Imię i nazwisko: _____ Data: _____ Wynik: _____

Czym jest VPN Karta pracy

Ćwiczenia praktyczne z protokołów sieciowych, tunelowania i mechanizmów kontroli bezpieczeństwa.

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 pojęcie tunelowania danych i enkapsulacji.
- Rozpoznaj standardowe konfiguracje protokołów i metody szyfrowania.
- Przeanalizuj rolę serwerów i maskowania adresu IP w wirtualnych sieciach prywatnych.
- Zrozum, jak dostawcy internetu śledzą przeglądanie i jak VPN temu zapobiega.
- Rozróżnij operacyjne granice topologii sieci wirtualnej.

INSTRUKCJE DO PRZEWODNIKA „CO TO JEST 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 rzeczywistych scenariuszy w części ze studiami przypadków. Zakończ zadaniem dodatkowym Myśl szybko.

CO TO JEST VPN? (WPROWADZENIE)

Wirtualna sieć prywatna to coś więcej niż przełącznik prywatności. To zaszyfrowany tunel, który kieruje Twój ruch internetowy przez zdalny serwer. Ukrywa to Twój adres IP, uniemożliwia Twojemu ISP tworzenie logów Twoich działań online i zabezpiecza Twoje dane w sieciach publicznych. Zrozumienie terminologii jest niezbędne do zachowania bezpieczeństwa cyfrowego.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Jaka jest podstawowa funkcja wirtualnej sieci prywatnej (VPN)?

- A. Aby zwiększyć szybkość renderowania w przeglądarce internetowej
- B. Aby szyfrować pakiety danych i maskować twój publiczny adres IP
- C. Aby przechowywać lokalnie bazy danych plików cookie strony
- D. Aby zastąpić fizyczny sprzęt komputerowy

2. Czym jest tunelowanie sieciowe w kontekście VPN?

- A. Usuwanie zduplikowanych plików logów sieciowych
- B. Instalowanie lokalnych plików magazynu bazy danych
- C. Udostępnianie plików innym komputerom w sieci lokalnej
- D. Hermetyzowanie jednego pakietu sieciowego wewnątrz innego bezpiecznego pakietu

3. Jaki standard szyfrowania jest szeroko stosowany do ochrony ruchu VPN?

- A. Przestarzałe szyfrowanie DES
- B. Nowoczesny standard AES-256
- C. Kodowanie base64 w postaci jawnej
- D. Standardowy szyfr rot13

4. Który element twojego ruchu sieciowego jest szyfrowany przez VPN?

- A. Tylko lokalne zadania drukowania w sieci urządzenia
- B. Fizyczna ścieżka kabla ethernetowego
- C. Cała część pakietu sieciowego zawierająca dane (payload)
- D. Tylko historie wyszukiwania w Twojej przeglądarce internetowej

5. Co oznacza termin „szyfrowanie” w sieciach?

- A. Przekształcanie danych jawnych w nieczytelny szyfrogram
- B. Usuwanie starych zapisów komunikacji
- C. Zwiększanie lokalnych limitów szybkości łącza
- D. Publiczne udostępnianie kluczy dostępu do bazy danych

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. VPN szyfruje Twój ruch, aby zapobiec lokalnemu podsłuchiwaniu w publicznych sieciach Wi-Fi.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. VPN fizycznie zmienia konfigurację sprzętową Twojego routera.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Protokoły tunelowania opakowują pakiety danych w szyfrowaną warstwę transportową.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Szyfrowanie symetryczne używa tego samego klucza do szyfrowania i deszyfrowania ruchu.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Używanie VPN sprawia, że Twoje połączenie internetowe jest fizycznie odporne na wszelkie przerwy w zasilaniu.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Aby zabezpieczyć twój ruch, VPN opakowuje pakiety danych w inny protokół — ten proces nazywa się _____ .

2. Jeśli podczas streamingu pobieranie jest wolne, przyczyną może być ograniczona _____ sieci.

3. Usługa streamingowa dostępna tylko w jednym kraju ogranicza dostęp użytkownikom z całego świata za pomocą mechanizmu zwanego: _____ .

4. Reguły połączenia określające parametry szyfrowania i połączenia nazywa się _____ VPN.

5. Twój komputer monitoruje ruch sieciowy i blokuje niebezpieczne połączenia dzięki lokalnemu mechanizmowi, którym jest _____ .

