Jméno: _____ Datum: _____ Body: _____

Jak vybrat VPN Pracovní list

Hodnocení poskytovatelů VPN, bezpečnostních standardů, auditů a zásad logování

VPN – 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 základními principy virtuálních privátních sítí (VPN). Prozkoumáte, jak šifrované tunely zabezpečují vaše data, jak fungují síťové protokoly a jak rozpoznat a zmírnit úniky soukromí.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte koncepty a protokoly VPN.**
- [ ] **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 VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/

Váš studijní plán: VPN

- Vyhodnoťte jurisdikci poskytovatele a zásady nulových logů pro soukromí.
- Porovnejte tunelovací protokoly jako WireGuard a OpenVPN z hlediska rychlosti.
- Analyzujte bezpečnostní funkce, jako jsou kill switche a serverové uzly pouze v RAM.
- Určete nezávislé bezpečnostní audity a cenové plány při výběru.
- Vybírejte serverové lokality podle svých potřeb rychlosti a odblokování geografických omezení.

POKYNY K PRACOVNÍMU LISTU O VÝBĚRU

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 výběr zabezpečené infrastruktury VPN. Zakončete bonusovou aktivitou Mysli rychle.

VÝBĚR VPN (ÚVOD)

Výběr správné VPN vyžaduje dívat se za marketingové sliby. Spolehlivý poskytovatel musí mít prokázanou politiku nulových logů, bezpečné šifrovací protokoly a open-source klienty. Zhodnocením bezpečnostních funkcí, jurisdikcí a rychlosti si můžete vybrat VPN, která odpovídá vašim potřebám digitální ochrany.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Jaký je klíčový faktor při výběru bezpečného poskytovatele VPN?
   - A. Počet zemí se servery
   - B. Nezávisle auditované zásady no-logs
   - C. Nejnižší měsíční cenová úroveň
   - D. Okázalé reklamní sponzoringy

2. Jaký VPN protokol nabízí nejlepší rovnováhu rychlosti a auditovatelnosti?
   - A. PPTP (zastaralý)
   - B. L2TP/IPSec
   - C. Pouze OpenVPN přes TCP
   - D. WireGuard

3. Proč by se uživatelé měli vyhýbat bezplatným VPN při citlivých aktivitách?
   - A. Jsou ve Spojených státech zakázány
   - B. Často prodávají vaši historii prohlížení webu
   - C. Nepodporují základní prohlížení webu
   - D. K připojení vyžadují speciální hardware

4. Co určuje domovská právní jurisdikce poskytovatele?
   - A. Rychlost připojení k serveru
   - B. Typy podporovaných zařízení
   - C. Místní zákony upravující uchovávání dat a příkazy k prohlídce
   - D. Vizuální téma klientské aplikace

5. Jaký je primární účel funkce 'kill switch' VPN klienta?
   - A. Zablokovat přístup k internetu, pokud spojení VPN vypadne
   - B. Smazat všechny nainstalované aplikace v zařízení
   - C. Zdvojnásobit rychlost připojení k serveru
   - D. Restartovat operační systém při nečinnosti

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. VPN chrání vaše zařízení před stahováním malwaru a virovými soubory.

○ Pravda ○ Nepravda

7 Otázka 7

7. Nezávislé audity firem jako Deloitte ověřují tvrzení o nulovém logování.

○ Pravda ○ Nepravda

8 Otázka 8

8. Zákony domovské země poskytovatele nemají vliv na soukromí uživatelských dat.

○ Pravda ○ Nepravda

9 Otázka 9

9. Kompaktní kódová základna WireGuardu se audituje snáze než u OpenVPN.

○ Pravda ○ Nepravda

10 Otázka 10

10. Bezplatné VPN často prodávají reklamu nebo sledují uživatele, aby pokryly náklady na servery.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Nezávisle ověřená zásada typu _____ zavazuje poskytovatele VPN nezaznamenávat vaši online historii.

