Jméno: _____ Datum: _____ Body: _____

Recenze IPVanish

Technická analýza IPVanish VPN se sídlem v USA, převážně vlastní serverová

PŘEHLED VÝUKY K RECENZI IPVANISH

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 technickým přehledem IPVanish. Prozkoumáte vlastní fyzickou infrastrukturu, proxy SOCKS5 pro P2P torrentování, výkon WireGuard a americké jurisdikční předpisy o datech.

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/ipvanish/

Váš studijní plán: IPVanish

- Analyzujte technickou architekturu a šifrovací standardy recenze IPVanish.
- Nakonfigurujte nastavení klienta tak, aby bránilo únikům IP, DNS a WebRTC provozu.
- Porovnejte proprietární tunelovací protokoly se standardními implementacemi.

POKYNY K RECENZI IPVANISH

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 proxy SOCKS5 a vlastní serverovou infrastrukturu. Zakončete bonusovou aktivitou Mysli rychle.

VLASTNÍ INFRASTRUKTURA A SOCKS5 P2P PROXY (ÚVOD)

IPVanish vyniká tím, že vlastní a spravuje velkou část své fyzické serverové sítě, což zlepšuje výkon i zabezpečení. Nabízí vysokorychlostní protokol WireGuard a SOCKS5 proxy pro P2P torrenting, ale působí pod jurisdikcí USA v rámci Five Eyes.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Jaký open-source protokol je výchozí pro vysokou rychlost v klientských aplikacích IPVanish?**

- A) WireGuard
- B) L2TP/IPSec
- C) PPTP
- D) Catapult Hydra

2 **2. Jaký typ serverové proxy poskytuje IPVanish pro pomoc s nastavením P2P torrentování?**

- A) Proxy SOCKS5
- B) HTTP proxy
- C) Relay Toru
- D) Shadowsocks

3 **3. Která firma provedla první nezávislý audit no-logs IPVanish v roce 2022?**

- A) Leviathan Security Group
- B) PwC
- C) Deloitte
- D) Cure53

4 **4. Pod jakou primární národní jurisdikcí působí korporátní subjekty IPVanish?**

- A) Spojené státy
- B) Švýcarsko
- C) Panama
- D) Britské Panenské ostrovy

5 **5. Kolik simultánních připojení zařízení je povoleno v rámci prémiového plánu IPVanish?**

- A) Neomezeně
- B) Pět
- C) Deset
- D) Sedm

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. IPVanish spravuje a vlastní velkou část své fyzické serverové infrastruktury.

○ Pravda ○ Nepravda

7 Otázka 7

7. Provoz SOCKS5 proxy je při přenosu plně šifrován stejně jako běžné VPN tunely.

○ Pravda ○ Nepravda

8 Otázka 8

8. Desktopový klient IPVanish postrádá funkci Kill Switch na úrovni systému.

○ Pravda ○ Nepravda

9 Otázka 9

9. IPVanish působí ze Spojených států, člena zpravodajské aliance Five Eyes.

○ Pravda ○ Nepravda

10 Otázka 10

10. Split tunneling v IPVanish umožňuje směrovat provoz aplikací mimo tunel VPN.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Moderní protokol _____ je ve výchozím nastavení nakonfigurován pro optimální směrovací výkon.

