Jméno: _____ Datum: _____ Body: _____

Zabezpečení ProtonVPN

Analýza bezpečnostní architektury ProtonVPN včetně serverů Secure Core, DNS filtrování NetShield, švýcarské jurisdikce ochrany soukromí, open-source auditovaných aplikací a protokolu Stealth.

PŘEHLED VÝUKY: ZABEZPEČENÍ PROTONVPN

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 Proton VPN. Prozkoumáte servery Secure Core s dvojím skokem, DNS blokování NetShield, švýcarské zákony na ochranu soukromí a obfuskaci Stealth.

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/protonvpn/zabezpeceni/

Váš studijní plán: zabezpečení ProtonVPN

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

POKYNY K PRŮVODCI ZABEZPEČENÍM PROTONVPN

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 dvojité směrování Secure Core a švýcarskou správu ochrany soukromí. Zakončete bonusovou aktivitou Mysli rychle.

ARCHITEKTURA DVOJITÉHO SKOKU SECURE CORE A ŠVÝCARSKÁ JURISDIKCE SOUKROMÍ

Proton VPN chrání provoz uživatelů servery Secure Core ve vlastnictví Protonu ve Švýcarsku, na Islandu a ve Švédsku, open source auditovanými aplikacemi a obfuskačním protokolem Stealth navrženým k obcházení hloubkové inspekce paketů.

(ÚVOD)

Proton VPN chrání provoz uživatelů servery Secure Core ve vlastnictví Protonu ve Švýcarsku, na Islandu a ve Švédsku, open source auditovanými aplikacemi a obfuskačním protokolem Stealth navrženým k obcházení hloubkové inspekce paketů.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. V jakých zařízeních jsou umístěny servery Secure Core Protonu?**
   - A) Veřejné cloudové VM
   - B) Vysoce zabezpečená místa
   - C) Veřejná datová centra
   - D) Sdílené racky

2. **2. Jaký protokol pomáhá obcházet přísnou vládní cenzuru?**
   - A) PPTP
   - B) Protokol Stealth
   - C) OpenVPN UDP
   - D) IKEv2

3. **3. Jaká je funkce NetShield od Proton VPN?**
   - A) Speed Booster
   - B) Blokování reklam a malwaru přes DNS
   - C) Cloudové úložiště
   - D) Přesměrování portů

4. **4. Podle zákonů o ochraně soukromí které země působí Proton AG?**
   - A) Spojené státy
   - B) Spojené království
   - C) Švýcarsko
   - D) Panama

5. **5. Jak jsou klientské aplikace Proton VPN ověřovány experty?**
   - A) Tajný kód
   - B) Open source audity
   - C) Proprietární licence
   - D) Vládní přezkum

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Secure Core směruje provoz před výstupem přes země příznivé pro soukromí.

○ Pravda ○ Nepravda

7 Otázka 7

7. Švýcarsko je členem zpravodajské sledovací aliance 14-Eyes.

○ Pravda ○ Nepravda

8 Otázka 8

8. NetShield blokuje reklamy a škodlivé domény přímo na úrovni DNS.

○ Pravda ○ Nepravda

9 Otázka 9

9. Aplikace Proton VPN jsou 100% open source a veřejně auditované.

○ Pravda ○ Nepravda

10 Otázka 10

10. Protokol Stealth používá standardní hlavičky WireGuard bez obfuskace.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Vícenásobné směrování přes servery Protonu v zemích příznivých soukromí se nazývá architektura _____ .
2. K poražení hloubkové inspekce paketů a firewallů uživatelé aktivují režim _____ .
3. Malwarové domény, sledovače a reklamní skripty filtruje DNS služba _____ .
4. Proton uvádí, že _____ mu neukládá povinnost uchovávat logy aktivit uživatelů.
5. Pokud se VPN tunel nečekaně odpojí, internetový provoz zablokuje _____ .
6. Nezávislí výzkumníci mohou ověřit integritu klientů, protože aplikace jsou _____ .

