Jméno: _____ Datum: _____ Body: _____

# Jak nastavit VPN Pracovní list

Konfigurace VPN na Windows, macOS, Androidu, iOS, Linuxu a routerech

## 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

- Porovnejte komerční VPN aplikace s nastavením nativních klientů.
- Nakonfigurujte VPN připojení na routerech pro ochranu celé domácnosti.
- Nastavujte a spravujte konfigurační soubory, jako jsou OVPN nebo klíče WireGuard.
- Otevřete a zabezpečte konkrétní porty routeru pro provoz tunelu.
- Ověřujte nastavení klienta pomocí kontrol úniků DNS a testů připojení.

## POKYNY K PRACOVNÍMU LISTU KONFIGURACE

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 nastavení a testování VPN klientů. Zakončete bonusovou aktivitou Mysli rychle.

## KONFIGURACE VPN (ÚVOD)

Ruční nastavení VPN vám dává plnou kontrolu nad šifrovacími klíči a směrováním sítě. Ať už konfigurujete nativního klienta na mobilním zařízení, nebo instalujete tunel VPN přímo na router, správná konfigurace je klíčem k prevenci úniků DNS a zabezpečení veškerého síťového provozu.

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

## Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký je nejjednodušší způsob nastavení VPN na mobilních zařízeních?**
   - A. Stažení oficiální aplikace VPN z obchodu s aplikacemi
   - B. Ruční úprava souborů jádra operačního systému
   - C. Nahrání vlastního firmwaru do hardwaru zařízení
   - D. Připojení telefonu ke stolnímu počítači přes USB

2. **2. Jaká je výhoda instalace VPN přímo na router?**
   - A. Zvyšuje rychlost připojení všech místních zařízení
   - B. Automaticky zabezpečí všechna připojená síťová zařízení
   - C. Obchází nutnost platit předplatné místnímu ISP
   - D. Zcela odstraňuje potřebu hardwarových routerů

3. **3. Na co odkazuje 'nativní' konfigurace VPN?**
   - A. Nastavení připojení pomocí nativních vestavěných nastavení OS
   - B. Používání VPN pouze ve vašem domovském městě
   - C. Připojování pouze k serverům v domovské zemi
   - D. Napsání vlastního protokolu v assembleru

4. **4. Co je vyžadováno pro manuální externí konfiguraci OpenVPN?**
   - A. Návrh vlastního loga pro připojení k serveru
   - B. Import profilu .ovpn obsahujícího certifikační klíče
   - C. Změna fyzického umístění domácího routeru
   - D. Úplné vypnutí firewallu operačního systému

5. **5. Proč by administrátor použil split tunneling v nastavení?**
   - A. Úplně zablokovat veškerý internetový provoz
   - B. Umožnit vybraným bezpečným aplikacím obejít zabezpečený tunel
   - C. Rozdělit fyzický router na dvě samostatné jednotky
   - D. Vypnout šifrování kvůli administrativnímu dohledu

## Kontrolní bod 2: Výzva Pravda/Nepravda

**6 Otázka 6**

6. Nastavení VPN na routeru je jednoduchý proces nevyžadující žádné technické dovednosti.

- ( ) Pravda
- ( ) Nepravda

**7 Otázka 7**

7. Windows a macOS mají nativní klienty podporující IKEv2 a L2TP.

- ( ) Pravda
- ( ) Nepravda

**8 Otázka 8**

8. Nastavení WireGuardu vyžaduje vygenerování veřejného a soukromého klíče.

- ( ) Pravda
- ( ) Nepravda

**9 Otázka 9**

9. Tunel VPN zabezpečuje vaše tiskárny v místní síti a tiskové úlohy.

- ( ) Pravda
- ( ) Nepravda

**10 Otázka 10**

10. Chytré zámky, které neumí spouštět aplikace VPN, potřebují k pokrytí VPN na úrovni routeru.

- ( ) Pravda
- ( ) Nepravda

## Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Instalace VPN na zařízení, jakým je domácí _____ , chrání i chytré televize a herní konzole.

