemctl a příkazem resolvectl status ověřte, že DNS je vázáno na rozhraní tun0.

B PŘÍPADOVÁ STUDIE 2: AUTOMATIZACE ODCHOZÍHO KILL SWITCHE

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Administrátor chce zajistit, aby headless terminálové připojení zahodilo veškerý veřejný provoz, pokud VPN tunel vypadne.
- Doporučená strategie a řešení: Nakonfigurujte pravidla iptables tak, aby zahazovala veškerý provoz na eth0 kromě paketů určených na port VPN serveru, a povolte veškerý provoz na rozhraní tun0.