2. P2P provoz lze směrovat přes rychlou _____ maskující skutečnou polohu klienta.

3. Připojením ke geograficky blízkému uzlu se maximalizuje skutečná _____ .

4. Aby se zabránilo únikům dat, měli by uživatelé zapnout vestavěnou funkci zvanou _____ .

5. O závazku poskytovatele k soukromí svědčí _____ , které zveřejňuje po nezávislých prověrkách.

6. Na rozdíl od některých konkurentů IPVanish neuplatňuje na účtech žádný _____ .

ZÁSOBNÍK SLOV

AUDITOVANÉ LOGY | IP ADRESA | KILL SWITCH | LIMIT ZAŘÍZENÍ | RYCHLOST SERVERU | SOCKS5 PROXY | WIREGUARD | ZABEZPEČENÍ

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

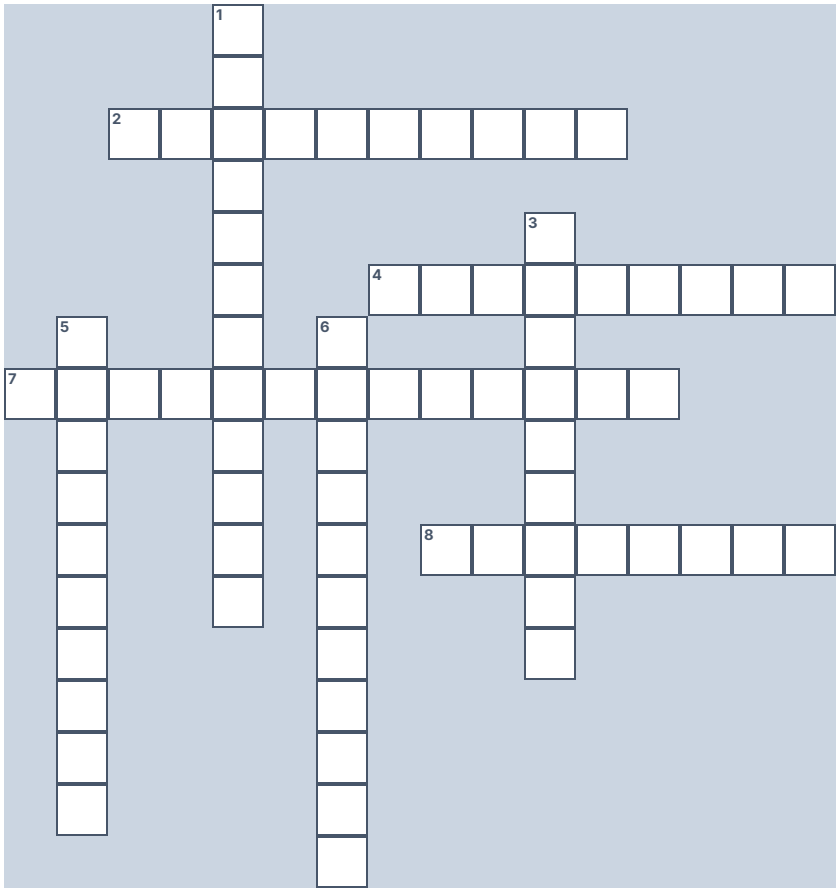
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. WireGuard	A	Pojistný mechanismus, který blokuje internetový provoz, pokud VPN selže.
☐	2. SOCKS5 proxy	B	Open source protokol známý rychlostí a moderní kryptografií.
☐	3. Rychlost serveru	C	Omezení počtu aktivních relací zařízení.
☐	4. Kill Switch	D	Propustnost serverového uzlu při aktivním provozním zatížení.
☐	5. Auditované logy	E	Jedinečný síťový identifikátor přidělovaný zařízením na internetu.
☐	6. Limit zařízení	F	Celkový stav ochrany systému šifrovaného tunelu.
☐	7. IP adresa	G	Ověřené záznamy potvrzující, že se nesleduje žádná aktivita uživatelů.
☐	8. Zabezpečení	H	Nešifrovaný systém směrování přes proxy používaný k maskování polohy klientů P2P.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

2. Nešifrovaný proxy systém (SOCKS5) používaný k maskování polohy P2P klientů (10)

4. Ověřené záznamy potvrzující, že se nesleduje žádná aktivita uživatelů (9)

7. Omezení počtu aktivních relací zařízení (13)

8. Jedinečný síťový identifikátor přidělovaný zařízením na internetu (8)

SVISLÉ NÁPOVĚDY

1. Propustnost serverového uzlu pod aktivní zátěží provozu (12)

3. Open-source protokol známý rychlostí a moderní kryptografií (9)

5. Pojistný mechanismus blokující internetový provoz při selhání VPN (10)

6. Celková úroveň ochrany šifrovaného tunelového systému (11)

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: Nešifrovaný proxy systém (SOCKS5) používaný k maskování polohy P2P klientů (10 písmen):

4 vodorovně: Ověřené záznamy potvrzující, že se nesleduje žádná aktivita uživatelů (9 písmen):

7 vodorovně: Omezení počtu aktivních relací zařízení (13 písmen):

8 vodorovně: Jedinečný síťový identifikátor přidělovaný zařízením na internetu (8 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Propustnost serverového uzlu pod aktivní zátěží provozu (12 písmen):

3 svisle: Open-source protokol známý rychlostí a moderní kryptografií (9 písmen):

5 svisle: Pojistný mechanismus blokující internetový provoz při selhání VPN (10 písmen):

6 svisle: Celková úroveň ochrany šifrovaného tunelového systému (11 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

WIREGUARD, SOCKSPROXY, RYCHLOSTUZLŮ, KILLSWITCH, AUDITLOGŮ, LIMITZAŘÍZENÍ, IPADRESA, ZABEZPEČENÍ

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. SOCKSPROXY**
- **C. RYCHLOSTUZLŮ**
- **D. KILLSWITCH**
- **E. AUDITLOGŮ**
- **F. LIMITZAŘÍZENÍ**
- **G. IPADRESA**
- **H. ZABEZPEČENÍ**

