Imię i nazwisko: _____ Data: _____ Wynik: _____

Bezpieczeństwo ExpressVPN

Ocena infrastruktury bezpieczeństwa ExpressVPN, niestandardowego otwartoźródłowego protokołu Lightway, technologii TrustedServer działającej wyłącznie w pamięci RAM, niezależnych audytów bezpieczeństwa i kill switcha Network Lock.

PRZEGLĄD NAUKI: BEZPIECZEŃSTWO EXPRESSVPN

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 funkcje bezpieczeństwa ExpressVPN. Poznasz otwartoźródłowe protokoły, węzły serwerowe działające wyłącznie w pamięci RAM, szyfry i Internet Kill Switch.

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/expressvpn/bezpieczenstwo/

Twoja ścieżka nauki: bezpieczeństwo ExpressVPN

- Przeanalizuj architekturę techniczną i zasady konfiguracji zabezpieczeń ExpressVPN.
- Skonfiguruj ustawienia klienta, aby zapobiec wyciekom ruchu IP, DNS i WebRTC.
- Porównaj niestandardowe ceny, wersje próbne i funkcje wydajności ze standardowymi modelami.

INSTRUKCJE: PRZEWODNIK PO BEZPIECZEŃSTWIE EXPRESSVPN

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 protokołów o otwartym kodzie źródłowym i węzłów serwerowych działających wyłącznie w pamięci RAM. Zakończ zadaniem dodatkowym Myśl szybko.

MACIERZE SERWERÓW DZIAŁAJĄCYCH WYŁĄCZNIE W PAMIĘCI RAM I OTWARTE PROTOKOŁY POŁĄCZEŃ

ExpressVPN wykorzystuje technologię TrustedServer działającą wyłącznie w pamięci RAM, aby zapobiegać lokalnym logom, w połączeniu z własnym otwartoźródłowym protokołem Lightway i funkcją Internet Kill Switch, aby zapewnić kompleksowe bezpieczeństwo danych użytkownika.

(WPROWADZENIE)

ExpressVPN wykorzystuje technologię TrustedServer działającą wyłącznie w pamięci RAM, aby zapobiegać lokalnym logom, w połączeniu z własnym otwartoźródłowym protokołem Lightway i funkcją Internet Kill Switch, aby zapewnić kompleksowe bezpieczeństwo danych użytkownika.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **1. Jaki jest autorski protokół open source firmy ExpressVPN?**
   - A) Lightway
   - B) WireGuard
   - C) OpenVPN
   - D) Chameleon

2. **2. Jaka technologia serwerowa działa wyłącznie w ulotnej pamięci RAM?**
   - A) TrustedServer
   - B) RAM-Core
   - C) SecureRAM
   - D) Serwer NoSpy

3. **3. Co się dzieje, gdy połączenie VPN nieoczekiwanie zostanie przerwane?**
   - A) Kill switch blokuje ruch
   - B) Ruch wycieka do dostawcy internetu
   - C) System się restartuje
   - D) Dane stają się nieszyfrowane

4. **4. Gdzie ExpressVPN jest zarejestrowany, aby chronić prywatność?**
   - A) Brytyjskie Wyspy Dziewicze
   - B) Szwajcaria
   - C) Panama
   - D) Rumunia

5. **5. Jakiego symetrycznego szyfru używa się domyślnie?**
   - A) AES-256-GCM
   - B) Blowfish
   - C) DES-64
   - D) RC4

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Technologia TrustedServer przechowuje logi serwera na dyskach twardych.

○ Prawda ○ Fałsz

7 Pytanie 7

7. ExpressVPN przeszedł audyty bezpieczeństwa przeprowadzone przez strony trzecie.

○ Prawda ○ Fałsz

8 Pytanie 8

8. Protokół Lightway został zbudowany na bazie kodu OpenVPN.

○ Prawda ○ Fałsz

9 Pytanie 9

9. Kill switch jest domyślnie włączony w aplikacjach na komputery.

○ Prawda ○ Fałsz

10 Pytanie 10

10. ExpressVPN obsługuje prywatny DNS na każdym serwerze.

○ Prawda ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Wewnętrzny, szybki protokół opracowany przez ExpressVPN to _____ .

