Imię i nazwisko: _____ Data: _____ Wynik: _____

# Jak skonfigurować VPN
# Karta pracy

Konfigurowanie VPN w systemach Windows, macOS, Android, iOS, Linux i na routerach

## 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 komercyjne aplikacje VPN z konfigurowaniem klientów natywnych.
- Skonfiguruj połączenia VPN na routerach, aby chronić cały dom.
- Konfiguruj pliki konfiguracyjne i zarządzaj nimi, np. OVPN lub klucze WireGuard.
- Otwórz i zabezpiecz wybrane porty routera dla ruchu tunelu.
- Zweryfikuj konfiguracje klienta za pomocą testów wycieków DNS i testów połączenia.

## INSTRUKCJE DO KARTY PRACY O KONFIGURACJI

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 konfigurowania i testowania klientów VPN. Zakończ zadaniem dodatkowym Myśl szybko.

## KONFIGURACJA VPN (WPROWADZENIE)

Ręczna konfiguracja VPN daje pełną kontrolę nad kluczami szyfrowania i routingiem sieciowym. Niezależnie od tego, czy konfigurujesz natywnego klienta na urządzeniu mobilnym, czy instalujesz tunel VPN bezpośrednio na routerze, prawidłowa konfiguracja jest kluczem do zapobiegania wyciekom DNS i zabezpieczenia całego ruchu sieciowego.

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

## Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

**1. Jaki jest najłatwiejszy sposób skonfigurowania VPN na urządzeniach mobilnych?**

- A. Pobranie oficjalnej aplikacji VPN ze sklepu z aplikacjami
- B. Ręczna edycja plików jądra systemu operacyjnego
- C. Wgranie niestandardowego oprogramowania układowego na sprzęt urządzenia
- D. Podłączenie telefonu do komputera stacjonarnego przez USB

**2. Jaka jest korzyść z zainstalowania VPN bezpośrednio na routerze?**

- A. Zwiększa prędkość połączenia wszystkich lokalnych urządzeń
- B. Automatycznie zabezpiecza wszystkie podłączone urządzenia sieciowe
- C. Eliminuje opłaty za abonament u lokalnego dostawcy internetu
- D. Całkowicie eliminuje potrzebę stosowania sprzętowych routerów

**3. Co oznacza „natywna” konfiguracja VPN?**

- A. Konfigurowanie połączenia za pomocą natywnych, wbudowanych ustawień systemu operacyjnego
- B. Używanie VPN tylko w rodzinnym mieście
- C. Łączenie się wyłącznie z serwerami w kraju lokalnym
- D. Pisanie własnego protokołu w języku asemblera

**4. Co jest wymagane do ręcznej, zewnętrznej konfiguracji OpenVPN?**

- A. Projektowanie niestandardowego logo dla połączenia z serwerem
- B. Zaimportowanie profilu .ovpn zawierającego klucze certyfikatów
- C. Zmiana fizycznej lokalizacji routera domowego
- D. Całkowite wyłączenie zapory sieciowej systemu operacyjnego

**5. Dlaczego administrator miałby zastosować tunelowanie dzielone (split tunneling) w konfiguracji?**

- A. Aby całkowicie zablokować cały ruch internetowy
- B. Aby pozwolić wybranym bezpiecznym aplikacjom ominąć bezpieczny tunel
- C. Aby podzielić fizyczny router na dwie osobne jednostki
- D. Aby wyłączyć szyfrowanie na potrzeby monitoringu administracyjnego

## Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

**6 Pytanie 6**

6. Konfiguracja VPN na routerze to prosty proces niewymagający żadnych umiejętności technicznych.

○ Prawda ○ Fałsz

**7 Pytanie 7**

7. Windows i macOS mają natywne klienty obsługujące IKEv2 i L2TP.

○ Prawda ○ Fałsz

**8 Pytanie 8**

8. Konfiguracja WireGuard wymaga wygenerowania kluczy publicznego i prywatnego.

○ Prawda ○ Fałsz

**9 Pytanie 9**

9. Tunel VPN zabezpiecza drukarki w Twojej sieci lokalnej i zadania drukowania.

○ Prawda ○ Fałsz

**10 Pytanie 10**

10. Inteligentne zamki, które nie mogą uruchamiać aplikacji VPN, wymagają VPN na poziomie routera, aby były objęte ochroną.

