Jméno: _____ Datum: _____ Body: _____

Zabezpečení ExpressVPN

Hodnocení bezpečnostní infrastruktury ExpressVPN, vlastního open-source protokolu Lightway, technologie TrustedServer pouze s RAM, nezávislých bezpečnostních auditů a kill switche Network Lock.

ZABEZPEČENÍ EXPRESSVPN – 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 bezpečnostními funkcemi ExpressVPN. Prozkoumáte open-source protokoly, serverové uzly pouze s RAM, šifry a Internet Kill Switch.

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/expressvpn/bezpecnost/

Váš studijní plán: zabezpečení ExpressVPN

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

ZABEZPEČENÍ EXPRESSVPN – POKYNY K PRŮVODCI

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 open-source protokoly a RAM-only serverové uzly. Zakončete bonusovou aktivitou Mysli rychle.

POLE RAM-ONLY SERVERŮ A OPEN SOURCE PROTOKOLY PŘIPOJENÍ

ExpressVPN využívá technologii TrustedServer pouze s RAM k zabránění místním logům, v kombinaci s vlastním open-source protokolem Lightway a funkcí Internet Kill Switch pro kompletní zabezpečení uživatelských dat.

(ÚVOD)

ExpressVPN využívá technologii TrustedServer pouze s RAM k zabránění místním logům, v kombinaci s vlastním open-source protokolem Lightway a funkcí Internet Kill Switch pro kompletní zabezpečení uživatelských dat.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký je vlastní open-source protokol ExpressVPN?**
   - A) Lightway
   - B) WireGuard
   - C) OpenVPN
   - D) Chameleon

2. **2. Jaká serverová technologie běží výhradně v energeticky závislé RAM?**
   - A) TrustedServer
   - B) RAM-Core
   - C) SecureRAM
   - D) Server NoSpy

3. **3. Co se stane, když se připojení VPN nečekaně přeruší?**
   - A) Kill switch zablokuje provoz
   - B) Provoz unikne k ISP
   - C) Systém se restartuje
   - D) Data zůstanou nezašifrovaná

4. **4. Kde je ExpressVPN registrována kvůli ochraně soukromí?**
   - A) Britské Panenské ostrovy
   - B) Švýcarsko
   - C) Panama
   - D) Rumunsko

5. **5. Která symetrická šifra se používá ve výchozím nastavení?**
   - A) AES-256-GCM
   - B) Blowfish
   - C) DES-64
   - D) RC4

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Technologie TrustedServer ukládá serverové logy na pevné disky.

○ Pravda ○ Nepravda

7 Otázka 7

7. ExpressVPN prošel bezpečnostními audity třetích stran.

○ Pravda ○ Nepravda

8 Otázka 8

8. Protokol Lightway je postaven na kódové základně OpenVPN.

○ Pravda ○ Nepravda

9 Otázka 9

9. Kill switch je v desktopových aplikacích ve výchozím nastavení zapnutý.

○ Pravda ○ Nepravda

10 Otázka 10

10. ExpressVPN provozuje soukromé DNS na každém jednotlivém serveru.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Interní vysokorychlostní protokol navržený ExpressVPN je _____ .
2. Proti uchovávání dat se serverová síť spoléhá na uzly _____ běžící pouze v RAM.
3. Kill switch ExpressVPN se dříve nazýval Network _____ .
4. Firma ExpressVPN je registrována v jurisdikci Britské Panenské _____ .
5. Datové přenosy jsou zabezpečeny robustní symetrickou šifrou _____ .
6. Prohlášení o politice nulových logů bylo nezávisle ověřeno a _____ .