2. Moderní protokol _____ poskytuje vysokou rychlost a využívá velmi malou kódovou základnu.

3. Bezpečnostní funkce zvaná _____ zastaví veškerý provoz, pokud připojení VPN náhle selže.

4. Zda poskytovatel podléhá dohodám o sledování, určuje jeho _____ .

5. Zabezpečení serverů pomocí disků typu _____ pomáhá zajistit, aby uživatelská data nepřežila restart.

6. Ověření tvrzení o nulových znalostech vyžaduje bezpečnostní _____ provedený třetí stranou.

ZÁSOBNÍK SLOV

AUDIT | JURISDIKCE | KILL SWITCH | NO-LOGS | PĚT OČÍ | RAM-ONLY | VPN ZDARMA | WIREGUARD

Sem napište své odpovědi:

1. **2.**

3. **4.**

5. **6.**

Kontrolní bod 4: Přiřazování síťových pojmů

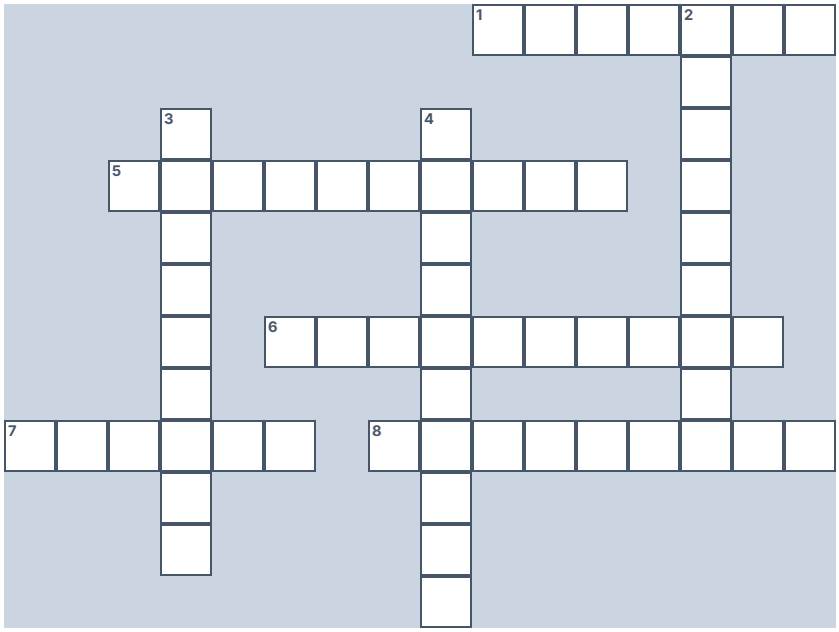
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. WireGuard	A	Vysoce riziková služba připojení, která se často monetizuje logováním a prodejem dat z prohlížeče.
☐	2. Auditované logy	B	Bezpečnostní mechanismus, který blokuje směrování do internetu, pokud se zabezpečený tunel odpojí.
☐	3. Jurisdikce	C	Mezinárodní aliance pro sdílení zpravodajských informací mezi USA, UK, CA, AU a NZ.
☐	4. Kill switch	D	Hardwarová infrastruktura běžící na volatilní paměti, takže data nejsou ukládána na disk.
☐	5. Pět očí	E	Geografická oblast určující právní povinnosti poskytovatele VPN.
☐	6. Bezplatná VPN	F	Moderní, rychlý protokol využívající asi 4,000 řádků dobře auditovatelného kódu.
☐	7. Servery pouze v RAM	G	Vyzrálý, široce auditovaný open-source protokol s mnohem větší kódovou základnou než WireGuard.
☐	8. OpenVPN	H	Tvrzení o ochraně soukromí ověřené nezávislými kyberbezpečnostními firmami.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

