Jméno: _____ Datum: _____ Body: _____

Recenze PureVPN

Technická analýza PureVPN se sídlem na BVI, nezávislé audity Always-On, upgrady kvantově odolného šifrování, NAT traversal s přesměrováním portů a právní výhody BVI.

PŘEHLED VÝUKY: RECENZE PUREVPN

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 PureVPN. Prozkoumáte jurisdikci BVI, konfigurace auditu Always-On, kvantově odolné šifrování a příchozí port forwarding.

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/purevpn/

Váš studijní plán: PureVPN

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

POKYNY K RECENZI PUREVPN

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 postkvantové klíče a přesměrování portů. Zakončete bonusovou aktivitou Mysli rychle.

POSTKVANTOVÁ KRYPTOGRAFIE A INFRASTRUKTURY PRŮBĚŽNÝCH AUDITŮ

PureVPN využívá šifrovací klíče odolné vůči kvantovým útokům, aby pomohl chránit data před budoucím dešifrováním. Sídlí na BVI, udržuje politiku průběžných auditů Always-On (v roce 2021 jej auditovala KPMG) a nabízí pokročilé ovládání přesměrování portů.

(ÚVOD)

PureVPN využívá šifrovací klíče odolné vůči kvantovým útokům, aby pomohl chránit data před budoucím dešifrováním. Sídlí na BVI, udržuje politiku průběžných auditů Always-On (v roce 2021 jej auditovala KPMG) a nabízí pokročilé ovládání přesměrování portů.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. V jakém útočišti soukromí v současnosti sídlí PureVPN?

- A) Britské Panenské ostrovy
- B) Hongkong
- C) Panama
- D) Kypr

2. Jakou auditní politiku uplatňuje PureVPN pro zero-logs?

- A) Nepřetržitý audit
- B) Každoroční plánovaný audit
- C) Pololetní sebehodnocení
- D) Interní audit vlastními zaměstnanci

3. Jaké vylepšení PureVPN chrání před kvantovým dešifrováním?

- A) Kvantově odolné klíče
- B) 1024bitová výměna klíčů RSA
- C) Šifrovací bloky AES-128
- D) Dvojité SHA-256 hashe

4. Jaký doplněk PureVPN umožňuje hostování lokálních herních serverů?

- A) Přesměrování portů
- B) Dedikovaná IP adresa
- C) Rozdělené tunelování
- D) Ochrana proti únikům DNS

5. Který moderní protokol nabízí PureVPN kromě OpenVPN?

- A) WireGuard
- B) PPTP
- C) L2TP
- D) SSTP

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. PureVPN přesunula své sídlo z Hongkongu na Britské Panenské ostrovy, které nemají povinné zákony o uchovávání dat.

○ Pravda ○ Nepravda

7 Otázka 7

7. Podle zásad Always-On auditu PureVPN může její nezávislá auditorská firma kontrolovat servery bez předchozího ohlášení.

○ Pravda ○ Nepravda

8 Otázka 8

8. PureVPN používá standardní šifrovací klíče, které jsou vysoce zranitelné vůči základnímu kvantovému hrubému útoku.

○ Pravda ○ Nepravda

9 Otázka 9

9. Doplněk Port Forwarding umožňuje požadavkům příchozího provozu projít zabezpečeným NAT firewallem.

○ Pravda ○ Nepravda

10 Otázka 10

10. PureVPN postrádá funkční systémový kill switch pro desktopové klienty.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. PureVPN přesunul svou právní jurisdikci na _____ , aby působil pod příznivými zákony o soukromí.

2. K ověření nulových logů kdykoli udržuje poskytovatel se svým auditorem dohodu _____ .

3. PureVPN zavedl _____ odolné šifrovací klíče proti budoucím dešifrovacím technologiím.

4. Pro pokročilý hosting a herní servery lze nastavit doplněk _____ od PureVPN.

5. Aplikace PureVPN nabízejí vedle OpenVPN a IKEv2 i moderní protokol _____ .

6. Příchozí škodlivé pokusy o připojení automaticky blokuje vestavěný _____ na serveru VPN.

ZÁSOBNÍK SLOV

ALWAYS-ON BVI KILL SWITCH KVANTOVÉ NAT FIREWALL PORT FORWARDING SPLIT TUNNEL WIREGUARD

Sem napište své odpovědi:

1. 2.

