Imię i nazwisko: _____ Data: _____ Wynik: _____

Bezpieczeństwo Surfshark

Analiza funkcji bezpieczeństwa Surfshark, w tym blokowania reklam CleanWeb, dynamicznego routingu MultiHop, architektury Nexus SDN, floty serwerów działających wyłącznie w pamięci RAM i trybu Camouflage.

SURFSHARK – BEZPIECZEŃSTWO – PRZEGLĄD NAUKI

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 architekturę bezpieczeństwa Surfshark. Poznasz sprzęt serwerowy działający wyłącznie w pamięci RAM, dynamiczną rotację IP w Nexus SDN, blokery reklam CleanWeb i routing MultiHop.

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/surfshark/bezpieczenstwo/

Twoja ścieżka nauki: bezpieczeństwo Surfshark

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

INSTRUKCJE DO PRZEWODNIKA O BEZPIECZEŃSTWIE SURFSHARK

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 infrastruktury działającej wyłącznie w pamięci RAM, Nexus SDN i CleanWeb. Zakończ zadaniem dodatkowym Myśl szybko.

FLOTA SERWERÓW DZIAŁAJĄCYCH WYŁĄCZNIE W PAMIĘCI RAM, NEXUS SDN I ARCHITEKTURA CLEANWEB (WPROWADZENIE)

Surfshark chroni prywatność użytkowników dzięki flocie serwerów działających wyłącznie w pamięci RAM, sieci programowej Nexus z IP Rotator, blokowaniu reklam CleanWeb i ścieżkom szyfrowania Dynamic MultiHop.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **1. Jak nazywa się zintegrowany bloker reklam i złośliwego oprogramowania w Surfshark?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Jakiej architektury sprzętowej używa Surfshark na wszystkich serwerach?**
   - A) Dyski twarde
   - B) 100% wyłącznie w pamięci RAM
   - C) Pamięć optyczna
   - D) Taśma magnetyczna

3. **3. Jaka funkcja kieruje ruch przez dwa różne serwery VPN?**
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Sieć Nexus
   - D) Statyczny adres IP

4. **4. Jaka funkcja obfuskacji maskuje ruch VPN jako zwykłe dane internetowe?**
   - A) Kill Switch
   - B) Tryb maskowania
   - C) CleanWeb 2.0
   - D) Dzielony tunel

5. **5. Jaka jest funkcja narzędzia Surfshark Bypasser?**
   - A) Speed Booster
   - B) Tunelowanie podzielone
   - C) Menedżer haseł
   - D) Resolver DNS

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Serwery działające wyłącznie w pamięci RAM natychmiast usuwają wszystkie dane operacyjne po ponownym uruchomieniu serwera.

○ Prawda ○ Fałsz

7 Pytanie 7

7. Tryb Camouflage uniemożliwia dostawcom internetu wykrycie, że korzystasz z VPN.

○ Prawda ○ Fałsz

8 Pytanie 8

8. CleanWeb 2.0 działa w rozszerzeniach przeglądarki, aby blokować wyskakujące okna zgody na pliki cookie.

○ Prawda ○ Fałsz

9 Pytanie 9

9. Surfshark przechowuje tymczasowe znaczniki czasu połączeń i logi zużycia przepustowości.

○ Prawda ○ Fałsz

10 Pytanie 10

10. Sieć Nexus okresowo zmienia adresy IP użytkowników bez rozłączania.

○ Prawda ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Irytujące reklamy internetowe, skrypty śledzące i linki phishingowe blokują filtry _____ .