ZÁSOBNÍK SLOV

AES-256 AUDITOVÁNO LIGHTWAY LOCK OSTROVY PŘEKLADAČ DNS TRUSTED SERVER ÚNIK DAT

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

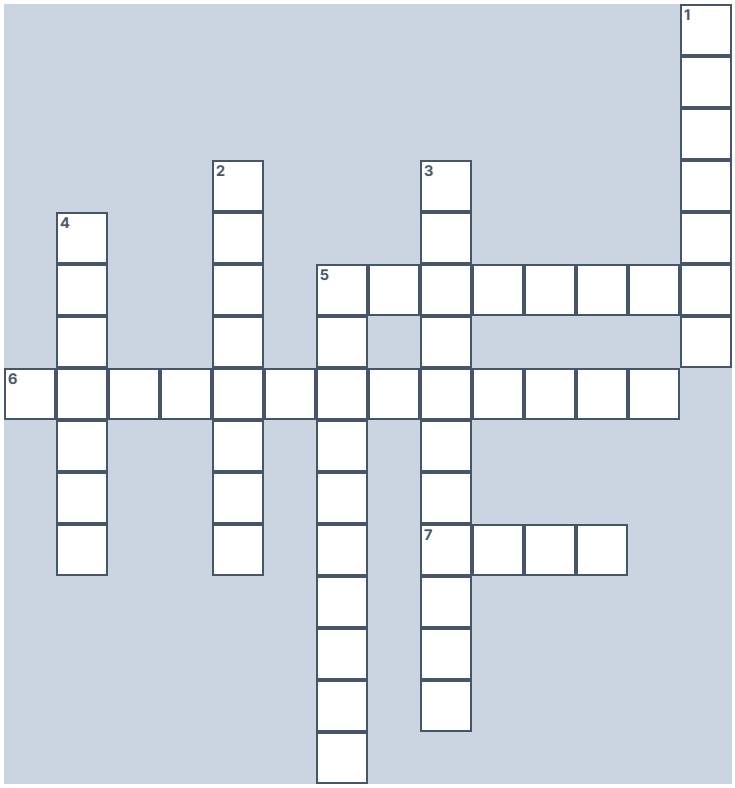
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. LIGHTWAY	A	Jurisdikce Britských Panenských ostrovů nabízející silné soukromí
☐	2. TRUSTED SERVER	B	Nechtěné odhalení privátní IP, DNS nebo WebRTC dat
☐	3. LOCK	C	Resolvery systému DNS běží soukromě na každém serverovém uzlu
☐	4. OSTROVY	D	Nezávisle ověřeno bezpečnostními firmami třetích stran
☐	5. AES-256	E	Architektura RAM-only serverů zabraňující ukládání dat na disk
☐	6. AUDITOVÁNO	F	Poslední slovo názvu Network Lock, dřívějšího označení kill switche
☐	7. ÚNIK	G	Odlehčený open-source protokol připojení od ExpressVPN
☐	8. DNS	H	Standard symetrického šifrování zabezpečující přenos dat

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

5. Symetrický šifrovací standard (AES-256) zabezpečující přenos dat (8)

6. Serverová architektura pouze v RAM bránící ukládání dat na disk (13)

7. Poslední slovo názvu Network Lock, dřívějšího jména kill switche (4)

SVISLÉ NÁPOVĚDY

1. Nechtěné odhalení soukromých dat IP, DNS nebo WebRTC (7)

2. Lehký open-source protokol připojení od ExpressVPN (8)

3. Překladače doménových jmen (DNS) provozované soukromě na každém serverovém uzlu (11)

4. Jurisdikce Britských Panenských ostrovů nabízející silné soukromí (7)

5. Nezávisle ověřeno bezpečnostními firmami třetích stran (10)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

5 vodorovně: Symetrický šifrovací standard (AES-256) zabezpečující přenos dat (8 písmen):

6 vodorovně: Serverová architektura pouze v RAM bránící ukládání dat na disk (13 písmen):

7 vodorovně: Poslední slovo názvu Network Lock, dřívějšího jména kill switche (4 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Nechtěné odhalení soukromých dat IP, DNS nebo WebRTC (7 písmen):

2 svisle: Lehký open-source protokol připojení od ExpressVPN (8 písmen):

3 svisle: Překladače doménových jmen (DNS) provozované soukromě na každém serverovém uzlu (11 písmen):

4 svisle: Jurisdikce Britských Panenských ostrovů nabízející silné soukromí (7 písmen):

5 svisle: Nezávisle ověřeno bezpečnostními firmami třetích stran (10 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

LIGHTWAY TRUSTEDSERVER LOCK OSTROVY AESŠIFRA AUDITOVÁNO ÚNIKDAT DNSRESOLVER

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. LIGHTWAY**
- **B. TRUSTEDSERVER**
- **C. LOCK**
- **D. OSTROVY**
- **E. AESŠIFRA**
- **F. AUDITOVÁNO**
- **G. ÚNIKDAT**
- **H. DNSRESOLVER**

