Imię i nazwisko: _____ Data: _____ Wynik: _____

Jak ukryć swój adres IP Karta pracy

Ukrywanie adresów IP, maskowanie lokalizacji, proxy, Tor oraz zapobieganie wyciekom DNS/WebRTC

PRZEGLĄD NAUKI: VPN

UCZEŃ
STATUS STUDENTA
Ścieżka obrońcy sieci

BEZPIECZNY
STAN POŁĄCZENIA
Ochrona pakietów danych

AKTYWNE
OCHRONA PRZED WYCIEKAMI
Ochrona przed wyciekami DNS i IPv6

Witaj! Ten pakiet ćwiczeń przeprowadzi cię przez podstawowe zasady wirtualnych sieci prywatnych (VPN). Poznasz, jak zaszyfrowane tunele zabezpieczają Twoje dane, jak działają protokoły sieciowe oraz jak rozpoznawać i ograniczać wycieki prywatności.

PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj pojęcia i protokoły VPN.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

Otwórz przewodnik VPN.com po VPN

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

Twoja ścieżka nauki: VPN

- Wyjaśnij, jak działają adresy IP i jak ujawniają lokalizację.
- Porównaj proxy, Tora i VPN pod kątem maskowania adresów sieciowych.
- Rozpoznaj metody wykrywania i zapobiegania wyciekom DNS i WebRTC.
- Zrozum, jak strony internetowe śledzą użytkowników przez ich publiczny adres IP.
- Oceń routing multi-hop i szyfrowane tunele pod kątem ochrony adresu IP.

INSTRUKCJE DO KARTY PRACY O OCHRONIE IP

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 ukrywania adresu IP i zapobiegania wyciekom. Zakończ zadaniem dodatkowym Myśl szybko.

UKRYWANIE ADRESU IP (WPROWADZENIE)

Twój adres IP to cyfrowy adres pocztowy, który ujawnia Twoją fizyczną lokalizację i nawyki sieciowe. Ukrycie adresu IP to pierwsza linia obrony przed śledzeniem w sieci, profilowaniem celów i blokadami geolokalizacyjnymi. Zrozumienie, jak bezpiecznie zamaskować adres, pomaga chronić Twoją prywatność w internecie.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Co publiczny adres IP urządzenia ujawnia odwiedzanym przez ciebie stronom?

- A. Numer karty kredytowej użytkownika
- B. Twoją przybliżoną lokalizację i nazwę twojego dostawcy internetu
- C. Pełny lokalny katalog plików
- D. Ustawienia języka klawiatury

2. Która metoda ukrywa twój adres IP i szyfruje cały ruch w całym systemie?

- A. Standardowe proxy internetowe
- B. Czyszczenie plików cookie przeglądarki
- C. Wirtualna sieć prywatna (VPN)
- D. Wyłączenie natywnej zapory sieciowej

3. Jakie jest główne ograniczenie prywatności przy korzystaniu z bezpłatnego proxy WWW?

- A. Nie szyfruje ruchu danych w sieciach publicznych
- B. Wymaga zainstalowania zewnętrznego systemu operacyjnego
- C. Jest całkowicie nielegalna w Stanach Zjednoczonych
- D. Wymaga dedykowanego połączenia linii telefonicznej

4. W jaki sposób sieć Tor zapewnia użytkownikom wysoką anonimowość?

- A. Przyspieszając połączenia
- B. Kierując ruch przez trzy przekaźniki prowadzone przez wolontariuszy
- C. Rejestrując twoje imię i nazwisko w globalnej bazie danych
- D. Ograniczając dostęp tylko do agencji rządowych

5. Czym jest wyciek DNS?

- A. Błąd wysłania e-maila na niewłaściwy adres
- B. Gdy zapytania DNS omijają tunel VPN i trafiają do ISP
- C. Awaria sprzętowa zasilacza lokalnego routera
- D. Aktualizacja sterownika lokalnego adaptera sieciowego

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Serwer proxy szyfruje ruch systemu operacyjnego działający w tle tak samo jak VPN.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Routing Tor jest bardzo bezpieczny, ale zmniejsza szybkość przeglądania sieci.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Wycieki WebRTC mogą ujawnić twój prawdziwy adres IP podczas aktywnej sesji VPN.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Przy włączonym VPN i braku wycieków twój dostawca internetu nie widzi, jakie strony odwiedzasz.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Ukrycie adresu IP blokuje śledzenie przez odcisk palca przeglądarki.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Sytuację, w której zapytania o domeny wydostają się poza bezpieczny tunel, nazywa się _____ .