2. Aby zapobiec przechowywaniu danych, sieć serwerów opiera się na węzłach działających wyłącznie w pamięci RAM, a ta architektura nazywa się _____ .

3. Przełącznik awaryjny (kill switch) ExpressVPN nazywał się dawniej Network _____ .

4. ExpressVPN jest zarejestrowany zgodnie z prawem terytorium: Brytyjskie _____ .

5. Dane są zabezpieczane solidnym szyfrem symetrycznym _____ .

6. Polityka zerowych logów przeszła niezależny _____ przeprowadzony przez czołowe firmy.

BANK SŁÓW

AES-256 AUDYT LIGHTWAY LOCK RESOLWERY DNS TRUSTED SERVER WYCIEK WYSPY DZIEWICZE

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć dotyczących VPN i sieci

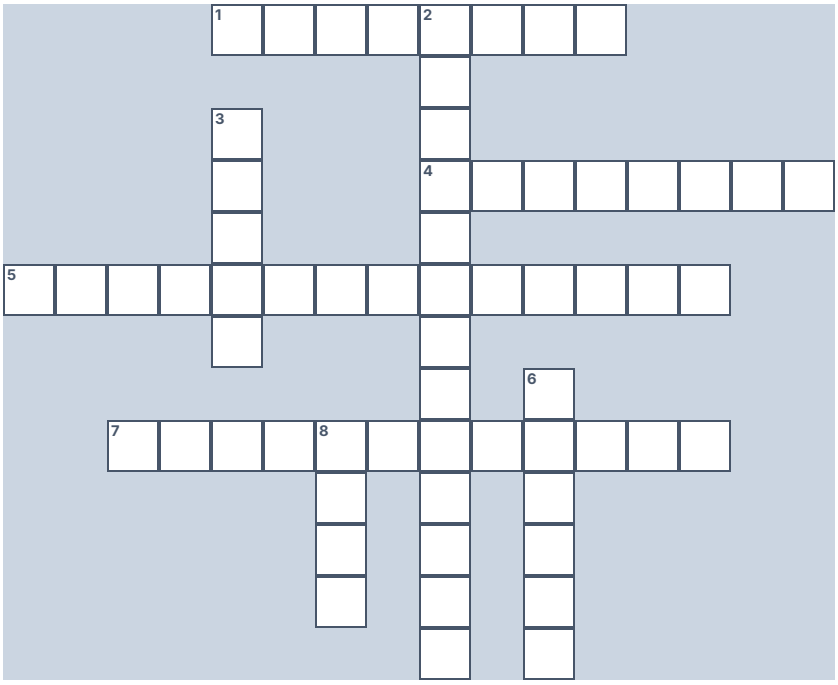
DOPASOWYWANIE DEFINICJI

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

☐	1. LIGHTWAY	A	Jurysdykcja Brytyjskich Wysp Dziewiczych zapewniająca silną ochronę prywatności
☐	2. TRUSTED SERVER	B	Niezamierzone ujawnienie prywatnych danych IP, DNS lub WebRTC
☐	3. BLOKADA	C	Resolwery systemu nazw domen działają prywatnie na każdym węźle serwera
☐	4. WYSPY	D	Niezależnie zweryfikowane przez zewnętrzne firmy z branży bezpieczeństwa
☐	5. AES-256	E	Architektura serwerów działających wyłącznie w pamięci RAM, uniemożliwiająca zapisywanie danych na dysku
☐	6. ZAUDYTOWANY	F	Ostatni wyraz nazwy Network Lock, dawnej nazwy kill switcha
☐	7. WYCIEK	G	Lekki, otwartoźródłowy protokół połączenia ExpressVPN
☐	8. DNS	H	Standard szyfrowania symetrycznego zabezpieczający transmisję danych

