Imię i nazwisko: _____ Data: _____ Wynik: _____

# Proxy a VPN Karta pracy

Porównanie serwerów proxy i wirtualnych sieci prywatnych, różnic w szyfrowaniu oraz routingu aplikacji a routingu w całym systemie

## PRZEGLĄD NAUKI: VPN

**UCZEŃ**
**STATUS STUDENTA**
Ścieżka obrońcy sieci

**BEZPIECZNY**
**STAN POŁĄCZENIA**
Ochrona pakietów danych

**AKTYWNE**
**OCHRONA PRZED WYCIEKAMI**
Ochrona przed wyciekami DNS i IPv6

**Witaj!** Ten pakiet ćwiczeń przeprowadzi cię przez podstawowe zasady wirtualnych sieci prywatnych (VPN). Poznasz, jak zaszyfrowane tunele zabezpieczają Twoje dane, jak działają protokoły sieciowe oraz jak rozpoznawać i ograniczać wycieki prywatności.

### PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj pojęcia i protokoły VPN.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

**Otwórz przewodnik VPN.com po VPN**

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

# Twoja ścieżka nauki: VPN

- Porównaj proxy aplikacji z szyfrowaniem VPN w całym systemie.
- Rozpoznaj możliwości SOCKS5 w porównaniu z podstawowymi serwerami proxy HTTP.
- Przeanalizuj, w jaki sposób proxy działające w przeglądarce pozostawiają aplikacje w tle bez ochrony.
- Zrozum, jak dostawcy internetu rejestrują niezaszyfrowany ruch w tunelach proxy.
- Wybierz odpowiednie narzędzie do routingu w zależności od potrzeb dotyczących prędkości i bezpieczeństwa.

## INSTRUKCJE DO KARTY PRACY: PORÓWNANIE PROXY

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu porównywania serwerów proxy i VPN. Zakończ zadaniem dodatkowym Myśl szybko.

## PROXY A VPN (WPROWADZENIE)

Serwery proxy i VPN pełnią różne funkcje w zakresie prywatności cyfrowej. Serwer proxy działa jako przekierowanie w warstwie aplikacji, maskując twój adres IP dla wybranych programów bez szyfrowania danych. VPN działa na poziomie sieci, zabezpieczając cały ruch systemowy szyfrowaniem. Wybór odpowiedniego narzędzia zależy od twoich wymagań dotyczących bezpieczeństwa.

**PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.**

## Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **1. Na której warstwie modelu OSI działa standardowe proxy HTTP?**
   - A. Warstwa fizyczna
   - B. Warstwa sieciowa
   - C. Warstwa aplikacji
   - D. Warstwa łącza danych

2. **2. Jaka jest kluczowa zaleta protokołu SOCKS5 w porównaniu ze standardowymi serwerami proxy HTTP?**
   - A. Wymusza pełne szyfrowanie ładunku
   - B. Obsługuje routing dowolnego ruchu TCP/UDP
   - C. Jest odporna na wycieki DNS
   - D. Działa bezpośrednio w przestrzeni jądra

3. **3. Dlaczego VPN jest zazwyczaj bezpieczniejszy niż serwer proxy?**
   - A. Działa na szybszym sprzęcie zdalnym
   - B. Szyfruje cały ruch sieciowy w całym systemie
   - C. Nie wymaga lokalnych tablic routingu
   - D. Całkowicie eliminuje opóźnienia sieci

4. **4. Jaki typ proxy domyślnie przekierowuje ruch bez żadnego szyfrowania?**
   - A. Podstawowe proxy HTTP
   - B. Szyfrowane proxy HTTPS
   - C. Bezpieczny klient WireGuard
   - D. Serwer VPN z obfuskacją

5. **5. Co dzieje się z ruchem aplikacji działających w tle, gdy używasz proxy w przeglądarce?**
   - A. Jest szyfrowane automatycznie
   - B. Jest blokowane przez serwer proxy
   - C. Jest kierowany przez tunel proxy
   - D. Omija proxy i ujawnia Twoje IP

## Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

**6 Pytanie 6**

6. Proxy SOCKS5 szyfruje wszystkie dane pakietów przechodzące przez serwer.

○ Prawda ○ Fałsz

**7 Pytanie 7**

7. VPN działa w warstwie sieciowej, aby zabezpieczyć cały ruch systemowy.

○ Prawda ○ Fałsz

**8 Pytanie 8**

8. Serwery proxy są zazwyczaj szybsze niż VPN, ponieważ wykonują głębokie szyfrowanie pakietów.

○ Prawda ○ Fałsz

**9 Pytanie 9**

9. Skonfigurowanie proxy wymaga ustawienia przekierowań ruchu wewnątrz konkretnych aplikacji.

○ Prawda ○ Fałsz

**10 Pytanie 10**

10. Używanie serwera proxy nie zabezpiecza Twojego ruchu danych przed śledzeniem przez lokalnego dostawcę internetu.

○ Prawda ○ Fałsz

# Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Serwer _____ warstwy aplikacji przekierowuje ruch wybranej przeglądarki bez zabezpieczania innych aplikacji.