2. Przeglądarkowe API komunikacji _____ może przypadkowo ujawnić twój natywny adres IP.

3. Serwer _____ przekierowuje ruch przeglądarki, ale nie szyfruje zawartości pakietów.

4. Wielowarstwowe szyfrowanie w sieci o nazwie _____ zapewnia wysoki poziom anonimowości.

5. Twój publiczny _____ jest przydzielany przez operatora telekomunikacyjnego i zdradza twój obszar.

6. Omijanie regionalnych blokad mediów osiąga się za pomocą techniki, której nazwa to _____ lokalizacji.

BANK SŁÓW

ADRES IP | MASKOWANIE | PROXY | ŚLEDZENIE ISP | TOR | TUNEL VPN | WEBRTC | WYCIEK DNS

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć sieciowych

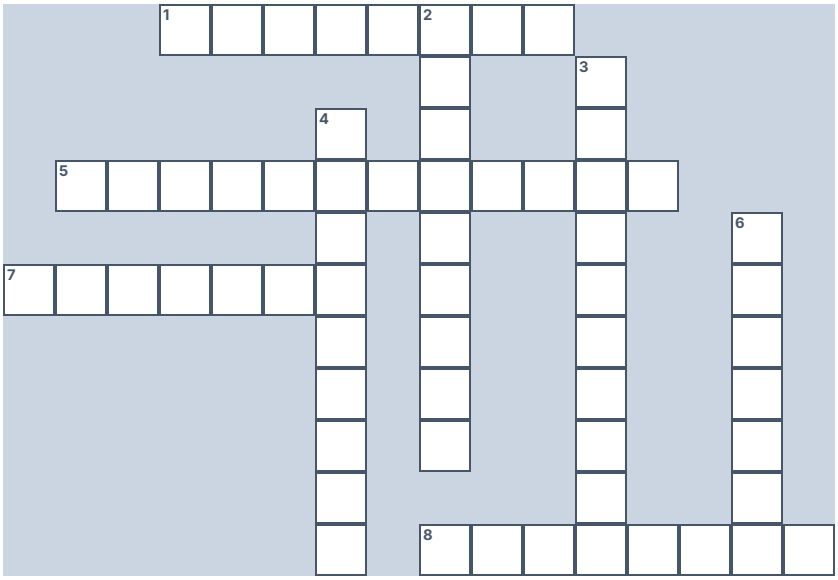
DOPASOWYWANIE DEFINICJI

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

☐	1. Adres IP	A	Szyfruje cały ruch urządzenia i kieruje go przez serwer VPN.
☐	2. Tunel VPN	B	Kieruje dane przez trzy serwery wolontariuszy, szyfrując warstwy na każdym etapie.
☐	3. Sieć Tor	C	Kierowanie połączenia przez serwer w innym kraju w celu ominięcia blokad geograficznych.
☐	4. Proxy sieciowe	D	Unikalna etykieta liczbowa identyfikująca interfejs urządzenia w internecie.
☐	5. Wyciek DNS	E	Przekierowuje ruch przeglądarki na warstwie aplikacji bez szyfrowania systemowego.
☐	6. API WebRTC	F	Rejestrowanie przez Twojego operatora telekomunikacyjnego miejsc docelowych niezaszyfrowanego ruchu internetowego.
☐	7. Maskowanie lokalizacji	G	Zapytania rozwiązywane poza tunelem VPN, ujawniające odwiedzane domeny dostawcy internetu.
☐	8. Śledzenie przez ISP	H	Funkcja przeglądarki dla głosu/wideo, która może omijać tunele i ujawniać prawdziwe adresy IP.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

