Imię i nazwisko: _____ Data: _____ Wynik: _____

Opinia o IPVanish

Analiza techniczna IPVanish VPN z siedzibą w USA, w dużej mierze własnych serwerów

OMÓWIENIE NAUKI: OPINIA O IPVANISH

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 techniczny przegląd IPVanish. Poznasz własną fizyczną infrastrukturę, proxy SOCKS5 do pobierania torrentów P2P, wydajność WireGuard i amerykańskie przepisy jurysdykcyjne dotyczące danych.

PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj konfiguracje VPN i bezpieczeństwa sieci.**
- [ ] **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 najlepszych VPN

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

Twoja ścieżka nauki: IPVanish

- Przeanalizuj architekturę techniczną i standardy szyfrowania w recenzji IPVanish.
- Skonfiguruj ustawienia klienta, aby zapobiec wyciekom ruchu IP, DNS i WebRTC.
- Porównaj autorskie protokoły tunelowania ze standardowymi implementacjami.

INSTRUKCJE DO OPINII O IPVANISH

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 serwerów proxy SOCKS5 i infrastruktury serwerów należących do dostawcy. Zakończ zadaniem dodatkowym Myśl szybko.

WŁASNA INFRASTRUKTURA I PROXY SOCKS5 P2P (WPROWADZENIE)

IPVanish wyróżnia się tym, że jest właścicielem dużej części swojej fizycznej sieci serwerów i nią zarządza, co poprawia wydajność i bezpieczeństwo. Oferuje szybki protokół WireGuard i proxy SOCKS5 do torrentów P2P, ale działa w amerykańskiej jurysdykcji Five Eyes.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Który protokół open source jest domyślny dla dużej prędkości w aplikacjach klienckich IPVanish?

- A) WireGuard
- B) L2TP/IPSec
- C) PPTP
- D) Catapult Hydra

2. Jaki typ serwera proxy udostępnia IPVanish, aby pomóc w konfiguracji torrentów P2P?

- A) Proxy SOCKS5
- B) Proxy HTTP
- C) Przekaźnik Tora
- D) Shadowsocks

3. Która firma przeprowadziła pierwszy niezależny audyt braku logów IPVanish w 2022 roku?

- A) Leviathan Security Group
- B) PwC
- C) Deloitte
- D) Cure53

4. W jakiej głównej jurysdykcji krajowej działają podmioty korporacyjne IPVanish?

- A) Stany Zjednoczone
- B) Szwajcaria
- C) Panama
- D) Brytyjskie Wyspy Dziewicze

5. Ile jednoczesnych połączeń urządzeń jest dozwolonych w płatnym planie IPVanish?

- A) Bez limitu
- B) Pięć
- C) Dziesięć
- D) Siedem

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. IPVanish zarządza dużą częścią swojej fizycznej infrastruktury serwerowej i jest jej właścicielem.

Prawda Fałsz

7 Pytanie 7

7. Ruch proxy SOCKS5 jest w pełni szyfrowany w tranzycie, tak jak w standardowych tunelach VPN.

Prawda Fałsz

8 Pytanie 8

8. Klient IPVanish na komputerze nie ma systemowej funkcji Kill Switch.

Prawda Fałsz

9 Pytanie 9

9. IPVanish działa ze Stanów Zjednoczonych, członka sojuszu wywiadowczego Five Eyes.

Prawda Fałsz

10 Pytanie 10

10. Tunelowanie dzielone w IPVanish pozwala kierować ruch aplikacji poza tunelem VPN.

Prawda Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Nowoczesny protokół _____ jest domyślnie skonfigurowany pod kątem zoptymalizowanej wydajności routingu.

2. Ruch P2P można kierować przez szybki serwer proxy _____ , aby ukryć rzeczywiste lokalizacje klientów.

3. Połączenie z bliskim geograficznie węzłem maksymalizuje rzeczywistą _____ .

4. Aby zapobiec wyciekom danych, użytkownicy powinni skonfigurować wbudowaną funkcję o nazwie _____ .

5. Niezależne audyty bezpieczeństwa potwierdziły zobowiązanie dostawcy w zakresie, który określa się jako: _____ .

6. W przeciwieństwie do niektórych konkurentów IPVanish nie narzuca na kontach tego rodzaju ograniczenia: _____ .

BANK SŁÓW

ADRES IP | AUDYTOWANE LOGI | BEZPIECZEŃSTWO | KILL SWITCH | LIMIT URZĄDZEŃ | SOCKS5 | SZYBKOŚĆ SERWERA | WIREGUARD

Wpisz tutaj swoje odpowiedzi:

