Imię i nazwisko: _____ Data: _____ Wynik: _____

Przewodnik po najbezpieczniejszym VPN

Analiza techniczna projektu VPN o wysokim poziomie bezpieczeństwa, serwerów z pamięcią ulotną działających wyłącznie w RAM, zabezpieczeń dostępu Zero Trust, prywatnych zaszyfrowanych zabezpieczeń przed wyciekami DNS i audytowanych konfiguracji WireGuard.

PRZEGLĄD NAUKOWY: PRZEWODNIK PO NAJBEZPIECZNIEJSZYM 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 standardy techniczne wysoce bezpiecznych sieci VPN. Poznasz sprzęt serwerowy działający wyłącznie w pamięci RAM, bezpieczeństwo dostępu Zero Trust, prywatne szyfrowane resolwery DNS i audytowane konfiguracje WireGuard.

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/najbezpieczniejszy-vpn/

Twoja ścieżka nauki: najbezpieczniejszy VPN

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

INSTRUKCJE: PRZEWODNIK PO NAJBEZPIECZNIEJSZYM VPN

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 sprzętu serwerowego działającego wyłącznie w pamięci RAM i systemów Zero Trust. Zakończ zadaniem dodatkowym Myśl szybko.

INFRASTRUKTURY DZIAŁAJĄCE WYŁĄCZNIE W PAMIĘCI RAM I SIECI ZERO TRUST (WPROWADZENIE)

Naprawdę bezpieczny VPN opiera się na modelu zero trust, serwerach działających wyłącznie w pamięci RAM, które zapobiegają ujawnieniu logów po przejęciu dysków, prywatnych szyfrowanych resolwerach DNS i audytowanych protokołach, takich jak WireGuard. Te połączone zabezpieczenia chronią cenne zasoby cyfrowe przed zagrożeniami związanymi z przechwytywaniem.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Jaka architektura ma fundamentalne znaczenie dla zapewnienia najwyższego bezpieczeństwa we współczesnych serwerach VPN?

- A) Infrastruktura serwerowa działająca wyłącznie w pamięci RAM
- B) Przechowywanie na dyskach
- C) Dynamiczny routing DNS
- D) Włączenie przekierowania portów

2. Jaki protokół jest powszechnie zalecany dla najbezpieczniejszych i najnowocześniejszych konfiguracji VPN?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3. Jakie ramy bezpieczeństwa wymagają ciągłego, bezwyjątkowego weryfikowania każdego połączenia?

- A) Architektura Zero Trust
- B) Zapory obwodowe
- C) Routing dynamiczny
- D) Współdzielone klucze tajne

4. Jaka jest główna rola ochrony przed wyciekami DNS w kliencie VPN?

- A) Kieruj wszystkie żądania DNS przez prywatne szyfrowane resolwery
- B) Zaciemnianie pakietów IP
- C) Lokalne buforowanie zapytań DNS
- D) Wyłącz serwery nazw

5. W jaki sposób routing Multi-Hop zwiększa ogólne bezpieczeństwo tunelu VPN?

- A) Kieruje dane przez dwa oddzielne serwery po kolei
- B) Zwiększa szybkość kompresji
- C) Szyfruje dane szyframi o niskim poziomie bezpieczeństwa
- D) Omija zapory sieciowe

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Serwery działające wyłącznie w pamięci RAM przechowują pliki logów w pamięci ulotnej, która jest czyszczona przy ponownym uruchomieniu.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. WireGuard używa nowoczesnych algorytmów kryptograficznych, które są mniej podatne na wąskie gardła prędkości.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Kill switch VPN działa, blokując cały ruch sieciowy, jeśli tunel zostanie zerwany.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Niezależne audyty stron trzecich nie mają znaczenia dla weryfikacji zobowiązań dotyczących bezpieczeństwa.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Modele Zero Trust zakładają, że wszystkie wewnętrzne połączenia sieciowe są domyślnie bezpieczne.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Administratorzy wymuszają bezpieczeństwo, wdrażając ścisły model bezpieczeństwa o nazwie _____ .