2. Ruční konfigurace OpenVPN vyžaduje import serverového profilu s příponou _____ .

3. Vestavěná konfigurace operačního systému využívá _____ nastavení klienta.

4. Ověřování ve WireGuardu se opírá o kryptografický _____ tvořený veřejným a soukromým klíčem.

5. Nejsnazší instalaci nabízí oficiální _____ poskytovatele.

6. Únikům umožňujícím sledování překladu jmen brání směrování dotazů přes _____ servery provozované VPN.

**ZÁSOBNÍK SLOV**

APLIKACE DNS LOGY PŘIPOJENÍ NATIVNÍ OVPN PÁR KLÍČŮ ROUTER SPLIT TUNNELING

**Sem napište své odpovědi:**

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

# Kontrolní bod 4: Přiřazování síťových pojmů

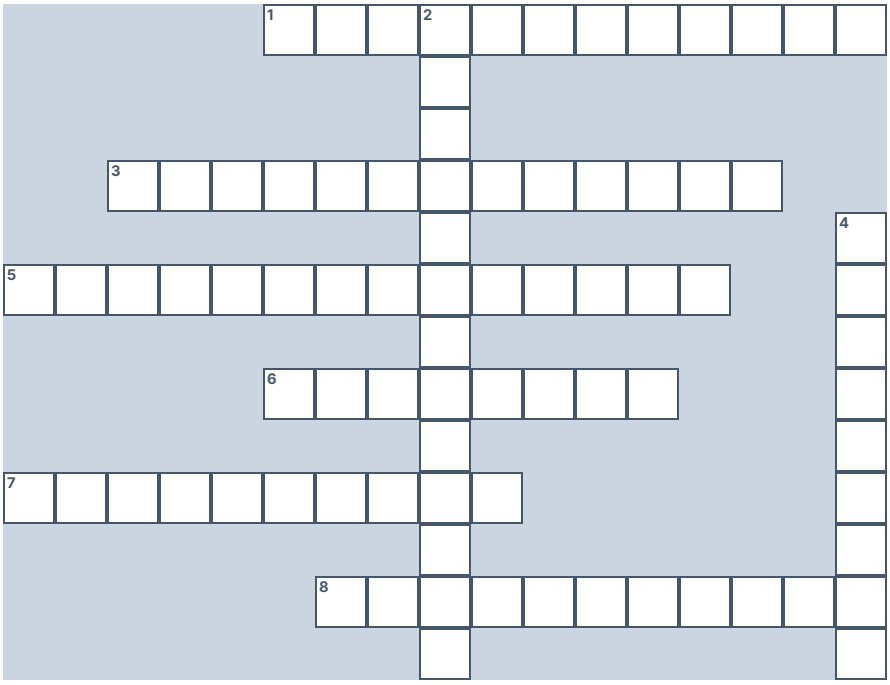
## PŘIŘAZOVÁNÍ DEFINIC

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

| | | | |
|---|---|---|---|
| ☐ | 1. VPN aplikace | A | Šifrování na úrovni brány chránící všechny chytré spotřebiče v místní síti. |
| ☐ | 2. Router VPN | B | Softwarový balíček poskytovaný předplatitelskou službou pro snadné nastavení jedním kliknutím. |
| ☐ | 3. Nativní klient | C | Kontrola chybových výstupů a stavových logů klienta při ladění nezdařených instalací. |
| ☐ | 4. Profil .ovpn | D | Rozlišování tras provozu, aby vybrané aplikace obcházely šifrovaný tunel. |
| ☐ | 5. Pár klíčů | E | Zabezpečení provozu v nativním nastavení operačního systému bez instalace aplikací. |
| ☐ | 6. Split tunneling | F | Konfigurace adres síťových resolverů k zabránění únikům doménových dotazů. |
| ☐ | 7. Nastavení serveru DNS | G | Kryptografické tokeny (veřejný/soukromý) vyžadované k navázání WireGuard handshaků. |
| ☐ | 8. Protokoly připojení | H | Formát souboru OpenVPN obsahující servery, nastavení portů a certifikátové klíče. |