3. 4.

5. 6.

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

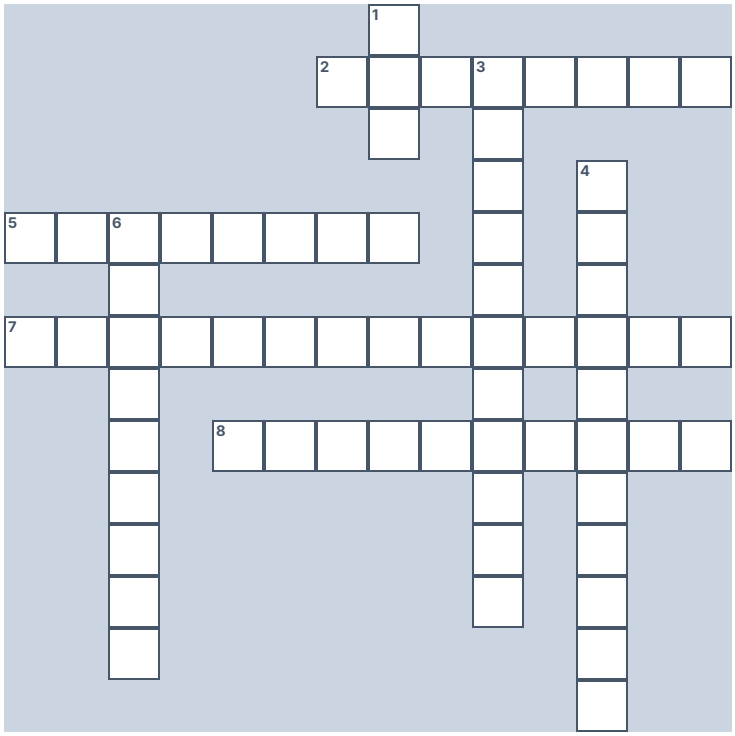
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. WireGuard	A	Doplněk umožňující směrování příchozího provozu přes VPN.
☐	2. BVI	B	Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích.
☐	3. Always-On	C	Nástroj pro konfiguraci směrování podle konkrétních aplikací.
☐	4. Quantum	D	Korporátní jurisdikce Britských Panenských ostrovů chránící soukromí.
☐	5. Přesměrování portů	E	Serverová bezpečnostní vrstva filtrující příchozí požadavky paketů.
☐	6. NAT firewall	F	Moderní vysokorychlostní open-source protokol pro připojení.
☐	7. Kill Switch	G	Generování kryptografických šifrovacích klíčů odolných do budoucna.
☐	8. Split Tunnel	H	Dohoda o neohlášeném nezávislém auditování nulových logů.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

2. Generování šifrovacích klíčů odolných vůči budoucím technologiím (8)

5. Dohoda o nezávislém neohlášeném auditování nulových logů (8)

7. Doplněk umožňující směrování příchozího provozu skrze VPN (14)

8. Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích (10)

SVISLÉ NÁPOVĚDY

1. Britské Panenské ostrovy, firemní jurisdikce ochrany soukromí (3)

3. Serverová bezpečnostní vrstva filtrující příchozí paketové požadavky (11)

4. Nástroj pro konfiguraci směrování jednotlivých aplikací (11)

6. Moderní vysokorychlostní open-source protokol připojení (9)

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: Generování šifrovacích klíčů odolných vůči budoucím technologiím (8 písmen):

5 vodorovně: Dohoda o nezávislém neohlášeném auditování nulových logů (8 písmen):

7 vodorovně: Doplněk umožňující směrování příchozího provozu skrze VPN (14 písmen):

8 vodorovně: Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích (10 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Britské Panenské ostrovy, firemní jurisdikce ochrany soukromí (3 písmen):

3 svisle: Serverová bezpečnostní vrstva filtrující příchozí paketové požadavky (11 písmen):

4 svisle: Nástroj pro konfiguraci směrování jednotlivých aplikací (11 písmen):

6 svisle: Moderní vysokorychlostní open-source protokol připojení (9 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

WIREGUARD BVI ALWAYSON KVANTOVÉ PORTFORWARDING NATFIREWALL KILLSWITCH SPLITTUNNEL

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. BVI**
- **C. ALWAYSON**
- **D. KVANTOVÉ**
- **E. PORTFORWARDING**
- **F. NATFIREWALL**
- **G. KILLSWITCH**
- **H. SPLITTUNNEL**

