Jméno: _____ Datum: _____ Body: _____

Zabezpečení NordVPN

Zkoumání bezpečnostních funkcí NordVPN včetně protokolu NordLynx, Dvojité VPN, Onion Over VPN, Threat Protection, auditů nulových logů a šifrování AES-256.

ZABEZPEČENÍ NORDVPN – 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 NordVPN. Prozkoumáte proprietární NordLynx, bezdiskové RAM uzly, kaskády Double VPN a nezávislé audity nulových logů.

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/nordvpn/zabezpeceni/

Váš studijní plán: zabezpečení NordVPN

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

PRŮVODCE ZABEZPEČENÍM NORDVPN – POKYNY

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na proprietární šifrovací protokoly a RAM-only serverové uzly. Zakončete bonusovou aktivitou Mysli rychle.

PROPRIETÁRNÍ PROTOKOL NORDLYNX A ZMÍRŇOVÁNÍ ZRANITELNOSTÍ

Vlastní protokol NordLynx od NordVPN integruje WireGuard se systémem dvojitého NAT, navržený pro rychlost bez ukládání uživatelských dat. Jeho servery běží na bezdiskovém RAM hardwaru a PwC a Deloitte jeho zásady no-logs ověřily šestkrát.

(ÚVOD)

Vlastní protokol NordLynx od NordVPN integruje WireGuard se systémem dvojitého NAT, navržený pro rychlost bez ukládání uživatelských dat. Jeho servery běží na bezdiskovém RAM hardwaru a PwC a Deloitte jeho zásady no-logs ověřily šestkrát.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký je proprietární protokol připojení NordVPN?**
   - A) OpenVPN
   - B) NordLynx
   - C) IKEv2
   - D) Lightway

2. **2. Jaká architektura provozuje servery výhradně v energeticky závislé RAM?**
   - A) Duální NAT
   - B) Meshnet
   - C) Bezdiskové RAM úrovně
   - D) Split Tunneling

3. **3. Jaká funkce blokuje reklamy, trackery a malwarové domény?**
   - A) Double VPN
   - B) NordLynx
   - C) Threat Protection
   - D) Onion Over VPN

4. **4. Jak Double VPN zvyšuje zabezpečení přenosu?**
   - A) Řetězí dva servery
   - B) Zdvojnásobuje šířku pásma
   - C) Komprimuje pakety
   - D) Obchází daně ISP

5. **5. Která nezávislá firma auditovala zásady zero-logs NordVPN?**
   - A) BDO
   - B) KPMG
   - C) Ernst & Young
   - D) Deloitte / PwC

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. NordLynx je postaven přímo na protokolu WireGuard.

○ Pravda ○ Nepravda

7 Otázka 7

7. Threat Protection Pro vyžaduje ke svému běhu aktivní připojení VPN.

○ Pravda ○ Nepravda

8 Otázka 8

8. Dedikovaná IP dává jednomu uživateli adresu, kterou nikdo jiný nesdílí.

○ Pravda ○ Nepravda

9 Otázka 9

9. App Kill Switch blokuje provoz v celém systému, pokud tunel spadne.

○ Pravda ○ Nepravda

10 Otázka 10

10. NordVPN zvolil bezdiskové RAM servery místo serverů s pevnými disky.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Vlastní připojovací protokol NordVPN založený na WireGuardu se jmenuje _____ .
2. Data před fyzickým zabavením hardwaru chrání bezdiskové _____ .
3. Malware a invazivní trackery blokuje vestavěná funkce zvaná _____ .
4. Směrování provozu přes dva šifrovací uzly zajišťují tunely typu _____ .
5. Společnosti PwC a Deloitte potvrdily, že NordVPN dodržuje přísnou zásadu typu _____ .
6. Přístup k internetu při výpadku tunelu okamžitě přeruší pojistka zvaná _____ .
7. Bezpečná spojení podobná LAN lze mezi zařízeními vybudovat pomocí funkce _____ .
8. Zabezpečení datového obsahu vynucují _____ AES-256 a ChaCha20.