## Kontrolní bod 5: Křížovka

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




### VODOROVNÉ NÁPOVĚDY

**1. Konfigurace adres síťových překladačů proti únikům překladu domén (12)**

**3. Kontrola chybových výstupů a stavových logů klienta při ladění neúspěšných nastavení (13)**

**5. Rozlišení tras provozu, aby vybrané aplikace obcházely šifrovaný tunel (14)**

**6. Kryptografické tokeny (veřejný/soukromý) nutné k navázání WireGuard handshake (8)**

**7. Formát souboru OpenVPN obsahující servery, nastavení portů a certifikační klíče (10)**

**8. Softwarový balík od předplacené služby pro snadné nastavení jedním kliknutím (11)**

### SVISLÉ NÁPOVĚDY

**2. Zabezpečení provozu v nativním nastavení operačního systému bez instalace aplikací (13)**

**4. Šifrování na úrovni brány chránící všechny chytré spotřebiče v místní síti (9)**

# 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: Konfigurace adres síťových překladačů proti únikům překladu domén (12 písmen):**

**3 vodorovně: Kontrola chybových výstupů a stavových logů klienta při ladění neúspěšných nastavení (13 písmen):**

**5 vodorovně: Rozlišení tras provozu, aby vybrané aplikace obcházely šifrovaný tunel (14 písmen):**

**6 vodorovně: Kryptografické tokeny (veřejný/soukromý) nutné k navázání WireGuard handshake (8 písmen):**

**7 vodorovně: Formát souboru OpenVPN obsahující servery, nastavení portů a certifikační klíče (10 písmen):**

**8 vodorovně: Softwarový balík od předplacené služby pro snadné nastavení jedním kliknutím (11 písmen):**

## SVISLÉ NÁPOVĚDY

**2 svisle: Zabezpečení provozu v nativním nastavení operačního systému bez instalace aplikací (13 písmen):**

**4 svisle: Šifrování na úrovni brány chránící všechny chytré spotřebiče v místní síti (9 písmen):**

## Kontrolní bod 6: Hledání skrytých slov

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

T Ý J J Ů J Z W Y Q J I Ž I Í

N Ň A E H Á T A J É W E K Ž K

E Ď L Ř V P N A P L I K A C E

I Ň J A Ě P K O Č Ň C D G I B

L Á P S M Q V U I Ý Ě Z Š F Y

K W H É S U Ó Ú K S D Ť T M Q

Í L Ň T H K Q H Z P M W Ú O Ý

N Ř Í N E V A T S A N S N D Ř

V Á Á M Q Ň Á L I É Í O Ý B Ž

I Ž Z B Ň Ů Ů Č Í L K R Á P Y

T S P L I T T U N N E L I N G

A N Č O V P N P R O F I L É P

N X L O G Y P Ř I P O J E N Í

R R Y G Ď Z C W M E F G Ž W Č

R E T U O R N P V P Ř J X Y S

### SEZNAM SLOV

VPNAPLIKACE VPNROUTER NATIVNÍKLIENT OVPNPROFIL PÁRKLÍČŮ
SPLITTUNNELING DNSNASTAVENÍ LOGYPŘIPOJENÍ

# 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. VPNAPLIKACE**
- **B. VPNROUTER**
- **C. NATIVNÍKLIENT**
- **D. OVPNPROFIL**
- **E. PÁRKLÍČŮ**
- **F. SPLITTUNNELING**
- **G. DNSNASTAVENÍ**
- **H. LOGYPŘIPOJENÍ**

