Jméno: _____ Datum: _____ Body: _____

Zabezpečení Mullvad

Analýza bezpečnostní architektury Mullvad VPN včetně bezdiskových serverů pouze v RAM, auditovaných zásad nulových logů, místního generování klíčů, šifrování WireGuard a kvantově odolných konfigurací tunelů.

ZABEZPEČENÍ MULLVAD – 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 bezpečnostní architekturou Mullvadu. Prozkoumáte bezdiskové servery jen s RAM, auditované zásady nulových logů, lokální generování klíčů a kvantově odolné tunely.

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/mullvad/bezpecnost/

Váš studijní plán: zabezpečení Mullvad

- Analyzujte technickou architekturu a konfigurační pravidla zabezpečení Mullvad.
- Nakonfigurujte nastavení klienta tak, aby bránilo únikům IP, DNS a WebRTC provozu.
- Porovnejte vlastní ceny, zkušební verze a výkonnostní funkce se standardními modely.

PRŮVODCE ZABEZPEČENÍM MULLVAD – 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 serverové ovládací prvky Mullvadu zaměřené na soukromí. Zakončete bonusovou aktivitou Mysli rychle.

HODNOCENÍ INFRASTRUKTURY S ANONYMITOU NA PRVNÍM MÍSTĚ A ÚROVNÍ RAM (ÚVOD)

Mullvad nepoužívá standardní účty s hesly a spoléhá na náhodně generované 16místné kódy. Jeho infrastruktura je postavena na bezdiskových uzlech běžících pouze v RAM, klíčích WireGuard generovaných lokálně a auditovaných zásadách nulového uchovávání.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. 1. Jaký tunelovací protokol je výchozí v aplikaci Mullvad?
   - A) OpenVPN
   - B) WireGuard
   - C) IKEv2
   - D) PPTP

2. 2. Co Mullvad vyžaduje k vytvoření nového účtu?
   - A) Vůbec nic
   - B) E-mailovou adresu
   - C) Telefonní číslo
   - D) Doklad totožnosti

3. 3. Jaký kryptografický tunel chrání před kvantovými počítači?
   - A) AES-256-GCM
   - B) Quantum WireGuard
   - C) RSA-4096
   - D) SOCKS5 proxy

4. 4. Jaký bezpečnostní mechanismus blokuje rizika úniků WebRTC?
   - A) Rozšíření prohlížeče
   - B) Síťový Kill Switch
   - C) Směrování WebRTC přes rozhraní VPN
   - D) Split Tunneling

5. 5. Jaká multihop funkce směruje provoz přes více uzlů?
   - A) Dvojitý NAT
   - B) WireGuard Multihop
   - C) Protokol Chameleon
   - D) Bypasser

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Mullvad vyžaduje při generování účtu e-mailovou adresu.

○ Pravda ○ Nepravda

7 Otázka 7

7. SOCKS5 proxy lze nastavit uvnitř tunelů Mullvadu.

○ Pravda ○ Nepravda

8 Otázka 8

8. Mullvad vlastní a provozuje veškerý svůj serverový hardware.

○ Pravda ○ Nepravda

9 Otázka 9

9. Síťový Kill Switch je ve výchozím nastavení vždy aktivní.

○ Pravda ○ Nepravda

10 Otázka 10

10. Platby v hotovosti zaslané poštou jsou zcela nevratné.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Jako primární vysokorychlostní protokol zabezpečeného tunelu využívá Mullvad _____ .

2. Směrování dat přes dvě serverové lokality se nazývá konfigurace _____ .

3. Aby na discích nevznikaly žádné záznamy, nasazuje Mullvad _____ .

4. Systémový provoz při selhání tunelu blokuje vestavěná pojistka zvaná _____ .

5. Auditní zprávy potvrzují, že Mullvad udržuje přísnou a ověřenou architekturu typu _____ .

6. Interní směrování aplikací lze izolovat pomocí vlastního nastavení _____ .

7. Data uvnitř tunelu chrání postkvantové šifrovací algoritmy, jejichž předností je _____ odolnost.

8. Soukromé jmenné servery jsou nasazeny globálně, aby pomáhaly blokovat rizika známá jako _____ .

ZÁSOBNÍK SLOV

BEZ LOGŮ | KILL SWITCH | KVANTOVÁ | MULTI-HOP | RAM-ONLY | SOCKS5 | ÚNIKY DNS | WIREGUARD

Sem napište své odpovědi:

1.
2.
3.
4.
5.
6.
7.
8.