2. Solidny _____ enkapsuluje i szyfruje wszystkie pakiety danych urządzenia.

3. Protokół _____ znajduje się między warstwą aplikacji a transportową.

4. Serwery proxy HTTP działają w warstwie aplikacji modelu OSI, która jest określana jako: _____ .

5. Standardowe serwery proxy nie zapewniają zabezpieczenia ładunku w postaci: _____ , przez co dane są podatne na ataki.

6. VPN chroni wszystkie adaptery sieciowe w trybie obejmującym: _____ .

**BANK SŁÓW**

CAŁY SYSTEM | OBSŁUGA UDP | PROXY | SOCKS5 | SZYFROWANIE | TUNEL VPN | WARSTWA SIÓDMA | WIDOCZNOŚĆ

**Wpisz tutaj swoje odpowiedzi:**

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

# Punkt kontrolny 4: Dopasowywanie pojęć sieciowych

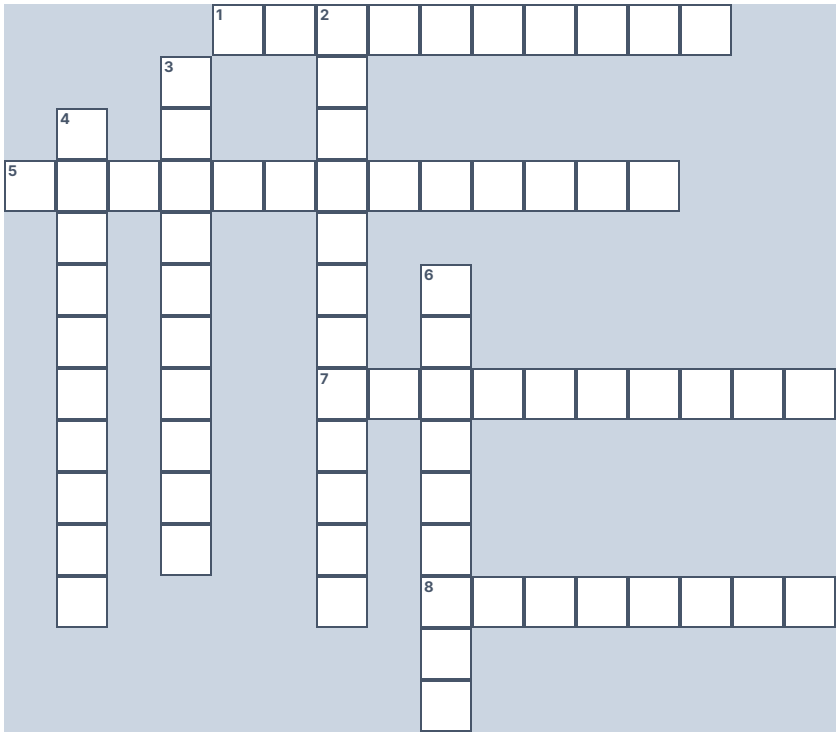
## DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

| | | | |
|---|---|---|---|
| ☐ | 1. Proxy HTTP | A | Trasowanie na poziomie systemu operacyjnego, które szyfruje cały ruch aplikacji. |
| ☐ | 2. Proxy SOCKS5 | B | Warstwa aplikacji, w której działają standardowe protokoły serwerów proxy dla sieci web. |
| ☐ | 3. Tunel VPN | C | Zdolność SOCKS5 do przekazywania UDP oraz TCP, w przeciwieństwie do zwykłych serwerów proxy HTTP. |
| ☐ | 4. Obejmujący cały system | D | Rozszerzenie klienta, które ukrywa ruch wyłącznie wewnątrz piaskownicy przeglądarki. |
| ☐ | 5. Warstwa 7 modelu OSI | E | Szyfrowanie i enkapsulacja obejmujące cały ruch urządzenia działający w tle. |
| ☐ | 6. Obsługa UDP | F | Stan ruchu, w którym niezaszyfrowane dane proxy pozostają widoczne dla dostawców internetu. |
| ☐ | 7. Proxy przeglądarki | G | Proxy warstwy aplikacji, które przekierowuje ruch wybranej przeglądarki internetowej. |
| ☐ | 8. Widoczność dla ISP | H | Protokół proxy działający między warstwą aplikacji a warstwą transportową, bez szyfrowania. |

# Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.