**DEFINICE A POLE K PŘIŘAZENÍ**

1. Konfigurace adres síťových překladačů proti únikům překladu domén.
2. Rozlišení tras provozu, aby vybrané aplikace obcházely šifrovaný tunel.
3. Šifrování na úrovni brány chránící všechny chytré spotřebiče v místní síti.
4. Kryptografické tokeny (veřejný/soukromý) nutné k navázání WireGuard handshake.
5. Zabezpečení provozu v nativním nastavení operačního systému bez instalace aplikací.
6. Kontrola chybových výstupů a stavových logů klienta při ladění neúspěšných nastavení.
7. Formát souboru OpenVPN obsahující servery, nastavení portů a certifikační klíče.
8. Softwarový balík od předplacené služby pro snadné nastavení jedním kliknutím.

## Kontrolní bod 7: Výzva s přeházenými slovy

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

1. PICPLKVANEA
2. NVANTNEÍTLIKI
3. KÁPLÍŮČR
4. NAASTÍSEVDNN
5. TOPRURVEN
6. IPNOFOVRLP
7. LNESNPLGTINIUT
8. OGPŘEPÍLIONJY

# Bonusová aktivita: Mysli rychle

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

| | | | | |
|---|---|---|---|---|
| 1 | Věci, které je třeba zkontrolovat po nastavení | | | |
| 2 | Zařízení, která mohou používat VPN | | | |
| 3 | VPN služby, které znáte | | | |
| 4 | Důvody, proč používat VPN na cestách | | | |
| 5 | Chyby, které lidé dělají při nastavování | | | |
| 6 | Slova z tohoto pracovního listu, která si chcete zapamatovat | | | |
| 7 | Nastavení, která zapnete jako první | | | |
| 8 | Sliby, které dává dobrý poskytovatel VPN | | | |
| 9 | Kroky při nastavování VPN | | | |
| 10 | Místa, kde byste použili VPN | | | |
| 11 | Způsoby, jak poznat falešnou Wi-Fi síť | | | |
| 12 | Věci, které VPN dokáže skrýt | | | |
| 13 | Věci, které vidí váš poskytovatel internetu | | | |
| 14 | Místa, kde najít pomoc | | | |
| 15 | Věci, které potřebujete na začátek | | | |

# 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 konfigurace serverů dešifrujte tuto skrytou zprávu o nastavování bezpečných tunelů.

**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 | 1 | 14 | 20 | 28 | 30 | 1 | 18 | 32 | 16 | 30 | 8 | | 3 | 26 | 2 | 20 | 32 | | 28 | 8 |
| | | | | | | | | | | | | | | | | | | | | |
| 40 | 1 | 3 | 8 | 40 | 24 | 8 | 5 | 8 | 20 | 39 | 19 | | 6 | 9 | 19 | 22 | 20 | 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: Co potřebuji k zahájení?

Potřebujete aktivní předplatné VPN nebo vlastní server VPN, podporované zařízení a buď aplikaci poskytovatele, nebo údaje pro ruční nastavení: adresu serveru, protokol a své přihlašovací údaje, klíče či certifikáty. Většina lidí si prostě nainstaluje oficiální aplikaci, přihlásí se a klepne na připojit.

### Q3: Jak na Windows nastavím VPN bez aplikace?

Otevřete Nastavení > Síť a internet > VPN, zvolte Přidat VPN a zadejte název serveru poskytovatele, typ VPN (například IKEv2 nebo L2TP/IPsec) a své přihlašovací údaje. Poté vyberte Připojit.

### 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 nastavím macOS?

Nainstalujte macOS aplikaci poskytovatele, nebo otevřete Nastavení systému > VPN, přidejte konfiguraci VPN, zvolte IKEv2, L2TP přes IPSec nebo Cisco IPSec a zadejte adresu serveru a přihlašovací údaje od svého poskytovatele.

