Jméno: _____ Datum: _____ Body: _____

WireGuard vs OpenVPN Pracovní list

Porovnání protokolů WireGuard a OpenVPN, velikostí kódových základen, rychlosti a kryptografických standardů

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 složitost kódové základny a rychlost auditu protokolů.
- Analyzujte výkonnostní přínosy běhu v prostoru jádra.
- Porovnejte šifry OpenSSL s moderní kryptografií WireGuardu.
- Nastavte páry veřejných a soukromých klíčů pro handshake mezi peery.
- Směrujte VPN provoz přes TCP a UDP porty firewallu.

POKYNY K PRACOVNÍMU LISTU SROVNÁNÍ PROTOKOLŮ

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 auditování moderních protokolů. Zakončete bonusovou aktivitou Mysli rychle.

WIREGUARD VS OPENVPN (ÚVOD)

Výběr protokolu VPN vyžaduje vyvážení rychlosti a možností konfigurace. OpenVPN byl standardem po desetiletí a nabízí flexibilitu konfigurace TCP/UDP. WireGuard je moderní náhrada běžící přímo v prostoru jádra s pouhými 4,000 řádky kódu. Pochopení rozdílů mezi protokoly je klíčem k optimalizaci vašich zabezpečených sítí.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaká je přibližná velikost kódové základny protokolu WireGuard?**
   - A. Zhruba 70,000 řádků
   - B. Přes 100,000 řádků
   - C. Méně než 1,000 řádků
   - D. Kolem 4,000 řádků

2. **2. V jakém prostoru operačního systému běží WireGuard?**
   - A. Uživatelský prostor
   - B. Prostor jádra
   - C. Aplikační prostor
   - D. Virtuální prostor

3. **3. Na kterou kryptografickou knihovnu se OpenVPN primárně spoléhá?**
   - A. ChaCha20-Poly1305
   - B. Kryptografická knihovna OpenSSL
   - C. Framework protokolu Noise
   - D. Kódování DES v prostém textu

4. **4. Jaká je klíčová výkonnostní výhoda WireGuardu oproti OpenVPN?**
   - A. Rychlejší navazování spojení a nižší latence
   - B. Obejitím potřeby veřejných IP adres
   - C. Vestavěná nativní podpora zastaralého vytáčeného připojení
   - D. Nulová zátěž baterie na mobilních zařízeních

5. **5. Jak WireGuard ověřuje připojení protistran (peerů)?**
   - A. Výměnou standardních uživatelských hesel
   - B. Ověřováním certifikátů registrace domény
   - C. Použitím statických párů veřejného a soukromého klíče
   - D. Kontrolou sériových čísel hardwaru

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Kompaktní kódová základna WireGuardu výrazně usnadňuje audit.

○ Pravda ○ Nepravda

7 Otázka 7

7. OpenVPN je obecně rychlejší než WireGuard, protože běží v prostoru jádra.

○ Pravda ○ Nepravda

8 Otázka 8

8. OpenVPN je vysoce konfigurovatelný a podporuje protokoly UDP i TCP.

○ Pravda ○ Nepravda

9 Otázka 9

9. WireGuard používá moderní kryptografii jako ChaCha20 pro rychlé šifrování paketů.

○ Pravda ○ Nepravda

10 Otázka 10

10. WireGuard vyžaduje k autentizaci složitá nastavení certifikační autority.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Moderní protokol _____ pracuje přímo v jádře operačního systému.
2. Starší protokol _____ spoléhá na kryptografickou knihovnu OpenSSL.
3. Režii přepínání kontextu snižuje běh kódu v oblasti zvané _____ .
4. OpenVPN směruje pakety přes virtuální rozhraní a běží v oblasti zvané _____ .
5. K identifikaci partnerů připojení používá WireGuard veřejné a soukromé _____ .
6. Malá velikost kódové základny zlepšuje bezpečnostní vlastnost zvanou _____ .