○ Prawda ○ Fałsz

## Punkt kontrolny 3: Wstawianie kluczowych terminów

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

**1. Instalacja VPN na bramie sieciowej, czyli urządzeniu o nazwie _____ , chroni telewizory smart i konsole do gier.**

**2. Ręczne konfiguracje OpenVPN wymagają zaimportowania profilu serwera z plikiem o rozszerzeniu _____ .**

**3. Wbudowane konfiguracje systemu operacyjnego korzystają z ustawień klienta typu: _____ .**

**4. Uwierzytelnianie WireGuard opiera się na elemencie o nazwie _____ , czyli kryptograficznym kluczu publicznym i prywatnym.**

**5. Prostą instalację zapewnia oficjalna _____ dostawcy.**

**6. Kierowanie zapytań przez serwery _____ należące do VPN zapobiega wyciekom śledzenia rozpoznawania nazw.**

**BANK SŁÓW**

APLIKACJA DNS LOGI POŁĄCZEŃ NATYWNY OVPN PARA KLUCZY PODZIAŁ TUNELU ROUTER

**Wpisz tutaj swoje odpowiedzi:**

**1.** **2.**

**3.** **4.**

**5.** **6.**

# Punkt kontrolny 4: Dopasowywanie pojęć sieciowych

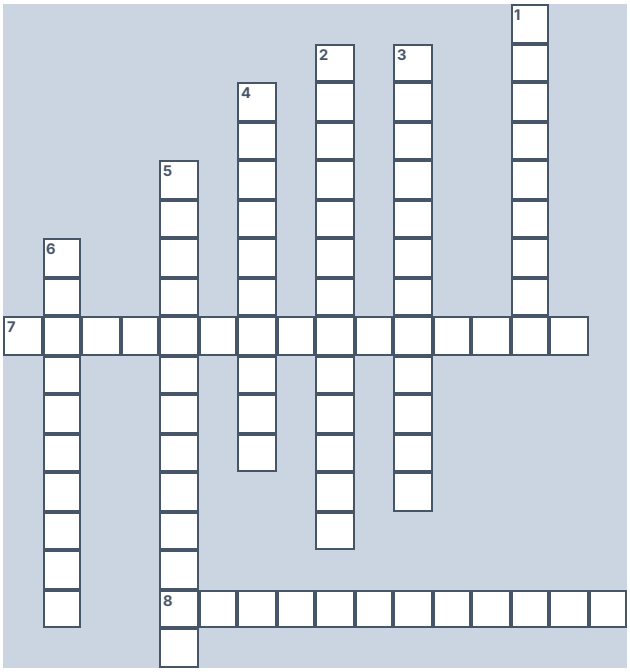
## DOPASOWYWANIE DEFINICJI

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

| | | | |
|---|---|---|---|
| ☐ | 1. Aplikacja VPN | A | Szyfrowanie na poziomie bramy chroniące wszystkie inteligentne urządzenia w sieci lokalnej. |
| ☐ | 2. VPN na routerze | B | Pakiet oprogramowania dostarczany przez usługę subskrypcyjną w celu łatwej konfiguracji jednym kliknięciem. |
| ☐ | 3. Klient natywny | C | Sprawdzanie danych wyjściowych błędów i dzienników stanu klienta w celu debugowania nieudanych konfiguracji. |
| ☐ | 4. Profil .ovpn | D | Rozróżnianie tras ruchu, aby wybrane aplikacje mogły omijać szyfrowany tunel. |
| ☐ | 5. Para kluczy | E | Zabezpieczanie ruchu w natywnych ustawieniach systemu operacyjnego bez instalowania aplikacji. |
| ☐ | 6. Tunelowanie podzielone | F | Konfigurowanie adresów resolverów sieciowych, aby zapobiegać wyciekom zapytań o domeny. |
| ☐ | 7. Konfiguracja serwera DNS | G | Tokeny kryptograficzne (publiczne/prywatne) wymagane do ustanowienia handshake'ów WireGuard. |
| ☐ | 8. Logi połączeń | H | Format pliku OpenVPN zawierający serwery, ustawienia portów i klucze certyfikatów. |