DEFINICE A POLE K PŘIŘAZENÍ

1. Dohoda o nezávislém neohlášeném auditování nulových logů.
2. Serverová bezpečnostní vrstva filtrující příchozí paketové požadavky.
3. Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích.
4. Doplněk umožňující směrování příchozího provozu skrze VPN.
5. Nástroj pro konfiguraci směrování jednotlivých aplikací.
6. Generování šifrovacích klíčů odolných vůči budoucím technologiím.
7. Moderní vysokorychlostní open-source protokol připojení.
8. Britské Panenské ostrovy, firemní jurisdikce ochrany soukromí.

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. AANLOSYW
3. PAONWGRDRR FOIT
4. WCSHLTIKIL
5. IVB
6. VÉNOKTVA
7. WINAELALTRF
8. NULTLSTPENI

Bonusová aktivita: Mysli rychle

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

1	Slova, která popisují dobrou VPN aplikaci			
2	Situace, kdy pomůže kill switch			
3	Streamovací služby, které sledujete			
4	Známky toho, že je vaše VPN připojení pomalé			
5	Zařízení, na která byste nainstalovali PureVPN			
6	Tlačítka nebo nabídky ve VPN aplikaci			
7	Věci, které PureVPN dokáže skrýt před vaší sítí			
8	Místa, kde byste zapnuli PureVPN			
9	VPN služby jiné než PureVPN			
10	Data, která by VPN nikdy neměla ukládat			
11	Důvody, proč si vybrat PureVPN			
12	Co si ověřit před koupí VPN			
13	VPN protokoly, které znáte			
14	Bezpečnostní pojmy, které jste se naučili v tomto pracovním listu			
15	Aplikace, které byste používali spolu s PureVPN			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: TRVALE ZAPNUTÁ OCHRANA S AUDITEM



Scénář: Korporátní podnikový klient potřebuje důkaz o dodržování zásady nulových logů, než integruje PureVPN. Prověřuje proto její nezávislou zprávu z auditu Always-On, která ukazuje, že auditorská firma smí kdykoli bez předchozího ohlášení zkontrolovat konfigurace serverů.

Otázka k diskusi: Proč je auditní rámec typu Always-On spolehlivější než standardní plánovaný roční audit?

PŘÍPADOVÁ STUDIE 2: INTEGRACE KVANTOVĚ ODOLNÝCH KLÍČŮ



Scénář: Vládní dodavatel si potřebuje vyměňovat šifrované datové soubory, které musí zůstat důvěrné dalších 20 let, a volí PureVPN kvůli kvantově odolným šifrovacím klíčům na OpenVPN.

Otázka k diskusi: Jakou hrozbu představuje kvantové počítání pro současné standardní výměny klíčů VPN?

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

17 18 14 8 20 30 24 32 26 8 35 24 20

35 38 20 32 4 32 16 8 28 30 2 18 8 1 32 6 14 30 38

1 17 18 15 5 8

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: Ve které zemi je PureVPN registrován a sídlí?

PureVPN je registrován a sídlí na Britských Panenských ostrovech (BVI), které nevynucují povinné zákony o uchovávání dat. [1]

Q2: Co je politika průběžných auditů Always-On u PureVPN?

Umožňuje nezávislé auditorské firmě PureVPN (KPMG v roce 2021) provádět překvapivé, neohlášené audity její serverové infrastruktury k ověření zásad zero-logs. [4]

Q3: Co je kvantově odolné šifrování?

Verze PureVPN používá šifrovací klíče OpenVPN generované z ověřeného kvantového zdroje prostřednictvím partnera Quantinuum. [5]

Q4: Podporuje PureVPN přesměrování portů?

Ano, PureVPN nabízí doplněk Port Forwarding, který umožňuje otevřít konkrétní porty pro hostování serverů, hraní nebo vzdálený přístup.

Q5: Které protokoly podporuje PureVPN?

PureVPN podporuje protokoly WireGuard, OpenVPN (UDP/TCP) a IKEv2 napříč aplikacemi všech platforem. [7]

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

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

Q6: Kolik serverů provozuje PureVPN?

PureVPN uvádí 6 000+ serverů v 80+ lokalitách ve více než 65 zemích (k září 2026) pro obcházení geoblokací. [7]

Q7: Co je doplněk dedikované IP adresy od PureVPN?