DEFINICE A POLE K PŘIŘAZENÍ

1. Nešifrovaný proxy systém (SOCKS5) používaný k maskování polohy P2P klientů.
2. Celková úroveň ochrany šifrovaného tunelového systému.
3. Omezení počtu aktivních relací zařízení.
4. Propustnost serverového uzlu pod aktivní zátěží provozu.
5. Open-source protokol známý rychlostí a moderní kryptografií.
6. Jedinečný síťový identifikátor přidělovaný zařízením na internetu.
7. Pojistný mechanismus blokující internetový provoz při selhání VPN.
8. Ověřené záznamy potvrzující, že se nesleduje žádná aktivita uživatelů.

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. ŮYLORZLCTUSH
3. ALTUOŮIGD
4. DSAERIPA
5. OPYOKRSSXC
6. CSLITKIWHL
7. ZEŘZLIÍTÍNMAI
8. EEÍPBZZANČE

Bonusová aktivita: Mysli rychle

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

1	Slova, která popisují dobrou VPN aplikaci			
2	Věci, které IPVanish dokáže skrýt před vaší sítí			
3	Místa, kde byste zapnuli IPVanish			
4	VPN protokoly, které znáte			
5	Otázky pro zákaznickou podporu IPVanish			
6	Země, kde byste chtěli servery IPVanish			
7	VPN služby jiné než IPVanish			
8	Situace, kdy pomůže kill switch			
9	Důvody, proč si vybrat IPVanish			
10	Známky toho, že je vaše VPN připojení pomalé			
11	Věci, které děláte online každý den			
12	Lidé, kterým byste doporučili IPVanish			
13	Co si ověřit před koupí VPN			
14	Bezpečnostní pojmy, které jste se naučili v tomto pracovním listu			
15	Vlastnosti, které hledáte u IPVanish			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: KONFIGURACE MEDIÁLNÍHO CENTRA



Scénář: Klient chce pomocí IPVanish zabezpečit svůj mediální přehrávač Android Fire TV, aby mohl bezpečně streamovat při zachování rychlé propustnosti.

Otázka k diskusi: Proč je protokol WireGuard upřednostňován před OpenVPN pro streamovací hardware s omezenými prostředky?

PŘÍPADOVÁ STUDIE 2: PROXY PRO TORRENTOVÉ SÍTĚ



Scénář: P2P uploader chce pomocí konfigurace SOCKS5 skrýt svou polohu bez režie plného šifrování dat.

Otázka k diskusi: Porovnejte kompromisy bezpečnosti a rychlosti při použití SOCKS5 proxy oproti plnému tunelu VPN IPVanish.

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

14	24	35	1	20	14	28	13		24	26	22	28	1	40	32	16	8

24	27	15	28	20	39		26	8	41	14	19		3	8	40		18	22	12	34

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: Jaký protokol je výchozí v IPVanish?

Ve výchozím nastavení směruje přes vysokorychlostní WireGuard.

Q2: Vlastní IPVanish svůj serverový hardware?

Ano, vlastní a spravuje velkou část své fyzické serverové sítě.

Q3: Kde sídlí IPVanish?

Sídlí ve Spojených státech a podléhá zákonům USA.

Q4: Kolik zařízení se může připojit současně?

IPVanish nabízí neomezený počet souběžných připojení zařízení na účet.

Q5: Uchovává nějaké logy o připojení?

Ne, uplatňuje přísné zásady nulových logů potvrzené nezávislými audity. [6]

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

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

Q6: Nabízí IPVanish proxy službu?

Ano, poskytuje bezplatný proxy server SOCKS5 pro torrentování.

Q7: Obsahuje kill switch?

Ano, kill switch je dostupný na Windows, macOS, Androidu a iOS.

Q8: Mohu s IPVanish obejít geografické blokace?

Ano, její globální síť serverů umožňuje přístup k omezeným knihovnám.

Q9: Podporuje split tunneling?

Ano, split tunneling je k dispozici, mimo jiné na Windows a Androidu.

Q10: Jaké šifrovací šifry používá?

Zabezpečuje připojení pomocí šifrování AES-256 a ChaCha20.

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 se konfiguruje SOCKS5 proxy?

Je podporována platícími uživateli prémiové úrovně, což jí umožňuje nabízet omezený, bezpečný bezplatný plán bez monetizace dat.

Q2: Jak vlastnictví serverového hardwaru zlepšuje bezpečnost?

Snižuje rizika pronájmu serverů od třetích stran a dává poskytovateli přímou kontrolu nad konfiguracemi serverů.