1. **2.**

3. **4.**

5. **6.**

Punkt kontrolny 4: Dopasowywanie pojęć dotyczących VPN i sieci

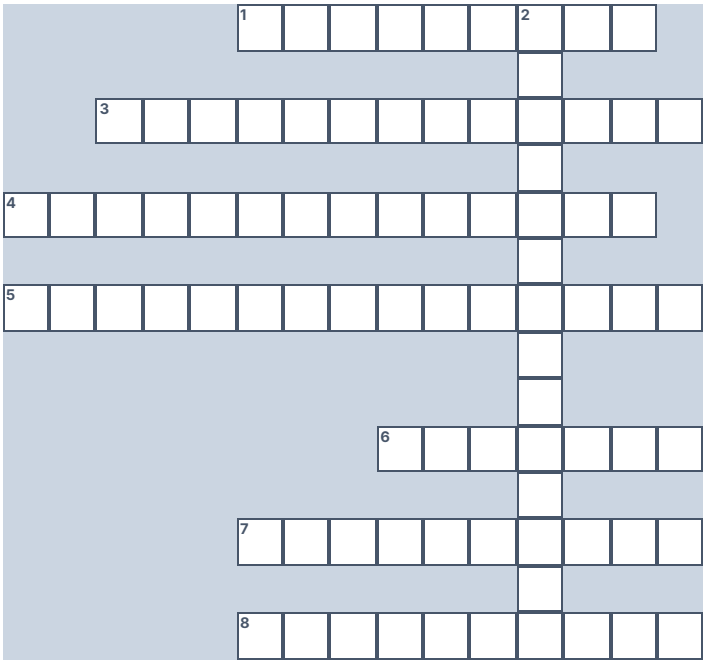
DOPASOWYWANIE DEFINICJI

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

☐	1. WireGuard	A	Awaryjny mechanizm blokujący ruch internetowy, jeśli VPN przestanie działać.
☐	2. Proxy SOCKS5	B	Protokół o otwartym kodzie znany z szybkości i nowoczesnej kryptografii.
☐	3. Prędkość serwera	C	Ograniczenie liczby aktywnych sesji urządzeń.
☐	4. Kill Switch	D	Przepustowość węzła serwera pod aktywnym obciążeniem ruchem.
☐	5. Audytowane dzienniki	E	Unikalny identyfikator sieciowy przypisany urządzeniom w internecie.
☐	6. Limit urządzeń	F	Ogólny stan ochrony zaszyfrowanego systemu tunelowego.
☐	7. Adres IP	G	Zweryfikowane rejestry potwierdzające, że aktywność użytkowników nie jest w ogóle śledzona.
☐	8. Bezpieczeństwo	H	Niezaszyfrowany system routingu proxy używany do maskowania lokalizacji klientów P2P.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

1. Protokół open source znany z szybkości i nowoczesnej kryptografii (9)

3. Ograniczenie liczby aktywnych sesji urządzeń (13)

4. Ogólny poziom ochrony zaszyfrowanego systemu tunelowego (14)

5. Przepustowość węzła serwera pod aktywnym obciążeniem ruchem (15)

6. Unikalny identyfikator sieciowy przypisany urządzeniom w internecie (7)

7. Nieszyfrowany system trasowania proxy używany do maskowania lokalizacji klientów P2P (10)

8. Mechanizm zabezpieczający, który blokuje ruch internetowy, gdy VPN przestaje działać (10)

PIONOWO

2. Zweryfikowane zapisy potwierdzające, że aktywność użytkowników nie jest w ogóle śledzona (14)

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: Protokół open source znany z szybkości i nowoczesnej kryptografii (9 liter):

3 poziomo: Ograniczenie liczby aktywnych sesji urządzeń (13 liter):

4 poziomo: Ogólny poziom ochrony zaszyfrowanego systemu tunelowego (14 liter):

5 poziomo: Przepustowość węzła serwera pod aktywnym obciążeniem ruchem (15 liter):

6 poziomo: Unikalny identyfikator sieciowy przypisany urządzeniom w internecie (7 liter):

7 poziomo: Nieszyfrowany system trasowania proxy używany do maskowania lokalizacji klientów P2P (10 liter):