ZÁSOBNÍK SLOV

AES-GCM | KILL SWITCH | NETSHIELD | OPEN SOURCE | SECURE CORE | STEALTH | ŠVÝCARSKÉ PRÁVO | WIREGUARD

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

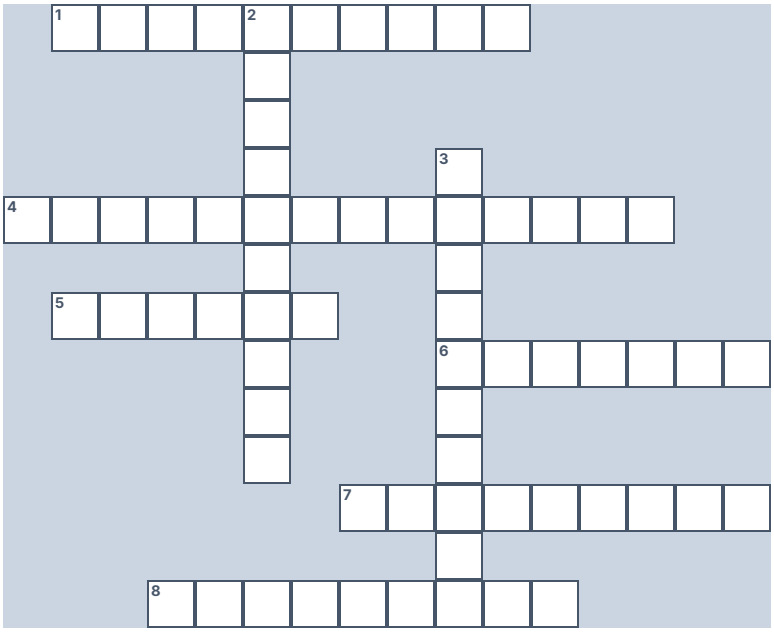
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. SECURE CORE	A	Veřejně přístupný a nezávisle auditovaný software klientské aplikace.
☐	2. STEALTH	B	Standard symetrické šifry, který šifruje datové pakety VPN.
☐	3. NETSHIELD	C	Přísné zákony na ochranu soukromí ve Švýcarsku mimo jurisdikci 14-Eyes.
☐	4. ŠVÝCARSKÉ PRÁVO	D	Obfuskovaný tunelovací protokol maskovaný jako standardní webový provoz HTTPS.
☐	5. KILL SWITCH	E	Moderní odlehčený protokol poskytující robustní kryptografii a vysoké rychlosti.
☐	6. OPEN SOURCE	F	Filtr založený na DNS blokující reklamy, telemetrické trackery a malware.
☐	7. WIREGUARD	G	Multi-hop design směrující provoz přes servery prvního skoku vlastněné Protonem.
☐	8. AES-GCM	H	Bezpečnostní pojistka zastavující síťový přenos během výpadků připojení.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

1. Bezpečnostní pojistka zastavující síťový přenos při výpadku připojení (10)

4. Přísné právní předpisy o soukromí ve Švýcarsku mimo jurisdikci 14 očí (14)

5. Symetrická šifra vojenské úrovně zabezpečující všechny zapouzdřené VPN pakety (6)

6. Obfuskovaný tunelovací protokol maskovaný jako běžný HTTPS provoz (7)

7. Moderní lehký protokol poskytující robustní kryptografii a vysoké rychlosti (9)

8. DNS filtr blokující reklamy, telemetrické sledovače a malware (9)

SVISLÉ NÁPOVĚDY

2. Vícenásobné směrování přes servery prvního skoku vlastněné Protonem (10)

3. Veřejně dostupný a nezávisle auditovaný software klientských aplikací (10)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

1 vodorovně: Bezpečnostní pojistka zastavující síťový přenos při výpadku připojení (10 písmen):

4 vodorovně: Přísné právní předpisy o soukromí ve Švýcarsku mimo jurisdikci 14 očí (14 písmen):

5 vodorovně: Symetrická šifra vojenské úrovně zabezpečující všechny zapouzdřené VPN pakety (6 písmen):