## Punkt kontrolny 5: Krzyżówka

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




### POZIOMO

**7. Konfigurowanie adresów resolwerów sieciowych, aby zapobiec wyciekom podczas wyszukiwania domen (15)**

**8. Sprawdzanie komunikatów o błędach i logów stanu klienta w celu debugowania nieudanych konfiguracji (12)**

### PIONOWO

**1. Szyfrowanie na poziomie bramy chroniące wszystkie inteligentne urządzenia w sieci lokalnej (9)**

**2. Zabezpieczanie ruchu w natywnych ustawieniach systemu operacyjnego bez instalowania aplikacji (13)**

**3. Pakiet oprogramowania udostępniany przez usługę subskrypcyjną w celu łatwej konfiguracji jednym kliknięciem (12)**

**4. Tokeny kryptograficzne (publiczny i prywatny) wymagane do nawiązania uzgodnień WireGuard (10)**

**5. Rozróżnianie tras ruchu, aby wybrane aplikacje omijały zaszyfrowany tunel (13)**

**6. Format pliku OpenVPN zawierający serwery, ustawienia portów i klucze certyfikatów (10)**

# 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

**7 poziomo: Konfigurowanie adresów resolwerów sieciowych, aby zapobiec wyciekom podczas wyszukiwania domen (15 liter):**

**8 poziomo: Sprawdzanie komunikatów o błędach i logów stanu klienta w celu debugowania nieudanych konfiguracji (12 liter):**

## PIONOWO

**1 pionowo: Szyfrowanie na poziomie bramy chroniące wszystkie inteligentne urządzenia w sieci lokalnej (9 liter):**

**2 pionowo: Zabezpieczanie ruchu w natywnych ustawieniach systemu operacyjnego bez instalowania aplikacji (13 liter):**

**3 pionowo: Pakiet oprogramowania udostępniany przez usługę subskrypcyjną w celu łatwej konfiguracji jednym kliknięciem (12 liter):**

**4 pionowo: Tokeny kryptograficzne (publiczny i prywatny) wymagane do nawiązania uzgodnień WireGuard (10 liter):**

**5 pionowo: Rozróżnianie tras ruchu, aby wybrane aplikacje omijały zaszyfrowany tunel (13 liter):**

**6 pionowo: Format pliku OpenVPN zawierający serwery, ustawienia portów i klucze certyfikatów (10 liter):**

## Punkt kontrolny 6: Ukryte słowa w wykreślance

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

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

**LISTA SŁÓW**

APLIKACJAVPN ROUTERVPN KLIENTNATYWNY PROFILOVPN PARAKLUCZY
PODZIAŁTUNELU KONFIGURACJADNS LOGIPOŁĄCZEŃ

# 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. APLIKACJAVPN**
- **B. ROUTERVPN**
- **C. KLIENTNATYWNY**
- **D. PROFILOVPN**
- **E. PARAKLUCZY**
- **F. PODZIAŁTUNELU**
- **G. KONFIGURACJADNS**
- **H. LOGIPOŁĄCZEŃ**

**DEFINICJE I POLA DOPASOWANIA**

1. Konfigurowanie adresów resolwerów sieciowych, aby zapobiec wyciekom podczas wyszukiwania domen.
2. Rozróżnianie tras ruchu, aby wybrane aplikacje omijały zaszyfrowany tunel.
3. Szyfrowanie na poziomie bramy chroniące wszystkie inteligentne urządzenia w sieci lokalnej.
4. Tokeny kryptograficzne (publiczny i prywatny) wymagane do nawiązania uzgodnień WireGuard.
5. Zabezpieczanie ruchu w natywnych ustawieniach systemu operacyjnego bez instalowania aplikacji.
6. Sprawdzanie komunikatów o błędach i logów stanu klienta w celu debugowania nieudanych konfiguracji.
7. Format pliku OpenVPN zawierający serwery, ustawienia portów i klucze certyfikatów.
8. Pakiet oprogramowania udostępniany przez usługę subskrypcyjną w celu łatwej konfiguracji jednym kliknięciem.