2. Kierowanie pakietów przez wiele punktów wejścia wymaga bezpiecznej konfiguracji typu _____ .

3. Aby zapobiec wyciekom danych ze skradzionych dysków, stosujemy konstrukcję typu _____ .

4. Przejmowaniu ruchu przez dostawcę internetu (ISP) zapobiega się, konfigurując natywną funkcję: _____ .

5. Aby blokować ruch podczas awarii połączenia, włącz mechanizm _____ .

6. Aby zminimalizować przechowywane logi baz danych, wybierz dostawcę, który jest w pełni _____ .

BANK SŁÓW

AUDYTOWANY KILL SWITCH MULTI-HOP OCHRONA DNS PROTOKÓŁ SERWER RAM-ONLY SZYFROWANIE ZERO TRUST

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć dotyczących VPN i sieci

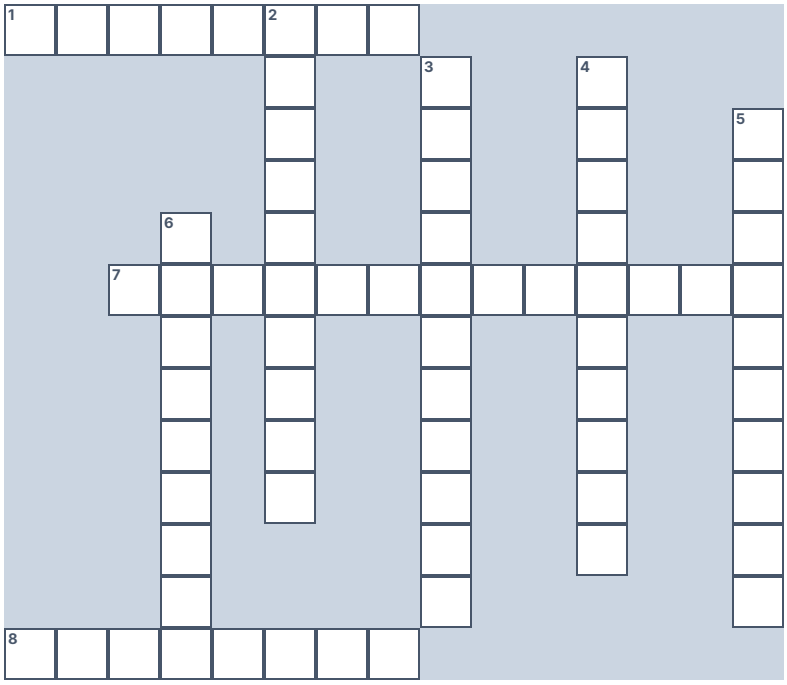
DOPASOWYWANIE DEFINICJI

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

☐	1. Zero Trust	A	Niezależnie skontrolowana konfiguracja potwierdzająca, że nie są przechowywane żadne logi.
☐	2. Multi-Hop	B	Kryptograficzne zniekształcanie ładunków danych w celu zabezpieczenia transmisji.
☐	3. Serwer działający wyłącznie w pamięci RAM	C	Framework bezpieczeństwa wymagający ciągłego uwierzytelniania wszystkich użytkowników.
☐	4. Ochrona DNS	D	Zestaw reguł technicznych określających, jak dane są pakowane i wysyłane.
☐	5. Kill Switch	E	Kaskadowy routing VPN łączący dwa węzły serwerów w łańcuch.
☐	6. Audytowany system	F	Architektura serwerowa wykorzystująca pamięć ulotną do przechowywania ładunków danych.
☐	7. Szyfrowanie	G	Wymuszanie prywatnych zapytań DNS w celu ochrony wyszukiwań serwerów nazw.
☐	8. Protokół	H	Mechanizm bezpieczny w razie awarii, który blokuje ruch, jeśli VPN przestanie działać.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

1. Zbiór reguł technicznych określających, jak dane są pakowane i wysyłane (8)

7. Architektura serwera wykorzystująca pamięć ulotną do przechowywania ładunków danych (13)

8. Kaskadowe trasowanie VPN łączące ze sobą dwa węzły serwerów (8)

PIONOWO

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

3. Kryptograficzne maskowanie ładunków danych w celu zabezpieczenia tranzytu (11)

4. Wymuszanie prywatnych zapytań DNS w celu ochrony wyszukiwań serwerów nazw (10)

5. Niezależnie sprawdzona konfiguracja potwierdzająca, że nie są przechowywane żadne logi (10)

6. Ramy bezpieczeństwa wymagające ciągłego uwierzytelniania wszystkich użytkowników (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: Zbiór reguł technicznych określających, jak dane są pakowane i wysyłane (8 liter):