DEFINICE A POLE K PŘIŘAZENÍ

1. Nechtěné odhalení soukromých dat IP, DNS nebo WebRTC.
2. Jurisdikce Britských Panenských ostrovů nabízející silné soukromí.
3. Překladače doménových jmen (DNS) provozované soukromě na každém serverovém uzlu.
4. Lehký open-source protokol připojení od ExpressVPN.
5. Poslední slovo názvu Network Lock, dřívějšího jména kill switche.
6. Symetrický šifrovací standard (AES-256) zabezpečující přenos dat.
7. Serverová architektura pouze v RAM bránící ukládání dat na disk.
8. Nezávisle ověřeno bezpečnostními firmami třetích stran.

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. AHTLWIYG
2. LCKO
3. ŠEAIFARS
4. TNDKAÚI
5. EVRUSTRERDTES
6. VTOORYS
7. UIAVOÁNOTD
8. VORSSDENELR

Bonusová aktivita: Mysli rychle

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

1	Vlastnosti, které hledáte u ExpressVPN			
2	Hrozby na veřejné Wi-Fi			
3	Typy úniků u VPN			
4	Způsoby, jak vytvořit silné heslo			
5	Tlačítka nebo nabídky ve VPN aplikaci			
6	Věci, které děláte online každý den			
7	Lidé, kterým byste doporučili ExpressVPN			
8	Země známé přísnými zákony na ochranu soukromí			
9	VPN protokoly, které znáte			
10	Věci, které může audit prověřit			
11	Bezpečnostní funkce v ExpressVPN			
12	Co si ověřit před koupí VPN			
13	Nastavení, která zapnete pro extra bezpečnost			
14	Věci, které šifrování chrání			
15	Věci, které ExpressVPN dokáže skrýt před vaší sítí			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: VYNUCENÍ OCHRAN POUZE V RAM



Scénář: Vládní agentura zabaví server ExpressVPN, aby získala uživatelské protokoly a historii připojení.

Otázka k diskusi: Jaké informace na serveru najdou a proč?

PŘÍPADOVÁ STUDIE 2: TUNELY NA NESTABILNÍM WI-FI PŘIPOJENÍ



Scénář: Vzdálený pracovník při úpravách dokumentů používá veřejnou hotelovou Wi-Fi, která každých pár minut vypadává.

Otázka k diskusi: Jak ExpressVPN chrání jeho data před únikem během výpadků?

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

30	26	32	28	30	8	6	28	8	26	35	8	26		6	8	20	20	10	
19	1	41	8		35	29	8	4	13	20	38		18	22	12	38			

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: Jaké šifrování používá ExpressVPN?

ExpressVPN ve výchozím nastavení používá symetrické šifrování AES-256-GCM.

Q2: Co je protokol Lightway?

Lightway je vlastní protokol ExpressVPN vytvořený pro rychlost, bezpečnost a stabilitu.

Q3: Zaznamenává ExpressVPN historii mého vyhledávání?

Ne, ExpressVPN uplatňuje přísné, nezávisle auditované zásady nulových logů.

Q4: Co je Internet Kill Switch?

Je to nativní kill switch ExpressVPN, který blokuje internetový provoz, pokud připojení spadne.

Q5: Je protokol Lightway open source?

Ano, jádro kódu protokolu Lightway je open source a je na GitHubu. [9]

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

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

Q6: Provozuje ExpressVPN privátní DNS?

Ano, ExpressVPN provozuje vlastní soukromé šifrované DNS na každém serveru. [7]

Q7: Co je technologie TrustedServer?

Je to serverové uspořádání, kde OS a aplikace běží výhradně ve volatilní paměti RAM.

Q8: Byl ExpressVPN auditován?

Ano, ExpressVPN byla auditována firmami jako PwC, Cure53 a F-Secure. [1]

Q9: Chrání ExpressVPN před úniky DNS a IPv6?

Ano, Internet Kill Switch blokuje provoz IPv4, IPv6 a DNS mimo tunel.