1. Przekierowuje ruch przeglądarki na poziomie aplikacji bez szyfrowania na poziomie systemu (8)

5. Rejestrowanie miejsc docelowych niezaszyfrowanego ruchu internetowego przez twojego operatora telekomunikacyjnego (12)

7. Kieruje dane przez trzy serwery wolontariuszy, szyfrując warstwy na każdym etapie (7)

8. Szyfruje cały ruch urządzenia i kieruje go przez serwer VPN (8)

PIONOWO

2. Zapytania rozwiązywane poza tunelem VPN, ujawniające dostawcy internetu odwiedzane domeny (9)

3. Kierowanie połączenia przez serwer w innym kraju w celu obejścia blokad geograficznych (10)

4. Funkcja przeglądarki do głosu i wideo, która może omijać tunele i ujawniać prawdziwe adresy IP (9)

6. Unikalna etykieta numeryczna identyfikująca interfejs urządzenia w internecie (7)

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: Przekierowuje ruch przeglądarki na poziomie aplikacji bez szyfrowania na poziomie systemu (8 liter):

5 poziomo: Rejestrowanie miejsc docelowych niezaszyfrowanego ruchu internetowego przez twojego operatora telekomunikacyjnego (12 liter):

7 poziomo: Kieruje dane przez trzy serwery wolontariuszy, szyfrując warstwy na każdym etapie (7 liter):

8 poziomo: Szyfruje cały ruch urządzenia i kieruje go przez serwer VPN (8 liter):

PIONOWO

2 pionowo: Zapytania rozwiązywane poza tunelem VPN, ujawniające dostawcy internetu odwiedzane domeny (9 liter):

3 pionowo: Kierowanie połączenia przez serwer w innym kraju w celu obejścia blokad geograficznych (10 liter):

4 pionowo: Funkcja przeglądarki do głosu i wideo, która może omijać tunele i ujawniać prawdziwe adresy IP (9 liter):

6 pionowo: Unikalna etykieta numeryczna identyfikująca interfejs urządzenia w internecie (7 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 D R E S I P W Ś Ź V C Ż W Ę
L W G Ż Ć N D E Q Y T Ó C U B
E W A Ż Ń Ć L B A D U O D Ę G
I W I Ć R Q M R E I N S Ż Ś Ę
N Y Q V E A A T Q Ó E N P W T
A X Y Q K R T C S Ć L N Ź Y B
W O Ę S Y X J A A R V Ż Z C Z
O R Ł F I N R P K M P M T I O
K P G P Q G Ż I Ą O N V F E V
S B Ź S Ź B G M Ż G K O P K Ń
A Ś L E D Z E N I E I S P D X
M C M Ż Ź F Z O X U L V Ó N B
Ń W S I E Ć T O R T M G V S Ć
Z V L R Ą Y Ż Z M S Q Y I Ó D
A Ć K Q W X X L J H T H F Ą E

LISTA SŁÓW

ADRESIP TUNELVPN SIEĆTOR PROXYWWW WYCIEKDNS WEBRTCAPI MASKOWANIE ŚLEDZENIEISP

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. ADRESIP**
- **B. TUNELVPN**
- **C. SIEĆTOR**
- **D. PROXYWWW**
- **E. WYCIEKDNS**
- **F. WEBRTCAPI**
- **G. MASKOWANIE**
- **H. ŚLEDZENIEISP**

DEFINICJE I POLA DOPASOWANIA

1. Przekierowuje ruch przeglądarki na poziomie aplikacji bez szyfrowania na poziomie systemu.
2. Kierowanie połączenia przez serwer w innym kraju w celu obejścia blokad geograficznych.
3. Funkcja przeglądarki do głosu i wideo, która może omijać tunele i ujawniać prawdziwe adresy IP.
4. Unikalna etykieta numeryczna identyfikująca interfejs urządzenia w internecie.
5. Kieruje dane przez trzy serwery wolontariuszy, szyfrując warstwy na każdym etapie.
6. Rejestrowanie miejsc docelowych niezaszyfrowanego ruchu internetowego przez twojego operatora telekomunikacyjnego.
7. Zapytania rozwiązywane poza tunelem VPN, ujawniające dostawcy internetu odwiedzane domeny.
8. Szyfruje cały ruch urządzenia i kieruje go przez serwer VPN.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z VPN. Wpisz odpowiedzi w polach do wypełnienia.