## POZIOMO

**1. Stan ruchu, w którym niezaszyfrowane dane proxy pozostają widoczne dla dostawców internetu (10)**

**5. Warstwa aplikacji, w której działają standardowe protokoły proxy WWW (13)**

**7. Protokół proxy działający między warstwą aplikacji a transportową, bez szyfrowania (10)**

**8. Szyfrowanie i enkapsulacja obejmujące cały ruch urządzenia działający w tle (8)**

## PIONOWO

**2. Rozszerzenie klienta, które ukrywa ruch tylko wewnątrz piaskownicy przeglądarki (12)**

**3. Zdolność SOCKS5 do przekazywania UDP oraz TCP, w przeciwieństwie do zwykłych proxy HTTP (10)**

**4. Routing na poziomie systemu operacyjnego, który szyfruje ruch wszystkich aplikacji (10)**

**6. Proxy warstwy aplikacji przekierowujące ruch wybranej przeglądarki internetowej (9)**

# Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

## POZIOMO

**1 poziomo: Stan ruchu, w którym niezaszyfrowane dane proxy pozostają widoczne dla dostawców internetu (10 liter):**

**5 poziomo: Warstwa aplikacji, w której działają standardowe protokoły proxy WWW (13 liter):**

**7 poziomo: Protokół proxy działający między warstwą aplikacji a transportową, bez szyfrowania (10 liter):**

**8 poziomo: Szyfrowanie i enkapsulacja obejmujące cały ruch urządzenia działający w tle (8 liter):**

## PIONOWO

**2 pionowo: Rozszerzenie klienta, które ukrywa ruch tylko wewnątrz piaskownicy przeglądarki (12 liter):**

**3 pionowo: Zdolność SOCKS5 do przekazywania UDP oraz TCP, w przeciwieństwie do zwykłych proxy HTTP (10 liter):**

**4 pionowo: Routing na poziomie systemu operacyjnego, który szyfruje ruch wszystkich aplikacji (10 liter):**

**6 pionowo: Proxy warstwy aplikacji przekierowujące ruch wybranej przeglądarki internetowej (9 liter):**

## Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Y | H | P | T | H | Ó | V | P | U | O | U | T | K | A | E |
| X | Ó | N | L | Ą | Ń | V | R | F | F | P | Q | Y | Ź | J |
| O | K | V | K | W | I | D | O | C | Z | N | O | Ś | Ć | Ź |
| R | X | Z | Ó | K | I | Ż | X | I | J | N | A | E | I | Ą |
| P | M | E | T | S | Y | S | Y | Ł | A | C | Ś | A | K | Ę |
| K | X | E | K | Ż | K | D | S | L | Q | N | K | A | Ę | O |
| E | K | Ń | Ć | N | C | Ć | O | G | I | Ą | Ą | Ó | R | Ł |
| T | P | W | T | I | Ź | Ę | C | Ź | S | G | Y | X | H | Ę |
| A | R | T | Ń | U | K | R | K | Ć | T | S | Ł | P | Ł | N |
| D | Ś | H | L | P | H | Ź | S | Ó | Ł | X | V | Ń | Z | Q |
| O | W | A | R | S | T | W | A | S | I | Ó | D | M | A | Q |
| D | Ą | A | P | R | O | X | Y | H | T | T | P | Ł | Ó | N |
| Ą | Ł | O | B | S | Ł | U | G | A | U | D | P | I | Ę | J |
| Ń | Z | B | Ż | Ż | Ź | B | N | V | Y | M | C | Ę | Ó | X |
| P | N | P | V | L | E | N | U | T | Q | Y | G | D | Ź | B |

**LISTA SŁÓW**

PROXYHTTP PROXYSOCKS TUNELVPN CAŁYSYSTEM WARSTWASIÓDMA OBSŁUGAUDP DODATEKPROXY WIDOCZNOŚĆ

# Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

**TERMINY ZE SŁOWNICZKA**

- **A. PROXYHTTP**
- **B. PROXYSOCKS**
- **C. TUNELVPN**
- **D. CAŁYSYSTEM**
- **E. WARSTWASIÓDMA**
- **F. OBSŁUGAUDP**
- **G. DODATEKPROXY**
- **H. WIDOCZNOŚĆ**

**DEFINICJE I POLA DOPASOWANIA**

1. Warstwa aplikacji, w której działają standardowe protokoły proxy WWW.
2. Zdolność SOCKS5 do przekazywania UDP oraz TCP, w przeciwieństwie do zwykłych proxy HTTP.
3. Proxy warstwy aplikacji przekierowujące ruch wybranej przeglądarki internetowej.
4. Rozszerzenie klienta, które ukrywa ruch tylko wewnątrz piaskownicy przeglądarki.
5. Szyfrowanie i enkapsulacja obejmujące cały ruch urządzenia działający w tle.
6. Routing na poziomie systemu operacyjnego, który szyfruje ruch wszystkich aplikacji.
7. Stan ruchu, w którym niezaszyfrowane dane proxy pozostają widoczne dla dostawców internetu.
8. Protokół proxy działający między warstwą aplikacji a transportową, bez szyfrowania.

## Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z VPN. Wpisz odpowiedzi w polach do wypełnienia.