## 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. AAJKPCVAPLNI
2. NNLTIKWNYTYAE
3. PLZUAKYACR
4. UNJFOACGSRDAKNI
5. VEONRTRPU
6. PIFOVPRLNO
7. NETAPOUIULDŁZ
8. ĄGPZŁŃLOOECI

# Zadanie dodatkowe: Myśl szybko

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

| | | | | |
|---|---|---|---|---|
| 1 | Rzeczy do sprawdzenia po skonfigurowaniu | | | |
| 2 | Urządzenia, które mogą korzystać z VPN | | | |
| 3 | Usługi VPN, które znasz | | | |
| 4 | Powody, dla których warto używać VPN podczas podróży | | | |
| 5 | Błędy, które ludzie popełniają podczas konfiguracji | | | |
| 6 | Słowa z tej karty pracy, które chcesz zapamiętać | | | |
| 7 | Ustawienia, które włączasz najpierw | | | |
| 8 | Obietnice, które składa dobry dostawca VPN | | | |
| 9 | Kroki podczas konfigurowania VPN | | | |
| 10 | Miejsca, w których używałbyś VPN | | | |
| 11 | Sposoby na rozpoznanie fałszywej sieci Wi-Fi | | | |
| 12 | Rzeczy, które VPN może ukryć | | | |
| 13 | Rzeczy, które może zobaczyć twój dostawca internetu | | | |
| 14 | Miejsca, w których można znaleźć pomoc | | | |
| 15 | Rzeczy, których potrzebujesz na początek | | | |

# Punkt kontrolny 8: Studia przypadków dotyczących VPN

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

### SARAH (STUDENTKA W KAWIARNI)

👩‍💻 „Hej! Siedzę w Coffee & Bytes. Jest tu niezabezpieczona sieć publiczna o nazwie 'Free_Wi-Fi_No_Password'. Chcę zalogować się na szkolną pocztę i wysłać zadanie, ale boję się hakerów. Jakie są zagrożenia związane z korzystaniem z tej sieci bez VPN i jak VPN zabezpiecza moje dane?”

### ALEX (STUDENT PODRÓŻNIK)

👩‍💻 „O nie! Podróżuję za granicą w związku z projektem i próbuję obejrzeć dokument biologiczny hostowany na serwerze w moim kraju. Ale strona pokazuje komunikat 'Ten film nie jest dostępny w Twojej obecnej lokalizacji.' Dlaczego jestem zablokowany i jak VPN może pomóc mi go obejrzeć?”

## Punkt kontrolny 9: Odszyfruj szyfr

Aby ukończyć szkolenie z konfiguracji serwera, odszyfruj tę ukrytą wiadomość o konfigurowaniu bezpiecznych tuneli.

**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**

33 1 12 18 25 27 1 15 28 13 25 30 20 13 2

3 24 1 17 8 33 3 7 33 22 12 7 4 33 18 32 17

6 7 17 20 18 7 17

**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: Czego potrzebuję, aby zacząć?

Potrzebujesz aktywnej subskrypcji VPN lub własnego serwera VPN, obsługiwanego urządzenia oraz aplikacji dostawcy albo danych do ręcznej konfiguracji: adresu serwera, protokołu i swoich danych logowania, kluczy lub certyfikatów. Większość osób po prostu instaluje oficjalną aplikację, loguje się i klika połącz.