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

1. Lekki protokół połączenia ExpressVPN o otwartym kodzie źródłowym (8)

4. Standard szyfrowania symetrycznego zabezpieczający transmisję danych (8)

5. Brytyjska jurysdykcja zapewniająca silną ochronę prywatności (Brytyjskie Wyspy Dziewicze) (14)

7. Resolwery systemu nazw domen działają prywatnie na każdym węźle serwera (12)

PIONOWO

2. Architektura serwerów działających wyłącznie w pamięci RAM, która uniemożliwia zapis danych na dysku (13)

3. Niezależna weryfikacja przez zewnętrzne firmy zajmujące się bezpieczeństwem (5)

6. Niezamierzone ujawnienie prywatnych danych IP, DNS lub WebRTC (6)

8. Ostatni wyraz nazwy Network Lock, dawnej nazwy przełącznika awaryjnego (kill switch) (4)

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: Lekki protokół połączenia ExpressVPN o otwartym kodzie źródłowym (8 liter):

4 poziomo: Standard szyfrowania symetrycznego zabezpieczający transmisję danych (8 liter):

5 poziomo: Brytyjska jurysdykcja zapewniająca silną ochronę prywatności (Brytyjskie Wyspy Dziewicze) (14 liter):

7 poziomo: Resolwery systemu nazw domen działają prywatnie na każdym węźle serwera (12 liter):

PIONOWO

2 pionowo: Architektura serwerów działających wyłącznie w pamięci RAM, która uniemożliwia zapis danych na dysku (13 liter):

3 pionowo: Niezależna weryfikacja przez zewnętrzne firmy zajmujące się bezpieczeństwem (5 liter):

6 pionowo: Niezamierzone ujawnienie prywatnych danych IP, DNS lub WebRTC (6 liter):

8 pionowo: Ostatni wyraz nazwy Network Lock, dawnej nazwy przełącznika awaryjnego (kill switch) (4 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

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

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

LISTA SŁÓW

LIGHTWAY TRUSTEDSERVER LOCK WYSPYDZIEWICZE SZYFRAES AUDYT WYCIEK RESOLWERYDNS

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. LIGHTWAY**
- **B. TRUSTEDSERVER**
- **C. LOCK**
- **D. WYSPYDZIEWICZE**
- **E. SZYFRAES**
- **F. AUDYT**
- **G. WYCIEK**
- **H. RESOLWERYDNS**

DEFINICJE I POLA DOPASOWANIA

1. Niezamierzone ujawnienie prywatnych danych IP, DNS lub WebRTC.
2. Brytyjska jurysdykcja zapewniająca silną ochronę prywatności (Brytyjskie Wyspy Dziewicze).
3. Resolwery systemu nazw domen działają prywatnie na każdym węźle serwera.
4. Lekki protokół połączenia ExpressVPN o otwartym kodzie źródłowym.
5. Ostatni wyraz nazwy Network Lock, dawnej nazwy przełącznika awaryjnego (kill switch).
6. Standard szyfrowania symetrycznego zabezpieczający transmisję danych.
7. Architektura serwerów działających wyłącznie w pamięci RAM, która uniemożliwia zapis danych na dysku.
8. Niezależna weryfikacja przez zewnętrzne firmy zajmujące się bezpieczeństwem.

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. AHTLWIYG
2. LCKO
3. FZSRASEY
4. KICEWY
5. EVRUSTRERDTES
6. DZIYSCIZWWYEEP
7. YTADU
8. RSLDESRWENYO

Zadanie dodatkowe: Myśl szybko

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

1	Funkcje, których szukasz w ExpressVPN			
2	Zagrożenia w publicznych sieciach Wi-Fi			
3	Rodzaje wycieków VPN			
4	Sposoby na stworzenie silnego hasła			
5	Przyciski lub menu w aplikacji VPN			
6	Rzeczy, które robisz online codziennie			
7	Osoby, którym poleciłbyś ExpressVPN			
8	Kraje znane z silnych przepisów o prywatności			
9	Protokoły VPN, które znasz			
10	Rzeczy, które może sprawdzić audyt			
11	Funkcje bezpieczeństwa w ExpressVPN			
12	Rzeczy do sprawdzenia przed zakupem VPN			
13	Ustawienia, które włączasz dla dodatkowego bezpieczeństwa			
14	Rzeczy, które chroni szyfrowanie			
15	Rzeczy, które ExpressVPN może ukryć w twojej sieci			

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: WYMUSZANIE OCHRONY TYLKO W PAMIĘCI RAM



Scenariusz: Agencja rządowa zajmuje serwer ExpressVPN, aby wydobyć logi użytkowników i historię połączeń.