1. HYXRPTTPO
2. ETNUPVLN
3. AWSÓIMARAT WDS
4. XPTDKYEORD OA
5. CSSRXOYPKO
6. ESYSTCAYMŁ
7. BŁOAGUDPUS
8. ŚOZĆWCINOD

# Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

| | | | | |
|---|---|---|---|---|
| 1 | Różnice między serwerem proxy a VPN | | | |
| 2 | Rzeczy pozostawione bez szyfrowania bez VPN | | | |
| 3 | Sposoby na rozpoznanie fałszywej sieci Wi-Fi | | | |
| 4 | Rzeczy, które pośrednik robi w codziennym życiu | | | |
| 5 | Sytuacje, w których wystarczy serwer proxy | | | |
| 6 | Urządzenia, które mogą korzystać z VPN | | | |
| 7 | Rodzaje serwerów proxy, które znasz | | | |
| 8 | Rzeczy, które VPN może ukryć | | | |
| 9 | Mity o VPN | | | |
| 10 | Obietnice, które składa dobry dostawca VPN | | | |
| 11 | Rzeczy, przed którymi VPN cię nie ochroni | | | |
| 12 | Słowa z tej karty pracy, które chcesz zapamiętać | | | |
| 13 | Powody, dla których warto używać VPN podczas podróży | | | |
| 14 | Sytuacje, w których chcesz VPN | | | |
| 15 | Miejsca, w których używałbyś VPN | | | |

# Punkt kontrolny 8: Studia przypadków dotyczących VPN

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

### SARAH (STUDENTKA W KAWIARNI)

👩‍💻 „Hej! Jestem w Coffee & Bytes w otwartej sieci o nazwie 'Free_Wi-Fi_No_Password'. Muszę zalogować się na szkolną pocztę, a znajomy mówi, że darmowe proxy w przeglądarce wystarczy, żeby być bezpiecznym. Czy proxy ochroni moje logowanie i pliki, czy potrzebuję VPN?”

### ALEX (STUDENT PODRÓŻNIK)

👩‍💻 „Jestem za granicą, a dokument biologiczny hostowany w moim kraju pokazuje komunikat 'Ten film nie jest dostępny w Twojej obecnej lokalizacji.' Kolega z klasy używa proxy, a ja mam VPN. Dlaczego jestem zablokowany i które narzędzie zadziałałoby lepiej?”

## Punkt kontrolny 9: Odszyfruj szyfr

Aby ukończyć szkolenie z porównywania serwerów proxy, odszyfruj tę tajną wiadomość o bezpiecznym tunelowaniu.

**KLUCZ SZYFROWANIA LITERA-LICZBA**

**A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12**

**J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24**

**S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35**

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 22 | 24 | 33 | 7 | 14 | 12 | 7 | 24 | 28 | 13 | | 25 | 30 | 21 | 13 | | 24 | 28 | 4 | 11 |
| | | | | | | | | | | | | | | | | | | | |
| 22 | 24 | 33 | 7 | 33 | | 25 | 7 | 24 | 30 | 7 | 24 | | 22 | 24 | 20 | 31 | 32 | | |
| | | | | | | | | | | | | | | | | | | | |

**Odszyfrowana wiadomość:**

**WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).**

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o VPN (Część A)

Przejrzyj najczęstsze pytania i odpowiedzi, które potencjalni klienci mają na temat korzystania z wirtualnych sieci prywatnych.

### Q1: Czym jest VPN i jak działa?

Wirtualna sieć prywatna (VPN) szyfruje Twoje połączenie z internetem i kieruje ruch przez bezpieczny zdalny serwer. Maskuje to Twój publiczny adres IP i ogranicza to, co lokalni obserwatorzy sieci i Twój ISP mogą zobaczyć w ruchu kierowanym przez tunel VPN.

### Q2: Czym jest serwer proxy?

Serwer proxy to pośrednik, który przekazuje żądania między Twoją aplikacją a serwerem docelowym. Strona widzi adres IP proxy zamiast Twojego, ale przekierowywany jest tylko ruch z aplikacji skonfigurowanych do używania proxy, a podstawowe proxy nie szyfruje tego ruchu.

### Q3: Czy VPN zapewnia mi całkowitą anonimowość w internecie?

Nie. Chociaż VPN ukrywa twój adres IP i szyfruje ruch, nadal możesz być śledzony za pomocą plików cookie przeglądarki, aktywnych kont (np. Google lub Facebook), fingerprintingu przeglądarki lub jeśli dostawca VPN rejestruje twoje dane.

### Q4: Czy VPN spowolni moje połączenie z internetem?

Tak, nieznacznie. Proces szyfrowania i fizyczna odległość od serwera VPN dodają opóźnienie i narzut. Wpływ zależy od dostawcy, protokołu, odległości serwera, urządzenia i warunków sieciowych.

### Q5: Czy serwer proxy to VPN?

Nie. Proxy przekazuje ruch dla wybranych aplikacji, zwykle bez szyfrowania. VPN buduje zaszyfrowany tunel na warstwie sieciowej, który przenosi cały ruch urządzenia, w tym aplikacje działające w tle.

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o VPN (Część B)

Przejrzyj najczęstsze pytania i odpowiedzi, które potencjalni klienci mają na temat korzystania z wirtualnych sieci prywatnych.