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

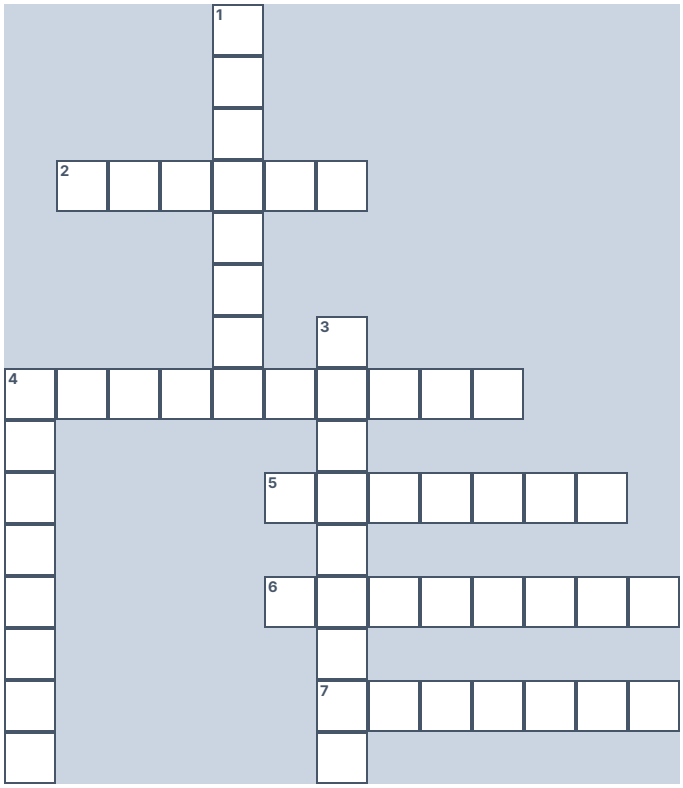
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. WIREGUARD	A	Bezpečnostní funkce, která přeruší provoz, když VPN vypadne.
☐	2. MULTI-HOP	B	Odlehčený, vysoce výkonný protokol zabezpečeného tunelování.
☐	3. RAM-ONLY	C	Interní proxy protokol používaný k izolaci klientských aplikací.
☐	4. KILL SWITCH	D	Směrování provozu přes vstupní a výstupní serverový uzel.
☐	5. BEZ LOGŮ	E	Šifrovací mechanismy navržené tak, aby odolaly kvantovým útokům.
☐	6. SOCKS5	F	Únik cílů dotazů DNS mimo tunel VPN.
☐	7. KVANTOVÁ	G	Serverový hardware s volatilní pamětí, který po restartu neuchovává žádná data.
☐	8. ÚNIKY DNS	H	Standard nulového uchovávání dat ověřený nezávislými audity.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

2. Interní proxy protokol používaný k izolaci klientských aplikací (6)

4. Bezpečnostní funkce přerušující provoz při výpadku VPN (10)

5. Standard nulového uchovávání dat ověřený nezávislými audity (7)

6. Směrování provozu přes vstupní a výstupní serverový uzel (8)

7. Serverový hardware s volatilní pamětí, který po restartu neuchová žádná data (7)

SVISLÉ NÁPOVĚDY

1. Odhalení cílů DNS dotazů mimo VPN tunel (8)

3. Lehký a vysoce výkonný zabezpečený tunelovací protokol (9)

4. Šifrovací mechanismy navržené tak, aby odolaly kvantovým útokům (8)

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: Interní proxy protokol používaný k izolaci klientských aplikací (6 písmen):

4 vodorovně: Bezpečnostní funkce přerušující provoz při výpadku VPN (10 písmen):

5 vodorovně: Standard nulového uchovávání dat ověřený nezávislými audity (7 písmen):

6 vodorovně: Směrování provozu přes vstupní a výstupní serverový uzel (8 písmen):

7 vodorovně: Serverový hardware s volatilní pamětí, který po restartu neuchová žádná data (7 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Odhalení cílů DNS dotazů mimo VPN tunel (8 písmen):

3 svisle: Lehký a vysoce výkonný zabezpečený tunelovací protokol (9 písmen):