2. Aktywność użytkownika nie zostawia śladów kryminalistycznych, ponieważ serwery działają na pamięci typu _____ .

3. Kierowanie danych przez dwa osobne zaszyfrowane przeskoki serwerów umożliwiają tunele _____ .

4. Aby ukryć korzystanie z VPN przed dostawcami internetu, użytkownicy aktywują tryb _____ .

5. Zezwalaniem aplikacjom bankowym na omijanie tunelu VPN zarządzają ustawienia _____ .

6. Architektura SDN nowej generacji łącząca flotę serwerów to system _____ .

BANK SŁÓW

BYPASSER | CLEANWEB | KAMUFLAŻ | KILL SWITCH | MULTI-HOP | NEXUS | ROTACJA IP | WYŁĄCZNIE RAM

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć dotyczących VPN i sieci

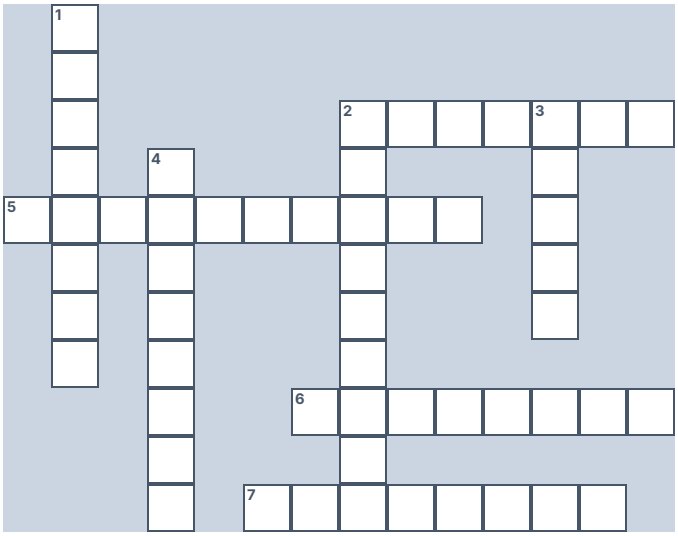
DOPASOWYWANIE DEFINICJI

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

☐	1. CLEANWEB	A	Automatyczna funkcja bezpieczeństwa blokująca ruch sieciowy, gdy VPN się rozłączy.
☐	2. WYŁĄCZNIE RAM	B	Funkcja tunelowania dzielonego pozwalająca wybranym aplikacjom omijać VPN.
☐	3. MULTI-HOP	C	Zaawansowany filtr blokujący reklamy, złośliwe oprogramowanie i banery zgody na pliki cookie.
☐	4. KAMUFLAŻ	D	Sprzęt serwerowy z pamięcią ulotną, który usuwa wszystkie dane przy każdym cyklu zasilania.
☐	5. OMIJACZ	E	Funkcja, która regularnie zmienia Twój zewnętrzny adres IP bez przerywania tuneli.
☐	6. KILL SWITCH	F	Technologia obfuskacji, która ukrywa sygnatury VPN, aby naśladować zwykły ruch HTTPS.
☐	7. NEXUS NET	G	Funkcja routingu podwójnego VPN szyfrująca ruch przez dwa różne węzły serwerów.
☐	8. ROTACYJNE	H	Własnościowa sieć definiowana programowo łącząca wszystkie serwery w jedną spójną siatkę.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

2. Sprzęt serwerowy z pamięcią ulotną, który wymazuje wszystkie dane przy każdym cyklu zasilania (7)

5. Automatyczne zabezpieczenie blokujące ruch sieciowy, gdy VPN przestaje działać (10)

6. Technologia zaciemniania, która ukrywa sygnatury VPN, aby naśladować zwykły ruch HTTPS (8)

7. Funkcja podziału tunelu pozwalająca wybranym aplikacjom omijać VPN (8)

PIONOWO

1. Funkcja podwójnego VPN szyfrująca ruch przez dwa różne węzły serwerów (8)

2. Funkcja regularnie zmieniająca zewnętrzny adres IP bez przerywania tuneli (9)

3. Własna sieć definiowana programowo łącząca wszystkie serwery w jedną siatkę (5)

4. Zaawansowany filtr blokujący reklamy, złośliwe oprogramowanie i banery zgody na pliki cookie (8)

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

2 poziomo: Sprzęt serwerowy z pamięcią ulotną, który wymazuje wszystkie dane przy każdym cyklu zasilania (7 liter):