ZÁSOBNÍK SLOV

BEZ LOGŮ DOUBLE VPN KILL SWITCH MESHNET NORDLYNX RAM-ONLY ŠIFRY THREATPROTECT

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

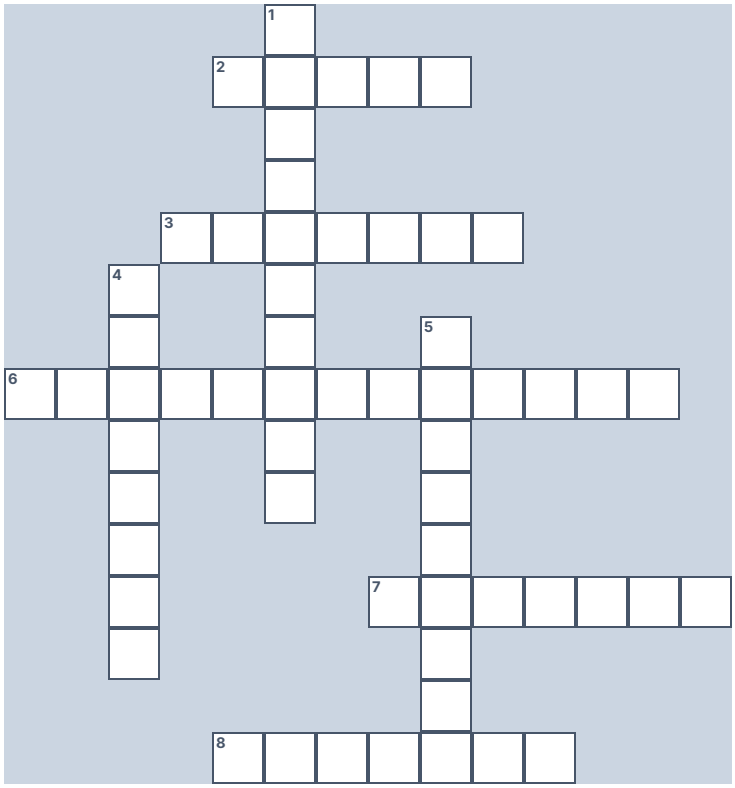
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. NORDLYNX	A	Decentralizovaný směrovací nástroj pro přímé propojení zařízení.
☐	2. RAM-ONLY	B	Místní bezpečnostní sada, která blokuje trackery, reklamy a malware.
☐	3. THREATPROTECT	C	Kryptografické algoritmy používané k zabezpečení přenášených dat.
☐	4. DOUBLE VPN	D	Serverový hardware s volatilní pamětí, který po opětovném spuštění neuchovává žádná data.
☐	5. BEZ LOGŮ	E	Řetězení dvou VPN serverů pro dvojí šifrování dat.
☐	6. KILL SWITCH	F	Vlastní protokol NordVPN postavený na standardu WireGuard.
☐	7. MESHNET	G	Přísný standard uchovávání dat ověřený externími audity.
☐	8. ŠIFRY	H	Bezpečnostní funkce, která přeruší provoz, když VPN vypadne.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

2. Kryptografické algoritmy používané k zabezpečení datových zátěží (5)

3. Decentralizovaný směrovací nástroj pro přímé propojení zařízení (7)

6. Lokální bezpečnostní sada blokující sledovače, reklamy a malware (13)

7. Přísný standard uchovávání dat ověřený externími audity (7)

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

SVISLÉ NÁPOVĚDY

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

4. Vlastní protokol NordVPN postavený na standardu WireGuard (8)

5. Řetězení dvou VPN serverů pro dvojité šifrování dat (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: Kryptografické algoritmy používané k zabezpečení datových zátěží (5 písmen):

3 vodorovně: Decentralizovaný směrovací nástroj pro přímé propojení zařízení (7 písmen):