### Q3: Jak skonfigurować VPN w systemie Windows bez aplikacji?

Otwórz Ustawienia > Sieć i internet > VPN, wybierz Dodaj VPN i wpisz nazwę serwera dostawcy, typ VPN (na przykład IKEv2 lub L2TP/IPsec) oraz dane logowania. Następnie wybierz Połącz.

### 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: Jak skonfigurować macOS?

Zainstaluj aplikację dostawcy dla macOS lub otwórz System Settings > VPN, dodaj konfigurację VPN, wybierz IKEv2, L2TP przez IPSec lub Cisco IPSec i wpisz adres serwera oraz dane logowania od swojego dostawcy.

# 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 VPN?

Darmowe VPN mogą opierać się na reklamach, ograniczonych funkcjach, analityce użytkowania, limitach danych lub innych modelach zarabiania. Przed użyciem użytkownicy powinni zapoznać się z polityką prywatności dostawcy, jego właścicielem, audytami i modelem biznesowym.

### Q7: Jak używać pliku .ovpn?

Zainstaluj klienta OpenVPN, zaimportuj profil .ovpn od swojego dostawcy lub administratora i połącz się. Plik zawiera adres serwera, port, ustawienie UDP lub TCP, a często także certyfikaty i klucze.

### Q8: Jak wybrać najlepszy VPN?

Szukaj audytowanych polityk braku logów, silnych protokołów (WireGuard, OpenVPN), bezpiecznych lokalizacji serwerów, dużej szybkości, serwerów działających wyłącznie w pamięci RAM, funkcji kill switch oraz jurysdykcji spoza sojuszy wymiany informacji wywiadowczych (takich jak 5/9/14 Eyes).

### Q9: Czy mogę używać VPN na telefonie i telewizorze Smart TV?

Tak. Nowoczesni dostawcy VPN oferują dedykowane aplikacje na iOS, Androida, macOS, Windows, Linux i telewizory smart, a także konfiguracje routerów chroniące wszystkie urządzenia w sieci domowej.

### Q10: Czym jest kill switch?

Kill Switch to funkcja bezpieczeństwa, która automatycznie odłącza urządzenie od internetu, jeśli połączenie VPN zostanie zerwane. Zapobiega to wyciekowi Twoich nieszyfrowanych danych lub prawdziwego adresu IP.

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

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

### Q1: Jaka jest różnica między WireGuard, OpenVPN i IKEv2?

WireGuard to nowoczesny, lekki protokół (tylko ok. 4000 wierszy kodu), który zapewnia dużą prędkość i szybkie nawiązywanie połączeń. OpenVPN to bardzo bezpieczny, sprawdzony w boju protokół open source. IKEv2 doskonale sprawdza się na urządzeniach mobilnych dzięki możliwości szybkiego ponownego łączenia po zmianie sieci.

### Q2: Jak ręcznie skonfigurować WireGuard?

Wygeneruj parę kluczy za pomocą wg genkey i wg pubkey, udostępnij serwerowi swój klucz publiczny i utwórz konfigurację zawierającą Twój klucz prywatny, klucz publiczny partnera, dozwolone adresy IP i punkt końcowy. Narzędzie wg-quick uruchamia połączenie. [2]

### 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: Jak bezpiecznie skonfigurować VPN na domowym routerze?

Sprawdź, czy Twój router obsługuje tryb klienta VPN, zaloguj się na jego stronę administracyjną i prześlij plik OpenVPN lub WireGuard od dostawcy. Niektóre routery wymagają wcześniej aktualizacji oprogramowania układowego; potem każde urządzenie w sieci korzysta z tunelu.

### 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: Jak sprawdzić, czy moja nowa konfiguracja VPN działa?

Połącz się, a następnie odwiedź stronę sprawdzającą IP: powinna pokazać adres IP i lokalizację serwera VPN. Uruchom testy wycieków DNS i WebRTC oraz na chwilę przerwij połączenie, aby potwierdzić, że kill switch blokuje ruch.