Poskytuje statickou IP adresu přiřazenou výhradně vašemu účtu, čímž předchází CAPTCHA a umožňuje bezpečný whitelisting na vzdálených serverech.

Q8: Podporuje PureVPN split tunneling?

Ano, klient PureVPN obsahuje split tunneling, který umožňuje určit, které aplikace používají VPN a které jdou přes lokálního ISP.

Q9: Jak PureVPN chrání relace na veřejné Wi-Fi?

Klient má spouštěč automatického připojení, který aktivuje zabezpečený tunel, jakmile detekuje nezabezpečenou nebo veřejnou bezdrátovou síť.

Q10: Mohu s PureVPN sledovat geograficky omezené streamovací služby?

Ano, PureVPN poskytuje streamingově optimalizované servery navržené k obcházení geografických omezení na hlavních streamovacích platformách.

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

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

Q1: Proč PureVPN přesunul své sídlo na Britské Panenské ostrovy?

Jurisdikce BVI nemá žádné povinnosti protokolování dat, působí mimo jurisdikci soudů USA/EU a udržuje nezávislé právní systémy, které přejí důvěrnosti uživatelských dat.

Q2: Jak doplněk PureVPN Port Forwarding řeší příchozí průchod NAT?

Doplněk vytváří na VPN bráně vyhrazené statické mapování portu. Obchází carrier-grade NAT na serveru a směruje nevyžádané příchozí pakety přímo na klientské zařízení.

Q3: Jaké algoritmy používá PureVPN v kvantově odolných výměnách klíčů?

Klíče OpenVPN u PureVPN pocházejí z ověřeného kvantového zdroje společnosti Quantinuum; PureVPN uvádí, že přijetí kvantově odolných algoritmů schválených NIST je jeho dalším krokem. [9]

Q4: Jak funguje split tunneling v desktopovém klientovi PureVPN?

Split tunneling funguje úpravou systémové směrovací tabulky. Provoz vybraných aplikací směruje na bránu lokální sítě, zatímco ostatní provoz směruje přes virtuální síťový adaptér VPN.

Q5: Chrání PureVPN před úniky IP přes WebRTC?

Ano, klient PureVPN blokuje úniky WebRTC IPv6 i WebRTC IPv4 na úrovni prohlížeče i systému a brání webům zjistit skutečnou lokální IP uživatele přes API prohlížeče.

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 jurisdikce BVI chrání PureVPN před mezinárodními soudními příkazy?

Britské Panenské ostrovy jsou zámořské území s vlastním nezávislým soudním systémem. Nemají žádné zákony o povinném uchovávání dat a jsou mimo právní dosah EU a USA; jakékoli žádosti o data vyžadují příkaz místního soudu.

Q7: Jaké postkvantové algoritmy výměny klíčů používá PureVPN?

PureVPN zatím neoznámil Kyber ani žádný jiný postkvantový algoritmus; uvádí, že přechod na algoritmy schválené NIST je jeho dalším krokem.

Q8: Jak doplněk Port Forwarding zvládá dynamické mapování?

Doplněk vytváří v bránovém firewallu PureVPN stavové pravidlo předávání, které mapuje veřejný port na VPN serveru přímo na zabezpečenou tunelovou IP uživatele.

Q9: Jaký je v PureVPN rozdíl mezi AES-256-CBC a AES-256-GCM?

AES-256-GCM poskytuje šifrování i vestavěné ověřování integrity (AEAD), takže je rychlejší a bezpečnější než režim CBC, který vyžaduje samostatný blok MAC.

Q10: Jak PureVPN brání únikům DNS a WebRTC na Windows?

Klient instaluje proprietární ovladač virtuálního síťového adaptéru, který blokuje veškerý provoz IPv6 a váže překlad DNS výhradně na rozhraní zabezpečeného tunelu.