6 vodorovně: Obfuskovaný tunelovací protokol maskovaný jako běžný HTTPS provoz (7 písmen):

7 vodorovně: Moderní lehký protokol poskytující robustní kryptografii a vysoké rychlosti (9 písmen):

8 vodorovně: DNS filtr blokující reklamy, telemetrické sledovače a malware (9 písmen):

SVISLÉ NÁPOVĚDY

2 svisle: Vícenásobné směrování přes servery prvního skoku vlastněné Protonem (10 písmen):

3 svisle: Veřejně dostupný a nezávisle auditovaný software klientských aplikací (10 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

SECURECORE STEALTH NETSHIELD ŠVÝCARSKÉPRÁVO KILLSWITCH
OPENSOURCE WIREGUARD AESGCM

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. SECURECORE**
- **B. STEALTH**
- **C. NETSHIELD**
- **D. ŠVÝCARSKÉPRÁVO**
- **E. KILLSWITCH**
- **F. OPENSOURCE**
- **G. WIREGUARD**
- **H. AESGCM**

DEFINICE A POLE K PŘIŘAZENÍ

1. Obfuskovaný tunelovací protokol maskovaný jako běžný HTTPS provoz.
2. Moderní lehký protokol poskytující robustní kryptografii a vysoké rychlosti.
3. Přísné právní předpisy o soukromí ve Švýcarsku mimo jurisdikci 14 očí.
4. Vícenásobné směrování přes servery prvního skoku vlastněné Protonem.
5. Symetrická šifra vojenské úrovně zabezpečující všechny zapouzdřené VPN pakety.
6. Bezpečnostní pojistka zastavující síťový přenos při výpadku připojení.
7. DNS filtr blokující reklamy, telemetrické sledovače a malware.
8. Veřejně dostupný a nezávisle auditovaný software klientských aplikací.

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. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. RSRAÝÁKVPŠ VÉOC
7. PNOUORCESE
8. SMACGE

Bonusová aktivita: Mysli rychle

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

1	Věci, které děláte online každý den			
2	Země známé přísnými zákony na ochranu soukromí			
3	Bezpečnostní funkce v Proton VPN			
4	Typy úniků u VPN			
5	Situace, kdy pomůže kill switch			
6	Věci, které může audit prověřit			
7	Nastavení, která zapnete pro extra bezpečnost			
8	Věci, které šifrování chrání			
9	Slova, která popisují dobrou VPN aplikaci			
10	Důvody, proč si vybrat Proton VPN			
11	Tlačítka nebo nabídky ve VPN aplikaci			
12	Streamovací služby, které sledujete			
13	Hrozby na veřejné Wi-Fi			
14	Způsoby, jak vytvořit silné heslo			
15	Země, kde byste chtěli servery Proton VPN			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: OBCHÁZENÍ RESTRIKTIVNÍCH FIREWALLŮ



Scénář: Uživatel cestuje do země, kde je standardní provoz VPN, jako OpenVPN a WireGuard, blokován pomocí DPI.

Otázka k diskusi: Která konfigurace protokolu Proton VPN uživateli umožní obejít státní inspekci?

PŘÍPADOVÁ STUDIE 2: OCHRANA PŘED POKROČILÝM PROTIVNÍKEM



Scénář: Finanční auditor má podezření, že výstupní uzel jeho místního ISP může být kompromitován pokročilými přetrvávajícími hrozbami.

Otázka k diskusi: Jak Secure Core chrání identitu auditora před kompromitací výstupního uzlu?

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

28	8	26	35	8	26	38		28	8	4	32	26	8		4	22	26	8

4	13	26	2	20	15		6	1	30	1		32	41	14	35	1	30	8	18	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: Co je Proton VPN Secure Core?

Secure Core směruje provoz přes více serverů v zemích příznivých pro soukromí, než jej vypustí ven.

Q2: Co je protokol Stealth?

Stealth je obfuskovaný protokol, který skrývá připojení VPN jako běžný provoz TLS/HTTPS.