1. Vyzrálý, široce auditovaný open-source protokol s výrazně větší kódovou základnou než WireGuard (7)

5. Geografická oblast určující právní povinnosti poskytovatele VPN (10)

6. Hardwarová infrastruktura běžící výhradně v těkavé paměti, bránící ukládání dat (10)

7. Mezinárodní aliance sdílení zpravodajských informací mezi USA, UK, Kanadou, Austrálií a NZ (6)

8. Moderní rychlý protokol s přibližně 4 000 řádky dobře auditovatelného kódu (9)

SVISLÉ NÁPOVĚDY

2. Riziková služba připojení často vydělávající logováním a prodejem dat z prohlížeče (9)

3. Tvrzení o soukromí ověřené nezávislými kyberbezpečnostními firmami (9)

4. Pojistka blokující internetové směrování při rozpojení bezpečného tunelu (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: Vyzrálý, široce auditovaný open-source protokol s výrazně větší kódovou základnou než WireGuard (7 písmen):

5 vodorovně: Geografická oblast určující právní povinnosti poskytovatele VPN (10 písmen):

6 vodorovně: Hardwarová infrastruktura běžící výhradně v těkavé paměti, bránící ukládání dat (10 písmen):

7 vodorovně: Mezinárodní aliance sdílení zpravodajských informací mezi USA, UK, Kanadou, Austrálií a NZ (6 písmen):

8 vodorovně: Moderní rychlý protokol s přibližně 4 000 řádky dobře auditovatelného kódu (9 písmen):

SVISLÉ NÁPOVĚDY

2 svisle: Riziková služba připojení často vydělávající logováním a prodejem dat z prohlížeče (9 písmen):

3 svisle: Tvrzení o soukromí ověřené nezávislými kyberbezpečnostními firmami (9 písmen):

4 svisle: Pojistka blokující internetové směrování při rozpojení bezpečného tunelu (10 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

U T Ť E L Í B A A B C P Y L J

Y L Y U K Ď Ř U N J V D I O Ň

H K R Q F Ň Ň D Ř S P T U Ť F

C Í C T R Ó H I Š B N V D T Z

T Č Ů C Ž J V T Ě K Z G Ž R D

I O Ň Ď Ř U X L Q C D Ú B A A

W T Ž O D R L O W A A Ď Ó M Ď

S Ě É G I I D G I O R S Ř S N

L P E I Š S Ž Ů R P M T É E Ř

L Ů E A Á D Ř P E E A O Q R U

I Y R J S I U Š G N Č Ň Ý V B

K Ě Š X W K Í A U V S Ž Ý E Ý

L F I N S C J N A P M Ť P R G

R Ř G Ž Á E Ó Ů R N Ě Ú C Y Ý

Š Ý B G M Ž F J D Ó Q O X C N

SEZNAM SLOV

WIREGUARD AUDITLOGŮ JURISDIKCE KILLSWITCH PĚTOČÍ VPNZDARMA

RAMSERVERY OPENVPN

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. AUDITLOGŮ**
- **C. JURISDIKCE**
- **D. KILLSWITCH**
- **E. PĚTOČÍ**
- **F. VPNZDARMA**
- **G. RAMSERVERY**
- **H. OPENVPN**

DEFINICE A POLE K PŘIŘAZENÍ

1. Mezinárodní aliance sdílení zpravodajských informací mezi USA, UK, Kanadou, Austrálií a NZ.
2. Moderní rychlý protokol s přibližně 4 000 řádky dobře auditovatelného kódu.
3. Vyzrálý, široce auditovaný open-source protokol s výrazně větší kódovou základnou než WireGuard.
4. Riziková služba připojení často vydělávající logováním a prodejem dat z prohlížeče.
5. Pojistka blokující internetové směrování při rozpojení bezpečného tunelu.
6. Hardwarová infrastruktura běžící výhradně v těkavé paměti, bránící ukládání dat.
7. Geografická oblast určující právní povinnosti poskytovatele VPN.
8. Tvrzení o soukromí ověřené nezávislými kyberbezpečnostními firmami.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny VPN. Odpovědi pište do vyplnitelných polí.