1. EIASPRD
2. SEROTĆI
3. WKEYDSINC
4. WIOEKNAMAS
5. LVUNETPN
6. WWXWPYRO
7. CWPIARETB
8. IEZINPŚELSED

Zadanie dodatkowe: Myśl szybko

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

1	Powody, dla których warto używać VPN podczas podróży			
2	Przeglądarki, które znasz			
3	Rzeczy, które VPN może ukryć			
4	Słowa związane z prywatnością			
5	Słowa z tej karty pracy, które chcesz zapamiętać			
6	Rzeczy, które strona internetowa może odgadnąć na podstawie twojego adresu IP			
7	Liczby lub symbole w adresie IP			
8	Mity o VPN			
9	Usługi VPN, które znasz			
10	Rzeczy, które może zobaczyć twój dostawca internetu			
11	Obietnice, które składa dobry dostawca VPN			
12	Rzeczy, które mogą ujawnić twój prawdziwy adres IP			
13	Powody, dla których warto ukryć swoją lokalizację			
14	Sposoby na ukrycie adresu IP			
15	Urządzenia, które mogą korzystać z VPN			

Punkt kontrolny 8: Studia przypadków dotyczących VPN

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

SARAH (STUDENTKA W KAWIARNI)

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

ALEX (STUDENT PODRÓŻNIK)

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

Punkt kontrolny 9: Odszyfruj szyfr

Aby ukończyć szkolenie z maskowania IP, odszyfruj tę tajną wiadomość o ukrywaniu cyfrowych śladów.

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

28	14	24	32	13		1	6	24	7	25		6	33	12	8	14	12
28	14	24	32	27	7	17	28		25	32	25	27	7	17	20	30	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, które potencjalni klienci mają na temat korzystania z wirtualnych sieci prywatnych.

Q1: Czym jest VPN i jak działa?

Wirtualna sieć prywatna (VPN) szyfruje Twoje połączenie z internetem i kieruje ruch przez bezpieczny zdalny serwer. Maskuje to Twój publiczny adres IP i ogranicza to, co lokalni obserwatorzy sieci i Twój ISP mogą zobaczyć w ruchu kierowanym przez tunel VPN.

Q2: Dlaczego powinienem używać VPN?

VPN chroni Twoją prywatność cyfrową, zabezpiecza połączenie w publicznych sieciach Wi-Fi (np. w kawiarniach lub na lotniskach), może ograniczać dławienie oparte na aktywności, gdy ISP nie potrafi rozpoznać rodzaju zaszyfrowanego ruchu, omija ograniczenia geograficzne, aby uzyskać dostęp do globalnych treści, i pomaga zabezpieczyć zasoby pracy zdalnej.

Q3: Czy VPN zapewnia mi całkowitą anonimowość w internecie?

Nie. Chociaż VPN ukrywa twój adres IP i szyfruje ruch, nadal możesz być śledzony za pomocą plików cookie przeglądarki, aktywnych kont (np. Google lub Facebook), fingerprintingu przeglądarki lub jeśli dostawca VPN rejestruje twoje dane.

Q4: Czy serwer proxy WWW ukrywa mój adres IP?

Tak, ale tylko dla ruchu przesyłanego przez niego, zwykle z przeglądarki. Większość serwerów proxy WWW nie szyfruje twoich danych, więc twój dostawca internetu lub operator sieci nadal może zobaczyć, co wysyłasz i odbierasz.

Q5: Czy ukrywanie mojego adresu IP jest legalne?

W wielu krajach tak, ale niektóre ograniczają lub zakazują VPN i innych narzędzi do ukrywania adresu IP. Ukrycie adresu IP nigdy nie czyni czynu niezgodnego z prawem legalnym, więc sprawdź lokalne przepisy, zanim go użyjesz.