5 poziomo: Automatyczne zabezpieczenie blokujące ruch sieciowy, gdy VPN przestaje działać (10 liter):

6 poziomo: Technologia zaciemniania, która ukrywa sygnatury VPN, aby naśladować zwykły ruch HTTPS (8 liter):

7 poziomo: Funkcja podziału tunelu pozwalająca wybranym aplikacjom omijać VPN (8 liter):

PIONOWO

1 pionowo: Funkcja podwójnego VPN szyfrująca ruch przez dwa różne węzły serwerów (8 liter):

2 pionowo: Funkcja regularnie zmieniająca zewnętrzny adres IP bez przerywania tuneli (9 liter):

3 pionowo: Własna sieć definiowana programowo łącząca wszystkie serwery w jedną siatkę (5 liter):

4 pionowo: Zaawansowany filtr blokujący reklamy, złośliwe oprogramowanie i banery zgody na pliki cookie (8 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 S Ś E Ł J B K A B C Ó Z Ł K
Z L Y T L D Q A N K B D I Ń N
L Q Ó G N N Q M R S Y T T F B
P Ś P O H S B U W Ć P Ś Ź V C
I S Ż W Ę K L F G Ż A Ć N C D
A U Q Y Ó I C L U B S A Ż L Ń
J X Ć L A L D A M O S D Ę E G
C E I Ć R L Q Ż U R E M E A I
A N S Ż Ś S Ę Q L A R V E N A
T A Q Ó N W P T T M Y Q K W R
O T S Ć N I Ź B I O Ę S Y E X
R J A R Ż T Z Z H N Ł F I B N
R K M M T C O G O L P Q G Ż Ą
O V F V B H Ź S P Y Ź B G M Ż
G K O P Ń X C M Ż Ź F Z O X U

LISTA SŁÓW

CLEANWEB RAMONLY MULTIHOP KAMUFLAŻ BYPASSER KILLSWITCH NEXUS ROTACJAIP

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. CLEANWEB**
- **B. RAMONLY**
- **C. MULTIHOP**
- **D. KAMUFLAŻ**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. ROTACJAIP**

DEFINICJE I POLA DOPASOWANIA

1. Technologia zaciemniania, która ukrywa sygnatury VPN, aby naśladować zwykły ruch HTTPS.
2. Automatyczne zabezpieczenie blokujące ruch sieciowy, gdy VPN przestaje działać.
3. Zaawansowany filtr blokujący reklamy, złośliwe oprogramowanie i banery zgody na pliki cookie.
4. Funkcja podziału tunelu pozwalająca wybranym aplikacjom omijać VPN.
5. Sprzęt serwerowy z pamięcią ulotną, który wymazuje wszystkie dane przy każdym cyklu zasilania.
6. Funkcja regularnie zmieniająca zewnętrzny adres IP bez przerywania tuneli.
7. Funkcja podwójnego VPN szyfrująca ruch przez dwa różne węzły serwerów.
8. Własna sieć definiowana programowo łącząca wszystkie serwery w jedną siatkę.

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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. NYOMRLA
6. AŻULKFAM
7. ILKIWTCHSL
8. PCIRAOJAT

Zadanie dodatkowe: Myśl szybko

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

1	Funkcje bezpieczeństwa w Surfshark			
2	Oznaki, że twoje połączenie VPN jest wolne			
3	Protokoły VPN, które znasz			
4	Rzeczy, które chroni szyfrowanie			
5	Zagrożenia w publicznych sieciach Wi-Fi			
6	Kraje znane z silnych przepisów o prywatności			
7	Sposoby na stworzenie silnego hasła			
8	Urządzenia, na których zainstalowałbyś Surfshark			
9	Pytania do pomocy technicznej Surfshark			
10	Ustawienia, które włączasz dla dodatkowego bezpieczeństwa			
11	Rzeczy, które Surfshark może ukryć w twojej sieci			
12	Rodzaje wycieków VPN			
13	Dane, których VPN nigdy nie powinien przechowywać			
14	Słowa opisujące dobrą aplikację VPN			
15	Rzeczy, które może sprawdzić audyt			

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: OMIJANIE FILTRÓW W KAMPUSIE I MIEJSCU PRACY

👷

Scenariusz: Student stwierdza, że Wi-Fi na kampusie jego uczelni blokuje wszystkie standardowe porty OpenVPN i WireGuard.