# 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: Jak použiji soubor .ovpn?

Nainstalujte klienta OpenVPN, importujte profil .ovpn od svého poskytovatele nebo administrátora a připojte se. Soubor obsahuje adresu serveru, port, nastavení UDP nebo TCP a často i certifikáty a klíče.

### 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: Jak nastavím WireGuard ručně?

Vygenerujte pár klíčů pomocí wg genkey a wg pubkey, sdílejte svůj veřejný klíč se serverem a napište konfiguraci obsahující váš soukromý klíč, veřejný klíč protistrany, povolené IP adresy a endpoint. Nástroj wg-quick spojení aktivuje. [2]

### 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: Jak si bezpečně nastavím VPN na domácím routeru?

Ověřte, že váš router podporuje režim VPN klienta, přihlaste se do jeho administrace a nahrajte soubor OpenVPN nebo WireGuard od poskytovatele. Některé routery nejprve potřebují aktualizaci firmwaru; poté tunel používá každé zařízení v síti.

### Q5: Jak obfuskace obchází blokování VPN?

Obfuskace (neboli „Stealth VPN“) maskuje VPN provoz tak, aby vypadal jako běžný provoz HTTPS (port 443). To mu může pomoci 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 mohu ověřit, že mé nové nastavení VPN funguje?

Připojte se a poté navštivte web pro kontrolu IP: měl by ukázat IP adresu a polohu VPN serveru. Spusťte testy úniků DNS a WebRTC a krátce přerušte připojení, abyste ověřili, že kill switch blokuje provoz.

### Q8: Co mám zkontrolovat, když se VPN po nastavení nepřipojí?

Zkontrolujte přihlašovací údaje nebo klíče, adresu serveru a to, zda zvolený port a protokol nejsou blokovány. Zkuste přepnout mezi UDP a TCP nebo na jiný server a přečtěte si chyby v logu připojení aplikace.

### 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: Měla by se VPN spouštět automaticky?

Obvykle ano. Většina aplikací se umí spustit při startu a připojit automaticky, případně na nedůvěryhodné Wi-Fi, takže jste chráněni dřív, než ostatní aplikace začnou odesílat data.

# 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. NATIVNÍ KLIENTI

Windows i macOS obsahují vestavěné VPN klienty s podporou IKEv2 a L2TP/IPsec, takže mnoho připojení lze nastavit bez další aplikace.

### 2. GENEROVÁNÍ KLÍČŮ

Rychlý start WireGuardu vytvoří soukromý klíč pomocí wg genkey a odvodí z něj veřejný klíč pomocí wg pubkey. [2]

### 3. REVOLUCE WIREGUARD

WireGuard má vysoce zjednodušenou kódovou základnu navrženou pro efektivitu, takže se snáze audituje na bezpečnostní zranitelnosti než tradiční protokoly. [1]

### 4. SOUBORY PROFILŮ

Profil .ovpn obsahuje adresu serveru, port, protokol a certifikáty, takže jeden import nastaví připojení OpenVPN.

### 5. VÝCHOZÍ PORTY

OpenVPN běžně používá port 1194, zatímco oficiální příklady WireGuard používají UDP port 51820; firewally a routery mohou vyžadovat povolení těchto portů, aby se tunel připojil.

### 6. HLOUBKOVÁ INSPEKCE PAKETŮ

Hloubková inspekce paketů (DPI) umí rozpoznat a blokovat běžné VPN protokoly; pomoci může přechod na OpenVPN přes TCP port 443 nebo obfuskovaný režim.

### 7. POKRYTÍ ROUTERŮ

VPN na routeru chrání každé zařízení za ním, včetně konzolí a chytrých televizí, které nemohou spustit aplikaci VPN, aniž by bylo nutné cokoli instalovat na jednotlivá zařízení.