4 svisle: Šifrovací mechanismy navržené tak, aby odolaly kvantovým útokům (8 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

U T Ť E L Í B Ú A B C P Y L J
Y L Y U K Ď Ř N N J R D I O Ň
K R Q F Ň Ň Ř I S T A U Ť F C
D 5 T R Ó H Š K B V M D T Z Ů
R S C Ž V K Ě Y K G O Ž D M Ň
A K Ď Ř X I Q D C Ú N B A U Ž
U C O D L L A N K Ď L Ó Ď L É
G O G I D L S S V B Y Ř N T E
E S I Š Ž S T É A E Ř Ů E I A
R Á Ř P O W Q U N Z Y R J H S
I U Š Č Ň I Ý B T L Ě Š X O W
W Í A S Ž T Ý Ý O O L F I P N
S J N M Ť C P G V G R Ř G Ž Á
Ó Ů Ě Ú C H Ý Š Á Ů Ý B G M Ž
F J Ó Q O X C N Ž Z Ě Ý P W Ú

SEZNAM SLOV

WIREGUARD MULTIHOP RAMONLY KILLSWITCH BEZLOGŮ SOCKS5
KVANTOVÁ ÚNIKYDNS

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. WIREGUARD**
- **B. MULTIHOP**
- **C. RAMONLY**
- **D. KILLSWITCH**
- **E. BEZLOGŮ**
- **F. SOCKS5**
- **G. KVANTOVÁ**
- **H. ÚNIKYDNS**

DEFINICE A POLE K PŘIŘAZENÍ

1. Interní proxy protokol používaný k izolaci klientských aplikací.
2. Šifrovací mechanismy navržené tak, aby odolaly kvantovým útokům.
3. Lehký a vysoce výkonný zabezpečený tunelovací protokol.
4. Serverový hardware s volatilní pamětí, který po restartu neuchová žádná data.
5. Bezpečnostní funkce přerušující provoz při výpadku VPN.
6. Směrování provozu přes vstupní a výstupní serverový uzel.
7. Odhalení cílů DNS dotazů mimo VPN tunel.
8. Standard nulového uchovávání dat ověřený nezávislými audity.

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. **UGEIWARDR**
2. **RMYLNOA**
3. **LBOŮZGE**
4. **NVÁOTKVA**
5. **IHUPTMOL**
6. **CSLITKIWHL**
7. **SSK5CO**
8. **KNYSÚNDI**

Bonusová aktivita: Mysli rychle

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

1	Bezpečnostní funkce v Mullvad			
2	Otázky pro zákaznickou podporu Mullvad			
3	Způsoby, jak vytvořit silné heslo			
4	Lidé, kterým byste doporučili Mullvad			
5	Věci, které může audit prověřit			
6	Země známé přísnými zákony na ochranu soukromí			
7	Věci, které děláte online každý den			
8	Země, kde byste chtěli servery Mullvad			
9	Nastavení, která zapnete pro extra bezpečnost			
10	Věci, které šifrování chrání			
11	Typy úniků u VPN			
12	Bezpečnostní pojmy, které jste se naučili v tomto pracovním listu			
13	Hrozby na veřejné Wi-Fi			
14	Aplikace, které byste používali spolu s Mullvad			
15	Zařízení, na která byste nainstalovali Mullvad			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: INTEGRACE KVANTOVÉ ODOLNOSTI



Scénář: Finanční společnost potřebuje zabezpečit přenosy souborů proti budoucímu kvantovému dešifrování.

Otázka k diskusi: Jakou konfiguraci tunelu mají nasadit v aplikaci Mullvad?

PŘÍPADOVÁ STUDIE 2: DISKRÉTNÍ INVESTIGATIVNÍ SMĚROVÁNÍ



Scénář: Vyšetřovatel chce svou síť směrovat dvojitě, aby zamaskoval svůj vstupní bod.

Otázka k diskusi: Kterou funkci Mullvadu je třeba zapnout k dosažení směrování přes více serverů?

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

33	5	30	38		19	32	18	18	35	1	6		20	8	19	1	16	15

13	8	28	18	22		1	20	14		8	19	1	14	18

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: Jak Mullvad zabezpečuje účty?

Mullvad používá vygenerované 16místné číslo účtu bez nutnosti hesla či e-mailu. [1]

Q2: Který protokol Mullvad upřednostňuje?