6 vodorovně: Lokální bezpečnostní sada blokující sledovače, reklamy a malware (13 písmen):

7 vodorovně: Přísný standard uchovávání dat ověřený externími audity (7 písmen):

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

SVISLÉ NÁPOVĚDY

1 svisle: Bezpečnostní funkce přerušující provoz při výpadku VPN (10 písmen):

4 svisle: Vlastní protokol NordVPN postavený na standardu WireGuard (8 písmen):

5 svisle: Řetězení dvou VPN serverů pro dvojité šifrování dat (9 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

NORDLYNX RAMONLY THREATPROTECT DOUBLEVPN BEZLOGŮ KILLSWITCH MESHNET ŠIFRY

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. NORDLYNX**
- **B. RAMONLY**
- **C. THREATPROTECT**
- **D. DOUBLEVPN**
- **E. BEZLOGŮ**
- **F. KILLSWITCH**
- **G. MESHNET**
- **H. ŠIFRY**

DEFINICE A POLE K PŘIŘAZENÍ

1. Kryptografické algoritmy používané k zabezpečení datových zátěží.
2. Bezpečnostní funkce přerušující provoz při výpadku VPN.
3. Decentralizovaný směrovací nástroj pro přímé propojení zařízení.
4. Lokální bezpečnostní sada blokující sledovače, reklamy a malware.
5. Řetězení dvou VPN serverů pro dvojité šifrování dat.
6. Vlastní protokol NordVPN postavený na standardu WireGuard.
7. Přísný standard uchovávání dat ověřený externími audity.
8. Serverový hardware s volatilní pamětí, který po restartu neuchová žádná data.

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. **NDLNYOXR** _____
2. **CAHTRTEPTO TRE** _____
3. **LBOŮZGE** _____
4. **TENHEMS** _____
5. **NYOMRLA** _____
6. **PBOVEDLNU** _____
7. **ILKIWTCHSL** _____
8. **YŠFRI** _____

Bonusová aktivita: Mysli rychle

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

1	Známky toho, že je vaše VPN připojení pomalé			
2	Způsoby, jak vytvořit silné heslo			
3	Aplikace, které byste používali spolu s NordVPN			
4	Důvody, proč si vybrat NordVPN			
5	Země, kde byste chtěli servery NordVPN			
6	Typy úniků u VPN			
7	VPN protokoly, které znáte			
8	Věci, které může audit prověřit			
9	Vlastnosti, které hledáte u NordVPN			
10	Země známé přísnými zákony na ochranu soukromí			
11	Otázky pro zákaznickou podporu NordVPN			
12	Bezpečnostní funkce v NordVPN			
13	Hrozby na veřejné Wi-Fi			
14	Nastavení, která zapnete pro extra bezpečnost			
15	Věci, které šifrování chrání			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: NASAZENÍ DVOJITÉHO ŠIFROVÁNÍ



Scénář: Novinář potřebuje přenést vysoce citlivé dokumenty ze země s vysokou mírou cenzury.

Otázka k diskusi: Který profil serveru NordVPN mají použít k maximalizaci bezpečnosti šifrování?

PŘÍPADOVÁ STUDIE 2: PREVENCE MALWARU NA SDÍLENÝCH SÍTÍCH



Scénář: Vzdáleně fungující firma chce zabránit zaměstnancům ve stahování škodlivých souborů přes veřejnou Wi-Fi.

Otázka k diskusi: Jakou funkci mají v klientovi NordVPN nechat neustále spuštěnou?

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

20	22	26	6	18	38	20	37	20	1	30	14	35	20	10

22	3	28	1	13	32	16	8	24	26	22	30	22	17	22	18				

36	14	26	8	12	32	1	26	6

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 NordLynx?

Vlastní protokol NordVPN postavený na WireGuardu, optimalizovaný pro rychlost a bezpečnost.

Q2: Ukládá NordVPN záznamy?