1. **UGEIWARDR**
2. **CIJUSEIKDR**
3. **PTOÍČĚ**
4. **RREYSEVRAM**
5. **OTUŮLIAGD**
6. **CSLITKIWHL**
7. **AVMARZPDN**
8. **PNNOPVE**

Bonusová aktivita: Mysli rychle

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

1	Věci, které VPN dokáže skrýt			
2	Věci, na kterých záleží víc než na ceně			
3	Místa, kde si přečíst recenze VPN			
4	Věci, před kterými vás VPN neochrání			
5	Otázky pro obchodní tým poskytovatele VPN			
6	Věci, které vidí váš poskytovatel internetu			
7	Položky na vašem kontrolním seznamu při výběru VPN			
8	Místa, kde byste použili VPN			
9	Varovné signály u poskytovatele VPN			
10	Slova související se soukromím			
11	Věci, které byste otestovali jako první			
12	Sliby, které dává dobrý poskytovatel VPN			
13	Důvody, proč používat VPN na cestách			
14	Zařízení, která mohou používat VPN			
15	Mýty o VPN			

Kontrolní bod 8: Případové studie VPN

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

SARAH (STUDENTKA V KAVÁRNĚ)

👩‍💻 "Ahoj! Sedím v Coffee & Bytes. Je tu nezabezpečená veřejná síť 'Free_Wi-Fi_No_Password'. Chci se přihlásit do školního e-mailu a nahrát úkol, ale bojím se hackerů. Jaká jsou rizika používání této sítě bez VPN a jak VPN zabezpečí moje data?"

ALEX (CESTUJÍCÍ STUDENT)

👩‍💻 "Ale ne! Cestuji kvůli projektu v zahraničí a snažím se sledovat biologický dokument hostovaný na serveru v mé domovské zemi. Web ale hlásí 'Toto video není ve vaší aktuální lokalitě dostupné.' Proč jsem blokován a jak mi VPN pomůže ho sledovat?"

Kontrolní bod 9: Dešifrování šifry

K dokončení výcviku výběru řešení dešifrujte tuto skrytou zprávu o volbě bezpečné infrastruktury.

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

24	22	26	22	35	20	8	16	30	8		40	24	26	2	35	38
3	8	40	24	8	5	20	39	19		28	38	28	30	9	19	8	19

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 zájemců o používání virtuálních privátních sítí.

Q1: Co je VPN a jak funguje?

Virtuální privátní síť (VPN) šifruje vaše internetové připojení a směruje váš provoz přes zabezpečený vzdálený server. Tím maskuje vaši veřejnou IP adresu a omezuje, co mohou místní pozorovatelé sítě a váš ISP vidět o provozu vedeném tunelem VPN.

Q2: Proč bych měl používat VPN?

VPN chrání vaše digitální soukromí, zabezpečuje připojení na veřejných Wi-Fi sítích (například v kavárnách nebo na letištích), může omezit zpomalování podle typu aktivity, když ISP nedokáže identifikovat druh šifrovaného provozu, obchází geografická omezení pro přístup ke globálnímu obsahu a pomáhá zabezpečit prostředky pro práci na dálku.

Q3: Zajistí mi VPN na internetu úplnou anonymitu?

Ne. VPN sice skrývá vaši IP adresu a šifruje provoz, ale stále vás lze sledovat přes cookies prohlížeče, aktivní účty (jako Google nebo Facebook), otisk prohlížeče, nebo pokud váš poskytovatel VPN loguje vaše data.

Q4: Zpomalí VPN mé internetové připojení?

Ano, mírně. Proces šifrování a fyzická vzdálenost k serveru VPN přidávají latenci a režii. Dopad se liší podle poskytovatele, protokolu, vzdálenosti serveru, zařízení a stavu sítě.