ZÁSOBNÍK SLOV

AUDITOVATELNOST OPENSSL OPENVPN PÁRY KLÍČŮ PROSTOR JÁDRA TCP/UDP UŽIVATELSKÝ PROSTOR WIREGUARD

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování síťových pojmů

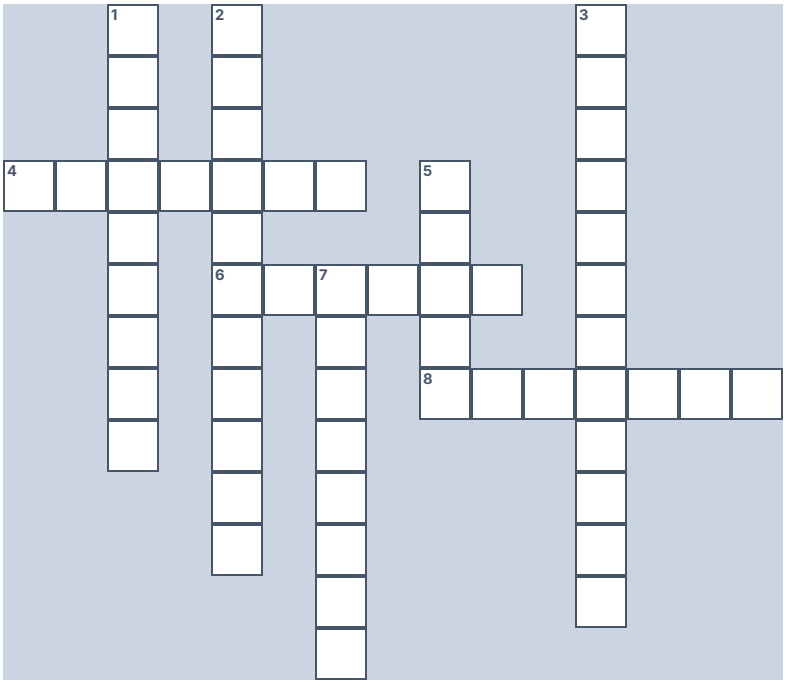
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. WireGuard	A	Oblast běhu, kde OpenVPN pracuje, vytvářející režii přepínání kontextu.
☐	2. OpenVPN	B	Kompaktní velikost kódové základny WireGuard, díky níž se mnohem snáze audituje.
☐	3. Prostor jádra	C	Kryptografická knihovna, na kterou OpenVPN spoléhá při šifrovacích algoritmech.
☐	4. Uživatelský prostor	D	Transportní protokoly podporované OpenVPN; samotný WireGuard běží jen přes UDP.
☐	5. 4,000 řádků	E	Oblast běhu operačního systému, kde WireGuard běží kvůli rychlosti.
☐	6. OpenSSL	F	Asymetrické tokeny používané WireGuardem k ověření spojení mezi peery.
☐	7. Pár klíčů	G	Moderní protokol VPN navržený pro vysokou rychlost a snadné auditování kódu.
☐	8. TCP/UDP	H	Robustní starší protokol s rozsáhlou a složitou konfigurační kódovou základnou.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

4. Robustní starší protokol s rozsáhlou a složitou konfigurační kódovou základnou (7)

6. Transportní protokoly podporované OpenVPN; samotný WireGuard běží jen přes UDP (6)

8. Kryptografická knihovna, na kterou OpenVPN spoléhá pro šifrovací algoritmy (7)

SVISLÉ NÁPOVĚDY

1. Moderní VPN protokol navržený pro vysokou rychlost a snadný audit kódu (9)

2. Uživatelský prostor, kde běží OpenVPN, což vytváří režii přepínání kontextu (11)

3. Kompaktní velikost kódové základny WireGuardu, díky níž se snáz audituje (12)

5. Oblast běhu v jádře operačního systému, kde WireGuard běží kvůli rychlosti (5)

7. Asymetrické tokeny používané WireGuardem k ověření spojení mezi peery (8)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

4 vodorovně: Robustní starší protokol s rozsáhlou a složitou konfigurační kódovou základnou (7 písmen):

6 vodorovně: Transportní protokoly podporované OpenVPN; samotný WireGuard běží jen přes UDP (6 písmen):

8 vodorovně: Kryptografická knihovna, na kterou OpenVPN spoléhá pro šifrovací algoritmy (7 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Moderní VPN protokol navržený pro vysokou rychlost a snadný audit kódu (9 písmen):

2 svisle: Uživatelský prostor, kde běží OpenVPN, což vytváří režii přepínání kontextu (11 písmen):

3 svisle: Kompaktní velikost kódové základny WireGuardu, díky níž se snáz audituje (12 písmen):