Pytanie do dyskusji: Która funkcja Surfshark pozwala studentowi połączyć się bez wykrycia przez administratorów sieci?

STUDIUM PRZYPADKU 2: DZIENNIKARSKIE ŚLEDZTWO WYSOKIEGO RYZYKA

👷

Scenariusz: Dziennikarz śledczy potrzebuje dodatkowej ochrony przed inwigilacją podczas badania wrażliwych dokumentów korporacyjnych.

Pytanie do dyskusji: W jaki sposób Dynamic MultiHop zapewnia lepszą prywatność w porównaniu z routingiem przez jeden serwer?

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

25 28 24 9 25 11 1 24 14 18 7 31 28 25

24 20 27 28 13 7 12 22 30 33 17 1 4 18 12 1

22 24 32 30 1 27 18 20 26 5

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: Czym jest Surfshark CleanWeb?

CleanWeb to zintegrowana funkcja bezpieczeństwa, która blokuje reklamy, trackery, złośliwe oprogramowanie i strony phishingowe.

Q2: Czym są serwery działające wyłącznie w pamięci RAM?

Serwery działające wyłącznie w pamięci RAM korzystają z pamięci ulotnej, co oznacza, że dane przechowywane w pamięci są usuwane przy każdym ponownym uruchomieniu serwerów.

Q3: Czym jest Surfshark MultiHop?

MultiHop (Double VPN) kieruje i szyfruje twoje połączenie internetowe przez dwie różne lokalizacje serwerów.

Q4: Jak działa Camouflage Mode?

Tryb Camouflage ukrywa ruch VPN, aby Twój dostawca internetu nie mógł stwierdzić, że korzystasz z VPN.

Q5: Czym jest funkcja Bypasser?

Bypasser to narzędzie tunelowania podzielonego firmy Surfshark, które pozwala wybranym aplikacjom lub witrynom omijać VPN.

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 Surfshark ma Kill Switch?

Tak, Kill Switch odcina Cię od internetu, jeśli VPN nieoczekiwanie przestanie działać.

Q7: Jakiego standardu szyfrowania używa Surfshark?

Surfshark używa AES-256-GCM i ChaCha20, a w nowym protokole Dausos także AEGIS-256X2.

Q8: Czy polityka braku logów Surfshark została poddana audytowi?

Tak, Deloitte zweryfikował politykę braku dzienników Surfshark w 2023 roku i ponownie w 2025 roku.

Q9: Czym jest Surfshark Nexus?

Nexus to zaawansowana architektura SDN, która łączy wszystkie serwery w jedną sieć dla płynniejszego routingu.

Q10: Czym jest funkcja IP Rotator?

IP Rotator automatycznie zmienia Twój adres IP co kilka minut bez rozłączania sesji VPN.

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: Czym Dynamic MultiHop różni się od tradycyjnego Double VPN?

Dynamic MultiHop pozwala dostosować dowolną kombinację serwerów wejściowych i wyjściowych na całym świecie.

Q2: Czy CleanWeb 2.0 działa w rozszerzeniach przeglądarki?

Tak, CleanWeb 2.0 blokuje reklamy wideo, wyskakujące okienka zgody na pliki cookie i banery z alertami w przeglądarkach Chrome/Firefox.

Q3: Czym jest Alternative ID w pakiecie zabezpieczeń?

Alternative ID generuje unikalne osobiste pseudonimy, adresy e-mail i maski telefonu.