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

Przejrzyj najczęstsze pytania i odpowiedzi, które potencjalni klienci mają na temat korzystania z wirtualnych sieci prywatnych.

Q6: Czy Tor ukrywa mój adres IP?

Tak. Tor przesyła Twój ruch przez trzy przekaźniki wolontariuszy (wejściowy, środkowy i wyjściowy), więc strony widzą adres przekaźnika wyjściowego, a żaden pojedynczy przekaźnik nie wie jednocześnie, kim jesteś i dokąd idziesz. [1]

Q7: Co ujawnia mój adres IP?

Twój publiczny adres IP zwykle ujawnia Twojego dostawcę internetu i przybliżoną lokalizację, np. kraj lub miasto. Strony mogą też używać go do łączenia Twoich wizyt i stosowania blokad geograficznych.

Q8: Jak sprawdzić, czy jest ukryty?

Połącz się z VPN, następnie odwiedź stronę sprawdzającą IP i uruchom testy wycieków DNS i WebRTC. Wyświetlane IP i serwery DNS powinny należeć do VPN, a nie do Twojego dostawcy internetu. Jeśli widać Twoje prawdziwe IP, włącz ochronę przed wyciekami.

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

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

Q10: Czym jest kill switch?

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

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

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

Q1: Dlaczego witryny mogą mnie nadal śledzić po ukryciu adresu IP?

Ukrycie adresu IP nie powstrzymuje odcisków palca przeglądarki. Mechanizmy śledzące mogą połączyć takie szczegóły jak rozdzielczość ekranu, zainstalowane czcionki i ustawienia przeglądarki w jeden identyfikator, a Ciebie mogą też zidentyfikować pliki cookie lub zalogowane konta, więc używaj także przeglądarki skoncentrowanej na prywatności. [3]

Q2: Czym jest podwójny VPN lub routing Multi-Hop?

Multi-Hop kieruje twój ruch kolejno przez dwa lub więcej serwerów VPN. Dodaje to drugą warstwę szyfrowania i pomaga ukryć twój prawdziwy adres IP przed drugim skokiem, jeśli jeden serwer zostanie przejęty.

Q3: Czym jest wyciek WebRTC i jak VPN mu zapobiega?

WebRTC to protokół przeglądarki, który może ujawnić twoje prawdziwe lokalne i publiczne adresy IP nawet przy aktywnym VPN. Wysokiej klasy usługi VPN blokują lub podmieniają żądania WebRTC w swoich aplikacjach na komputery i urządzenia mobilne oraz w rozszerzeniach przeglądarek.

Q4: Czy ruch IPv6 może ujawnić mój prawdziwy adres IP?

Tak, jeśli Twój VPN tuneluje tylko IPv4. Urządzenie może wtedy wysyłać ruch IPv6 poza tunelem, ujawniając adres przydzielony przez dostawcę internetu. Użyj VPN, który tuneluje lub blokuje IPv6, i potwierdź to testem wycieku IPv6.

Q5: Jak obfuskacja omija blokady VPN?

Obfuskacja (lub „Stealth VPN”) ukrywa pakiety ruchu VPN tak, by wyglądały jak zwykły ruch internetowy HTTPS (port 443). Pomaga to ominąć system głębokiej inspekcji pakietów (DPI), którego rządy lub sieci szkolne i biurowe używają do blokowania VPN.

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

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

Q6: Czy tunelowanie dzielone ujawnia mój prawdziwy adres IP?

Tak, w przypadku aplikacji, które wykluczysz. Ruch wysyłany poza tunel używa Twojego prawdziwego adresu IP, a RFC 8828 zauważa, że WebRTC może ujawnić adres dostawcy internetu spod VPN z tunelowaniem dzielonym, o ile przeglądarka tego nie ogranicza. [2]

Q7: Czym jest współdzielony adres IP i jak pomaga w ochronie prywatności?

Przy współdzielonym adresie IP wielu użytkowników VPN jest jednocześnie widocznych w sieci pod tym samym adresem. Dzięki temu witrynie znacznie trudniej powiązać pojedynczą wizytę z tobą niż w przypadku dedykowanego adresu IP używanego tylko przez ciebie.