Pytanie do dyskusji: Jakie informacje znajdą na serwerze i dlaczego?

STUDIUM PRZYPADKU 2: NIESTABILNE TUNELE POŁĄCZENIA WI-FI



Scenariusz: Pracownik zdalny korzysta z publicznego Wi-Fi w hotelu, które rozłącza się co kilka minut podczas edycji dokumentów.

Pytanie do dyskusji: W jaki sposób ExpressVPN chroni jego dane przed wyciekiem podczas przerw w połączeniu?

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

27	24	28	25	27	7	6	25	7	24	29	7	24

4	20	6	33	12	7	18	18	12	7	28	25	28	30	1

30	25	33	32	25	27	14	12	7	15	20	10	12

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: Jakiego szyfrowania używa ExpressVPN?

ExpressVPN domyślnie używa szyfrowania symetrycznego AES-256-GCM.

Q2: Czym jest protokół Lightway?

Lightway to autorski protokół firmy ExpressVPN, stworzony z myślą o szybkości, bezpieczeństwie i stabilności.

Q3: Czy ExpressVPN rejestruje historię moich wyszukiwań?

Nie, ExpressVPN stosuje ścisłą, niezależnie audytowaną politykę braku logów.

Q4: Czym jest Internet Kill Switch?

To natywny kill switch ExpressVPN, który blokuje ruch internetowy, jeśli połączenie zostanie przerwane.

Q5: Czy protokół Lightway jest open source?

Tak, główny kod protokołu Lightway jest otwartoźródłowy i dostępny na GitHubie. [9]

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 ExpressVPN prowadzi prywatny DNS?

Tak, ExpressVPN prowadzi własny, prywatny, szyfrowany serwer DNS na każdym serwerze. [7]

Q7: Czym jest technologia TrustedServer?

To konfiguracja serwera, w której system operacyjny i aplikacje działają w całości w pamięci ulotnej RAM.

Q8: Czy ExpressVPN został poddany audytowi?

Tak, ExpressVPN był audytowany przez firmy takie jak PwC, Cure53 i F-Secure. [1]

Q9: Czy ExpressVPN chroni przed wyciekami DNS i IPv6?

Tak, Internet Kill Switch blokuje ruch IPv4, IPv6 i DNS poza tunelem.

Q10: Gdzie znajduje się ExpressVPN?

ExpressVPN jest zarejestrowany na Brytyjskich Wyspach Dziewiczych (BVI).

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 architektura wyłącznie w pamięci RAM zwiększa bezpieczeństwo?

Dane nie są zapisywane na dyskach twardych, a dane przechowywane w pamięci są usuwane za każdym razem, gdy serwer zostaje wyłączony.

Q2: Dlaczego jurysdykcja BVI ma znaczenie dla prywatności?

ExpressVPN ma siedzibę na BVI, więc prawne żądania udostępnienia danych podlegają prawu BVI.

Q3: Czy ExpressVPN obsługuje doskonałą poufność przekazywania (perfect forward secrecy)?

Tak, Lightway używa dynamicznych kluczy, które są regularnie usuwane i generowane na nowo.

Q4: Jak Network Lock zapobiega wyciekom adresu IP?

Blokuje cały ruch na poziomie systemu za każdym razem, gdy połączenie VPN zostanie przerwane.

Q5: Czy Lightway chroni przed atakami kwantowymi?

Tak, Lightway ma ochronę postkwantową opartą na standardzie NIST ML-KEM.

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: Czy agencje rządowe mogą przechwytywać ruch Lightway?

Mogą go przechwycić, ale nie mogą go odszyfrować dzięki szyfrowaniu AES-256/ChaCha20.

Q7: Jak prywatny DNS chroni logi wyszukiwań użytkownika?