### Q6: Czy mogę używać darmowego serwera proxy?

Możesz, ale darmowe serwery proxy często prowadzą nieznani operatorzy. Ponieważ podstawowe proxy nie szyfruje ruchu, jego operator może widzieć, a nawet zmieniać niezaszyfrowane strony. Sprawdź, kto prowadzi usługę, zanim z niej skorzystasz.

### Q7: Czy serwer proxy przechowuje logi?

Może. Proxy obsługuje każde żądanie, które przekazuje, więc jego operator może rejestrować Twój adres IP, odwiedzane strony i czas. Sprawdź, kto je prowadzi i co mówi jego polityka prywatności.

### Q8: Kiedy wystarczy serwer proxy?

Proxy może wystarczyć do zadań o niskim ryzyku, takich jak zmiana pozornej lokalizacji jednej przeglądarki. Do bankowości, publicznych sieci Wi-Fi lub ochrony każdej aplikacji na urządzeniu bezpieczniejszym wyborem jest VPN, ponieważ szyfruje cały ruch.

### Q9: Czy serwer proxy może chronić wszystkie aplikacje na moim telefonie?

Nie. Używają go tylko aplikacje, które respektują ustawienie proxy; reszta łączy się bezpośrednio. Aplikacja VPN kieruje natomiast wszystkie aplikacje telefonu przez swój zaszyfrowany tunel.

### Q10: Czym jest serwer proxy SOCKS5?

SOCKS5, zdefiniowany w RFC 1928, to protokół proxy znajdujący się między warstwą aplikacji a warstwą transportową. Może przekazywać połączenia TCP i datagramy UDP oraz obsługuje uwierzytelnianie, ale nie ma wbudowanego szyfrowania. [1]

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o VPN (Część C)

Poznaj techniczne i strukturalne aspekty wirtualnych sieci prywatnych i bezpiecznych protokołów tunelowania.

### Q1: W jakich warstwach sieci działają serwery proxy i VPN?

Proxy HTTP działa w warstwie aplikacji (warstwa 7) i rozumie żądania internetowe. SOCKS5 znajduje się między warstwą aplikacji a warstwą transportową. Protokoły VPN, takie jak IPsec lub WireGuard, działają w warstwie sieciowej, więc mogą przenosić cały ruch IP z urządzenia.

### Q2: Czy witryna HTTPS pozostaje szyfrowana przez serwer proxy?

Tak. Gdy otwierasz stronę HTTPS przez proxy, szyfrowanie TLS działa od końca do końca między Twoją przeglądarką a stroną, więc proxy widzi domenę, ale nie zawartość strony. Zwykłe strony HTTP pozostają czytelne.

### Q3: Czym jest wyciek WebRTC i jak VPN mu zapobiega?

WebRTC to protokół przeglądarki, który może ujawnić twoje prawdziwe lokalne i publiczne adresy IP nawet przy aktywnym VPN. Wysokiej klasy usługi VPN blokują lub podmieniają żądania WebRTC w swoich aplikacjach na komputery i urządzenia mobilne oraz w rozszerzeniach przeglądarek.

### Q4: Czym jest przezroczysty serwer proxy i kto z niego korzysta?

Przezroczyste proxy przechwytuje ruch bez żadnej konfiguracji na urządzeniu użytkownika. Szkoły, firmy i ISP używają ich do buforowania lub filtrowania treści. Użytkownicy często nie wiedzą, że takie proxy działa, i nie zapewnia ono im żadnej prywatności.

### Q5: Jak obfuskacja omija blokady VPN?

Obfuskacja (lub „Stealth VPN") ukrywa ruch VPN tak, by wyglądał jak zwykły ruch HTTPS (port 443). Może to pomóc ominąć system głębokiej inspekcji pakietów (DPI), którego rządy lub sieci szkolne i biurowe używają do blokowania VPN.

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o VPN (Część D)

Poznaj techniczne i strukturalne aspekty wirtualnych sieci prywatnych i bezpiecznych protokołów tunelowania.

### Q6: Czym jest tunelowanie dzielone (Split Tunneling) i kiedy warto z niego korzystać?

Tunelowanie dzielone pozwala wybrać, które aplikacje kierują ruch przez zaszyfrowany tunel VPN, a które łączą się bezpośrednio z internetem. Użyj go, aby kierować wrażliwe aplikacje bankowe przez VPN, podczas gdy lokalne gry łączą się bezpośrednio, co pozwala uniknąć opóźnienia dodawanego przez VPN.

### Q7: Dlaczego serwer proxy może wydawać się szybszy niż połączenie VPN?

Podstawowe proxy pomija szyfrowanie i obsługuje ruch tylko z jednej aplikacji, więc wymaga mniej przetwarzania. VPN szyfruje każdy pakiet z urządzenia. Przy nowoczesnych protokołach różnica jest często niewielka, a proxy zapewnia znacznie mniejszą ochronę.

### Q8: Czy strony internetowe potrafią rozpoznać, że używam proxy lub VPN?

Często tak. Wiele witryn sprawdza adresy IP na listach znanych serwerów proxy i VPN, a serwery proxy HTTP mogą dodawać nagłówki, takie jak Via lub X-Forwarded-For. Serwisy streamingowe zwykle blokują jedne i drugie.