5 svisle: Oblast běhu v jádře operačního systému, kde WireGuard běží kvůli rychlosti (5 písmen):

7 svisle: Asymetrické tokeny používané WireGuardem k ověření spojení mezi peery (8 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

WIREGUARD OPENVPN JÁDRO UŽIVATELSKÝ KOMPAKTNÍKÓD OPENSSL PÁRKLÍČŮ TCPUDP

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. OPENVPN**
- **C. JÁDRO**
- **D. UŽIVATELSKÝ**
- **E. KOMPAKTNÍKÓD**
- **F. OPENSSL**
- **G. PÁRKLÍČŮ**
- **H. TCPUDP**

DEFINICE A POLE K PŘIŘAZENÍ

1. Kryptografická knihovna, na kterou OpenVPN spoléhá pro šifrovací algoritmy.
2. Oblast běhu v jádře operačního systému, kde WireGuard běží kvůli rychlosti.
3. Robustní starší protokol s rozsáhlou a složitou konfigurační kódovou základnou.
4. Asymetrické tokeny používané WireGuardem k ověření spojení mezi peery.
5. Transportní protokoly podporované OpenVPN; samotný WireGuard běží jen přes UDP.
6. Kompaktní velikost kódové základny WireGuardu, díky níž se snáz audituje.
7. Moderní VPN protokol navržený pro vysokou rychlost a snadný audit kódu.
8. Uživatelský prostor, kde běží OpenVPN, což vytváří režii přepínání kontextu.

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. JORDÁ
3. KONTÓÍMKDA KP
4. KČŮÍLPÁR
5. VNNEOPP
6. AÝTLKSUŽEIV
7. OSSLPNE
8. PPTDUC

Bonusová aktivita: Mysli rychle

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

1	Důvody, proč zvolit WireGuard			
2	Sliby, které dává dobrý poskytovatel VPN			
3	Důvody, proč zvolit OpenVPN			
4	Důvody, proč používat VPN na cestách			
5	Věci, které vidí váš poskytovatel internetu			
6	Způsoby, jak poznat falešnou Wi-Fi síť			
7	Mýty o VPN			
8	Místa, kde byste použili VPN			
9	Rychlé věci v každodenním životě			
10	Věci, před kterými vás VPN neochrání			
11	Věci, které usnadňují kontrolu kódu			
12	Věci, které VPN dokáže skrýt			
13	Rozdíly mezi WireGuard a OpenVPN			
14	Slova související se soukromím			
15	Názvy šifrování, které znáte			

Kontrolní bod 8: Případové studie VPN

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

SARAH (STUDENTKA V KAVÁRNĚ)

👩‍💻 "Ahoj! Jsem na kavárenské Wi-Fi a moje aplikace VPN mi dává na výběr WireGuard nebo OpenVPN. Videohovory mi pořád padají, když přecházím mezi sítí kavárny a hotspotem telefonu. Který protokol si mám vybrat a proč by přepínání zvládl lépe?"

ALEX (CESTUJÍCÍ STUDENT)

👩‍💻 "Jsem v zahraničí na hotelové síti, která zřejmě blokuje většinu provozu VPN. WireGuard se vůbec nepřipojí, ale potřebuji se dostat ke školním zdrojům doma. Co je pravděpodobně blokováno a jak by mi OpenVPN pomohl projít?"

Kontrolní bod 9: Dešifrování šifry

K dokončení výcviku auditování protokolů dešifrujte tuto skrytou zprávu o vykonávání v prostoru jádra.

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

35	38	19	10	21	30	8		22	24	8	20	35	24	20		40	1

26	38	4	13	18	8	16	29	15		30	32	20	8	18

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 na protokolech záleží?

Protokol rozhoduje o tom, jak vaše VPN staví tunel, jaká kryptografie chrání vaše data a jak rychle se připojuje a znovu připojuje. WireGuard a OpenVPN jsou dva open source protokoly, které nabízí většina VPN aplikací, a každý volí jiný kompromis mezi jednoduchostí, rychlostí a konfigurovatelností.

Q3: Je jeden z nich soukromější než druhý?

Ani jeden protokol vás neučiní anonymními. Oba šifrují provoz tunelu silnými šiframi; vaše soukromí závisí hlavně na tom, co poskytovatel VPN loguje a jak spravuje klíče, účty a servery.

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: Jsou oba open source?