Przetwarza wszystkie zapytania DNS wewnątrz zaszyfrowanego tunelu, uniemożliwiając monitorowanie przez dostawcę internetu.

Q8: Do czego służy Lightway Turbo?

Używa tunelowania wielopasmowego, aby wysyłać więcej danych naraz i zwiększyć prędkość.

Q9: Jaka jest przewaga Lightway nad WireGuard?

Lightway został stworzony tak, aby szybko radzić sobie ze zmianami sieci (np. z Wi-Fi na sieć komórkową) bez zrywania połączenia.

Q10: Jak często oprogramowanie serwera jest instalowane ponownie?

W TrustedServer cały stos oprogramowania jest ładowany ponownie z bezpiecznego obrazu tylko do odczytu przy każdym ponownym uruchomieniu.

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

Lightway używa AES-256-GCM lub ChaCha20/Poly1305 na urządzeniach o niskim poborze mocy. [6]

2. WGLĄD W VPN

Technologia TrustedServer została zaprojektowana tak, aby wszystkie operacje serwera działały w pamięci RAM. [4]

3. WGLĄD W VPN

Brytyjskie Wyspy Dziewicze (BVI) są jurysdykcją, w której zarejestrowana jest firma. [8]

4. WGLĄD W VPN

Lightway został przepisany z języka C na Rust i zbadany przez Cure53 i Praetorian. [3]

5. WGLĄD W VPN

Internet Kill Switch blokuje ruch na poziomie systemu, jeśli VPN się rozłączy. [5]

6. WGLĄD W VPN

Wszystkie zapytania DNS są rozwiązywane przez prywatne, szyfrowane serwery DNS. [7]

7. WGLĄD W VPN

ExpressVPN opublikował ponad 20 niezależnych audytów przeprowadzonych przez strony trzecie. [1]

8. WGLĄD W VPN

Usługa nie rejestruje adresów IP, historii przeglądania ani metadanych ruchu.

9. WGLĄD W VPN

Doskonała poufność przekazywania (Perfect Forward Secrecy) jest zachowywana dzięki dynamicznej rotacji kluczy sesji. [1]

10. WGLĄD W VPN

Protokół Lightway obsługuje zarówno warstwę transportową UDP, jak i TCP.

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] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

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

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1 — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Jaki jest autorski protokół open source firmy ExpressVPN? → Lightway

2 Pytanie 2 — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Jaka technologia serwerowa działa wyłącznie w ulotnej pamięci RAM? → TrustedServer

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

UWAGA DLA NAUCZYCIELA

Co się dzieje, gdy połączenie VPN nieoczekiwanie zostanie przerwane? → A) Kill switch blokuje ruch

4 Pytanie 4 — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Gdzie ExpressVPN jest zarejestrowany, aby chronić prywatność? → Brytyjskie Wyspy Dziewicze

5 Pytanie 5 — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Jakiego symetrycznego szyfru używa się domyślnie? → AES-256-GCM

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

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

UWAGA DLA NAUCZYCIELA

Technologia TrustedServer przechowuje logi serwera na dyskach twardych.

7 **Pytanie 7** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

ExpressVPN przeszedł audyty bezpieczeństwa przeprowadzone przez strony trzecie.

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

UWAGA DLA NAUCZYCIELA

Protokół Lightway został zbudowany na bazie kodu OpenVPN.

9 **Pytanie 9** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Kill switch jest domyślnie włączony w aplikacjach na komputery.

10 **Pytanie 10** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

ExpressVPN obsługuje prywatny DNS na każdym serwerze.

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. LIGHTWAY	E 2. TRUSTED SERVER	F 3. BLOKADA	A 4. WYSPY
H 5. AES-256	D 6. ZAUDYTOWANY	B 7. WYCIEK	C 8. DNS

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 LIGHTWAY	2 TRUSTED SERVER	3 LOCK	4 WYSPY DZIEWICZE
5 AES-256	6 AUDYT		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 G – WYCIEK	2 D – WYSPYDZIEWICZE	3 H – RESOLWERYDNS	4 A – LIGHTWAY
5 C – LOCK	6 E – SZYFRAES	7 B – TRUSTEDSERVER	8 F – AUDYT

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia LIGHTWAY, TRUSTED SERVER i BLOKADA oraz podać przykład każdego z nich.