### Q9: Czym jest ochrona przed wyciekami DNS?

Ochrona przed wyciekami DNS sprawia, że Twoje urządzenie wysyła zapytania o strony internetowe (zapytania DNS) przez prywatne, szyfrowane serwery DNS usługi VPN zamiast przez serwery Twojego dostawcy internetu. Dzięki temu dostawca internetu nie może śledzić, jakie strony odwiedzasz.

### Q10: Czy serwer proxy może zatrzymać ograniczanie prędkości przez dostawcę internetu?

Rzadko. Podstawowy serwer proxy nie szyfruje ruchu, więc dostawca internetu nadal może zobaczyć, jakiego rodzaju jest ta aktywność. VPN ukrywa rodzaje ruchu, ale żadne z tych narzędzi nie rozwiązuje problemu przeciążenia ani limitów danych.

# Część 11: 10 ciekawych faktów o VPN i spostrzeżeń z praktyki

Przejrzyj te bardzo cenne, prawdziwe fakty i spostrzeżenia dotyczące historii, rynku i technologii VPN.

### 1. STANDARD SOCKS

Protokół SOCKS w wersji 5 został opublikowany przez IETF jako RFC 1928 w marcu 1996 roku i nadal jest specyfikacją referencyjną dla serwerów proxy SOCKS5 używanych dziś przez przeglądarki i aplikacje. [1]

### 2. WARSTWA SHIM

RFC 1928 opisuje SOCKS jako warstwę pośrednią między warstwą aplikacji a warstwą transportową, więc nie może przekazywać ruchu warstwy sieciowej, takiego jak ICMP. [1]

### 3. PRZEKAŹNIK UDP

SOCKS5 dodał polecenie UDP ASSOCIATE, które pozwala proxy przekazywać datagramy UDP oraz połączenia TCP, czego zwykłe proxy HTTP nie obsługują. [1]

### 4. DOMYŚLNY PORT SOCKS

Klienci SOCKS5 domyślnie łączą się z serwerem proxy na porcie TCP 1080, zgodnie z definicją w RFC 1928; wiele usług proxy pozwala użytkownikom wybrać inne porty. [1]

### 5. POŚREDNICY HTTP

Standard HTTP (RFC 9110) definiuje serwer proxy jako agenta przekazującego komunikaty, wybranego przez klienta, który przekazuje żądania w stronę serwera źródłowego.

### 6. GŁĘBOKA INSPEKCJA PAKIETÓW

Głęboka inspekcja pakietów (DPI) bada zawartość pakietów i wzorce ruchu; nieszyfrowany ruch proxy jest dla niej w pełni widoczny, natomiast ruch VPN ujawnia znacznie mniej.

### 7. VPN-Y WARSTWY SIECIOWEJ

IPsec, opisany w NIST SP 800-77, chroni ruch w warstwie sieciowej, dzięki czemu pakiety IP każdej aplikacji można zabezpieczyć bez konfiguracji dla poszczególnych aplikacji. [2]

### 8. ZAKRES TYLKO PRZEGLĄDARKI

Proxy ustawione w jednej przeglądarce wpływa tylko na tę przeglądarkę; klienci poczty, gry i aktualizacje systemu nadal korzystają ze zwykłego połączenia urządzenia.

### 9. TOR A PROXY

Tor kieruje ruch przez trzy przekaźniki wolontariuszy (wejściowy, środkowy i wyjściowy) i zwykle uzyskuje się do niego dostęp przez lokalny serwer proxy SOCKS, dodając warstwy, których pojedynczy serwer proxy nie zapewnia.

### 10. KOMPROMIS Z SZYBKOŚCIĄ

Serwery proxy mogą wydawać się szybsze, bo pomijają szyfrowanie, ale nowoczesne protokoły VPN, takie jak WireGuard, dodają niewielki narzut, a jednocześnie chronią cały ruch urządzenia.

# Źródła i odnośniki techniczne

Cytowane publikacje, specyfikacje kryptograficzne i oficjalne standardy dokumentów wykorzystane w tej karcie pracy.

## PUBLIKACJE NAUKOWE I BRANŻOWE

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

# Klucz odpowiedzi: Porównanie serwerów proxy i wirtualnych sieci prywatnych, różnic w szyfrowaniu i routingu na poziomie aplikacji i całego systemu

**1** **Warstwa OSI proxy** PROTOKOŁY — **Poprawna odpowiedź: C**

## UWAGA DLA NAUCZYCIELA

Standardowe serwery proxy HTTP/HTTPS działają w warstwie aplikacji (warstwa 7) i przekierowują ruch określonych przeglądarek. Nie zapewniają routingu sieciowego w całym systemie. Źródło: Tor Project Foundation.