8 poziomo: Mechanizm zabezpieczający, który blokuje ruch internetowy, gdy VPN przestaje działać (10 liter):

PIONOWO

2 pionowo: Zweryfikowane zapisy potwierdzające, że aktywność użytkowników nie jest w ogóle śledzona (14 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

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

A Ę O K Ń Ć N S C Ć G I Ą Ą Ó

R Ł P W T P I Z Ź Ę A Ź O S G

Ń Y X H Ę I R Y T Ń U U W K R

E Ć T S Ł S P B Ł N D Ś T H L

Z P K H S E Ź K Ó Ł Y X S V Ń

D Z I Q K R Q O Ą A T Ł Ń Ó W

Ą N L Ą C D Ł Ś I Ę O J E Ń I

Z Z L B O A Ż Ć Ż Ź W B Z N R

R V S Y S M C S Ę Ó A X C P E

U Q W Y Y G D E Ź B N X E Ł G

T E I G X G Ż R X C E O I Q U

I K T Y O Y R W L Ż L A P N A

M R C Ż R R M E F Ś O W Z F R

I Ł H X P J B R Ź C G B E Ź D

L O V Ż O Ż U A T Ą I H B W P

LISTA SŁÓW

WIREGUARD PROXYSOCKS SZYBKOŚĆSERWERA KILLSWITCH AUDYTOWANELOGI LIMITURZĄDZEŃ ADRESIP BEZPIECZEŃSTWO

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. WIREGUARD**
- **B. PROXYSOCKS**
- **C. SZYBKOŚĆSERWERA**
- **D. KILLSWITCH**
- **E. AUDYTOWANELOGI**
- **F. LIMITURZĄDZEŃ**
- **G. ADRESIP**
- **H. BEZPIECZEŃSTWO**

DEFINICJE I POLA DOPASOWANIA

1. Nieszyfrowany system trasowania proxy używany do maskowania lokalizacji klientów P2P.
2. Ogólny poziom ochrony zaszyfrowanego systemu tunelowego.
3. Ograniczenie liczby aktywnych sesji urządzeń.
4. Przepustowość węzła serwera pod aktywnym obciążeniem ruchem.
5. Protokół open source znany z szybkości i nowoczesnej kryptografii.
6. Unikalny identyfikator sieciowy przypisany urządzeniom w internecie.
7. Mechanizm zabezpieczający, który blokuje ruch internetowy, gdy VPN przestaje działać.
8. Zweryfikowane zapisy potwierdzające, że aktywność użytkowników nie jest w ogóle śledzona.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z wirtualną siecią prywatną (VPN). Wpisz odpowiedzi w przygotowanych polach.

1. UGEIWARDR
2. ZOEŚYĆESAR BRWSK
3. ANUGAIELDW TOOY
4. PDSEIAR
5. CSSRXOYPKO
6. CSLITKIWHL
7. DZZULIĄTŃE MRI
8. PZTEEŃEOBC ZWSI

Zadanie dodatkowe: Myśl szybko

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

1	Słowa opisujące dobrą aplikację VPN			
2	Rzeczy, które IPVanish może ukryć w twojej sieci			
3	Miejsca, w których włączyłbyś IPVanish			
4	Protokoły VPN, które znasz			
5	Pytania do pomocy technicznej IPVanish			
6	Kraje, w których chciałbyś mieć serwery IPVanish			
7	Usługi VPN inne niż IPVanish			
8	Sytuacje, w których kill switch pomaga			
9	Powody, dla których warto wybrać IPVanish			
10	Oznaki, że twoje połączenie VPN jest wolne			
11	Rzeczy, które robisz online codziennie			
12	Osoby, którym poleciłbyś IPVanish			
13	Rzeczy do sprawdzenia przed zakupem VPN			
14	Słowa z zakresu bezpieczeństwa, które poznałeś w tej karcie pracy			
15	Funkcje, których szukasz w IPVanish			

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: KONFIGURACJA CENTRUM MULTIMEDIALNEGO



Scenariusz: Klient chce zabezpieczyć swój odtwarzacz multimedialny Android Fire TV za pomocą IPVanish, aby bezpiecznie oglądać treści, zachowując dużą przepustowość.

Pytanie do dyskusji: Dlaczego protokół WireGuard jest preferowany nad OpenVPN w przypadku sprzętu streamingowego o ograniczonych zasobach?