Ano. WireGuard i komunitní edice OpenVPN zveřejňují svůj zdrojový kód, takže je mohou prověřovat nezávislí výzkumníci. Malá kódová základna WireGuard činí úplnou revizi mnohem rychlejší.

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

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

Q6: Který z nich je rychlejší?

WireGuard je obvykle rychlejší: běží v jádře, používá úsporné šifrování ChaCha20-Poly1305 a rychle dokončuje handshaky. OpenVPN má vyšší režii, ale skutečné rychlosti závisejí i na zatížení serveru a vzdálenosti.

Q7: Mohou oba běžet přes TCP i UDP?

Ne. OpenVPN může běžet přes UDP nebo TCP a režim TCP pomáhá na sítích blokujících UDP. WireGuard posílá své pakety pouze přes UDP, takže může selhat na sítích, které povolují jen TCP. [4]

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 na telefonu používat WireGuard i OpenVPN?

Ano. WireGuard je multiplatformní, s aplikacemi pro Windows, macOS, Linux, iOS a Android, a klienty OpenVPN existují pro stejné systémy. Většina aplikací VPN vám umožní vybrat kterýkoli z nich. [1]

Q10: Proč je WireGuard tak malý?

WireGuard podporuje jednu pevnou sadu moderních šifer místo mnoha možností. Jeho linuxová implementace potřebuje méně než 4,000 řádků kódu, což usnadňuje audit oproti větším VPN kódovým základnám. [3]

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: Které šifry používá WireGuard?

WireGuard používá ChaCha20 s Poly1305 pro šifrování, Curve25519 pro výměnu klíčů, BLAKE2s pro hashování a framework Noise pro handshake. Neexistuje vyjednávání šifer, takže uživatelé nemohou zvolit slabou možnost. [2]

Q3: Jaké šifry a knihovny může OpenVPN používat?

OpenVPN je těsně provázán s knihovnou OpenSSL a k výměně klíčů používá TLS. Správci mohou volit šifry datového kanálu, jako je AES-256-GCM, což přidává flexibilitu, ale i prostor pro slabá nastavení. [4]

Q4: Jak jednotlivé protokoly ověřují protistrany?

Peery WireGuard se navzájem identifikují statickými veřejnými klíči, podobně jako při výměně SSH klíčů, a každý klíč se mapuje na povolené tunelové IP. OpenVPN obvykle spoléhá na certifikační autoritu s certifikáty X.509, často v kombinaci s uživatelským jménem a heslem.

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 se stane při přechodu z Wi-Fi na mobilní data?

WireGuard je bezstavový: posílá pakety z nové adresy a tunel po rychlém handshaku pokračuje. OpenVPN udržuje stav relace, takže změna sítě může vyžadovat opětovné připojení, které trvá o něco déle.

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: Je OpenVPN stále dobrou volbou, když je WireGuard rychlejší?

Ano. OpenVPN je vyzrálý a široce nasazený, běží přes TCP, když je UDP blokováno, a podporuje podniková nasazení s certifikáty. Mnoho poskytovatelů nabízí oba protokoly, takže uživatelé mohou přepnout, pokud je jeden blokovaný nebo pomalý.

Q9: Které porty používají?

Standardní port OpenVPN je 1194, ale lze jej přesunout na libovolný UDP nebo TCP port, včetně 443. WireGuard naslouchá na UDP portu nastaveném v konfiguraci; 51820 je port používaný v jeho oficiálních příkladech.

Q10: Který protokol se snadněji nastavuje ručně?

WireGuard je obvykle jednodušší: vygenerujete pár klíčů, vyměníte veřejné klíče a uvedete povolené IP. OpenVPN potřebuje certifikáty, CA a více voleb, i když profily .ovpn je sdružují do jednoho souboru.