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

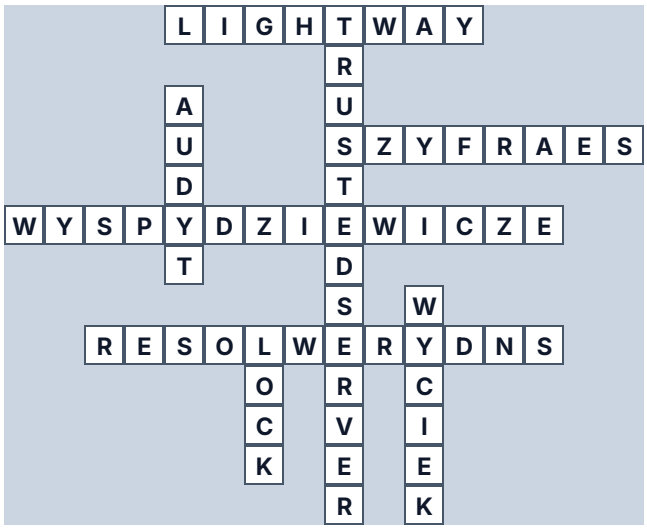
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

1 poziomo: LIGHTWAY Lekki protokół połączenia ExpressVPN o otwartym kodzie źródłowym (8 liter)

4 poziomo: SZYFRAES Standard szyfrowania symetrycznego zabezpieczający transmisję danych (8 liter)

5 poziomo: WYSPYDZIEWICZE Brytyjska jurysdykcja zapewniająca silną ochronę prywatności (Brytyjskie Wyspy Dziewicze) (14 liter)

7 poziomo: RESOLWERYDNS Resolwery systemu nazw domen działają prywatnie na każdym węźle serwera (12 liter)

PIONOWO

2 pionowo: TRUSTEDSERVER Architektura serwerów działających wyłącznie w pamięci RAM, która uniemożliwia zapis danych na dysku (13 liter)

3 pionowo: AUDYT Niezależna weryfikacja przez zewnętrzne firmy zajmujące się bezpieczeństwem (5 liter)

6 pionowo: WYCIEK Niezamierzone ujawnienie prywatnych danych IP, DNS lub WebRTC (6 liter)

8 pionowo: LOCK Ostatni wyraz nazwy Network Lock, dawnej nazwy przełącznika awaryjnego (kill switch) (4 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. AHTLWIYG — **LIGHTWAY**
2. LCKO — **LOCK**
3. FZSRASEY — **SZYFRAES**
4. KICEWY — **WYCIEK**
5. EVRUSTRERDTES — **TRUSTEDSERVER**
6. DZIYSCIZWWYEEP — **WYSPYDZIEWICZE**
7. YTADU — **AUDYT**
8. RSLDESRWENYO — **RESOLWERYDNS**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"TRUSTEDSERVER CODZIENNIE USUWA WSZYSTKIE LOGI"

Klucz odpowiedzi do studiów przypadków

A STUDIUM PRZYPADKU 1: WYMUSZANIE OCHRONY TYLKO W PAMIĘCI RAM

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Organ rządowy zajmuje serwer ExpressVPN, aby wydobyć logi użytkowników i historię połączeń.
- Zalecana strategia i rozwiązanie: Nic. Technologia TrustedServer od ExpressVPN działa w całości w pamięci RAM, więc wszystkie dane są natychmiast usuwane po utracie zasilania.

B STUDIUM PRZYPADKU 2: NIESTABILNE TUNELE POŁĄCZENIA WI-FI

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Pracownik zdalny korzysta z publicznego Wi-Fi w hotelu, które rozłącza się co kilka minut podczas edycji dokumentów.
- Zalecana strategia i rozwiązanie: Internet Kill Switch automatycznie blokuje cały ruch internetowy, dopóki tunel VPN nie zostanie ponownie nawiązany.