STUDIUM PRZYPADKU 2: PROXY W SIECIACH TORRENT



Scenariusz: Osoba udostępniająca pliki w P2P chce ukryć swoją lokalizację bez narzutu pełnego szyfrowania danych, używając konfiguracji SOCKS5.

Pytanie do dyskusji: Porównaj kompromisy w zakresie bezpieczeństwa i szybkości przy użyciu serwera proxy SOCKS5 w stosunku do pełnego tunelu VPN IPVanish.

Punkt kontrolny 9: Odszyfruj szyfr

Inżynier sieci zabezpiecza kanały routingu i tunele klientów. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

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

12	22	29	1	18	12	25	11		30	32	17	1	10	1

26	4	12	25	16	7	13		1	24	4	11	12	27	7	14	27	28	24	32

3	7	33		15	20	10	21	30

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 dotyczące wirtualnych sieci prywatnych (VPN) i tunelowania.

Q1: Jaki protokół jest domyślny w IPVanish?

Domyślnie kieruje ruch przez szybki WireGuard.

Q2: Czy IPVanish jest właścicielem sprzętu swoich serwerów?

Tak, jest właścicielem i zarządza dużą częścią swojej fizycznej sieci serwerów.

Q3: Gdzie ma siedzibę IPVanish?

Ma siedzibę w Stanach Zjednoczonych i podlega prawu USA.

Q4: Ile urządzeń może łączyć się jednocześnie?

IPVanish oferuje nieograniczoną liczbę jednoczesnych połączeń urządzeń na konto.

Q5: Czy przechowuje jakiekolwiek logi połączeń?

Nie, stosuje ścisłą politykę braku logów, potwierdzoną niezależnymi audytami. [6]

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

Przejrzyj najczęstsze pytania i odpowiedzi dotyczące wirtualnych sieci prywatnych (VPN) i tunelowania.

Q6: Czy IPVanish oferuje usługę proxy?

Tak, zapewnia bezpłatny serwer proxy SOCKS5 do pobierania torrentów.

Q7: Czy zawiera kill switch?

Tak, kill switch jest dostępny w systemach Windows, macOS, Android i iOS.

Q8: Czy mogę ominąć blokady geograficzne z IPVanish?

Tak, jego globalna sieć serwerów umożliwia dostęp do ograniczonych bibliotek.

Q9: Czy obsługuje tunelowanie dzielone?

Tak, tunelowanie dzielone jest dostępne, w tym w systemach Windows i Android.

Q10: Jakich szyfrów używa?

Zabezpiecza połączenia za pomocą szyfrowania AES-256 i ChaCha20.

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

Poznaj zaawansowane aspekty techniczne protokołów tunelowania VPN, integracji klientów mobilnych i wdrożeń w przedsiębiorstwach.

Q1: Jak skonfigurować serwer proxy SOCKS5?

Jest ustawiany w klientach torrent, aby ukryć adres IP użytkownika bez narzutu szyfrowania.

Q2: Jak posiadanie sprzętu serwerowego poprawia bezpieczeństwo?

Zmniejsza ryzyko związane z wynajmowaniem serwerów od stron trzecich i daje dostawcy bezpośrednią kontrolę nad konfiguracjami serwerów.

Q3: Jakie są konsekwencje jurysdykcji USA dla prywatności?

Choć przepisy USA nie wymagają przechowywania danych, dopuszczają national security letters i nakazy sądowe.

Q4: Jak kill switch zapobiega wyciekom adresu IP?

Blokuje wszystkie adaptery internetowe, jeśli połączenie VPN niespodziewanie zostanie przerwane.

Q5: Jakiego szyfrowania używa się z WireGuard?

WireGuard wykorzystuje szyfrowanie kluczem symetrycznym ChaCha20 i uwierzytelnianie Poly1305. [7]

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

Poznaj zaawansowane aspekty techniczne protokołów tunelowania VPN, integracji klientów mobilnych i wdrożeń w przedsiębiorstwach.

Q6: Jak weryfikuje się politykę zerowych logów?

Leviathan Security Group przeprowadziła audyt w 2022 roku, a Schellman w 2025; żadna z firm nie znalazła logów użytkowników. [3]

Q7: Jak obsługuje zapytania DNS przez IPv6?

Automatycznie kieruje wszystkie zapytania DNS i IPv6 przez swoje prywatne serwery nazw.

Q8: Czy IPVanish oferuje funkcje obfuskacji?