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) byl vyvinut skupinou dodavatelů včetně Microsoftu a publikován jako RFC 2637 v červenci 1999 pro podporu VPN se vzdáleným přístupem. [6]

2. DVA TRANSPORTY

OpenVPN může vést svůj tunel přes UDP nebo TCP a v režimu TLS sdílí jeho řídicí a datový kanál jediný port. [4]

3. REVOLUCE WIREGUARD

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

4. MODERNÍ KRYPTOGRAFIE

WireGuard kombinuje ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 a HKDF v rámci frameworku Noise, bez voleb šifer, které by uživatelé mohli zvolit špatně. [2]

5. OPENSSL UVNITŘ OPENVPN

OpenVPN je těsně provázán s knihovnou OpenSSL a odvozuje z ní mnoho svých kryptografických schopností, včetně TLS používaného k výměně klíčů. [4]

6. HLOUBKOVÁ INSPEKCE PAKETŮ

Hloubková inspekce paketů (DPI) zkoumá obsah paketů a vzorce provozu, nejen hlavičky, a některé firewally ji používají k detekci a blokování běžných VPN protokolů.

7. KLÍČE VE STYLU SSH

Připojení WireGuard se nastavují výměnou jednoduchých veřejných klíčů, podobně jako u SSH klíčů, bez potřeby certifikační autority. [1]

8. MULTIPLATFORMNÍ

WireGuard byl nejprve vydán pro linuxové jádro a nyní je dostupný pro Windows, macOS, BSD, iOS a Android, takže stejný protokol funguje na většině zařízení. [1]

9. DOPŘEDNÁ BEZPEČNOST

WireGuard opakuje svůj Noise_IK handshake každých několik minut k rotaci symetrických klíčů relace, což zajišťuje dokonalé dopředné utajení, i kdyby dlouhodobý klíč později unikl. [2]

10. ROZHRANÍ TUN/TAP

OpenVPN je navržen pro práci s virtuálním síťovým rozhraním TUN/TAP, které je dostupné na většině platforem a přenáší pakety tunelu. [4]

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.). Protocol & Cryptography.

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

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Klíč odpovědí: Porovnání protokolů WireGuard a OpenVPN, velikostí kódové základny, rychlosti a kryptografických standardů

1 **Velikost kódu WireGuard** PROTOKOLY **Správná odpověď: D**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard je extrémně kompaktní, běží na přibližně 4,000 řádcích kódu. To udržuje malou útočnou plochu a usnadňuje audit.

2 **Rychlost v prostoru jádra** LATENCE **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Díky přímému běhu v prostoru jádra se WireGuard vyhýbá režii přepínání kontextu, což umožňuje vysokou propustnost.

3 **Otázka 3** **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

OpenVPN je těsně integrován s OpenSSL, které dodává šifry jako AES-GCM a činí ho vysoce konfigurovatelným, ale složitějším.

4 **Výkon protokolu** ŘÍZENÍ SMĚROVÁNÍ **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard navazuje handshake v řádu milisekund a okamžitě reaguje na síťový roaming (např. přechod z Wi-Fi na mobilní data).

5 **Asymetrická kryptografie** SOUKROMÍ **Správná odpověď: C**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard používá Cryptokey Routing, který přiřazuje veřejné klíče k povoleným tunelovým IP adresám, podobně jako konfigurace SSH.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

Linuxová implementace WireGuardu má méně než 4,000 řádků, takže ji bezpečnostní týmy mohou prověřit mnohem rychleji než mnohem větší kódové základny VPN, jako je OpenVPN.

7 **Latence uživatelského prostoru** RYCHLOSTI **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

OpenVPN běží v uživatelském prostoru a předává pakety tam a zpět z virtuálního rozhraní jádra, což přidává režii přepínání kontextu (pokud se nepoužije offload v jádře, jako je OpenVPN DCO).

8 **Konfigurace OpenVPN** RIZIKO SNIFFINGU **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

OpenVPN podporuje běh přes TCP (pro spolehlivost/obcházení firewallů) nebo UDP (pro rychlost), díky čemuž je kompatibilní se složitými podnikovými firewally.

9 **Moderní kryptografie** FIREWALLY **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard opouští zastaralé šifry ve prospěch moderních, bezpečných primitiv jako ChaCha20 a Poly1305, která běží rychle na mobilních procesorech.

10 **Zjednodušení párů klíčů** NO-LOGS **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard nepoužívá certifikáty ani složité hierarchie CA; spoléhá na jednoduché páry veřejného/soukromého klíče vyměněné mezi peery.