Q3: Jaké dopady na soukromí má jurisdikce USA?

Ačkoli zákony USA nevyžadují uchovávání dat, umožňují national security letters a soudní příkazy.

Q4: Jak kill switch zabraňuje únikům IP?

Blokuje všechny internetové adaptéry, pokud VPN připojení nečekaně spadne.

Q5: Jaké šifrování se používá s WireGuardem?

WireGuard využívá symetrické šifrování ChaCha20 a autentizaci Poly1305. [7]

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 je ověřována politika nulových logů?

V roce 2022 ji auditovala Leviathan Security Group a v roce 2025 Schellman; ani jedna nenašla uživatelské logy. [3]

Q7: Jak nakládá s DNS dotazy IPv6?

Automaticky směruje všechny DNS a IPv6 dotazy přes své privátní nameservery.

Q8: Nabízí IPVanish funkce obfuskace?

Ano, její funkce Scramble obfuskuje provoz OpenVPN, aby obešla firewally.

Q9: Jak split tunneling funguje na mobilních zařízeních?

Umožňuje vybraným aplikacím obejít VPN tunel a připojit se přímo.

Q10: Podporuje konfigurace na routeru?

Ano, konfigurace OpenVPN a WireGuard lze na routery DD-WRT nahrát manuálně. [1]

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

IPVanish vlastní většinu své serverové infrastruktury, místo aby si ji pronajímal od třetích stran. [3]

2. VPN POSTŘEH

IPVanish funguje od roku 2012 a vlastní jej Ziff Davis, dříve známý jako J2 Global. [2]

3. VPN POSTŘEH

Proxy SOCKS5 skrývá veřejnou IP adresu klienta, ale nešifruje datové pakety.

4. VPN POSTŘEH

WireGuard je výchozím protokolem, v aplikacích jsou k dispozici také OpenVPN a IKEv2/IPSec. [2]

5. VPN POSTŘEH

Standardní OpenVPN Scramble přidává do hlaviček paketů obfuskační vrstvu XOR k obcházení firewallů.

6. VPN POSTŘEH

Politika neomezených současných připojení umožňuje uživatelům zabezpečit všechna zařízení v domácnosti najednou. [2]

7. POSTŘEH K VPN

Audity provedené Leviathan Security Group (2022) a Schellman (2025) ověřily jeho tvrzení o neukládání logů. [3]

8. POSTŘEH K VPN

Aplikace pro Android podporuje nastavení always-on VPN, která brání přístupu k internetu při odpojení tunelu.

9. POSTŘEH K VPN

Připojení OpenVPN mohou používat buď UDP pro rychlost, nebo TCP pro stabilní směrování přes firewally.

10. VPN POSTŘEH

Nabízí nepřetržitou podporu 24/7 přes live chat, plus telefonickou podporu ve stanovených pracovních hodinách všedních dnů. [5]

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). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Výchozí WireGuard** WIREGUARD — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard je nakonfigurován ve výchozím nastavení pro optimalizované rychlosti směrování.

2 **SOCKS5 proxy** SOCKS5 PROXY — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

SOCKS5 proxy maskují polohu klientů bez šifrovací režie.

3 **Otázka 3** — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Leviathan Security Group provedla první audit no-logs IPVanish v roce 2022; v roce 2025 následoval Schellman.

4 **Jurisdikce USA** SPOJENÉ STÁTY — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

IPVanish sídlí ve Spojených státech, pod pravidly aliance Five Eyes.

5 **Neomezená zařízení** NEOMEZENĚ — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

IPVanish umožňuje neomezený počet simultánních připojení zařízení.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Serverový hardware** VLASTNÍ SÍŤ — Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

IPVanish vlastní a spravuje velkou část své fyzické serverové sítě.

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: SOCKS5 proxy maskuje vaši IP adresu, ale data nešifruje.

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: IPVanish zahrnuje kill switch ve svých desktopových i mobilních aplikacích.

9 **Jurisdikce USA** FIVE EYES USA — Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

IPVanish sídlí v USA a podléhá pravidlům sledování aliance Five Eyes.

10 **Split Tunnel** ROZDĚLENÁ TRASA — Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Split tunneling směruje provoz konkrétních aplikací mimo zabezpečený tunel.