Q5: Jak vydělává peníze?

Prověřte obchodní model. Předplatné, freemium úrovně i prodej dat ovlivňují, nakolik můžete VPN důvěřovat, a služba, která vaše data nikdy nesbírá, je nemůže prodat. Nejprve si přečtěte zásady ochrany soukromí. [1]

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

Projděte si nejčastější otázky a odpovědi zájemců o používání virtuálních privátních sítí.

Q6: Mohu použít bezplatnou VPN?

Bezplatné VPN se mohou spoléhat na reklamu, omezené funkce, analytiku používání, datové limity nebo jiné modely monetizace. Uživatelé by si měli před použitím prostudovat zásady ochrany soukromí poskytovatele, jeho vlastnictví, audity a obchodní model.

Q7: Co je politika "nulových logů"?

Zásada nulových logů popisuje, která data o aktivitě a připojení poskytovatel podle svého prohlášení neuchovává. Přesný rozsah se liší, proto by si čtenáři měli prostudovat zásady i zjištění nezávislých auditů.

Q8: Jak si vyberu nejlepší VPN?

Hledejte auditované zásady no-logs, silné protokoly (WireGuard, OpenVPN), bezpečné lokality serverů, vysoké rychlosti, servery běžící pouze v RAM, funkci kill switch a jurisdikci mimo aliance sdílející zpravodajské informace (jako 5/9/14 očí).

Q9: Mohu VPN používat na telefonu i chytré televizi?

Ano. Moderní poskytovatelé VPN nabízejí vyhrazené aplikace pro iOS, Android, macOS, Windows, Linux a chytré televize a také nastavení na routeru pro ochranu všech zařízení ve vaší domácí síti.

Q10: Co je kill switch?

Kill switch je bezpečnostní funkce, která automaticky odpojí vaše zařízení od internetu, pokud spojení VPN vypadne. Tím zabraňuje úniku vašich nešifrovaných dat nebo skutečné IP adresy.

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

Prozkoumejte technické a strukturální aspekty virtuálních privátních sítí a zabezpečených tunelovacích protokolů.

Q1: Jaký je rozdíl mezi WireGuardem, OpenVPN a IKEv2?

WireGuard je moderní, odlehčený protokol (jen ~4,000 řádků kódu) nabízející vysoké rychlosti a rychlá připojení. OpenVPN je vysoce bezpečný, prověřený open-source protokol. IKEv2 je vynikající pro mobilní zařízení díky schopnosti rychle se znovu připojit při změně sítě.

Q2: Co je dvojitá VPN neboli směrování Multi-Hop?

Multi-Hop směruje váš provoz postupně přes dva a více serverů VPN. Přidává tak druhou vrstvu šifrování a pomáhá udržet vaši skutečnou IP adresu skrytou před druhým skokem, pokud by byl jeden server kompromitován.

Q3: Co je únik WebRTC a jak mu VPN zabraňuje?

WebRTC je protokol prohlížeče, který může odhalit vaši skutečnou lokální i veřejnou IP adresu, i když je VPN aktivní. Prémiové VPN blokují nebo podvrhují požadavky WebRTC ve svých desktopových/mobilních aplikacích a rozšířeních prohlížeče.

Q4: Co jsou RAM-only servery a proč na nich záleží?

Tradiční servery zapisují data na pevné disky, které lze zabavit nebo kompromitovat. RAM-only (bezdiskové) servery běží výhradně ve volatilní paměti (RAM). Při restartu nebo vypnutí serveru se data v paměti vymažou.

Q5: Jak obfuskace obchází blokování VPN?

Obfuskace (neboli „Stealth VPN“) maskuje pakety VPN provozu tak, aby vypadaly jako běžný webový provoz HTTPS (port 443). To pomáhá projít přes hloubkovou inspekci paketů (DPI), kterou vlády nebo školní/firemní sítě používají k blokování VPN.