7 poziomo: Architektura serwera wykorzystująca pamięć ulotną do przechowywania ładunków danych (13 liter):

8 poziomo: Kaskadowe trasowanie VPN łączące ze sobą dwa węzły serwerów (8 liter):

PIONOWO

2 pionowo: Mechanizm zabezpieczający, który blokuje ruch, gdy VPN przestaje działać (10 liter):

3 pionowo: Kryptograficzne maskowanie ładunków danych w celu zabezpieczenia tranzytu (11 liter):

4 pionowo: Wymuszanie prywatnych zapytań DNS w celu ochrony wyszukiwań serwerów nazw (10 liter):

5 pionowo: Niezależnie sprawdzona konfiguracja potwierdzająca, że nie są przechowywane żadne logi (10 liter):

6 pionowo: Ramy bezpieczeństwa wymagające ciągłego uwierzytelniania wszystkich użytkowników (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.

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

LISTA SŁÓW

ZEROTRUST MULTIHOP SERWERRAMONLY OCHRONADNS KILLSWITCH
AUDYTOWANY SZYFROWANIE PROTOKÓŁ

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. SERWERRAMONLY**
- **D. OCHRONADNS**
- **E. KILLSWITCH**
- **F. AUDYTOWANY**
- **G. SZYFROWANIE**
- **H. PROTOKÓŁ**

DEFINICJE I POLA DOPASOWANIA

1. Mechanizm zabezpieczający, który blokuje ruch, gdy VPN przestaje działać.
2. Wymuszanie prywatnych zapytań DNS w celu ochrony wyszukiwań serwerów nazw.
3. Kaskadowe trasowanie VPN łączące ze sobą dwa węzły serwerów.
4. Zbiór reguł technicznych określających, jak dane są pakowane i wysyłane.
5. Kryptograficzne maskowanie ładunków danych w celu zabezpieczenia tranzytu.
6. Architektura serwera wykorzystująca pamięć ulotną do przechowywania ładunków danych.
7. Niezależnie sprawdzona konfiguracja potwierdzająca, że nie są przechowywane żadne logi.
8. Ramy bezpieczeństwa wymagające ciągłego uwierzytelniania wszystkich użytkowników.

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. RTOEZUSTR
2. LEERRSNRYM OAW
3. KWCIISHLTL
4. WIEOYRNASZ F
5. IHUPTMOL
6. NORADOCNSH
7. UYAWOANYT D
8. TROŁPÓKO

Zadanie dodatkowe: Myśl szybko

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

1	Zamki lub klucze, których używasz codziennie			
2	Rzeczy, które VPN może ukryć			
3	Rzeczy, które sprawiają, że VPN jest bezpieczny			
4	Mity o VPN			
5	Powody, dla których warto używać VPN podczas podróży			
6	Bezpieczne miejsca w prawdziwym świecie			
7	Słowa oznaczające „chroniony”			
8	Obietnice, które składa dobry dostawca VPN			
9	Słowa związane z prywatnością			
10	Rodzaje audytu lub inspekcji			
11	Słowa z tej karty pracy, które chcesz zapamiętać			
12	Rzeczy, które haker chce ukraść			
13	Sposoby na rozpoznanie fałszywej sieci Wi-Fi			
14	Miejsca, w których używałbyś VPN			
15	Rzeczy, które może zobaczyć twój dostawca internetu			

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: WZMACNIANIE INFRASTRUKTURY FIRMOWEJ



Scenariusz: Bank korporacyjny przeprojektowuje topologię dostępu zdalnego. Wymaga architektury zero trust łączącej wszystkie urządzenia klienckie z bezpiecznymi serwerami.

Pytanie do dyskusji: Jaka jest główna korzyść mikrosegmentacji sieci w modelu VPN Zero Trust?

STUDIUM PRZYPADKU 2: OCHRONA SERWERÓW TYLKO Z RAM



Scenariusz: Dostawca VPN stawiający na bezpieczeństwo modernizuje swoje serwery, aby zapobiec temu, by fizyczne zajęcie serwera ujawniło historie logów użytkowników.