### Q8: Co sprawdzić, jeśli VPN nie łączy się po konfiguracji?

Sprawdź swój login lub klucze, adres serwera oraz to, czy wybrany port i protokół nie są blokowane. Spróbuj przełączyć się między UDP i TCP lub na inny serwer i sprawdź w dziennikach połączeń aplikacji, czy nie ma błędów.

### 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 VPN powinien uruchamiać się automatycznie?

Zwykle tak. Większość aplikacji może uruchamiać się przy starcie systemu i łączyć automatycznie albo w niezaufanych sieciach Wi-Fi, dzięki czemu jesteś chroniony, zanim inne aplikacje zaczną wysyłać dane.

## 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. KLIENCI NATYWNI**

Zarówno Windows, jak i macOS mają wbudowane klienty VPN obsługujące IKEv2 i L2TP/IPsec, więc wiele połączeń można skonfigurować bez dodatkowej aplikacji.

**2. GENEROWANIE KLUCZY**

Szybki start WireGuard tworzy klucz prywatny poleceniem wg genkey i wyprowadza z niego klucz publiczny poleceniem wg pubkey. [2]

**3. REWOLUCJA WIREGUARD**

WireGuard ma bardzo uproszczoną bazę kodu zaprojektowaną z myślą o wydajności, co ułatwia jego audyt pod kątem luk w zabezpieczeniach w porównaniu z tradycyjnymi protokołami. [1]

**4. PLIKI PROFILI**

Profil .ovpn zawiera adres serwera, port, protokół i certyfikaty, więc jeden import konfiguruje połączenie OpenVPN.

**5. PORTY DOMYŚLNE**

OpenVPN zwykle używa portu 1194, a oficjalne przykłady WireGuard używają portu UDP 51820; zapory sieciowe i routery mogą wymagać zezwolenia na te porty, aby tunel mógł się połączyć.

**6. GŁĘBOKA INSPEKCJA PAKIETÓW**

Głęboka inspekcja pakietów (DPI) może wykrywać i blokować popularne protokoły VPN; przełączenie na OpenVPN przez port TCP 443 lub tryb z obfuskacją może pomóc.

**7. ZASIĘG ROUTERA**

VPN na routerze chroni każde urządzenie za nim, w tym konsole i telewizory Smart TV, na których nie można uruchomić aplikacji VPN, bez instalowania czegokolwiek na każdym urządzeniu.

**8. KEEPALIVE**

Za NAT-em lub zaporą sieciową ustawienie PersistentKeepalive w WireGuard, zwykle 25 sekund, utrzymuje tunel osiągalnym. [2]

**9. STEROWNIKI TUN/TAP**

OpenVPN został zaprojektowany do pracy z wirtualnym interfejsem sieciowym TUN/TAP, który jest dostępny na większości platform i jest konfigurowany podczas instalacji klienta. [3]

**10. TUNELOWANIE PODZIELONE**

Podczas konfiguracji tunelowanie podzielone pozwala wyłączyć wybrane aplikacje lub adresy z VPN, co pomaga w przypadku lokalnych drukarek lub aplikacji blokujących adresy IP VPN.

# Źródła i odnośniki techniczne

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

## PUBLIKACJE NAUKOWE I BRANŻOWE

[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/

# Klucz odpowiedzi: Konfigurowanie VPN w systemach Windows, macOS, Android, iOS, Linux oraz na routerach

## 1 Pytanie 1

**Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Jaki jest najłatwiejszy sposób skonfigurowania VPN na urządzeniach mobilnych? → Pobranie oficjalnej aplikacji VPN ze sklepu z aplikacjami

## 2 Konfiguracja bramy routera OPÓŹNIENIE

**Poprawna odpowiedź: B**

### UWAGA DLA NAUCZYCIELA

VPN na routerze szyfruje ruch na bramie, chroniąc urządzenia IoT, konsole i inteligentne sprzęty, na których nie można zainstalować natywnej aplikacji VPN. Źródło: DD-WRT OpenVPN Clients, Linksys Router Config.