Ne, NordVPN drží přísné zásady nulových logů auditované firmami Deloitte a PwC. [2]

Q3: Co je Threat Protection?

Integrovaný nástroj, který blokuje reklamy a trackery a skenuje stahované soubory na malware.

Q4: Co je Double VPN?

Funkce, která směruje váš provoz přes dva samostatné servery VPN pro dvojité šifrování.

Q5: Jak funguje kill switch?

Zablokuje vašemu zařízení přístup k internetu, pokud VPN připojení spadne.

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

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

Q6: Jsou servery NordVPN bezdiskové?

Ano, NordVPN provozuje bezdiskovou serverovou síť pouze s RAM na ochranu uživatelských dat.

Q7: Kde sídlí NordVPN?

NordVPN sídlí v Panamě, která nemá žádné povinné zákony o uchovávání dat.

Q8: Jaká šifrovací šifra se používá?

AES-256 se používá pro OpenVPN/IKEv2, zatímco ChaCha20 pro NordLynx.

Q9: Co je Onion Over VPN?

Funkce, která směruje provoz přes NordVPN a poté síť Tor.

Q10: Chrání NordVPN před úniky?

Ano, NordVPN má ochranu proti únikům DNS; VPN.com při testování nezjistil žádné úniky DNS. [7]

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 NordLynx řeší soukromí?

Používá systém dvojitého NAT k přidělování bezpečných dočasných IP bez ukládání uživatelských dat na serverech. [8]

Q2: Jak bezpečný je hardware pouze s RAM?

Protože RAM při restartu ztratí všechna data, zabavení serveru nepřinese žádné historické protokoly provozu.

Q3: Co je App Kill Switch?

Na rozdíl od internetového kill switche ukončí při výpadku VPN jen vybrané aplikace.

Q4: Jsou servery NordVPN kolokované?

Ano, NordVPN zvyšuje počet co-located serverů, což znamená, že hardware vlastní přímo.

Q5: Jak probíhají bezpečnostní audity?

PwC prověřila jeho systém bez záznamů v letech 2018 a 2020; Deloitte tak činí každoročně od roku 2022. [3]

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

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

Q6: Co je Threat Protection Lite?

Dřívější název blokátoru založeného na DNS, nyní nazývaného Scam and phishing protection.

Q7: Jak Meshnet zabezpečuje směrování?

Vytváří šifrované tunely point-to-point mezi uživatelskými zařízeními pomocí klíčů NordLynx.

Q8: Podporuje NordVPN obfuskaci?

Ano, obfuskované servery obcházejí firewally maskováním provozu VPN jako paketů HTTPS.

Q9: Je zabráněno únikům WebRTC?

WebRTC může v prohlížečích odhalit IP adresy; nechte VPN připojenou a spusťte test úniků pro ověření.

Q10: Jak pomáhá jurisdikce PAN?

Panama stojí mimo aliance 5/9/14 očí a nemá legislativu vynucující uchovávání dat.

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

NordLynx je proprietární protokol NordVPN postavený přímo na základním kódu WireGuardu. [1]

2. VPN POSTŘEH

Panamská jurisdikce nemá žádné povinné zákony o uchovávání dat, což chrání soukromí uživatelů.

3. VPN POSTŘEH

Deloitte nezávisle auditovala a ověřila implementaci nulových logů NordVPN. [9]

4. VPN POSTŘEH

Threat Protection Pro běží na zařízení a blokuje škodlivé soubory, reklamy a trackery. [4]

5. VPN POSTŘEH

Dvojitá VPN směruje pakety přes dva uzly a datový payload šifruje dvakrát.

6. VPN POSTŘEH

Hardware RAM-only serverů brání trvalému ukládání provozních logů či klíčů. [5]

7. POSTŘEH K VPN

NordVPN využívá šifry AES-256-GCM a ChaCha20 k ochraně provozu uživatelů.