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

PureVPN je právně registrován a sídlí na Britských Panenských ostrovech, významném útočišti soukromí. [1]

2. VPN POSTŘEH

Podle zásady auditu 'Always-On' může auditorská firma PureVPN kontrolovat jeho servery bez ohlášení; audit v roce 2021 provedla KPMG. [4]

3. VPN POSTŘEH

PureVPN používá kvantově odolné šifrovací klíče k ochraně uživatelských dat před budoucím dešifrováním kvantovými počítači. [8]

4. VPN POSTŘEH

Přesměrování portů je k dispozici jako volitelný doplněk, který umožňuje příchozím připojením projít zabezpečeným firewallem. [6]

5. VPN POSTŘEH

Nativní klientský software podporuje WireGuard a přináší vynikající rychlosti a rychlé navázání spojení. [7]

6. VPN POSTŘEH

Systémový NAT firewall blokuje nevyžádané příchozí požadavky na úrovni brány VPN.

7. POSTŘEH K VPN

Klientská aplikace obsahuje Kill Switch, který ukončí přístup k internetu, pokud VPN připojení spadne.

8. POSTŘEH K VPN

Split Tunneling umožňuje uživatelům směrovat provoz konkrétních aplikací přes VPN, zatímco ostatní aplikace používají místního ISP. [7]

9. POSTŘEH K VPN

PureVPN provozuje velkou síť serverů ve více než 65 zemích (k září 2026). [7]

10. VPN POSTŘEH

Ochrana proti únikům WebRTC je ve výchozím nastavení zapnuta, aby prohlížeče neodhalovaly lokální IP adresy přes JavaScript API.

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] PureVPN. (2024). PureVPN Moves From Hong Kong To British Virgin Islands.
https://www.purevpn.com/blog/purevpn-hq-migration/

[2] PureVPN. (n.d.). No Log Assessment.
https://www.purevpn.com/no-log-assessment

[3] PureVPN. (2023). PureVPN's consistent privacy standards: Fourth no-logs audit affirms user trust.
https://www.purevpn.com/blog/fourth-successful-no-log-assessment/

[4] PR Newswire. (2021). PureVPN, The First No-Log VPN With An Always-On Audit, Passes Second KPMG Evaluation.
https://www.prnewswire.com/news-releases/purevpn-the-first-no-log-vpn-with-an-always-on-audit-passes-second-kpmg-evaluation-301349340.html

[5] PureVPN. (n.d.). Quantum-Resistant Encryption Keys.
https://www.purevpn.com/features/quantum-resistant-encryption

[6] PureVPN. (n.d.). Get the Best Port Forwarding VPN in 2026.
https://www.purevpn.com/port-forwarding

[7] PureVPN. (n.d.). Why PureVPN is the best VPN provider of all?
https://www.purevpn.com/why-purevpn

[8] CSO Online. (2022). PureVPN introduces quantum-resistant feature to enhance security, tackle threats.
https://www.csoonline.com/article/572599/purevpn-introduces-quantum-resistant-feature-to-enhance-security-tackle-threats.html

[9] Inside Quantum Technology. (2022). PureVPN uses Quantinuum platform as it advances quantum-resistant encryption roadmap.
https://www.insidequantumtechnology.com/news-archive/purevpn-uses-quantinuum-platform-as-it-advances-quantum-resistant-encryption-roadmap/

[10] NIST Computer Security Resource Center. (n.d.). Post-Quantum Cryptography.
https://csrc.nist.gov/projects/post-quantum-cryptography

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

V jakém útočišti soukromí v současnosti sídlí PureVPN? → Britské Panenské ostrovy

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Zásady Always-On auditu PureVPN umožňují její auditorské firmě kontrolovat servery kdykoli bez ohlášení. [4]

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

PureVPN nabízí kvantově odolné šifrovací klíče, generované s Quantinuum, na OpenVPN. [5]

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaký doplněk PureVPN umožňuje hostování lokálních herních serverů? → Přesměrování portů

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

PureVPN uvádí WireGuard jako moderní protokol vedle OpenVPN a IKEv2/IPSec.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: PureVPN odešla z Hongkongu na BVI s odkazem na tamní absenci povinných zákonů o uchovávání dat.

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: zásady Always-On umožňují neohlášené audity; audit v roce 2021 provedla KPMG. [4]

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: PureVPN používá kvantově odolné šifrovací klíče na OpenVPN.

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

POZNÁMKA PRO VYUČUJÍCÍ

Doplněk Port Forwarding umožňuje požadavkům příchozího provozu projít zabezpečeným NAT firewallem.

10 **Otázka 10** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: aplikace PureVPN zahrnují internetový kill switch.