Q4: Jak Surfshark zapobiega wyciekom DNS?

Surfshark kieruje wszystkie żądania domen przez własne prywatne serwery DNS na każdym węźle.

Q5: Czy Surfshark obsługuje szyfrowanie ChaCha20 na urządzeniach mobilnych?

Tak, WireGuard na Androidzie i iOS używa ChaCha20-Poly1305, co zapewnia lepszą wydajność na urządzeniach mobilnych.

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: Czym jest tryb NoBorders w Surfshark?

NoBorders automatycznie wykrywa restrykcyjne środowiska sieciowe i udostępnia wyspecjalizowane serwery.

Q7: Kto przeprowadził audyty bezpieczeństwa rozszerzeń przeglądarki Surfshark?

Niezależna firma z branży cyberbezpieczeństwa Cure53 przeprowadziła audyty rozszerzeń przeglądarki i systemów serwerowych.

Q8: Jak Surfshark chroni przed wyciekami IPv6?

Surfshark bezpiecznie kieruje ruch IPv6 lub bezpiecznie go ogranicza, aby zapobiec jakiemukolwiek wyciekowi bez szyfrowania.

Q9: Gdzie znajduje się jurysdykcja prawna Surfshark?

Surfshark działa na podstawie prawa holenderskiego, przestrzegając rygorystycznych europejskich standardów prywatności RODO (GDPR).

Q10: Czy Surfshark obsługuje uwierzytelnianie dwuskładnikowe (2FA)?

Tak, a Surfshark One dodaje blokadę 2FA, dzięki czemu tylko ty możesz zmieniać ustawienia funkcji.

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

1. Surfshark twierdzi, że cała jego sieć ponad 4,500 serwerów działa na bezdyskowym sprzęcie z ulotną pamięcią RAM.

2. WGLĄD W VPN

2. Firma z Wielkiej Czwórki, Deloitte, zweryfikowała politykę braku logów Surfshark w 2023 roku i ponownie w listopadzie 2025 roku.

3. WGLĄD W VPN

3. Własna architektura Nexus łączy wszystkie globalne serwery w dynamiczną sieć definiowaną programowo.

4. WGLĄD W VPN

4. Rotating IP zmienia Twój adres IP mniej więcej co pięć minut bez zrywania połączenia VPN.

5. WGLĄD W VPN

5. CleanWeb 2.0 blokuje natrętne wyskakujące okna zgody na pliki cookie i reklamy wideo bezpośrednio w przeglądarkach.

6. WGLĄD W VPN

6. Dynamic MultiHop pozwala użytkownikom tworzyć niestandardowe ścieżki szyfrowania dwóch serwerów w 100 krajach.

7. WGLĄD W VPN

7. Tryb kamuflażu usuwa sygnatury nagłówków VPN, przez co ruch jest nie do odróżnienia od zwykłego HTTPS.

8. WGLĄD W VPN

8. Alternative ID generuje jednorazowe pseudonimy i maski e-mail, aby chronić użytkowników przed wyciekami baz danych.

9. WGLĄD W VPN

9. Surfshark stosuje szyfrowanie symetryczne AES-256-GCM obok ChaCha20 w protokołach WireGuard.

10. WGLĄD W VPN

10. Tryb NoBorders włącza się automatycznie w sieciach z ograniczeniami, aby zapewnić odporny dostęp przez tunel.

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 **Zintegrowany bloker treści** OCHRONA PRZED REKLAMAMI I ZŁOŚLIWYM OPROGRAMOWANIEM **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

CleanWeb to zintegrowany filtr bezpieczeństwa Surfshark, który na poziomie sieci blokuje reklamy, domeny trackerów, strony phishingowe i złośliwe skrypty URL. Źródło: CleanWeb Security Specs.