8. POSTŘEH K VPN

Obfuskované servery maskují hlavičky VPN paketů, aby obešly restriktivní národní firewally.

9. POSTŘEH K VPN

Meshnet vytváří šifrované peer-to-peer sítě pomocí místních konfigurací NordLynx.

10. VPN POSTŘEH

Kill switche na úrovni aplikací ukončí vybrané procesy na pozadí, pokud tunel vypadne.

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] NordVPN. (2026). NordLynx protocol for fast, secure VPN connections.

https://nordvpn.com/blog/nordlynx-protocol-wireguard/

[2] NordVPN. (2026). A leading no-log VPN for online privacy in 2026.

https://nordvpn.com/features/no-log-vpn/

[3] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[4] NordVPN Support. (n.d.). What is NordVPN's Scam, Phishing, and Malware protection?

https://support.nordvpn.com/hc/en-us/articles/19508765521425-What-is-Threat-Protection-Pro-and-Threat-Protection

[5] NordVPN. (2024). Why does NordVPN use RAM-based servers?

https://nordvpn.com/blog/ram-based-servers/

[6] NordVPN. (2026). Buy a VPN with card, crypto, or PayPal: Monthly and yearly plans.

https://nordvpn.com/pricing/

[7] VPN.com. (n.d.). NordVPN Review: Speed, Pricing & Features.

https://www.vpn.com/vpn/nordvpn/

[8] NordVPN. (2020). NordVPN Is Rolling Out NordLynx -- New Generation VPN Protocol That Makes VPN Connection Faster Than Ever. PR Newswire.

https://www.prnewswire.com/news-releases/nordvpn-is-rolling-out-nordlynx--new-generation-vpn-protocol-that-makes-vpn-connection-faster-than-ever-301046715.html

[9] NordVPN. (2024). NordVPN verifies its no-logs claim for the fourth time. PR Newswire.

https://www.prnewswire.com/news-releases/nordvpn-verifies-its-no-logs-claim-for-the-fourth-time-302031533.html

[10] NordVPN. (2023). NordVPN has completed independent infrastructure and app security audits. PR Newswire.

https://www.prnewswire.com/news-releases/nordvpn-has-completed-independent-infrastructure-and-app-security-audits-301760758.html

[11] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[12] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Otázka 1** — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

NordLynx je vlastní protokol NordVPN, postavený na WireGuardu se systémem dvojitého NAT. [1]

2 **Otázka 2** — **Správná odpověď: C**

POZNÁMKA PRO VYUČUJÍCÍ

Bezdiskové RAM servery drží vše v nestálé paměti, která se po odpojení napájení vymaže.

3 **Otázka 3** — **Správná odpověď: C**

POZNÁMKA PRO VYUČUJÍCÍ

Threat Protection blokuje reklamy, trackery a škodlivé domény; verze Pro navíc kontroluje stahované soubory. [4]

4 **Otázka 4** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Double VPN řetězí dva servery VPN, takže provoz je před dosažením webu zašifrován dvakrát.

5 **Otázka 5** — **Správná odpověď: D**

POZNÁMKA PRO VYUČUJÍCÍ

PwC Švýcarsko (2018, 2020) a Deloitte (2022–2025) ověřily zásady no-logs NordVPN.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: NordLynx je postaven na WireGuardu a přidává systém dvojitého NAT pro soukromí.

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Threat Protection Pro funguje, i když je VPN vypnutá.

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: dedikovaná IP je přidělena jen jednomu uživateli, na rozdíl od sdílených IP adres VPN.

9 **Otázka 9** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: App Kill Switch zavírá jen vybrané aplikace; Internet Kill Switch blokuje veškerý provoz.

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: NordVPN uvádí, že zvolil bezdiskové RAM servery, které po vypnutí napájení neuchovávají žádná data.