Q8: Czy mój dostawca internetu widzi, że używam VPN do ukrycia adresu IP?

Zwykle tak. Twój dostawca internetu widzi, że łączysz się z adresem IP serwera VPN, kiedy się łączysz i ile danych wysyłasz, ale nie widzi odwiedzanych stron ani zawartości szyfrowanego tunelu.

Q9: Czym jest ochrona przed wyciekami DNS?

Ochrona przed wyciekami DNS sprawia, że Twoje urządzenie wysyła zapytania o strony internetowe (zapytania DNS) przez prywatne, szyfrowane serwery DNS usługi VPN zamiast przez serwery Twojego dostawcy internetu. Dzięki temu dostawca internetu nie może śledzić, jakie strony odwiedzasz.

Q10: Co lepsze do ukrywania adresu IP: serwer proxy czy VPN?

Zwykle lepszy jest VPN. Ukrywa Twój adres IP dla każdej aplikacji na urządzeniu i szyfruje ruch, a proxy internetowe zazwyczaj obejmuje tylko przeglądarkę i często nie dodaje szyfrowania.

Część 11: 10 ciekawych faktów o VPN i spostrzeżeń z praktyki

Przejrzyj te bardzo cenne, prawdziwe fakty i spostrzeżenia dotyczące historii, rynku i technologii VPN.

1. PIERWSZY PROTOKÓŁ VPN

PPTP (Point-to-Point Tunneling Protocol), wczesny protokół VPN stworzony w latach 1990-tych przez grupę kierowaną przez Microsoft, jest dziś uznawany za niebezpieczny, dlatego nowoczesne VPN używają WireGuard lub OpenVPN.

2. ODCISKI PALCÓW URZĄDZENIA

Ukrycie adresu IP nie powstrzymuje odcisków palca przeglądarki, które mogą Cię zidentyfikować na podstawie takich szczegółów jak rozdzielczość ekranu i zainstalowane czcionki. [3]

3. REWOLUCJA WIREGUARD

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

4. UJAWNIENIE ADRESU PRZEZ WEBRTC

RFC 8828 ostrzega, że WebRTC może wykryć zarówno publiczny adres VPN, jak i adres dostawcy internetu, przez którego działa VPN, chyba że przeglądarka to ogranicza. [2]

5. POCHODZENIE SOJUSZU 5 EYES

Partnerstwo wywiadowcze Five Eyes, tworzone przez USA, Wielką Brytanię, Kanadę, Australię i Nową Zelandię, wyrosło ze współpracy aliantów w dziedzinie wywiadu sygnałowego z czasów II wojny światowej.

6. GŁĘBOKA INSPEKCJA PAKIETÓW

Zaawansowane zapory sieciowe stosują Deep Packet Inspection (DPI), aby analizować metadane pakietów sieciowych i blokować standardowe cechy połączeń VPN.

7. PONOWNE UŻYCIE OBWODU TOR

Tor używa tego samego obwodu przez około dziesięć minut, a potem buduje nowy, co utrudnia powiązanie Twojej aktywności przeglądania. [1]

8. ZDECENTRALIZOWANE VPN-Y

Zdecentralizowane sieci VPN (dVPN) rozdzielają ruch w sieci węzłów prowadzonych przez użytkowników, zmniejszając zależność od jednego scentralizowanego dostawcy.

9. ANONIMOWOŚĆ: TOR A VPN

VPN tuneluje ruch przez jednego dostawcę, a Tor (The Onion Router) kieruje ruch przez trzy przekaźniki wolontariuszy (wejściowy, środkowy, wyjściowy), aby zmaksymalizować prywatność. [1]

10. PROXY A TUNELE VPN

Serwer proxy sieciowy zmienia adres IP, który strona widzi dla ruchu Twojej przeglądarki, ale w przeciwieństwie do VPN zwykle nie szyfruje tego ruchu ani nie obejmuje innych aplikacji na urządzeniu. [5]