Pytanie do dyskusji: Wyjaśnij, w jaki sposób konfiguracje sprzętowe wyłącznie z pamięcią RAM uniemożliwiają kryminalistyczne wydobycie danych podczas fizycznego zajęcia serwera.

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

3	7	33	22	12	7	4	33	18	7	29	22	18

4	11	24	20	18	12	2	4	7	18	18	7	33	1	25	20	3	32

4	32	9	24	20	30	7

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: Co sprawia, że VPN jest „najbezpieczniejszy”?

Połączenie Zero Trust, serwerów działających wyłącznie w pamięci RAM i audytowanych protokołów.

Q2: Czym są serwery działające wyłącznie w pamięci RAM?

Serwery działające w pamięci ulotnej, zaprojektowane tak, aby nie zapisywać logów na dysku.

Q3: Czym jest VPN Zero Trust?

Framework, który stale weryfikuje każde żądanie dostępu i połączenie.

Q4: Dlaczego WireGuard uważa się za bezpieczny?

Ma niewielką, łatwą do audytu bazę kodu i używa nowoczesnych szyfrów.

Q5: Jak bezpieczne VPN-y zapobiegają wyciekom DNS?

Przez kierowanie wszystkich zapytań przez prywatne, szyfrowane resolwery DNS.

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 bezpieczny VPN wymaga audytów?

Tak, niezależne audyty weryfikują deklaracje o braku logów i bezpieczeństwo kodu.

Q7: Jaką rolę pełni kill switch?

Natychmiast wstrzymuje ruch sieciowy, jeśli połączenie VPN zostanie przerwane.

Q8: Jakiego szyfrowania używają bezpieczne VPN-y?

AES-256 i ChaCha20 są branżowymi standardami szyfrowania.

Q9: Czy routing Multi-Hop jest bezpieczny?

Tak, łączy w łańcuch dwa lub więcej serwerów, aby zapobiec analizie ruchu.

Q10: Jak pomaga jurysdykcja offshore?

Może ograniczać to, jakie przepisy mają zastosowanie, ale nie zapewnia absolutnego immunitetu.

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 serwery działające wyłącznie w pamięci RAM zapobiegają ryzyku przejęcia danych?

Ponieważ działają w pamięci RAM, wyciągnięcie wtyczki z gniazdka usuwa dane przechowywane w pamięci.

Q2: Jak Zero Trust zastępuje standardowe zabezpieczenia perymetryczne?

Traktuje każdego klienta jako wrogiego, wymagając ciągłego uwierzytelniania.

Q3: Dzięki czemu kod WireGuard łatwiej poddać audytowi?

Jego kod dla Linuksa liczy mniej niż 4000 linii, znacznie mniej niż typowe stosy VPN. [4]

Q4: Jak DNSSEC chroni zapytania DNS?

Podpisuje rekordy DNS, aby resolwery mogły wykryć sfałszowane lub zmanipulowane odpowiedzi.

Q5: Jak Multi-Hop utrudnia korelację ruchu?

Przez rozdzielenie przychodzących i wychodzących adresów IP między różnych dostawców hostingu.

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: Dlaczego jurysdykcje Five Eyes są ryzykowne dla VPN-ów?

Państwa członkowskie dzielą się informacjami wywiadowczymi i mogą korzystać z nakazów prawnych, aby domagać się danych użytkowników.

Q7: Jak kill switch jest zaimplementowany na poziomie jądra?

Używa reguł zapory sieciowej systemu (takich jak iptables lub WFP), aby blokować ruch wychodzący.

Q8: Czym jest forward secrecy w uzgadnianiu połączenia VPN?

Generuje unikalne klucze sesji, dzięki czemu przeszłych sesji nie można odszyfrować.

Q9: Jak bezpieczne VPN-y ograniczają wycieki WebRTC?

Przez blokowanie żądań WebRTC lub kierowanie ich przez tunel.

Q10: Jak niezależne audyty zapewniają zgodność z zasadami prywatności?

Audytorzy przeprowadzają testy penetracyjne i sprawdzają konfiguracje serwerów.

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

Serwery działające wyłącznie w pamięci RAM ładują system operacyjny do pamięci podczas rozruchu, więc po ponownym uruchomieniu nic nie pozostaje na dysku.