**2** **Pytanie 2** — **Poprawna odpowiedź: B**

## UWAGA DLA NAUCZYCIELA

SOCKS5 przekazuje ruch TCP i UDP między warstwą aplikacji a warstwą transportową, ale domyślnie nie szyfruje, podczas gdy serwery proxy HTTP obsługują żądania sieciowe.

**3** **Szyfrowanie systemowe VPN** BEZPIECZEŃSTWO WI-FI — **Poprawna odpowiedź: B**

## UWAGA DLA NAUCZYCIELA

VPN enkapsuluje i szyfruje cały ruch systemu operacyjnego w całym systemie, a proxy przekierowuje ruch tylko dla konkretnych skonfigurowanych aplikacji. Źródło: Deloitte Advisory.

**4** **Brak szyfrowania w proxy** KONTROLA ROUTINGU — **Poprawna odpowiedź: A**

## UWAGA DLA NAUCZYCIELA

Serwery proxy HTTP przekazują ruch przeglądarki na poziomie warstwy aplikacji bez szyfrowania ładunku pakietów, co oznacza, że operator sieci lub dostawca internetu nadal może śledzić ruch z Twoimi treściami. Źródło: IETF Proxy Vulnerabilities.

**5** **Podatność na obejście** PRYWATNOŚĆ — **Poprawna odpowiedź: D**

## UWAGA DLA NAUCZYCIELA

Proxy w przeglądarce stosują reguły wyłącznie do samej przeglądarki internetowej. Aplikacje w tle, aktualizacje systemu operacyjnego i klienty poczty omijają proxy, ujawniając twój natywny adres IP. Źródło: W3C Consortium.

## Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

**6** **Pytanie 6** — **Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

SOCKS5 przekazuje ruch między warstwą aplikacji a warstwą transportową, ale domyślnie nie wykonuje szyfrowania, więc zawartość pakietów pozostaje czytelna podczas przesyłania.

**7** **Tunele warstwy sieciowej** PRĘDKOŚCI — **Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Działając na warstwie sieciowej, VPN kieruje i szyfruje ruch wychodzący z twojego urządzenia, co może pomóc chronić ruch w całym systemie. Źródło: Deloitte Advisory.

**8** **Ograniczenie szyfrowania w proxy** RYZYKO SNIFFINGU — **Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Serwery proxy bywają szybsze, ale dzieje się tak dlatego, że NIE szyfrują danych. Brak szyfrowania pozostawia dane podatne na podgląd. Źródło: IETF Proxy Vulnerabilities.

**9** **Przekierowanie na poziomie aplikacji** ZAPORY SIECIOWE — **Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

W przeciwieństwie do VPN obejmujących cały system serwery proxy wymagają ręcznej konfiguracji w ustawieniach przeglądarki lub w polach proxy właściwych dla aplikacji. Źródło: W3C Consortium.

**10** **Ryzyko śledzenia przez dostawcę internetu** BRAK LOGÓW — **Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Ponieważ standardowe proxy HTTP/SOCKS5 nie szyfrują przesyłanych danych, twój lokalny ISP zachowuje pełny wgląd w twoje działania w sieci. Źródło: EDRi Retention Guidelines.

# Klucze słownictwa i kryteria oceny

**Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).**

## PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

| | | | |
|---|---|---|---|
| G 1. Proxy HTTP | H 2. Proxy SOCKS5 | E 3. Tunel VPN | A 4. Obejmujący cały system |
| B 5. Warstwa 7 modelu OSI | C 6. Obsługa UDP | D 7. Proxy przeglądarki | F 8. Widoczność dla ISP |

## PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

| | | | |
|---|---|---|---|
| 1 PROXY | 2 TUNEL VPN | 3 SOCKS5 | 4 WARSTWA SIÓDMA |
| 5 SZYFROWANIE | 6 CAŁY SYSTEM | | |

## PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

| | | | |
|---|---|---|---|
| 1 E – WARSTWASIÓDMA | 2 F – OBSŁUGAUDP | 3 A – PROXYHTTP | 4 G – DODATEKPROXY |
| 5 C – TUNELVPN | 6 D – CAŁYSYSTEM | 7 H – WIDOCZNOŚĆ | 8 B – PROXYSOCKS |

## UWAGI DO DYSKUSJI DLA NAUCZYCIELI

**Kluczowe pojęcia:**
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Proxy HTTP, Proxy SOCKS5 i Tunel VPN oraz podać przykład każdego z nich.