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

B 1. WireGuard	H 2. SOCKS5 proxy	D 3. Rychlost serveru	A 4. Kill Switch
G 5. Auditované logy	C 6. Limit zařízení	E 7. IP adresa	F 8. Zabezpečení

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 WIREGUARD	2 SOCKS5 PROXY	3 RYCHLOST SERVERU	4 KILL SWITCH
5 AUDITOVANÉ LOGY	6 LIMIT ZAŘÍZENÍ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 B – SOCKSPROXY	2 H – ZABEZPEČENÍ	3 F – LIMITZAŘÍZENÍ	4 C – RYCHLOSTUZLŮ
5 A – WIREGUARD	6 G – IPADRESA	7 D – KILLSWITCH	8 E – AUDITLOGŮ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy WireGuard, SOCKS5 proxy a Rychlost serveru a ke každému uvést příklad.

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

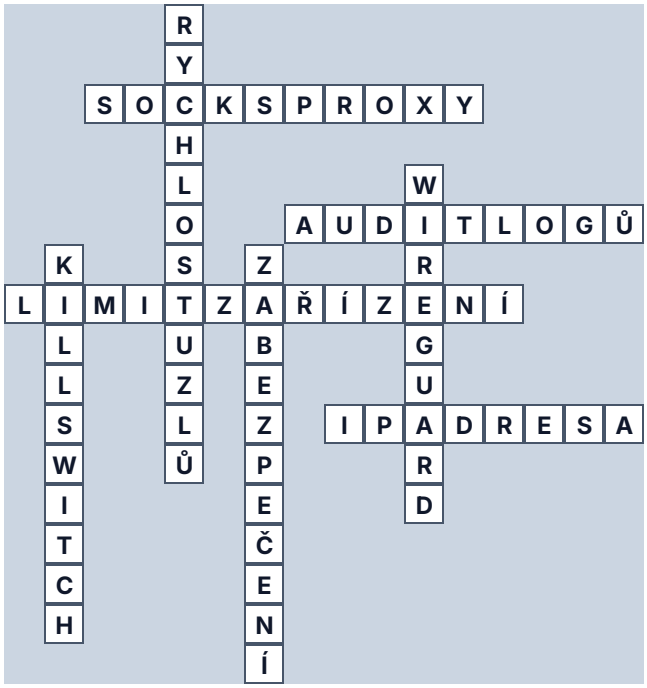
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: SOCKSPROXY Nešifrovaný proxy systém (SOCKS5) používaný k maskování polohy P2P klientů (10 písmen)

4 vodorovně: AUDITLOGŮ Ověřené záznamy potvrzující, že se nesleduje žádná aktivita uživatelů (9 písmen)

7 vodorovně: LIMITZAŘÍZENÍ Omezení počtu aktivních relací zařízení (13 písmen)

8 vodorovně: IPADRESA Jedinečný síťový identifikátor přidělovaný zařízením na internetu (8 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: RYCHLOSTUZLŮ Propustnost serverového uzlu pod aktivní zátěží provozu (12 písmen)

3 svisle: WIREGUARD Open-source protokol známý rychlostí a moderní kryptografií (9 písmen)

5 svisle: KILLSWITCH Pojistný mechanismus blokující internetový provoz při selhání VPN (10 písmen)

6 svisle: ZABEZPEČENÍ Celková úroveň ochrany šifrovaného tunelového systému (11 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. UGEIWARDR — **WIREGUARD**
2. ŮYLORZLCTUSH — **RYCHLOSTUZLŮ**
3. ALTUOŮIGD — **AUDITLOGŮ**
4. DSAERIPA — **IPADRESA**
5. OPYOKRSSXC — **SOCKSPROXY**
6. CSLITKIWHL — **KILLSWITCH**
7. ZEŘZLIÍTÍNMAI — **LIMITZAŘÍZENÍ**
8. EEÍPBZZANČE — **ZABEZPEČENÍ**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"IPVANISH PROSAZUJE PŘÍSNÝ REŽIM BEZ LOGŮ"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: KONFIGURACE MEDIÁLNÍHO CENTRA

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Klient chce pomocí IPVanish zabezpečit svůj přehrávač Android Fire TV, aby streamoval bezpečně a zároveň udržel vysokou propustnost.
- Doporučená strategie a řešení: Pokyny k hodnocení: Vysvětlete, že WireGuard má menší objem kódu, běží v prostoru jádra a spotřebovává méně cyklů CPU, čímž maximalizuje rychlost na slabém hardwaru.

B PŘÍPADOVÁ STUDIE 2: PROXY PRO TORRENTOVÉ SÍTĚ

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: P2P uploader chce skrýt svou polohu bez režie plného šifrování dat pomocí konfigurace SOCKS5.
- Doporučená strategie a řešení: Pokyny k hodnocení: Upozorněte, že SOCKS5 skrývá IP adresu bez šifrování provozu, což přináší vyšší rychlost, ale nulové soukromí vůči inspekci paketů ze strany ISP.