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

Prozkoumejte technické a strukturální aspekty virtuálních privátních sítí a zabezpečených tunelovacích protokolů.

Q6: Co je split tunneling a kdy jej mám použít?

Split Tunneling vám umožňuje zvolit, které aplikace se směrují šifrovaným tunelem VPN a které se připojují přímo k internetu. Použijte jej ke směrování citlivých bankovních aplikací přes VPN, zatímco lokální hry se připojují přímo a vyhnou se latenci přidané VPN.

Q7: Jak funguje Forward Secrecy (Perfect Forward Secrecy)?

PFS zajišťuje, že pro každou jednotlivou relaci se generuje jedinečný, dočasný šifrovací klíč. I když bude privátní klíč v budoucnu kompromitován, nelze jej použít k dešifrování minulých ani budoucích relací, protože ty používaly nezávislé klíče.

Q8: Co jsou aliance 5/9/14 Eyes a proč by mě měly zajímat?

Jurisdikce může ovlivnit právní proces, kterému poskytovatel může čelit, ale praktické riziko pro soukromí závisí také na tom, jaká data poskytovatel uchovává, na jeho technické architektuře, vlastnictví, zprávách o transparentnosti a historii auditů.

Q9: Co je ochrana proti únikům DNS?

Ochrana proti únikům DNS nutí vaše zařízení posílat dotazy na vyhledání webů (dotazy DNS) přes soukromé, šifrované DNS servery VPN místo serverů vašeho ISP. Tím brání vašemu ISP sledovat, které stránky navštěvujete.

Q10: Proč prověřovat, kdo VPN provozuje a doporučuje?

Na pověsti záleží. Prozkoumejte vlastníky a vedení společnosti, hledejte veřejné audity třetích stran a zjistěte, co říkají nezávislí bezpečnostní experti a tisk, než jí začnete důvěřovat. [1]

Část 11: 10 zajímavých faktů o VPN a poznatků z praxe

Projděte si tato velmi cenná fakta a poznatky z praxe o historii, trhu a technologii VPN.

1. PRVNÍ VPN PROTOKOL

PPTP (Point-to-Point Tunneling Protocol), raný VPN protokol od skupiny vedené Microsoftem z let po roce 1990, je dnes považován za nezabezpečený, takže moderní VPN používají WireGuard nebo OpenVPN. [1]

2. TRŽNÍ OCENĚNÍ

Globální trh s VPN zažil rychlý růst, tažený rostoucími požadavky práce na dálku a poptávkou po podnikové bezpečnosti.

3. REVOLUCE WIREGUARD

WireGuard má vysoce zjednodušenou kódovou základnu navrženou pro efektivitu, takže se snáze audituje na bezpečnostní zranitelnosti než tradiční protokoly. [3]

4. PŘÍSNÉ AUDITNÍ STANDARDY

Přední poskytovatelé VPN najímají firmy jako Deloitte, KPMG nebo PwC ke kontrole tvrzení o nulových lozích a bezpečnostní firmy jako Cure53 k testování svých aplikací a serverů. [4]

5. POČÁTKY ALIANCE 5 OČÍ

Zpravodajské partnerství Five Eyes mezi USA, Spojeným královstvím, Kanadou, Austrálií a Novým Zélandem vzniklo ze spolupráce spojenců v oblasti signálového zpravodajství za druhé světové války.

6. HLOUBKOVÁ INSPEKCE PAKETŮ

Pokročilé firewally nasazují hloubkovou inspekci paketů (DPI) k analýze metadat síťových paketů a blokování standardních charakteristik VPN připojení.

7. FIREMNÍ VYUŽITÍ

Mnoho organizací dává vzdáleným zaměstnancům VPN pro přístup k interním systémům, jako jsou databáze, což z VPN dělá běžný pracovní bezpečnostní nástroj.