Mullvad upřednostňuje WireGuard kvůli jeho rychlosti, jednoduchosti a moderní kryptografii. [9]

Q3: Jsou servery Mullvad auditovány?

Ano, nezávislé bezpečnostní firmy provádějí pravidelné audity infrastruktury a kódu.

Q4: Podporuje Mullvad OpenVPN?

Ne, Mullvad odstranil OpenVPN 15. ledna 2026; podporuje pouze WireGuard. [7]

Q5: Co je kill switch Mullvadu?

Je to integrované pravidlo firewallu, které zabrání internetovému provozu, pokud VPN selže.

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

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

Q6: Podporuje Mullvad IPv6?

Ano, Mullvad podporuje nativní IPv6 směrování a ochranu proti únikům.

Q7: Nabízí Mullvad multihop?

Ano, WireGuard multihop umožňuje řetězení více serverových lokalit.

Q8: Mohu použít vlastní DNS resolvery?

Ano, vlastní DNS adresy lze nastavit v nastavení klienta Mullvad.

Q9: Jak se předchází logům?

Systémové konfigurace vypínají protokolování a čistí mezipaměti na všech serverových démonech.

Q10: Kde je Mullvad registrován?

Mullvad je registrován ve švédském Göteborgu, pod švédskou jurisdikcí.

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 funguje rotace klíčů?

Aplikace střídá klíče WireGuard automaticky; výchozí interval v CLI je 30 dní. [3]

Q2: Co jsou kvantově odolné tunely?

K WireGuardu přidávají výměnu klíčů ML-KEM a Classic McEliece pro odolnost vůči budoucím kvantovým útokům. [2]

Q3: V čem jsou RAM-only uzly bezpečné?

Tyto uzly nezapisují žádná data na pevné disky, takže krádež fyzických serverů je k ničemu.

Q4: Jaká je funkce SOCKS5 proxy?

Pomáhá směrovat provoz konkrétních aplikací uvnitř tunelu a brání únikům do externích sítí.

Q5: Chrání Mullvad před úniky WebRTC?

Ano, aplikace vynucuje průchod dotazů WebRTC přes rozhraní VPN, aby chránila místní IP adresy.

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 Mullvad řeší policejní razie?

Mullvad nedrží žádné logy uživatelské databáze, takže žádné informace o uživatelích nelze získat.

Q7: Jaké je riziko švédské jurisdikce?

Švédsko je členem 14-Eyes, ale architektura nulových logů Mullvadu odstraňuje riziko dat.

Q8: Jsou audity klientských aplikací open source?

Ano, aplikace jsou open source (GPL-3) a auditované firmami jako X41 D-Sec. [6]

Q9: Jak funguje split tunneling?

Používá směrovací tabulky operačního systému k vyloučení konkrétních aplikací z režie VPN.

Q10: Jak Mullvad zpracovává platby v hotovosti?

Hotovost se posílá poštou s kódem tokenu, ručně se připisuje a obálky se skartují.

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

Mullvad založila v roce 2009 společnost Amagicom AB v Göteborgu ve Švédsku.

2. VPN POSTŘEH

Čísla účtů jsou jediným identifikátorem používaným k dobíjení a přístupu k účtům.

3. VPN POSTŘEH

V uživatelské DB nejsou uložena žádná jména, e-maily, hesla ani telefonní čísla.

4. VPN POSTŘEH

Klíče WireGuard se generují lokálně na klientských zařízeních, aby se předešlo kompromitaci na serveru.

5. VPN POSTŘEH

Audit infrastruktury Cure53 z roku 2024 nenašel žádnou chybu narušující anonymitu VPN provozu. [5]

6. VPN POSTŘEH

Každý WireGuard server Mullvadu provozuje SOCKS5 proxy, dostupnou pouze v tunelu. [8]

7. POSTŘEH K VPN

Provoz WireGuard lze obfuskovat pomocí Shadowsocks, QUIC nebo LWO pro průchod firewally. [10]

8. POSTŘEH K VPN

Mullvad dokončil migraci na servery VPN běžící pouze v RAM v září 2023. [4]

9. POSTŘEH K VPN

ML-KEM a Classic McEliece vyjednávají postkvantový předsdílený klíč pro WireGuard. [2]

10. VPN POSTŘEH

Obálky s hotovostí a jejich nepeněžní obsah se po připsání času skartují.