2 **Infrastruktura w 100% oparta wyłącznie na pamięci RAM** ARCHITEKTURA RAM **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

Surfshark używa serwerów działających wyłącznie w pamięci RAM, więc dane przechowywane w pamięci serwera są usuwane po wyłączeniu lub ponownym uruchomieniu serwera. Źródło: Cure53 Infrastructure Audit.

3 **Podwójne tunelowanie MultiHop** VPN MULTIHOP **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

MultiHop (Double VPN) szyfruje ruch przez dwa różne węzły serwerowe w oddzielnych krajach, aby zapobiegać atakom korelacji ruchu. Źródło: Surfshark MultiHop Guide.

4 **Obfuskacja w trybie Camouflage** OBFUSKACJA **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

Tryb Camouflage modyfikuje nagłówki pakietów OpenVPN, aby upodobnić ruch VPN do standardowego ruchu HTTPS i ominąć restrykcyjne blokady zapór sieciowych. Źródło: Surfshark Stealth Whitepaper.

5 **Tunelowanie podzielone Bypasser** TUNELOWANIE DZIELONE **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

Bypasser to narzędzie tunelowania podzielonego firmy Surfshark, które pozwala użytkownikom wybrać aplikacje lub witryny kierowane bezpośrednio przez ich zwykłe połączenie z ISP. Źródło: Surfshark Client Features.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Czyszczenie danych z pamięci ulotnej** BEZPIECZEŃSTWO SERWERA **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Serwery działające wyłącznie w pamięci RAM nie przechowują żadnych danych na stałych dyskach twardych; ponowne uruchomienie sprzętu natychmiast czyści całą pamięć operacyjną. Źródło: RAM Server Architecture.

7 **Ukrywanie przed dostawcą internetu w trybie Camouflage** UKRYWANIE RUCHU **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Tryb Camouflage usuwa sygnatury protokołu OpenVPN, uniemożliwiając dostawcom internetu wykrycie, że użytkownik jest połączony z tunelem VPN. Źródło: Deep Packet Inspection Guide.

8 **Rozszerzenia przeglądarki CleanWeb 2.0** ROZSZERZENIE PRZEGLĄDARKI **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

CleanWeb 2.0 działa w rozszerzeniach przeglądarki, aby w czasie rzeczywistym blokować wyskakujące okna zgody na pliki cookie, reklamy wideo i złośliwe skrypty przekierowujące. Źródło: CleanWeb 2.0 Release Notes.

9 **Brak przechowywania logów połączeń** POLITYKA BRAKU LOGÓW **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Surfshark stosuje ścisłą, niezależnie audytowaną politykę braku logów i nie rejestruje adresów IP, znaczników czasu połączeń ani logów przepustowości. Źródło: Deloitte No-Logs Audit.

10 **Dynamiczna rotacja IP Nexus** SIEĆ NEXUS **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Sieć definiowana programowo Surfshark Nexus dynamicznie zmienia adresy IP użytkowników co kilka minut bez przerywania aktywnego połączenia VPN. Źródło: Surfshark Nexus Architecture.

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. CLEANWEB	D 2. WYŁĄCZNIE RAM	G 3. MULTI-HOP	F 4. KAMUFLAŻ
B 5. OMIJACZ	A 6. KILL SWITCH	H 7. NEXUS NET	E 8. ROTACYJNE

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 CLEANWEB	2 WYŁĄCZNIE RAM	3 MULTI-HOP	4 KAMUFLAŻ
5 BYPASSER	6 NEXUS		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 D – KAMUFLAŻ	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMONLY	6 H – ROTACJAIP	7 C – MULTIHOP	8 G – NEXUS

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia CLEANWEB, WYŁĄCZNIE RAM i MULTI-HOP oraz podać przykład każdego z nich.