8. DECENTRALIZOVANÉ VPN

Decentralizované VPN (dVPN) rozdělují provoz přes síť uzlů provozovaných jednotlivci, čímž snižují závislost na jediném centralizovaném poskytovateli.

9. ANONYMITA TOR VS. VPN

VPN tuneluje provoz přes jediného poskytovatele, zatímco Tor (The Onion Router) posílá provoz přes tři dobrovolnická relé (vstupní, prostřední, výstupní) pro maximalizaci soukromí. [5]

10. NÁKLADY NA ÚNIKY DAT

Kombinace VPN s modelem přístupu zero-trust, který ověřuje každého uživatele i zařízení, pomáhá organizacím chránit data a omezit škody z úniků dat.

Technické reference a zdroje

Citované publikace, kryptografické specifikace a oficiální dokumentační standardy použité v celém tomto pracovním listu.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] 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

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

Klíč odpovědí: Hodnocení poskytovatelů VPN, bezpečnostních standardů, auditů a zásad logování

1 **Auditované zásady logování** PROTOKOLY — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Nezávisle auditovaná zásada nulových logů je nejpraktičtější způsob, jak ověřit tvrzení poskytovatele o soukromí s nulovou znalostí. Okázalý marketing nebo vlastní tvrzení nestačí.

2 **Převaha WireGuardu** LATENCE — **Správná odpověď: D**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard nabízí moderní, rychlé směrování připojení v prostoru jádra s kompaktní kódovou základnou (~4,000 řádků), díky čemuž jsou audity vysoce efektivní.

3 **Otázka 3** — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Bezplatné VPN stále platí za servery a FTC varuje, že některé aplikace VPN sdílejí data uživatelů s třetími stranami, například kvůli zobrazování reklam.

4 **Právní jurisdikce** ŘÍZENÍ SMĚROVÁNÍ — **Správná odpověď: C**

POZNÁMKA PRO VYUČUJÍCÍ

Jurisdikce určuje, zda VPN podléhá zákonům o sledování, místním mandátům uchovávání dat a tajným vládním příkazům.

5 **Ochrana kill switchem** SOUKROMÍ — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Kill switch při výpadku tunelu okamžitě přeruší směrování systémového síťového adaptéru a zabrání únikům skutečné IP a DNS.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Limity ochrany proti malwaru** MASKOVÁNÍ IP — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

VPN poskytuje zabezpečený šifrovaný kanál, ale neskenuje obsah ani soubory. K blokování malwaru je nutný antivirový software.

7 **Nezávislé audity** RYCHLOSTI — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Auditní zprávy ověřují konfigurace serverového softwaru, dodržování RAM-only nastavení a absenci logovacích databází.

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

POZNÁMKA PRO VYUČUJÍCÍ

Poskytovatelé musí dodržovat zákony své domovské země, což může zahrnovat pravidla uchovávání dat a příkazy k vydání dat, která drží.

9 **Velikost kódové základny protokolu** FIREWALLY — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Menší kódová základna zmenšuje potenciální plochu útoku a usnadňuje bezpečnostním týmům ověření integrity protokolu.

10 **Monetizace reklamou** NO-LOGS — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Bez předplatného se bezplatné VPN spoléhají na těžbu dat, profilování provozu a vkládání reklam do prohlížeče, aby generovaly příjmy.

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	H 2. Auditované logy	E 3. Jurisdikce	B 4. Kill switch
C 5. Pět očí	A 6. Bezplatná VPN	D 7. Servery pouze v RAM	G 8. OpenVPN

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 NO-LOGS	2 WIREGUARD	3 KILL SWITCH	4 JURISDIKCE
5 RAM-ONLY	6 AUDIT		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 E – PĚTOČÍ	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNZDARMA
5 D – KILLSWITCH	6 G – RAMSERVERY	7 C – JURISDIKCE	8 B – AUDITLOGŮ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy WireGuard, Auditované logy a Jurisdikce a ke každému uvést příklad.