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Mullvad VPN. (n.d.). Why Mullvad VPN?
https://mullvad.net/en/why-mullvad-vpn

[2] Mullvad VPN. (n.d.). Quantum-resistant tunnels with WireGuard.
https://mullvad.net/en/help/quantum-resistant-tunnels-with-wireguard

[3] Mullvad VPN. (n.d.). CLI commands for using WireGuard.
https://mullvad.net/en/help/cli-command-wg

[4] Mullvad VPN. (2023). We have successfully completed our migration to RAM-only VPN infrastructure.
https://mullvad.net/en/blog/we-have-successfully-completed-our-migration-to-ram-only-vpn-infrastructure

[5] Mullvad VPN. (2024). Fourth Infrastructure audit completed by Cure53.
https://mullvad.net/en/blog/fourth-infrastructure-audit-completed-by-cure53

[6] Mullvad VPN. (2024). The report for the 2024 security audit of the app is now available.
https://mullvad.net/en/blog/the-report-for-the-2024-security-audit-of-the-app-is-now-available

[7] Mullvad VPN. (2024). Removing OpenVPN 15th January 2026.
https://mullvad.net/en/blog/removing-openvpn-15th-january-2026

[8] Mullvad VPN. (n.d.). SOCKS5 proxy.
https://mullvad.net/en/help/socks5-proxy

[9] Mullvad VPN. (n.d.). Why WireGuard?
https://mullvad.net/en/help/why-wireguard

[10] Mullvad VPN. (n.d.). Using Mullvad VPN in restrictive locations.
https://mullvad.net/en/help/connecting-to-mullvad-vpn-from-restrictive-locations

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

[12] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Jaký tunelovací protokol je výchozí v aplikaci Mullvad? → WireGuard

2 Otázka 2 — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Kliknutím na "generate account" dostanete číslo účtu; nepožaduje se e-mail ani jiné osobní údaje.

3 Otázka 3 — Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Kvantově odolné tunely WireGuard u Mullvadu používají ML-KEM a Classic McEliece k dohodnutí předsdíleného klíče.

4 Otázka 4 — Správná odpověď: C

POZNÁMKA PRO VYUČUJÍCÍ

Jaký bezpečnostní mechanismus blokuje rizika úniků WebRTC? → Směrování WebRTC přes rozhraní VPN

5 Otázka 5 — Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Jaká multihop funkce směruje provoz přes více uzlů? → WireGuard Multihop

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Mullvad nikdy nežádá e-mail; účty jsou identifikovány pouze vygenerovaným číslem.

7 **Otázka 7** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

SOCKS5 proxy lze nastavit uvnitř tunelů Mullvadu.

8 **Otázka 8** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Mullvad některé servery vlastní, ale také si pronajímá dedikované servery od poskytovatelů.

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

POZNÁMKA PRO VYUČUJÍCÍ

Síťový Kill Switch je ve výchozím nastavení vždy aktivní.

10 **Otázka 10** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Platby v hotovosti zaslané poštou jsou zcela nevratné.

Klíče slovní zásoby a hodnoticí rubrika

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

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

B 1. WIREGUARD	D 2. MULTI-HOP	G 3. RAM-ONLY	A 4. KILL SWITCH
H 5. BEZ LOGŮ	C 6. SOCKS5	E 7. KVANTOVÁ	F 8. ÚNIKY DNS

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 WIREGUARD	2 MULTI-HOP	3 RAM-ONLY	4 KILL SWITCH
5 BEZ LOGŮ	6 SOCKS5	7 KVANTOVÁ	8 ÚNIKY DNS

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 F – SOCKS5	2 G – KVANTOVÁ	3 A – WIREGUARD	4 C – RAMONLY
5 D – KILLSWITCH	6 B – MULTIHOP	7 H – ÚNIKYDNS	8 E – BEZLOGŮ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy WIREGUARD, MULTI-HOP a RAM-ONLY a ke každému uvést příklad.