Tak, jego funkcja Scramble maskuje ruch OpenVPN, aby omijać zapory sieciowe.

Q9: Jak działa tunelowanie dzielone na urządzeniach mobilnych?

Pozwala wybranym aplikacjom ominąć tunel VPN i łączyć się bezpośrednio.

Q10: Czy obsługuje konfigurację na routerach?

Tak, konfiguracje OpenVPN i WireGuard można ręcznie załadować na routery DD-WRT. [1]

Część 11: 10 faktów o VPN z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące prędkości szyfrowania VPN, audytów protokołów, łączności mobilnej i pracy zdalnej w przedsiębiorstwach.

1. WGLĄD W VPN

IPVanish jest właścicielem większości swojej infrastruktury serwerowej, zamiast wynajmować ją od stron trzecich. [3]

2. WGLĄD W VPN

IPVanish działa od 2012 roku i należy do Ziff Davis, wcześniej znanej jako J2 Global. [2]

3. WGLĄD W VPN

Serwer proxy SOCKS5 ukrywa publiczny adres IP klienta, ale nie szyfruje pakietów danych.

4. WGLĄD W VPN

WireGuard jest protokołem domyślnym, a w aplikacjach dostępne są też OpenVPN i IKEv2/IPSec. [2]

5. WGLĄD W VPN

Standardowy OpenVPN Scramble dodaje warstwę obfuskacji XOR do nagłówków pakietów, aby omijać zapory sieciowe.

6. WGLĄD W VPN

Polityka nieograniczonej liczby równoczesnych połączeń pozwala użytkownikom zabezpieczyć jednocześnie wszystkie urządzenia w domu. [2]

7. WGLĄD W VPN

Audyty przeprowadzone przez Leviathan Security Group (2022) i Schellman (2025) zweryfikowały jego deklaracje o braku rejestrowania danych. [3]

8. WGLĄD W VPN

Aplikacja na Androida obsługuje ustawienia stale włączonego VPN, które uniemożliwiają dostęp do internetu, gdy tunel zostanie rozłączony.

9. WGLĄD W VPN

Połączenia OpenVPN mogą używać UDP dla szybkości albo TCP dla stabilnego trasowania przez zapory sieciowe.

10. WGLĄD W VPN

Oferuje wsparcie przez czat na żywo 24/7, a także wsparcie telefoniczne w określonych godzinach pracy w dni robocze. [5]

Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów technicznych, specyfikacji i ram regulacyjnych.

PUBLIKACJE NAUKOWE I BRANŻOWE

[1] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 **Domyślny WireGuard** WIREGUARD — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

WireGuard jest domyślnie skonfigurowany pod kątem zoptymalizowanych prędkości routingu. Źródło: IPVanish Features.

2 **Proxy SOCKS5** PROXY SOCKS5 — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Proxy SOCKS5 maskują lokalizacje klientów bez narzutu szyfrowania. Źródło: IPVanish Support.

3 **Pytanie 3** — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Leviathan Security Group przeprowadziła pierwszy audyt braku logów IPVanish w 2022 roku; Schellman dołączył w 2025 roku. [3]

4 **Jurysdykcja USA** STANY ZJEDNOCZONE — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

IPVanish ma siedzibę w Stanach Zjednoczonych i podlega zasadom sojuszu Five Eyes. Źródło: IPVanish Review.

5 **Nieograniczona liczba urządzeń** NIEOGRANICZONE — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

IPVanish pozwala na nieograniczoną liczbę jednoczesnych połączeń urządzeń. Źródło: IPVanish Support.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Sprzęt serwerowy** OWNS NETWORK — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

IPVanish jest właścicielem dużej części swojej fizycznej sieci serwerów i nią zarządza. Źródło: IPVanish Support.

7 **Pytanie 7** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: serwer proxy SOCKS5 maskuje twój adres IP, ale nie szyfruje danych.

8 **Pytanie 8** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: IPVanish zawiera kill switch w aplikacjach na komputery i urządzenia mobilne.

9 **Jurysdykcja USA** FIVE EYES USA — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

IPVanish ma siedzibę w USA i podlega zasadom inwigilacji Five Eyes. Źródło: IPVanish Review.

10 **Tunel dzielony** TRASA DZIELONA — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Tunelowanie dzielone kieruje ruch wybranych aplikacji poza bezpiecznym tunelem. Źródło: IPVanish Support.