Q3: Jak NetShield chrání uživatele?

NetShield je nástroj založený na DNS, který automaticky blokuje reklamy, trackery a malwarové domény.

Q4: Je Proton VPN právně chráněn ve Švýcarsku?

Ano, Švýcarsko má přísné zákony na ochranu soukromí a je mimo jurisdikci USA i EU/14 Eyes. [4]

Q5: Jsou aplikace Proton VPN open source?

Ano. Aplikace Proton VPN jsou open source a prošly zveřejněnými bezpečnostními audity.

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

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

Q6: Jaké šifrovací šifry se využívají?

Proton VPN používá AES-256-GCM nebo ChaCha20-Poly1305 s HMAC-SHA384 a handshaky RSA-4096.

Q7: Má Proton VPN kill switch?

Ano, Proton VPN zahrnuje standardní i permanentní Kill Switch k zabránění nešifrovaným únikům.

Q8: Může Proton VPN propouštět DNS dotazy?

Ne, všechny dotazy DNS jsou směrovány přes šifrované privátní DNS servery vlastněné Protonem.

Q9: Uchovává Proton VPN logy o připojení?

Ne, Proton VPN drží přísné zásady no-logs, potvrzované každoročními audity Securitum. [3]

Q10: Je Proton VPN zranitelný vůči únikům WebRTC?

Ne, klienti Proton obsahují vestavěná pravidla firewallu a zásady směrování blokující úniky WebRTC.

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

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

Q1: Kde jsou fyzicky umístěna datová centra Secure Core?

Nacházejí se ve Švýcarsku, na bývalé vojenské základně na Islandu a v podzemním areálu ve Švédsku. [1]

Q2: Jak v Proton VPN funguje dokonalé dopředné utajení?

Pro každou relaci se generuje jedinečný pomíjivý šifrovací klíč, což brání zpětnému dešifrování.

Q3: Co je Permanent Kill Switch na Windows/Linuxu?

Trvalý kill switch blokuje veškerý síťový provoz, i když je VPN aplikace zcela zavřená nebo spadne.

Q4: Podporuje Proton VPN směrování IPv6 a ochranu proti únikům?

Proton VPN plně směruje provoz IPv6 tunely, nebo jej bezpečně vypne, aby zabránil únikům.

Q5: Jak DNS filtrování NetShieldu nakládá s inspekcí HTTPS?

NetShield pracuje čistě na vrstvě překladu DNS a nevyžaduje invazivní dešifrování TLS.

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

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

Q6: Kdo provedl externí audity kódu Proton VPN?

SEC Consult auditoval aplikace a Securitum audituje aplikace i zásadu nulového logování.

Q7: Jak si protokol Stealth stojí proti OpenVPN XOR nebo Shadowsocks?

Stealth tuneluje WireGuard přes obfuskované TLS a překonává starší obfuskaci založenou na OpenVPN. [5]

Q8: Mohou švýcarské úřady přinutit Proton VPN logovat provoz?

Proton uvádí, že podle švýcarského práva není povinen uchovávat záznamy o aktivitě nebo datech uživatelů.

Q9: Jak jsou servery Proton VPN chráněny před zabavením?

Všechny servery Proton VPN jsou bare-metal stroje chráněné šifrováním celého disku. [2]

Q10: Podporuje Proton VPN konfiguraci vlastních DNS serverů?

Ano, platící předplatitelé mohou nastavit vlastní nadřazené servery DNS přímo v předvolbách aplikace.