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

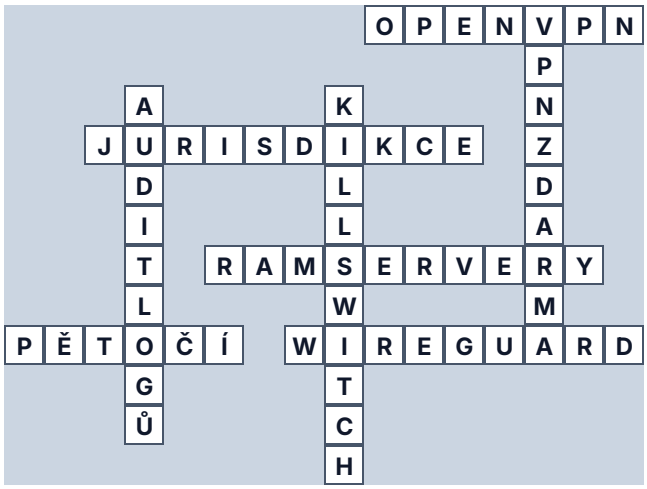
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: OPENVPN Vyzrálý, široce auditovaný open-source protokol s výrazně větší kódovou základnou než WireGuard (7 písmen)

5 vodorovně: JURISDIKCE Geografická oblast určující právní povinnosti poskytovatele VPN (10 písmen)

6 vodorovně: RAMSERVERY Hardwarová infrastruktura běžící výhradně v těkavé paměti, bránící ukládání dat (10 písmen)

7 vodorovně: PĚTOČÍ Mezinárodní aliance sdílení zpravodajských informací mezi USA, UK, Kanadou, Austrálií a NZ (6 písmen)

8 vodorovně: WIREGUARD Moderní rychlý protokol s přibližně 4 000 řádky dobře auditovatelného kódu (9 písmen)

SVISLÉ NÁPOVĚDY

2 svisle: VPNZDARMA Riziková služba připojení často vydělávající logováním a prodejem dat z prohlížeče (9 písmen)

3 svisle: AUDITLOGŮ Tvrzení o soukromí ověřené nezávislými kyberbezpečnostními firmami (9 písmen)

4 svisle: KILLSWITCH Pojistka blokující internetové směrování při rozpojení bezpečného tunelu (10 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. UGEIWARDR — **WIREGUARD**
2. CIJUSEIKDR — **JURISDIKCE**
3. PTOÍČĚ — **PĚTOČÍ**
4. RREYSEVRAM — **RAMSERVERY**
5. OTUŮLIAGD — **AUDITLOGŮ**
6. CSLITKIWHL — **KILLSWITCH**
7. AVMARZPDN — **VPNZDARMA**
8. PNNOPVE — **OPENVPN**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"POROVNEJTE ZPRÁVY BEZPEČNÝM SYSTÉMEM"

Klíč k případovým studiím

A Scénář A: Bezpečnost na veřejné síti

SNIFFING A ŠIFROVÁNÍ | Sarahino dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Rizika: Odposlech paketů (sniffing), zachycení dat a útoky man-in-the-middle. Někdo na stejné kavárenské síti by mohl zachytit její přihlašovací údaje nebo soubor s úkolem.
- Ochrana VPN: Šifruje obsah síťových paketů, takže zachycený tunelový provoz je pro pasivní odposlech v místní síti nečitelný, je-li VPN správně nakonfigurována.

B Scénář B: Přístup k blokovaným zdrojům

GEOBLOKACE A IP ADRESY | Alexovo dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Proč blokováno: Streamovací služba používá geoblokaci, která mapuje cestovatelovu lokální IP adresu na jeho fyzickou zemi a blokuje ji na základě územních licencí.
- Jak VPN pomáhá: Maskuje jeho skutečnou polohu směrováním provozu přes server v jeho domovské zemi. Web vidí IP adresu domovské země a umožní přístup.