Klíče slovní zásoby a hodnoticí rubrika

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

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

F 1. NORDLYNX	D 2. RAM-ONLY	B 3. THREATPROTECT	E 4. DOUBLE VPN
G 5. BEZ LOGŮ	H 6. KILL SWITCH	A 7. MESHNET	C 8. ŠIFRY

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 NORDLYNX	2 RAM-ONLY	3 THREATPROTECT	4 DOUBLE VPN
5 BEZ LOGŮ	6 KILL SWITCH	7 MESHNET	8 ŠIFRY

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 H – ŠIFRY	2 F – KILLSWITCH	3 G – MESHNET	4 C – THREATPROTECT
5 D – DOUBLEVPN	6 A – NORDLYNX	7 E – BEZLOGŮ	8 B – RAMONLY

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

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

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

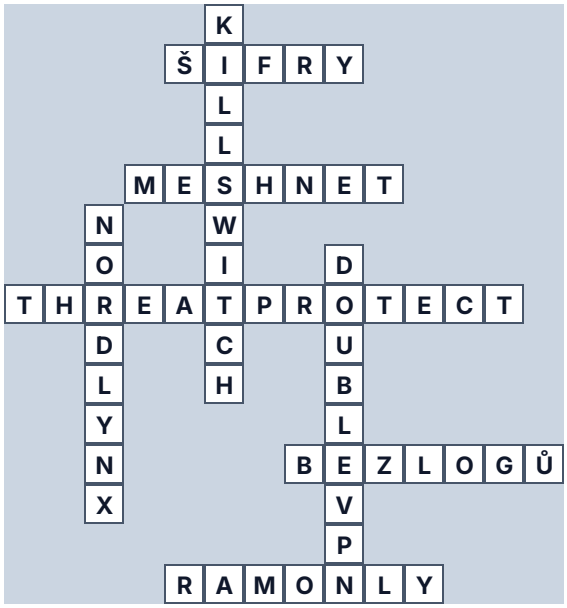
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: ŠIFRY Kryptografické algoritmy používané k zabezpečení datových zátěží (5 písmen)

3 vodorovně: MESHNET Decentralizovaný směrovací nástroj pro přímé propojení zařízení (7 písmen)

6 vodorovně: THREATPROTECT Lokální bezpečnostní sada blokující sledovače, reklamy a malware (13 písmen)

7 vodorovně: BEZLOGŮ Přísný standard uchovávání dat ověřený externími audity (7 písmen)

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

SVISLÉ NÁPOVĚDY

1 svisle: KILLSWITCH Bezpečnostní funkce přerušující provoz při výpadku VPN (10 písmen)

4 svisle: NORDLYNX Vlastní protokol NordVPN postavený na standardu WireGuard (8 písmen)

5 svisle: DOUBLEVPN Řetězení dvou VPN serverů pro dvojité šifrování dat (9 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	NDLNYOXR	NORDLYNX	5.	NYOMRLA	RAMONLY
2.	CAHTRTEPTOTRE	THREATPROTECT	6.	PBOVEDLNU	DOUBLEVPN
3.	LBOŮZGE	BEZLOGŮ	7.	ILKIWTCHSL	KILLSWITCH
4.	TENHEMS	MESHNET	8.	YŠFRI	ŠIFRY

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"NORDLYNX NATIVNĚ OBSAHUJE PROTOKOL WIREGUARD"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: NASAZENÍ DVOJITÉHO ŠIFROVÁNÍ

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Novinář potřebuje přenést vysoce citlivé dokumenty ze země s tvrdou cenzurou.
- Doporučená strategie a řešení: Zapněte profil Double VPN, který data šifruje přes dva samostatné serverové uzly.

B PŘÍPADOVÁ STUDIE 2: PREVENCE MALWARU NA SDÍLENÝCH SÍTÍCH

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Firma s prací na dálku chce zabránit zaměstnancům ve stahování škodlivých souborů přes veřejnou Wi-Fi.
- Doporučená strategie a řešení: Ponechte zapnutou funkci Threat Protection, která kontroluje stahované soubory a blokuje malware.