### 8. KEEPALIVES

Za NAT nebo firewallem udržuje tunel dosažitelný nastavení PersistentKeepalive ve WireGuardu, běžně 25 sekund. [2]

### 9. OVLADAČE TUN/TAP

OpenVPN je navržen pro práci s virtuálním síťovým rozhraním TUN/TAP, které je dostupné na většině platforem a nastaví se při instalaci klienta. [3]

### 10. SPLIT TUNNELING

Během nastavení vám split tunneling umožní vyloučit vybrané aplikace nebo adresy z VPN, což pomáhá u místních tiskáren nebo aplikací blokujících IP adresy VPN.

# Technické reference a zdroje

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

## AKADEMICKÉ A OBOROVÉ REFERENCE

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

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

[3] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[4] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

# Klíč odpovědí: Konfigurace VPN ve Windows, macOS, Androidu, iOS, Linuxu a na routerech

**1** **Otázka 1** — **Správná odpověď: A**

### POZNÁMKA PRO VYUČUJÍCÍ

Jaký je nejjednodušší způsob nastavení VPN na mobilních zařízeních? → Stažení oficiální aplikace VPN z obchodu s aplikacemi

**2** **Nastavení brány routeru** LATENCE — **Správná odpověď: B**

### POZNÁMKA PRO VYUČUJÍCÍ

VPN na routeru šifruje provoz na bráně a chrání IoT zařízení, konzole a chytré spotřebiče, které nemají možnost nativní instalace aplikace VPN.

**3** **Otázka 3** — **Správná odpověď: A**

### POZNÁMKA PRO VYUČUJÍCÍ

Windows a macOS obsahují vestavěné klienty pro protokoly jako IKEv2 a L2TP/IPsec, takže připojení lze nastavit bez instalace dalšího softwaru.

**4** **Import profilu OpenVPN** ŘÍZENÍ SMĚROVÁNÍ — **Správná odpověď: B**

### POZNÁMKA PRO VYUČUJÍCÍ

Ruční konfigurace vyžadují stažení profilových klíčů.ovpn obsahujících porty cílových serverů, parametry protokolu (UDP/TCP) a kryptografické certifikáty.

**5** **Směrování Split Tunnel** SOUKROMÍ — **Správná odpověď: B**

### POZNÁMKA PRO VYUČUJÍCÍ

Split tunneling umožňuje uživatelům směrovat citlivé pracovní aplikace šifrovaným tunelem, zatímco lokální streamování nebo hry se připojují přímo bez režie VPN.

## Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

**6** **Otázka 6**

**Správná odpověď: Nepravda**

### POZNÁMKA PRO VYUČUJÍCÍ

Nastavení na routeru znamená přihlášení do administrace, kontrolu podpory VPN a nahrání konfiguračních souborů.

**7** **Nativní integrace do OS** RYCHLOSTI

**Správná odpověď: Pravda**

### POZNÁMKA PRO VYUČUJÍCÍ

Hlavní operační systémy mají vestavěnou nativní integraci protokolů pro bezproblémové nastavení zabezpečených připojení.

**8** **Párování klíčů WireGuard** RIZIKO SNIFFINGU

**Správná odpověď: Pravda**

### POZNÁMKA PRO VYUČUJÍCÍ

WireGuard používá asymetrické klíče k navazování bezpečných P2P handshaků místo spoléhání na hesla nebo řetězce CA.

**9** **Blokace místního provozu** FIREWALLY

**Správná odpověď: Nepravda**

### POZNÁMKA PRO VYUČUJÍCÍ

VPN obvykle směrují veřejný internetový provoz a někdy mohou blokovat přístup k tiskárnám v místní síti, pokud nejsou nastaveny jinak.

**10** **Otázka 10**

**Správná odpověď: Pravda**

### POZNÁMKA PRO VYUČUJÍCÍ

Chytré zámky, které neumí spouštět aplikace VPN, potřebují k pokrytí VPN na úrovni routeru.