Źródła i odnośniki techniczne

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

PUBLIKACJE NAUKOWE I BRANŻOWE

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Klucz odpowiedzi: Ukrywanie adresów IP, maskowanie lokalizacji, proxy, Tor oraz zapobieganie wyciekom DNS/WebRTC

1 Pytanie 1

Poprawna odpowiedź: B

UWAGA DLA NAUCZYCIELA

Co publiczny adres IP urządzenia ujawnia odwiedzanym przez ciebie stronom? → Twoją przybliżoną lokalizację i nazwę twojego dostawcy internetu

2 Szyfrowanie systemowe VPN OPÓŹNIENIE

Poprawna odpowiedź: C

UWAGA DLA NAUCZYCIELA

W przeciwieństwie do serwerów proxy, które przekierowują tylko ruch przeglądarki, VPN tworzy szyfrowany tunel obejmujący cały system, zabezpieczając aplikacje działające w tle, gry i zapytania systemu operacyjnego. Źródło: Tor Project Relays, W3C WebRTC API.

3 Brak szyfrowania w proxy BEZPIECZEŃSTWO WI-FI

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Serwery proxy WWW jedynie przekazują ruch przeglądarki bez szyfrowania zawartości pakietów, co oznacza, że operator sieci lub dostawca internetu nadal może śledzić twój ruch z treściami. Źródło: IETF Proxy Vulnerabilities.

4 Pytanie 4

Poprawna odpowiedź: B

UWAGA DLA NAUCZYCIELA

W jaki sposób sieć Tor zapewnia użytkownikom wysoką anonimowość? → Kierując ruch przez trzy przekaźniki prowadzone przez wolontariuszy

5 Wycieki przez tunel DNS PRYWATNOŚĆ

Poprawna odpowiedź: B

UWAGA DLA NAUCZYCIELA

Wyciek DNS występuje, gdy zapytania o rozwiązywanie nazw domen omijają tunel VPN i trafiają bezpośrednio do resolwerów Twojego dostawcy internetu (ISP), ujawniając rekordy odwiedzanych domen. Źródło: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Szczegóły ograniczeń proxy** MASKOWANIE IP

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Serwery proxy działają w warstwie aplikacji i nie mają ogólnosystemowej integracji ze sterownikiem sieciowym, jaką ma tunel VPN. Źródło: IETF Proxy Vulnerabilities.

7 **Pytanie 7**

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Przekazywanie ruchu przez trzy przekaźniki wolontariuszy z warstwowym szyfrowaniem zwiększa opóźnienie, więc Tor jest zwykle wolniejszy niż połączenie bezpośrednie.

8 **Pytanie 8**

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

WebRTC może ujawniać adresy lokalne oraz, przy niektórych konfiguracjach VPN, publiczny adres IP przydzielony przez dostawcę internetu pod tunelem (RFC 8828).

9 **Pytanie 9**

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Bez wycieków DNS ani WebRTC dostawca internetu widzi tylko zaszyfrowany ruch do serwera VPN, a nie odwiedzane przez ciebie strony.

10 **Ograniczenia fingerprintingu** BRAK LOGÓW

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fingerprinting wykorzystuje metryki konfiguracji urządzenia (rozdzielczość ekranu, czcionki, wtyczki), które pozostają widoczne nawet wtedy, gdy adres IP jest ukryty. Źródło: EFF Tracking Evasion.

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

D 1. Adres IP	A 2. Tunel VPN	B 3. Sieć Tor	E 4. Proxy sieciowe
G 5. Wyciek DNS	H 6. API WebRTC	C 7. Maskowanie lokalizacji	F 8. Śledzenie przez ISP

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 WYCIEK DNS	2 WEBRTC	3 PROXY	4 TOR
5 ADRES IP	6 MASKOWANIE		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 D – PROXYWWW	2 G – MASKOWANIE	3 F – WEBRTCAPI	4 A – ADRESIP
5 C – SIEĆTOR	6 H – ŚLEDZENIEISP	7 E – WYCIEKDNS	8 B – TUNELVPN

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Adres IP, Tunel VPN i Sieć Tor oraz podać przykład każdego z nich.