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. WireGuard	D 2. BVI	H 3. Always-On	G 4. Quantum
A 5. Přesměrování portů	E 6. NAT firewall	B 7. Kill Switch	C 8. Split Tunnel

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 BVI	2 ALWAYS-ON	3 KVANTOVÉ	4 PORT FORWARDING
5 WIREGUARD	6 NAT FIREWALL		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 C – ALWAYSON	2 F – NATFIREWALL	3 G – KILLSWITCH	4 E – PORTFORWARDING
5 H – SPLITTUNNEL	6 D – KVANTOVÉ	7 A – WIREGUARD	8 B – BVI

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy WireGuard, BVI a Always-On a ke každému uvést příklad.

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

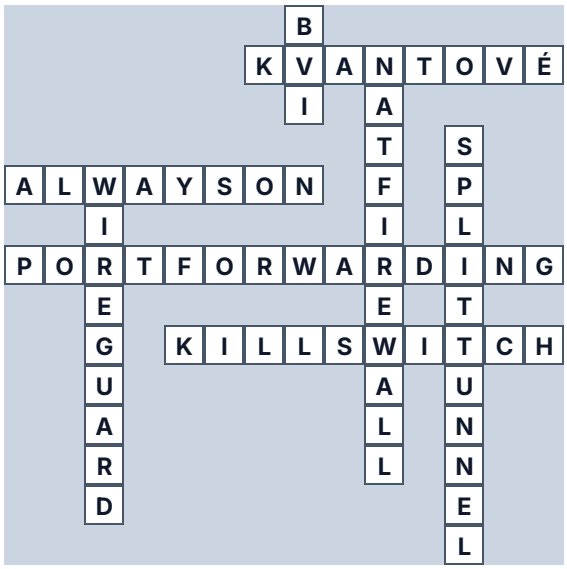
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: KVANTOVÉ Generování šifrovacích klíčů odolných vůči budoucím technologiím (8 písmen)

5 vodorovně: ALWAYSON Dohoda o nezávislém neohlášeném auditování nulových logů (8 písmen)

7 vodorovně: PORTFORWARDING Doplněk umožňující směrování příchozího provozu skrze VPN (14 písmen)

8 vodorovně: KILLSWITCH Pojistný bezpečnostní filtr přerušující síťový provoz při výpadcích (10 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: BVI Britské Panenské ostrovy, firemní jurisdikce ochrany soukromí (3 písmen)

3 svisle: NATFIREWALL Serverová bezpečnostní vrstva filtrující příchozí paketové požadavky (11 písmen)

4 svisle: SPLITTUNNEL Nástroj pro konfiguraci směrování jednotlivých aplikací (11 písmen)

6 svisle: WIREGUARD Moderní vysokorychlostní open-source protokol připojení (9 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.	IVB	BVI
2.	AANLOSYW	ALWAYSON	6.	VÉNOKTVA	KVANTOVÉ
3.	PAONWGRDRRFOIT	PORTFORWARDING	7.	WINAELALTRF	NATFIREWALL
4.	WCSHLTIKIL	KILLSWITCH	8.	NULTLSTPENI	SPLITTUNNEL

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"KLIENT PUREVPN VYNUCUJE STÁLE AUDITY A KLÍČE"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: TRVALE ZAPNUTÁ OCHRANA S AUDITEM

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Podnikový klient potřebuje před integrací PureVPN důkaz o souladu se zásadou nulového logování. Prostuduje jeho nezávislou zprávu z auditu Always-On, podle níž smí auditorská firma kdykoli bez předchozího ohlášení zkontrolovat konfigurace serverů.
- Doporučená strategie a řešení: Plánované audity dávají poskytovatelům čas vyčistit log soubory, zatímco neohlášené audity ověřují aktivní logovací konfigurace v reálném čase bez předchozího varování.

B PŘÍPADOVÁ STUDIE 2: INTEGRACE KVANTOVĚ ODOLNÝCH KLÍČŮ

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vládní dodavatel potřebuje vyměňovat šifrované datové soubory, které musí zůstat důvěrné dalších 20 let, a volí PureVPN kvůli kvantově odolným šifrovacím klíčům na OpenVPN.
- Doporučená strategie a řešení: Kvantové počítače se Shorovým algoritmem dokážou prolomit současnou kryptografii s veřejným klíčem (jako RSA), což třetím stranám umožní dešifrovat zachycený historický provoz.