## 3 Pytanie 3

**Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Windows i macOS zawierają wbudowanych klientów dla protokołów takich jak IKEv2 i L2TP/IPsec, więc połączenie można skonfigurować bez instalowania dodatkowego oprogramowania.

## 4 Import profilu OpenVPN KONTROLA ROUTINGU

**Poprawna odpowiedź: B**

### UWAGA DLA NAUCZYCIELA

Ręczne konfiguracje wymagają pobrania kluczy profilu.ovpn zawierających porty docelowego serwera, parametry protokołu (UDP/TCP) i certyfikaty kryptograficzne. Źródło: DD-WRT OpenVPN Clients.

## 5 Routing tunelu dzielonego PRYWATNOŚĆ

**Poprawna odpowiedź: B**

### UWAGA DLA NAUCZYCIELA

Tunelowanie dzielone pozwala kierować wrażliwe aplikacje służbowe przez zaszyfrowany tunel, podczas gdy lokalne streamingi lub gry łączą się bezpośrednio bez narzutu VPN. Źródło: IETF IKEv2 RFC.

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

**6** **Pytanie 6**

**Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Konfiguracja na routerze oznacza zalogowanie się na stronie administracyjnej, sprawdzenie obsługi VPN i wgranie plików konfiguracyjnych.

**7** **Natywna integracja z systemem operacyjnym** PRĘDKOŚCI

**Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Główne systemy operacyjne mają wbudowaną natywną obsługę protokołów, aby zapewnić bezproblemową konfigurację bezpiecznych połączeń. Źródło: Microsoft Native Gateway, Apple Support Profiles.

**8** **Parowanie kluczy WireGuard** RYZYKO SNIFFINGU

**Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

WireGuard używa kluczy asymetrycznych do nawiązywania bezpiecznych uzgodnień P2P, zamiast polegać na hasłach lub łańcuchach urzędów certyfikacji. Źródło: WireGuard CLI Specifications.

**9** **Blokady ruchu lokalnego** ZAPORY SIECIOWE

**Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

VPN zwykle kierują publiczny ruch internetowy i mogą czasem blokować dostęp do drukarek w sieci lokalnej, o ile nie zostaną skonfigurowane inaczej. Źródło: Microsoft Native Gateway.

**10** **Pytanie 10**

**Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Inteligentne zamki, które nie mogą uruchamiać aplikacji VPN, wymagają VPN na poziomie routera, aby były objęte ochroną.

# 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

| | | | |
|---|---|---|---|
| B 1. Aplikacja VPN | A 2. VPN na routerze | E 3. Klient natywny | H 4. Profil .ovpn |
| G 5. Para kluczy | D 6. Tunelowanie podzielone | F 7. Konfiguracja serwera DNS | C 8. Logi połączeń |

## PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

| | | | |
|---|---|---|---|
| 1 ROUTER | 2 OVPN | 3 NATYWNY | 4 PARA KLUCZY |
| 5 APLIKACJA | 6 DNS | | |

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

| | | | |
|---|---|---|---|
| 1 G – KONFIGURACJADNS | 2 F – PODZIAŁTUNELU | 3 B – ROUTERVPN | 4 E – PARAKLUCZY |
| 5 C – KLIENTNATYWNY | 6 H – LOGIPOŁĄCZEŃ | 7 D – PROFILOVPN | 8 A – APLIKACJAVPN |

## UWAGI DO DYSKUSJI DLA NAUCZYCIELI

**Kluczowe pojęcia:**
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Aplikacja VPN, VPN na routerze i Klient natywny oraz podać przykład każdego z nich.