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

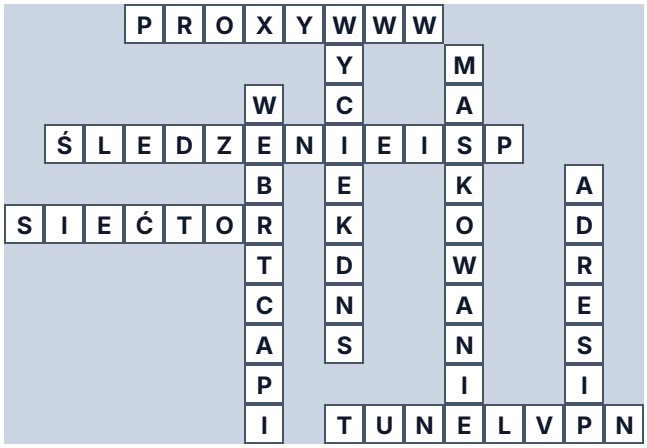
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

1 poziomo: PROXYWWW Przekierowuje ruch przeglądarki na poziomie aplikacji bez szyfrowania na poziomie systemu (8 liter)

5 poziomo: ŚLEDZENIEISP Rejestrowanie miejsc docelowych niezaszyfrowanego ruchu internetowego przez twojego operatora telekomunikacyjnego (12 liter)

7 poziomo: SIEĆTOR Kieruje dane przez trzy serwery wolontariuszy, szyfrując warstwy na każdym etapie (7 liter)

8 poziomo: TUNELVPN Szyfruje cały ruch urządzenia i kieruje go przez serwer VPN (8 liter)

PIONOWO

2 pionowo: WYCIEKDNS Zapytania rozwiązywane poza tunelem VPN, ujawniające dostawcy internetu odwiedzane domeny (9 liter)

3 pionowo: MASKOWANIE Kierowanie połączenia przez serwer w innym kraju w celu obejścia blokad geograficznych (10 liter)

4 pionowo: WEBRTCAPI Funkcja przeglądarki do głosu i wideo, która może omijać tunele i ujawniać prawdziwe adresy IP (9 liter)

6 pionowo: ADRESIP Unikalna etykieta numeryczna identyfikująca interfejs urządzenia w internecie (7 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. E I A S P R D — **ADRESIP**
2. S E R O T Ć I — **SIEĆTOR**
3. W K E Y D S I N C — **WYCIEKDNS**
4. W I O E K N A M A S — **MASKOWANIE**
5. L V U N E T P N — **TUNELVPN**
6. W W X W P Y R O — **PROXYWWW**
7. C W P I A R E T B — **WEBRTCAPI**
8. I E Z I N P Ś E L S E D — **ŚLEDZENIEISP**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"UKRYJ ADRES DZIĘKI UKRYTEMU SYSTEMOWI"

Klucz odpowiedzi do studiów przypadków

A Scenariusz A: Bezpieczeństwo sieci publicznej

SNIFFING I SZYFROWANIE | Dylemat Sarah

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Ryzyka: Podsłuchiwanie pakietów, przechwytywanie danych i ataki typu man-in-the-middle. Ktoś w tej samej sieci w kawiarni mógłby przechwycić jej dane logowania lub plik z pracą domową.
- Ochrona VPN: szyfruje dane użytkowe pakietów sieciowych, przez co przechwycony ruch tunelu jest nieczytelny dla pasywnych podsłuchiwaczy w sieci lokalnej, gdy VPN jest poprawnie skonfigurowany.

B Scenariusz B: Dostęp do zablokowanych zasobów

GEOBLOKADY I ADRESY IP | Dylemat Alexa

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Powód blokady: Serwis streamingowy stosuje blokadę geograficzną, która przypisuje lokalny adres IP podróżnika do jego fizycznego kraju i blokuje go na podstawie terytorialnych licencji.
- Jak pomaga VPN: maskuje jego prawdziwą lokalizację, kierując ruch przez serwer w jego kraju ojczystym. Strona widzi adres IP z kraju ojczystego, co umożliwia dostęp.