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

1. Proton vlastní a instaluje své servery Secure Core sám, ve vysoce zabezpečených lokalitách ve Švýcarsku, na Islandu a ve Švédsku. [1]

2. VPN POSTŘEH

2. Klientské aplikace Proton VPN jsou open source a procházejí opakovanými audity kódu třetích stran.

3. VPN POSTŘEH

3. Obfuskační protokol Stealth obchází hloubkovou inspekci paketů simulací standardního TLS provozu.

4. VPN POSTŘEH

4. Švýcarsko stojí mimo mezinárodní zpravodajské aliance 5 očí, 9 očí a 14 očí. [4]

5. VPN POSTŘEH

5. NetShield pracuje na úrovni DNS resolveru a blokuje reklamy a malware před stažením payloadu.

6. VPN POSTŘEH

6. Perfect Forward Secrecy zajišťuje, že kompromitované klíče nemohou dešifrovat dříve zachycené relace provozu. [7]

7. POSTŘEH K VPN

7. Proton VPN využívá k ochraně konfigurací serverů šifrování celého disku na bare-metal serverech. [2]

8. POSTŘEH K VPN

8. Permanent Kill Switch zabraňuje únikům nešifrovaných dat i během restartů operačního systému.

9. POSTŘEH K VPN

9. Securitum auditovalo a potvrdilo zásadu nulových logů Proton VPN v pěti po sobě jdoucích ročních auditech. [3]

10. VPN POSTŘEH

10. Proton VPN vyvinuli vědci, kteří se potkali v CERN (Evropská organizace pro jaderný výzkum). [4]

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Servery Secure Core sídlí ve vysoce zabezpečených lokalitách, včetně bývalé vojenské základny na Islandu a podzemního datového centra ve Švédsku.

2 Obfuskační protokol Stealth OBRANA PROTI CENZUŘE

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Protonův protokol Stealth maskuje připojení WireGuard jako standardní provoz TLS/HTTPS, aby obešel firewally s hloubkovou inspekcí paketů (DPI).

3 DNS blokátor reklam NetShield FILTROVÁNÍ DNS

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

NetShield používá filtrování na úrovni DNS k blokování malwarových domén, spywaru, dotěrné reklamy a telemetrických trackerů ještě před načtením webových stránek.

4 Švýcarská právní jurisdikce JURISDICTION

Správná odpověď: C

POZNÁMKA PRO VYUČUJÍCÍ

Proton AG sídlí v Ženevě ve Švýcarsku a těží ze silných švýcarských zákonů na ochranu soukromí mimo sledovací aliance USA a EU 14 očí.

5 Otázka 5

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

Všechny aplikace Proton VPN jsou open source; auditovaly je SEC Consult a později Securitum.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Secure Core napříč jurisdikcemi** ARCHITEKTURA SMĚROVÁNÍ — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Secure Core směruje provoz přes jurisdikce se silnou ochranou soukromí, než vystoupí do cílové země, což pomáhá chránit před kompromitovaným výstupním serverem.

7 **Švýcarská sledovací aliance** SLEDOVACÍ ALIANCE — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Švýcarsko není členem dohod o sdílení zpravodajských informací 5-Eyes, 9-Eyes ani 14-Eyes, čímž si zachovává nezávislou právní suverenitu.

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

POZNÁMKA PRO VYUČUJÍCÍ

NetShield používá DNS servery Protonu ke kontrole domén podle seznamů známých reklamních, trackovacích a malwarových domén.

9 **Audit open source klienta** TRANSPARENTNOST ZABEZPEČENÍ — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Proton zveřejnil své desktopové i mobilní aplikace jako open source a publikuje zprávy z auditů třetích stran.

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Stealth tuneluje WireGuard uvnitř obfuskovaného TLS přes TCP, takže provoz vypadá jako běžné HTTPS.

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. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. ŠVÝCARSKÉ PRÁVO
H 5. KILL SWITCH	A 6. OPEN SOURCE	E 7. WIREGUARD	B 8. AES-GCM

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 ŠVÝCARSKÉ PRÁVO
5 KILL SWITCH	6 OPEN SOURCE		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 B – STEALTH	2 G – WIREGUARD	3 D – ŠVÝCARSKÉPRÁVO	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – OPENSOURCE

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy SECURE CORE, STEALTH a NETSHIELD a ke každému uvést příklad.