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. WireGuard	H 2. Proxy SOCKS5	D 3. Prędkość serwera	A 4. Kill Switch
G 5. Audytowane dzienniki	C 6. Limit urządzeń	E 7. Adres IP	F 8. Bezpieczeństwo

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 WIREGUARD	2 SOCKS5	3 SZYBKOŚĆ SERWERA	4 KILL SWITCH
5 AUDYTOWANE LOGI	6 LIMIT URZĄDZEŃ		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 B – PROXYSOCKS	2 H – BEZPIECZEŃSTWO	3 F – LIMITURZĄDZEŃ	4 C – SZYBKOŚĆSERWERA
5 A – WIREGUARD	6 G – ADRESIP	7 D – KILLSWITCH	8 E – AUDYTOWANELOGI

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia WireGuard, Proxy SOCKS5 i Prędkość serwera 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

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

ROZWIĄZANIE KRZYŻÓWKI

				W	I	R	E	G	U	A	R	D		
										U				
			L	I	M	I	T	U	R	Z	Ą	D	Z	E	Ń
										Y				
B	E	Z	P	I	E	C	Z	E	Ń	S	T	W	O	
										O				
S	Z	Y	B	K	O	Ś	Ć	S	E	R	W	E	R	A
										A				
										N				
								A	D	R	E	S	I	P
										L				
					P	R	O	X	Y	S	O	C	K	S
										G				
					K	I	L	L	S	W	I	T	C	H

PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

1 poziomo: WIREGUARD Protokół open source znany z szybkości i nowoczesnej kryptografii (9 liter)

3 poziomo: LIMITURZĄDZEŃ Ograniczenie liczby aktywnych sesji urządzeń (13 liter)

4 poziomo: BEZPIECZEŃSTWO Ogólny poziom ochrony zaszyfrowanego systemu tunelowego (14 liter)

5 poziomo: SZYBKOŚĆSERWERA Przepustowość węzła serwera pod aktywnym obciążeniem ruchem (15 liter)

6 poziomo: ADRESIP Unikalny identyfikator sieciowy przypisany urządzeniom w internecie (7 liter)

7 poziomo: PROXYSOCKS Nieszyfrowany system trasowania proxy używany do maskowania lokalizacji klientów P2P (10 liter)

8 poziomo: KILLSWITCH Mechanizm zabezpieczający, który blokuje ruch internetowy, gdy VPN przestaje działać (10 liter)

PIONOWO

2 pionowo: AUDYTOWANELOGI Zweryfikowane zapisy potwierdzające, że aktywność użytkowników nie jest w ogóle śledzona (14 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. UGEIWARDR — **WIREGUARD**
2. ZOEŚYĆESARBRWSK — **SZYBKOŚĆSERWERA**
3. ANUGAIELDWTOOY — **AUDYTOWANELOGI**
4. PDSEIAR — **ADRESIP**
5. CSSRXOYPKO — **PROXYSOCKS**
6. CSLITKIWHL — **KILLSWITCH**
7. DZZULIĄTŃEMRI — **LIMITURZĄDZEŃ**
8. PZTEEŃEOBCZWSI — **BEZPIECZEŃSTWO**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"IPVANISH WYMAGA ŚCISŁEJ ARCHITEKTURY BEZ LOGÓW"

Klucz odpowiedzi do studiów przypadków

A STUDIUM PRZYPADKU 1: KONFIGURACJA CENTRUM MULTIMEDIALNEGO

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Klient chce zabezpieczyć swój odtwarzacz multimedialny Android Fire TV za pomocą IPVanish, aby bezpiecznie oglądać streamy, zachowując wysoką przepustowość.
- Zalecana strategia i rozwiązanie: Wskazówki do oceny: Wyjaśnij, że WireGuard ma mniejszy kod, działa w przestrzeni jądra i zużywa mniej cykli procesora, co maksymalizuje prędkość na słabszym sprzęcie.

B STUDIUM PRZYPADKU 2: PROXY W SIECIACH TORRENT

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Osoba udostępniająca pliki w sieci P2P chce ukryć swoją lokalizację bez narzutu pełnego szyfrowania danych, używając konfiguracji SOCKS5.
- Zalecana strategia i rozwiązanie: Wskazówki do oceny: Zauważ, że SOCKS5 ukrywa adres IP bez szyfrowania ruchu, co daje większą prędkość, ale zerową prywatność wobec inspekcji pakietów przez dostawcę internetu.