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

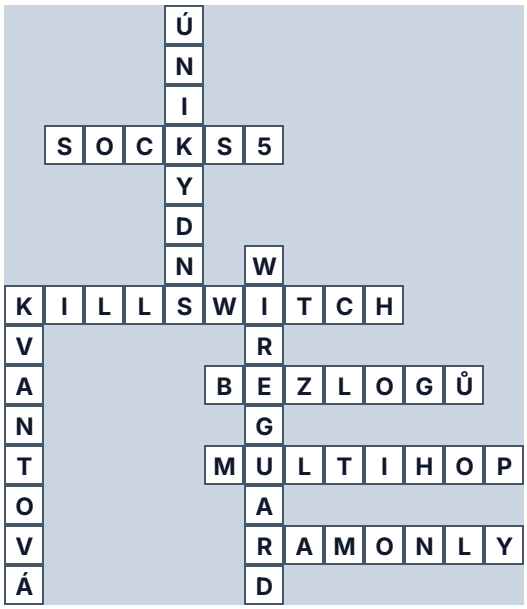
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

U	T	Ť	E	L	Í	B	Ú	A	B	C	P	Y	L	J
Y	L	Y	U	K	Ď	Ř	N	N	J	R	D	I	O	Ň
K	R	Q	F	Ň	Ň	Ř	I	S	T	A	U	Ť	F	C
D	5	T	R	Ó	H	Š	K	B	V	M	D	T	Z	Ů
R	S	C	Ž	V	K	Ě	Y	K	G	O	Ž	D	M	Ň
A	K	Ď	Ř	X	I	Q	D	C	Ú	N	B	A	U	Ž
U	C	O	D	L	L	A	N	K	Ď	L	Ó	Ď	L	É
G	O	G	I	D	L	S	S	V	B	Y	Ř	N	T	E
E	S	I	Š	Ž	S	T	É	A	E	Ř	Ů	E	I	A
R	Á	Ř	P	O	W	Q	U	N	Z	Y	R	J	H	S
I	U	Š	Č	Ň	I	Ý	B	T	L	Ě	Š	X	O	W
W	Í	A	S	Ž	T	Ý	Ý	O	O	L	F	I	P	N
S	J	N	M	Ť	C	P	G	V	G	R	Ř	G	Ž	Á
Ó	Ů	Ě	Ú	C	H	Ý	Š	Á	Ů	Ý	B	G	M	Ž
F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P	W	Ú

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: SOCKS5 Interní proxy protokol používaný k izolaci klientských aplikací (6 písmen)

4 vodorovně: KILLSWITCH Bezpečnostní funkce přerušující provoz při výpadku VPN (10 písmen)

5 vodorovně: BEZLOGŮ Standard nulového uchovávání dat ověřený nezávislými audity (7 písmen)

6 vodorovně: MULTIHOP Směrování provozu přes vstupní a výstupní serverový uzel (8 písmen)

7 vodorovně: RAMONLY Serverový hardware s volatilní pamětí, který po restartu neuchová žádná data (7 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ÚNIKYDNS Odhalení cílů DNS dotazů mimo VPN tunel (8 písmen)

3 svisle: WIREGUARD Lehký a vysoce výkonný zabezpečený tunelovací protokol (9 písmen)

4 svisle: KVANTOVÁ Šifrovací mechanismy navržené tak, aby odolaly kvantovým útokům (8 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	UGEIWARDR	WIREGUARD	5.	IHUPTMOL	MULTIHOP
2.	RMYLNOA	RAMONLY	6.	CSLITKIWHL	KILLSWITCH
3.	LBOŮZGE	BEZLOGŮ	7.	SSK5CO	SOCKS5
4.	NVÁOTKVA	KVANTOVÁ	8.	KNYSÚNDI	ÚNIKYDNS

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ÚČTY MULLVAD NEMAJÍ HESLO ANI EMAIL"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: INTEGRACE KVANTOVÉ ODOLNOSTI

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Finanční společnost potřebuje zabezpečit přenosy souborů proti budoucímu kvantovému dešifrování.
- Doporučená strategie a řešení: Nasaďte kvantově odolné WireGuard tunely s postkvantovými předsdílenými klíči.

B PŘÍPADOVÁ STUDIE 2: DISKRÉTNÍ INVESTIGATIVNÍ SMĚROVÁNÍ

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vyšetřovatel chce svou síť směrovat dvojitě, aby zamaskoval svůj vstupní bod.
- Doporučená strategie a řešení: Zapněte v Mullvadu funkci WireGuard Multihop pro kaskádování vstupních a výstupních uzlů.