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

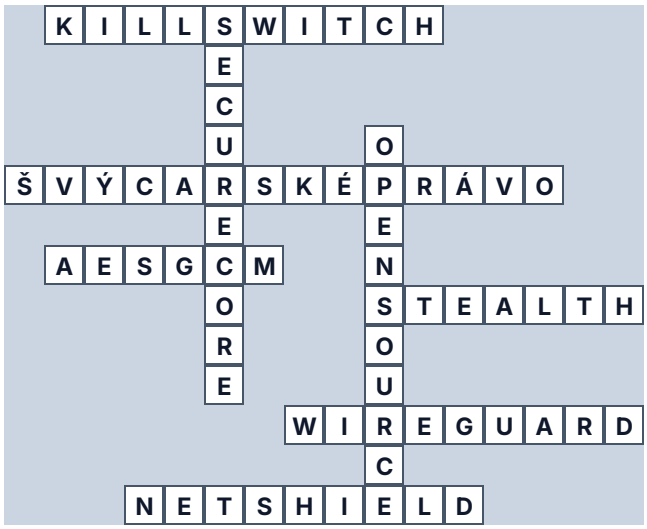
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: KILLSWITCH Bezpečnostní pojistka zastavující síťový přenos při výpadku připojení (10 písmen)

4 vodorovně: ŠVÝCARSKÉPRÁVO Přísné právní předpisy o soukromí ve Švýcarsku mimo jurisdikci 14 očí (14 písmen)

5 vodorovně: AESGCM Symetrická šifra vojenské úrovně zabezpečující všechny zapouzdřené VPN pakety (6 písmen)

6 vodorovně: STEALTH Obfuskovaný tunelovací protokol maskovaný jako běžný HTTPS provoz (7 písmen)

7 vodorovně: WIREGUARD Moderní lehký protokol poskytující robustní kryptografii a vysoké rychlosti (9 písmen)

8 vodorovně: NETSHIELD DNS filtr blokující reklamy, telemetrické sledovače a malware (9 písmen)

SVISLÉ NÁPOVĚDY

2 svisle: SECURECORE Vícenásobné směrování přes servery prvního skoku vlastněné Protonem (10 písmen)

3 svisle: OPENSOURCE Veřejně dostupný a nezávisle auditovaný software klientských aplikací (10 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. RCERESOEUC — SECURECORE
2. DNLSEIEHT — NETSHIELD
3. KWCIISHLTL — KILLSWITCH
4. GDREAUWIR — WIREGUARD
5. LHAESTT — STEALTH
6. RSRAÝÁKVPŠVÉOC — ŠVÝCARSKÉPRÁVO
7. PNOUORCESE — OPENSOURCE
8. SMACGE — AESGCM

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"SERVERY SECURE CORE CHRÁNÍ DATA UŽIVATELŮ"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: OBCHÁZENÍ RESTRIKTIVNÍCH FIREWALLŮ

Řešení pro vyučující

HODNOTICÍ RUBRIKA A POKYNY K ŘEŠENÍ

- Analýza scénáře: Uživatel cestuje do země, kde je standardní VPN provoz jako OpenVPN a WireGuard blokován pomocí DPI.
- Klíčová otázka: Která konfigurace protokolu Proton VPN umožňuje uživateli obejít inspekci na státní úrovni?
- Doporučená strategie a řešení: Uživatel by měl aktivovat protokol Stealth, který maskuje hlavičky VPN paketů jako běžný webový provoz TLS/HTTPS a proklouzne přes DPI filtry.

B PŘÍPADOVÁ STUDIE 2: OCHRANA PŘED POKROČILÝM PROTIVNÍKEM

Řešení pro vyučující

HODNOTICÍ RUBRIKA A POKYNY K ŘEŠENÍ

- Analýza scénáře: Finanční auditor má podezření, že výstupní uzel jeho místního ISP může být kompromitován pokročilými trvalými hrozbami.
- Klíčová otázka: Jak Secure Core chrání identitu auditora při kompromitaci výstupního uzlu?
- Doporučená strategie a řešení: Secure Core vede provoz nejprve přes servery vlastněné Protonem ve Švýcarsku, na Islandu nebo ve Švédsku, takže kompromitovaný výstupní server nemůže vystopovat IP uživatele.