# 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

| | | | |
|---|---|---|---|
| B 1. VPN aplikace | A 2. Router VPN | E 3. Nativní klient | H 4. Profil .ovpn |
| G 5. Pár klíčů | D 6. Split tunneling | F 7. Nastavení serveru DNS | C 8. Protokoly připojení |

## KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

| | | | |
|---|---|---|---|
| 1 ROUTER | 2 OVPN | 3 NATIVNÍ | 4 PÁR KLÍČŮ |
| 5 APLIKACE | 6 DNS | | |

## KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

| | | | |
|---|---|---|---|
| 1 G – DNSNASTAVENÍ | 2 F – SPLITTUNNELING | 3 B – VPNROUTER | 4 E – PÁRKLÍČŮ |
| 5 C – NATIVNÍKLIENT | 6 H – LOGYPŘIPOJENÍ | 7 D – OVPNPROFIL | 8 A – VPNAPLIKACE |

## POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

**Klíčové pojmy:**
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy VPN aplikace, Router VPN a Nativní klient 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

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

## ŘEŠENÍ KŘÍŽOVKY

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | D | N | S | N | A | S | T | A | V | E | N | Í |
| | | | | | | A | | | | | | | | |
| | | | | | | T | | | | | | | | |
| | | L | O | G | Y | P | Ř | I | P | O | J | E | N | Í |
| | | | | | | V | | | | | | | | V |
| S | P | L | I | T | T | U | N | N | E | L | I | N | G | P |
| | | | | | | Í | | | | | | | | N |
| | | | | P | Á | R | K | L | Í | Č | Ů | | | R |
| | | | | | | L | | | | | | | | O |
| O | V | P | N | P | R | O | F | I | L | | | | | U |
| | | | | | | E | | | | | | | | T |
| | | | | V | P | N | A | P | L | I | K | A | C | E |
| | | | | | | T | | | | | | | | R |

## PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

### VODOROVNÉ NÁPOVĚDY

**1 vodorovně: DNSNASTAVENÍ** Konfigurace adres síťových překladačů proti únikům překladu domén (12 písmen)

**3 vodorovně: LOGYPŘIPOJENÍ** Kontrola chybových výstupů a stavových logů klienta při ladění neúspěšných nastavení (13 písmen)

**5 vodorovně: SPLITTUNNELING** Rozlišení tras provozu, aby vybrané aplikace obcházely šifrovaný tunel (14 písmen)

**6 vodorovně: PÁRKLÍČŮ** Kryptografické tokeny (veřejný/soukromý) nutné k navázání WireGuard handshake (8 písmen)

**7 vodorovně: OVPNPROFIL** Formát souboru OpenVPN obsahující servery, nastavení portů a certifikační klíče (10 písmen)

**8 vodorovně: VPNAPLIKACE** Softwarový balík od předplacené služby pro snadné nastavení jedním kliknutím (11 písmen)

### SVISLÉ NÁPOVĚDY

**2 svisle: NATIVNÍKLIENT** Zabezpečení provozu v nativním nastavení operačního systému bez instalace aplikací (13 písmen)

**4 svisle: VPNROUTER** Šifrování na úrovni brány chránící všechny chytré spotřebiče v místní síti (9 písmen)

# Klíč řešení přesmyček a šifry

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

### KLÍČ K PŘESMYČKÁM

1. PICPLKVANEA — VPNAPLIKACE
2. NVANTNEÍTLIKI — NATIVNÍKLIENT
3. KÁPLÍŮČR — PÁRKLÍČŮ
4. NAASTÍSEVDNN — DNSNASTAVENÍ
5. TOPRURVEN — VPNROUTER
6. IPNOFOVRLP — OVPNPROFIL
7. LNESNPLGTINIUT — SPLITTUNNELING
8. OGPŘEPÍLIONJY — LOGYPŘIPOJENÍ

### KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

**"NAINSTALUJTE BRÁNU SE ZABEZPEČENÝM DÉMONEM"**

# 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.