Q10: Kde sídlí ExpressVPN?

ExpressVPN je registrován na Britských Panenských ostrovech (BVI).

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 architektura pouze v RAM zvyšuje bezpečnost?

Data se nezapisují na pevné disky a data držená v paměti se vymažou při každém vypnutí serveru.

Q2: Proč je jurisdikce BVI důležitá pro soukromí?

ExpressVPN sídlí na BVI, takže právní žádosti o data podléhají zákonům BVI.

Q3: Podporuje ExpressVPN perfect forward secrecy?

Ano, Lightway používá dynamické klíče, které jsou pravidelně mazány a znovu generovány.

Q4: Jak Network Lock zabraňuje únikům IP?

Blokuje veškerý provoz na úrovni systému, kdykoli VPN připojení spadne.

Q5: Chrání Lightway před kvantovými útoky?

Ano, Lightway má postkvantovou ochranu využívající standard NIST ML-KEM.

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

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

Q6: Mohou vládní agentury odposlouchávat provoz Lightway?

Mohou jej zachytit, ale kvůli šifrování AES-256/ChaCha20 jej nedokážou dešifrovat.

Q7: Jak privátní DNS chrání logy vyhledávání uživatelů?

Zpracovává všechny DNS dotazy uvnitř šifrovaného tunelu a brání monitorování ze strany ISP.

Q8: K čemu se používá Lightway Turbo?

Používá vícepruhové tunelování k odesílání více dat najednou pro vyšší rychlosti.

Q9: Jaká je výhoda Lightway oproti WireGuardu?

Lightway je navržen tak, aby rychle a bez výpadku zvládal přechody mezi sítěmi (např. z Wi-Fi na mobilní data).

Q10: Jak často se serverový software přeinstalovává?

Díky TrustedServer se celý softwarový stack při každém restartu znovu načítá z bezpečného obrazu určeného jen pro čtení.

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

Lightway používá AES-256-GCM, případně ChaCha20/Poly1305 na zařízeních s nízkou spotřebou. [6]

2. VPN POSTŘEH

Technologie TrustedServer je navržena tak, aby všechny serverové operace běžely v RAM. [4]

3. VPN POSTŘEH

Jako korporátní jurisdikce slouží Britské Panenské ostrovy (BVI). [8]

4. VPN POSTŘEH

Lightway byl přepsán z jazyka C do Rustu a auditován firmami Cure53 a Praetorian. [3]

5. VPN POSTŘEH

Internet Kill Switch blokuje provoz na úrovni systému, pokud VPN spadne. [5]

6. VPN POSTŘEH

Všechny dotazy DNS jsou překládány přes soukromé, šifrované servery DNS. [7]

7. POSTŘEH K VPN

ExpressVPN zveřejnil více než 20 nezávislých auditů třetích stran. [1]

8. POSTŘEH K VPN

Služba neloguje IP adresy, historii prohlížení ani metadata provozu.

9. POSTŘEH K VPN

Dokonalé dopředné utajení (Perfect Forward Secrecy) se udržuje dynamickou rotací klíčů relace. [1]

10. VPN POSTŘEH

Protokol Lightway podporuje transportní vrstvy UDP i TCP.

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaký je vlastní open-source protokol ExpressVPN? → Lightway

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká serverová technologie běží výhradně v energeticky závislé RAM? → TrustedServer

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co se stane, když se připojení VPN nečekaně přeruší? → A) Kill switch zablokuje provoz

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Kde je ExpressVPN registrována kvůli ochraně soukromí? → Britské Panenské ostrovy

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Která symetrická šifra se používá ve výchozím nastavení? → AES-256-GCM

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

Technologie TrustedServer ukládá serverové logy na pevné disky.

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

POZNÁMKA PRO VYUČUJÍCÍ

ExpressVPN prošel bezpečnostními audity třetích stran.

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

POZNÁMKA PRO VYUČUJÍCÍ

Protokol Lightway je postaven na kódové základně OpenVPN.

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

POZNÁMKA PRO VYUČUJÍCÍ

Kill switch je v desktopových aplikacích ve výchozím nastavení zapnutý.