2. WGLĄD W VPN

WireGuard używa frameworka Noise z Curve25519, ChaCha20, Poly1305, BLAKE2s i HKDF. [3]

3. WGLĄD W VPN

Zero Trust przyznaje dostęp do każdego zasobu osobno i nie daje domyślnego zaufania na podstawie lokalizacji w sieci (NIST SP 800-207). [1]

4. WGLĄD W VPN

Sojusz wywiadowczy Five Eyes obejmuje USA, Wielką Brytanię, Kanadę, Australię i Nową Zelandię.

5. WGLĄD W VPN

Wycieki WebRTC występują, gdy przeglądarki ujawniają prawdziwy publiczny adres IP klienta za pomocą zapytań STUN.

6. WGLĄD W VPN

Doskonała poufność przekazywania (PFS) zapewnia, że naruszenie klucza długoterminowego nie ujawnia kluczy poprzednich sesji. [3]

7. WGLĄD W VPN

Cure53, berlińska firma zajmująca się bezpieczeństwem, opublikowała audyty kilku dostawców VPN.

8. WGLĄD W VPN

Wycieki DNS występują, gdy zapytania DNS omijają tunel VPN i trafiają do serwerów nazw lokalnego dostawcy internetu.

9. WGLĄD W VPN

Ulotne układy RAM wymagają stałego zasilania, aby przechowywać dane, a po wyłączeniu zasilania tracą swoją zawartość.

10. WGLĄD W VPN

Systemy Zero Trust dla przedsiębiorstw wymuszają kontrole stanu urządzenia przed zezwoleniem na połączenie z zabezpieczonymi zasobami. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

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

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

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

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 **Serwer działający wyłącznie w pamięci RAM** WYŁĄCZNIE RAM — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Serwery działające wyłącznie w pamięci RAM nie przechowują logów na dysku i usuwają dane przy ponownym uruchomieniu. Źródło: Most Secure VPN.

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

UWAGA DLA NAUCZYCIELA

WireGuard łączy niewielką, możliwą do audytu bazę kodu z nowoczesnymi szyframi.

3 **Model Zero Trust** ZERO TRUST — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Modele Zero Trust stale weryfikują zgodność urządzenia przed udzieleniem dostępu. Źródło: Most Secure VPN.

4 **Ochrona DNS** OCHRONA DNS — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Ochrona przed wyciekami DNS kieruje zapytania wyszukiwania przez prywatne resolwery. Źródło: Most Secure VPN.

5 **Tunele Multi-Hop** MULTI-HOP — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Routing Multi-Hop łączy szeregowo dwa oddzielne węzły serwerowe. Źródło: Most Secure VPN.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Serwer działający wyłącznie w pamięci RAM** WYŁĄCZNIE RAM — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Sprzęt serwerów działających wyłącznie w pamięci RAM nie zapisuje danych na dysku i jest czyszczony przy ponownym uruchomieniu. Źródło: Most Secure VPN.

7 **Szybkość WireGuard** WIREGUARD — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

WireGuard używa nowoczesnej kryptografii, która unika wąskich gardeł przetwarzania. Źródło: Most Secure VPN.

8 **Kill Switch** PRZEŁĄCZNIK AWARYJNY — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Kill switch blokuje cały ruch, jeśli połączenie VPN zostanie zerwane. Źródło: Most Secure VPN.

9 **Audyty zewnętrzne** AUDYTY SĄ NIEZBĘDNE — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Audyty zewnętrzne są niezbędne do weryfikacji deklaracji firm dotyczących prywatności. Źródło: Most Secure VPN.

10 **Pytanie 10** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Zero Trust nie przyznaje domyślnego zaufania na podstawie lokalizacji w sieci. [1]

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

C 1. Zero Trust	E 2. Multi-Hop	F 3. Serwer działający wyłącznie w pamięci RAM	G 4. Ochrona DNS
H 5. Kill Switch	A 6. Audytowany system	B 7. Szyfrowanie	D 8. Protokół

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 ZERO TRUST	2 MULTI-HOP	3 SERWER RAM-ONLY	4 OCHRONA DNS
5 KILL SWITCH	6 AUDYTOWANY		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 E – KILLSWITCH	2 D – OCHRONADNS	3 B – MULTIHOP	4 H – PROTOKÓŁ
5 G – SZYFROWANIE	6 C – SERWERRAMONLY	7 F – AUDYTOWANY	8 A – ZEROTRUST

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Zero Trust, Multi-Hop i Serwer działający wyłącznie w pamięci RAM oraz podać przykład każdego z nich.