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

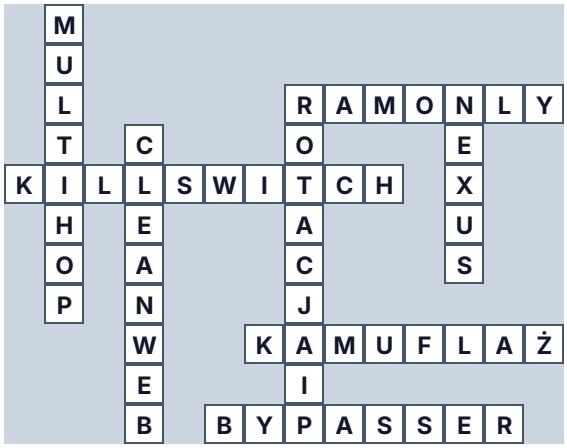
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: RAMONLY Sprzęt serwerowy z pamięcią ulotną, który wymazuje wszystkie dane przy każdym cyklu zasilania (7 liter)

5 poziomo: KILLSWITCH Automatyczne zabezpieczenie blokujące ruch sieciowy, gdy VPN przestaje działać (10 liter)

6 poziomo: KAMUFLAŻ Technologia zaciemniania, która ukrywa sygnatury VPN, aby naśladować zwykły ruch HTTPS (8 liter)

7 poziomo: BYPASSER Funkcja podziału tunelu pozwalająca wybranym aplikacjom omijać VPN (8 liter)

PIONOWO

1 pionowo: MULTIHOP Funkcja podwójnego VPN szyfrująca ruch przez dwa różne węzły serwerów (8 liter)

2 pionowo: ROTACJAIP Funkcja regularnie zmieniająca zewnętrzny adres IP bez przerywania tuneli (9 liter)

3 pionowo: NEXUS Własna sieć definiowana programowo łącząca wszystkie serwery w jedną siatkę (5 liter)

4 pionowo: CLEANWEB Zaawansowany filtr blokujący reklamy, złośliwe oprogramowanie i banery zgody na pliki cookie (8 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. EANCWLBE — **CLEANWEB**
2. TMPUOHIL — **MULTIHOP**
3. AYBSSREP — **BYPASSER**
4. XSUNE — **NEXUS**
5. NYOMRLA — **RAMONLY**
6. AŻULKFAM — **KAMUFLAŻ**
7. ILKIWTCHSL — **KILLSWITCH**
8. PCIRAOJAT — **ROTACJAIP**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"SURFSHARK NEXUS ROTUJE IP WZMACNIA PRYWATNOŚĆ"

Klucz odpowiedzi do studiów przypadków

A STUDIUM PRZYPADKU 1: OMIJANIE FILTRÓW W KAMPUSIE I MIEJSCU PRACY

Rozwiązanie dla nauczyciela

SCHEMAT OCENIANIA I WYTYCZNE DO ROZWIĄZAŃ

- Analiza scenariusza: Student stwierdza, że sieć Wi-Fi jego kampusu uniwersyteckiego blokuje wszystkie standardowe porty OpenVPN i WireGuard.
- Pytanie pomocnicze: Jaka funkcja Surfshark pozwala uczniowi połączyć się bez wykrycia przez administratorów sieci?
- Zalecana strategia i rozwiązanie: Aktywuj Camouflage Mode (OpenVPN), który ukrywa metadane VPN, dzięki czemu zapory widzą zwykłe przeglądanie przez HTTPS.

B STUDIUM PRZYPADKU 2: DZIENNIKARSKIE ŚLEDZTWO WYSOKIEGO RYZYKA

Rozwiązanie dla nauczyciela

SCHEMAT OCENIANIA I WYTYCZNE DO ROZWIĄZAŃ

- Analiza scenariusza: Dziennikarz śledczy potrzebuje dodatkowej ochrony przed inwigilacją podczas badania poufnych dokumentów firmowych.
- Pytanie pomocnicze: Jak Dynamic MultiHop zapewnia lepszą prywatność niż routing przez pojedynczy serwer?
- Zalecana strategia i rozwiązanie: Dynamic MultiHop kieruje ruch przez serwery wejściowe i wyjściowe w dwóch krajach, więc żaden pojedynczy serwer nie może ujawnić użytkownika.