**Studia przypadków:**
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

**Ocena źródeł:**
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

# Klucze do łamigłówek i uwagi dla nauczyciela

## ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

| Y | H | P | T | H | Ó | V | P | U | O | U | T | K | A | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | Ó | N | L | Ą | Ń | V | R | F | F | P | Q | Y | Ź | J |
| O | K | V | K | W | I | D | O | C | Z | N | O | Ś | Ć | Ź |
| R | X | Z | Ó | K | I | Ż | X | I | J | N | A | E | I | Ą |
| P | M | E | T | S | Y | S | Y | Ł | A | C | Ś | A | K | Ę |
| K | X | E | K | Ż | K | D | S | L | Q | N | K | A | Ę | O |
| E | K | Ń | Ć | N | C | Ć | O | G | I | Ą | Ą | Ó | R | Ł |
| T | P | W | T | I | Ź | Ę | C | Ź | S | G | Y | X | H | Ę |
| A | R | T | Ń | U | K | R | K | Ć | T | S | Ł | P | Ł | N |
| D | Ś | H | L | P | H | Ź | S | Ó | Ł | X | V | Ń | Z | Q |
| O | W | A | R | S | T | W | A | S | I | Ó | D | M | A | Q |
| D | Ą | A | P | R | O | X | Y | H | T | T | P | Ł | Ó | N |
| Ą | Ł | O | B | S | Ł | U | G | A | U | D | P | I | Ę | J |
| Ń | Z | B | Ż | Ż | Ź | B | N | V | Y | M | C | Ę | Ó | X |
| P | N | P | V | L | E | N | U | T | Q | Y | G | D | Ź | B |

## ROZWIĄZANIE KRZYŻÓWKI

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | W | I | D | O | C | Z | N | O | Ś | Ć | |
| | | | O | | | O | | | | | | | | |
| | C | | B | | | D | | | | | | | | |
| W | A | R | S | T | W | A | S | I | Ó | D | M | A | | |
| | Ł | | Ł | | | T | | | | | | | | |
| | Y | | U | | | E | | P | | | | | | |
| | S | | G | | | K | | R | | | | | | |
| | Y | | A | | | P | R | O | X | Y | S | O | C | K | S |
| | S | | U | | | R | | X | | | | | | |
| | T | | D | | | O | | Y | | | | | | |
| | E | | P | | | X | | H | | | | | | |
| | M | | | | | Y | | T | U | N | E | L | V | P | N |
| | | | | | | | | T | | | | | | |
| | | | | | | | | P | | | | | | |

## PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

### POZIOMO

**1 poziomo: WIDOCZNOŚĆ** Stan ruchu, w którym niezaszyfrowane dane proxy pozostają widoczne dla dostawców internetu (10 liter)

**5 poziomo: WARSTWASIÓDMA** Warstwa aplikacji, w której działają standardowe protokoły proxy WWW (13 liter)

**7 poziomo: PROXYSOCKS** Protokół proxy działający między warstwą aplikacji a transportową, bez szyfrowania (10 liter)

**8 poziomo: TUNELVPN** Szyfrowanie i enkapsulacja obejmujące cały ruch urządzenia działający w tle (8 liter)

### PIONOWO

**2 pionowo: DODATEKPROXY** Rozszerzenie klienta, które ukrywa ruch tylko wewnątrz piaskownicy przeglądarki (12 liter)

**3 pionowo: OBSŁUGAUDP** Zdolność SOCKS5 do przekazywania UDP oraz TCP, w przeciwieństwie do zwykłych proxy HTTP (10 liter)

**4 pionowo: CAŁYSYSTEM** Routing na poziomie systemu operacyjnego, który szyfruje ruch wszystkich aplikacji (10 liter)

**6 pionowo: PROXYHTTP** Proxy warstwy aplikacji przekierowujące ruch wybranej przeglądarki internetowej (9 liter)

# Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

## KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. HYXRPTTPO — **PROXYHTTP**
2. ETNUPVLN — **TUNELVPN**
3. AWSÓIMARATWDS — **WARSTWASIÓDMA**
4. XPTDKYEORDOA — **DODATEKPROXY**
5. CSSRXOYPKO — **PROXYSOCKS**
6. ESYSTCAYMŁ — **CAŁYSYSTEM**
7. BŁOAGUDPUS — **OBSŁUGAUDP**
8. ŚOZĆWCINOD — **WIDOCZNOŚĆ**

## KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

**"PRZEKIERUJ SWÓJ RUCH PRZEZ SERWER PROXY"**

# Klucz odpowiedzi do studiów przypadków

## A Scenariusz A: Bezpieczeństwo sieci publicznej

SNIFFING I SZYFROWANIE | Dylemat Sarah

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Ryzyka: Podsłuchiwanie pakietów, przechwytywanie danych i ataki typu man-in-the-middle. Ktoś w tej samej sieci w kawiarni mógłby przechwycić jej dane logowania lub plik z pracą domową.
- Proxy a VPN: Podstawowe proxy w przeglądarce nie szyfruje jej ruchu. VPN szyfruje wszystko na urządzeniu, przez co przechwycone pakiety są nieczytelne dla lokalnych podsłuchiwaczy.

## B Scenariusz B: Dostęp do zablokowanych zasobów

GEOBLOKADY I ADRESY IP | Dylemat Alexa

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Powód blokady: Serwis streamingowy stosuje blokadę geograficzną, która przypisuje lokalny adres IP podróżnika do jego fizycznego kraju i blokuje go na podstawie terytorialnych licencji.
- Co działa lepiej: oba dają mu adres IP z jego kraju, ale proxy obejmuje tylko skonfigurowaną aplikację, a VPN szyfruje też cały ruch z jego urządzenia.