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. WireGuard	H 2. OpenVPN	E 3. Prostor jádra	A 4. Uživatelský prostor
B 5. 4,000 řádků	C 6. OpenSSL	F 7. Pár klíčů	D 8. TCP/UDP

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 WIREGUARD	2 OPENVPN	3 PROSTOR JÁDRA	4 UŽIVATELSKÝ PROSTOR
5 PÁRY KLÍČŮ	6 AUDITOVATELNOST		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 F – OPENSSL	2 C – JÁDRO	3 B – OPENVPN	4 G – PÁRKLÍČŮ
5 H – TCPUDP	6 E – KOMPAKTNÍKÓD	7 A – WIREGUARD	8 D – UŽIVATELSKÝ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy WireGuard, OpenVPN a Prostor jádra a ke každému uvést příklad.

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

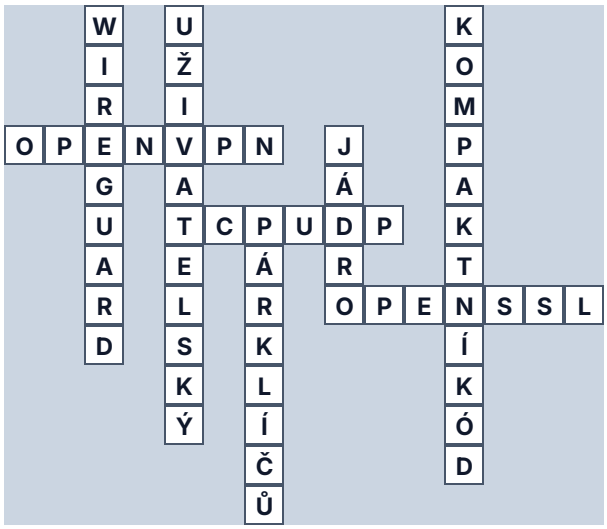
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

4 vodorovně: OPENVPN Robustní starší protokol s rozsáhlou a složitou konfigurační kódovou základnou (7 písmen)

6 vodorovně: TCPUDP Transportní protokoly podporované OpenVPN; samotný WireGuard běží jen přes UDP (6 písmen)

8 vodorovně: OPENSSL Kryptografická knihovna, na kterou OpenVPN spoléhá pro šifrovací algoritmy (7 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: WIREGUARD Moderní VPN protokol navržený pro vysokou rychlost a snadný audit kódu (9 písmen)

2 svisle: UŽIVATELSKÝ Uživatelský prostor, kde běží OpenVPN, což vytváří režii přepínání kontextu (11 písmen)

3 svisle: KOMPAKTNÍKÓD Kompaktní velikost kódové základny WireGuardu, díky níž se snáz audituje (12 písmen)

5 svisle: JÁDRO Oblast běhu v jádře operačního systému, kde WireGuard běží kvůli rychlosti (5 písmen)

7 svisle: PÁRKLÍČŮ Asymetrické tokeny používané WireGuardem k ověření spojení mezi peery (8 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. JORDÁ — **JÁDRO**
3. KONTÓÍMKDAKP — **KOMPAKTNÍKÓD**
4. KČŮÍLPÁR — **PÁRKLÍČŮ**
5. VNNEOPP — **OPENVPN**
6. AÝTLKSUŽEIV — **UŽIVATELSKÝ**
7. OSSLPNE — **OPENSSL**
8. PPTDUC — **TCPUDP**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"VYMĚŇTE OPENVPN ZA RYCHLEJŠÍ TUNEL"

Klíč k případovým studiím

A Scénář A: Volba protokolu

SNIFFING A ŠIFROVÁNÍ | Sarahino dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Doporučení: WireGuard. Jeho odlehčený, bezspojový návrh umožňuje tunelu rychlé zotavení při změně sítě a ChaCha20-Poly1305 udržuje šifrování rychlé.
- Zabezpečení: Oba protokoly šifrují její provoz na kavárenské Wi-Fi, takže při správné konfiguraci chrání její přihlášení kterýkoli z nich; volba ovlivňuje hlavně rychlost a stabilitu.

B Scénář B: Jak obejít blokování VPN

GEOBLOKACE A IP ADRESY | Alexovo dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Proč blokováno: WireGuard používá pouze UDP a hotelový firewall pravděpodobně blokuje UDP nebo rozpoznává pakety WireGuard filtrováním či hloubkovou inspekcí paketů.
- Jak OpenVPN pomáhá: Může běžet přes TCP, včetně portu 443 používaného HTTPS, který hotelové firewally zřídka blokují úplně, protože na něm závisí prohlížení webu.