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

POZNÁMKA PRO VYUČUJÍCÍ

ExpressVPN provozuje soukromé DNS na každém jednotlivém serveru. [7]

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

G 1. LIGHTWAY	E 2. TRUSTED SERVER	F 3. LOCK	A 4. OSTROVY
H 5. AES-256	D 6. AUDITOVÁNO	B 7. ÚNIK	C 8. DNS

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 LIGHTWAY	2 TRUSTED SERVER	3 LOCK	4 OSTROVY
5 AES-256	6 AUDITOVÁNO		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 G – ÚNIKDAT	2 D – OSTROVY	3 H – DNSRESOLVER	4 A – LIGHTWAY
5 C – LOCK	6 E – AESŠIFRA	7 B – TRUSTEDSERVER	8 F – AUDITOVÁNO

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy LIGHTWAY, TRUSTED SERVER a LOCK a ke každému uvést příklad.

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

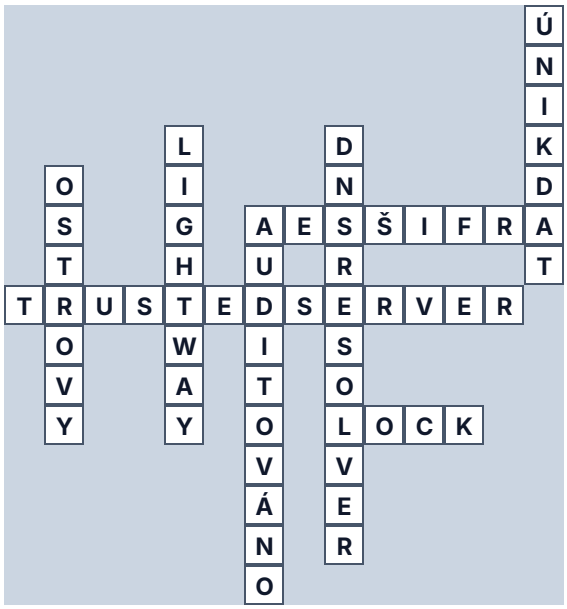
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

5 vodorovně: AESŠIFRA Symetrický šifrovací standard (AES-256) zabezpečující přenos dat (8 písmen)

6 vodorovně: TRUSTEDSERVER Serverová architektura pouze v RAM bránící ukládání dat na disk (13 písmen)

7 vodorovně: LOCK Poslední slovo názvu Network Lock, dřívějšího jména kill switche (4 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ÚNIKDAT Nechtěné odhalení soukromých dat IP, DNS nebo WebRTC (7 písmen)

2 svisle: LIGHTWAY Lehký open-source protokol připojení od ExpressVPN (8 písmen)

3 svisle: DNSRESOLVER Překladače doménových jmen (DNS) provozované soukromě na každém serverovém uzlu (11 písmen)

4 svisle: OSTROVY Jurisdikce Britských Panenských ostrovů nabízející silné soukromí (7 písmen)

5 svisle: AUDITOVÁNO Nezávisle ověřeno bezpečnostními firmami třetích stran (10 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. AHTLWIYG — LIGHTWAY
2. LCKO — LOCK
3. ŠEAIFARS — AESŠIFRA
4. TNDKAÚI — ÚNIKDAT
5. EVRUSTRERDTES — TRUSTEDSERVER
6. VTOORYS — OSTROVY
7. UIAVOÁNOTD — AUDITOVÁNO
8. VORSSDENELR — DNSRESOLVER

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"TRUSTEDSERVER DENNĚ MAŽE VŠECHNY LOGY"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: VYNUCENÍ OCHRAN POUZE V RAM

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vládní agentura zabaví server ExpressVPN, aby získala uživatelské logy a historii připojení.
- Doporučená strategie a řešení: Nic. Technologie TrustedServer od ExpressVPN běží výhradně v RAM, takže při výpadku napájení jsou všechna data okamžitě smazána.

B PŘÍPADOVÁ STUDIE 2: TUNELY NA NESTABILNÍM WI-FI PŘIPOJENÍ

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vzdálený pracovník používá veřejnou hotelovou Wi-Fi, která při úpravách dokumentů každých pár minut vypadává.
- Doporučená strategie a řešení: Internet Kill Switch automaticky blokuje veškerý internetový provoz, dokud není VPN tunel znovu navázán.