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

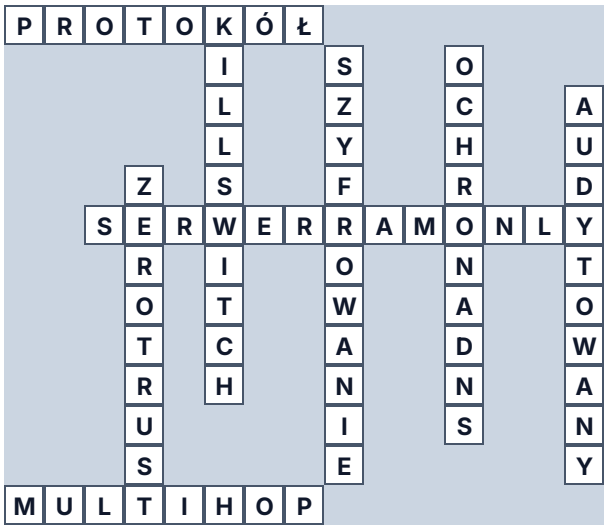
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

1 poziomo: PROTOKÓŁ Zbiór reguł technicznych określających, jak dane są pakowane i wysyłane (8 liter)

7 poziomo: SERWERRAMONLY Architektura serwera wykorzystująca pamięć ulotną do przechowywania ładunków danych (13 liter)

8 poziomo: MULTIHOP Kaskadowe trasowanie VPN łączące ze sobą dwa węzły serwerów (8 liter)

PIONOWO

2 pionowo: KILLSWITCH Mechanizm zabezpieczający, który blokuje ruch, gdy VPN przestaje działać (10 liter)

3 pionowo: SZYFROWANIE Kryptograficzne maskowanie ładunków danych w celu zabezpieczenia tranzytu (11 liter)

4 pionowo: OCHRONADNS Wymuszanie prywatnych zapytań DNS w celu ochrony wyszukiwań serwerów nazw (10 liter)

5 pionowo: AUDYTOWANY Niezależnie sprawdzona konfiguracja potwierdzająca, że nie są przechowywane żadne logi (10 liter)

6 pionowo: ZEROTRUST Ramy bezpieczeństwa wymagające ciągłego uwierzytelniania wszystkich użytkowników (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. RTOEZUSTR — **ZEROTRUST**
2. LEERRSNRYMOAW — **SERWERRAMONLY**
3. KWCIISHLTL — **KILLSWITCH**
4. WIEOYRNASZF — **SZYFROWANIE**
5. IHUPTMOL — **MULTIHOP**
6. NORADOCNSH — **OCHRONADNS**
7. UYAWOANYTD — **AUDYTOWANY**
8. TROŁPÓKO — **PROTOKÓŁ**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"BEZPIECZNE VPN CHRONIĄ CENNE ZASOBY CYFROWE"

Klucz odpowiedzi do studiów przypadków

A STUDIUM PRZYPADKU 1: WZMACNIANIE INFRASTRUKTURY FIRMOWEJ

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Bank korporacyjny przeprojektowuje topologię dostępu zdalnego. Wymaga architektury zero trust łączącej wszystkie urządzenia klienckie z bezpiecznymi serwerami.
- Zalecana strategia i rozwiązanie: Wskazówki do oceny: Wyjaśnij, że mikrosegmentacja ogranicza dostęp do konkretnych zasobów, zapobiegając bocznemu rozprzestrzenianiu się zagrożenia w razie przejęcia urządzenia.

B STUDIUM PRZYPADKU 2: OCHRONA SERWERÓW TYLKO Z RAM

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Dostawca VPN skoncentrowany na bezpieczeństwie modernizuje swoje serwery, aby fizyczne zajęcie serwera nie ujawniło historii logów użytkowników.
- Zalecana strategia i rozwiązanie: Wskazówki do oceny: Opisz, że serwery działające wyłącznie w pamięci RAM nie mają fizycznego dysku. Utrata zasilania automatycznie usuwa wszystkie ulotne dane z pamięci.