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

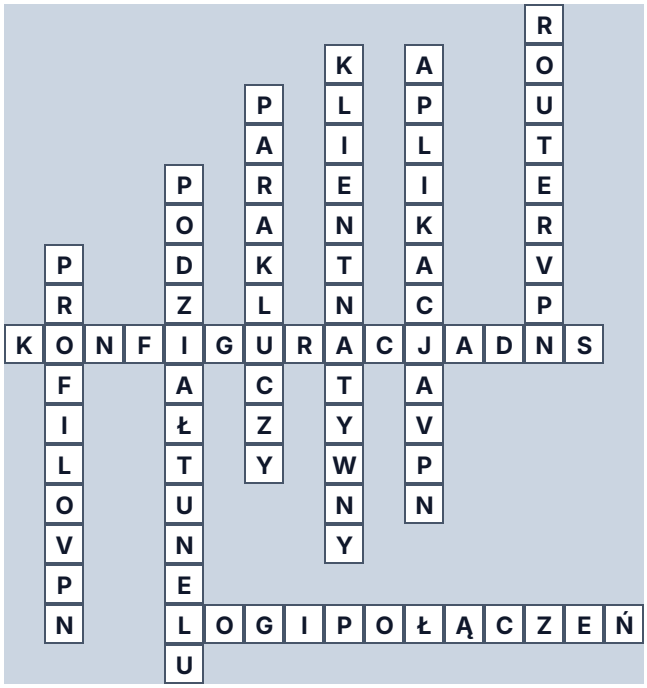
**Ocena źródeł:**
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

# Klucze do łamigłówek i uwagi dla nauczyciela

## ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

## ROZWIĄZANIE KRZYŻÓWKI




## PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

### POZIOMO

**7 poziomo: KONFIGURACJADNS** Konfigurowanie adresów resolwerów sieciowych, aby zapobiec wyciekom podczas wyszukiwania domen (15 liter)

**8 poziomo: LOGIPOŁĄCZEŃ** Sprawdzanie komunikatów o błędach i logów stanu klienta w celu debugowania nieudanych konfiguracji (12 liter)

### PIONOWO

**1 pionowo: ROUTERVPN** Szyfrowanie na poziomie bramy chroniące wszystkie inteligentne urządzenia w sieci lokalnej (9 liter)

**2 pionowo: KLIENTNATYWNY** Zabezpieczanie ruchu w natywnych ustawieniach systemu operacyjnego bez instalowania aplikacji (13 liter)

**3 pionowo: APLIKACJAVPN** Pakiet oprogramowania udostępniany przez usługę subskrypcyjną w celu łatwej konfiguracji jednym kliknięciem (12 liter)

**4 pionowo: PARAKLUCZY** Tokeny kryptograficzne (publiczny i prywatny) wymagane do nawiązania uzgodnień WireGuard (10 liter)

**5 pionowo: PODZIAŁTUNELU** Rozróżnianie tras ruchu, aby wybrane aplikacje omijały zaszyfrowany tunel (13 liter)

**6 pionowo: PROFILOVPN** Format pliku OpenVPN zawierający serwery, ustawienia portów i klucze certyfikatów (10 liter)

# Klucz do słów rozsypanych i rozwiązania szyfru

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

## KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. AAJKPCVAPLNI — **APLIKACJAVPN**
2. NNLTIKWNYTYAE — **KLIENTNATYWNY**
3. PLZUAKYACR — **PARAKLUCZY**
4. UNJFOACGSRDAKNI — **KONFIGURACJADNS**
5. VEONRTRPU — **ROUTERVPN**
6. PIFOVPRLNO — **PROFILOVPN**
7. NETAPOUIULDŁZ — **PODZIAŁTUNELU**
8. ĄGPZŁŃLOOECI — **LOGIPOŁĄCZEŃ**

## KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

**"ZAINSTALUJ SWOJĄ BRAMĘ Z BEZPIECZNYM DEMONEM"**

# 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.
- Ochrona VPN: szyfruje dane użytkowe pakietów sieciowych, przez co przechwycony ruch tunelu jest nieczytelny dla pasywnych podsłuchiwaczy w sieci lokalnej, gdy VPN jest poprawnie skonfigurowany.

## 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.
- Jak pomaga VPN: maskuje jego prawdziwą lokalizację, kierując ruch przez serwer w jego kraju ojczystym. Strona widzi adres IP z kraju ojczystego, co umożliwia dostęp.