6. Gdy łączysz się z VPN, twoje dane są kierowane przez zdalny _____ , aby ukryć twój publiczny adres IP.

BANK SŁÓW

DOSTAWCA ISP | GEOBLOKADA | PROTOKÓŁ | PRYWATNOŚĆ | SERWER | SZEROKOŚĆ PASMA | TUNELOWANIE | ZAPORA SIECIOWA

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć sieciowych

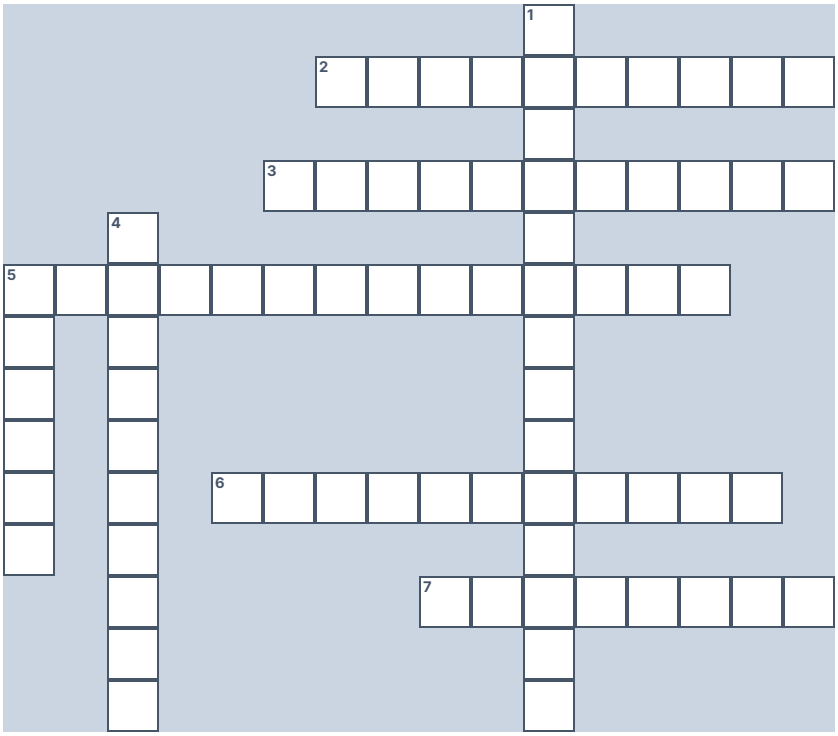
DOPASOWYWANIE DEFINICJI

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

	1. Tunelowanie	A	Zdalny komputer, który kieruje Twój ruch i maskuje Twój adres IP.
	2. Protokół	B	Dostawca internetu, który przenosi Twój ruch i może widzieć niezaszyfrowaną aktywność.
	3. Przepustowość	C	Ograniczenie uniemożliwiające dostęp do sieci na podstawie fizycznej lokalizacji.
	4. Serwer	D	System bezpieczeństwa, który monitoruje i blokuje nieautoryzowany ruch.
	5. Blokada geograficzna	E	Zestaw reguł określających, jak dane są przesyłane przez sieć.
	6. Zapora sieciowa	F	Stan wolności od śledzenia lub publicznej inwigilacji.
	7. Prywatność	G	Maksymalna szybkość transferu danych przez połączenie.
	8. DOSTAWCA INTERNETU	H	Opakowanie pakietów danych w inny pakiet na potrzeby bezpiecznego przesyłu.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

2. Stan wolności od śledzenia i publicznej inwigilacji (10)

3. Opakowywanie pakietów danych w inny pakiet w celu bezpiecznego przesyłu (11)

5. Maksymalna szybkość transferu danych w połączeniu (14)

6. Dostawca usług internetowych, który rejestruje twój ruch, jeśli nie jest zaszyfrowany (11)

7. Zbiór reguł określających, jak dane są przesyłane w sieci (8)

PIONOWO

1. System bezpieczeństwa monitorujący i blokujący nieautoryzowany ruch (14)

4. Ograniczenie uniemożliwiające dostęp do sieci w zależności od fizycznej lokalizacji (10)

5. Zdalny komputer, który kieruje twój ruch i maskuje twój adres IP (6)

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: Stan wolności od śledzenia i publicznej inwigilacji (10 liter):

3 poziomo: Opakowywanie pakietów danych w inny pakiet w celu bezpiecznego przesyłu (11 liter):

5 poziomo: Maksymalna szybkość transferu danych w połączeniu (14 liter):

6 poziomo: Dostawca usług internetowych, który rejestruje twój ruch, jeśli nie jest zaszyfrowany (11 liter):

7 poziomo: Zbiór reguł określających, jak dane są przesyłane w sieci (8 liter):

PIONOWO

1 pionowo: System bezpieczeństwa monitorujący i blokujący nieautoryzowany ruch (14 liter):

4 pionowo: Ograniczenie uniemożliwiające dostęp do sieci w zależności od fizycznej lokalizacji (10 liter):

5 pionowo: Zdalny komputer, który kieruje twój ruch i maskuje twój adres IP (6 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

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

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

LISTA SŁÓW

TUNELOWANIE, PROTOKÓŁZAPORASIECIOWA, SZEROKOŚĆPASMA, SERWER, GEOBLOKADA, PRYWATNOŚĆ, DOSTAWCAISP

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. TUNELOWANIE**
- **B. PROTOKÓŁ**
- **C. SZEROKOŚĆPASMA**
- **D. SERWER**
- **E. GEOBLOKADA**
- **F. ZAPORASIECIOWA**
- **G. PRYWATNOŚĆ**
- **H. DOSTAWCAISP**

DEFINICJE I POLA DOPASOWANIA

1. Zbiór reguł określających, jak dane są przesyłane w sieci.
2. Ograniczenie uniemożliwiające dostęp do sieci w zależności od fizycznej lokalizacji.
3. System bezpieczeństwa monitorujący i blokujący nieautoryzowany ruch.
4. Stan wolności od śledzenia i publicznej inwigilacji.
5. Dostawca usług internetowych, który rejestruje twój ruch, jeśli nie jest zaszyfrowany.
6. Opakowywanie pakietów danych w inny pakiet w celu bezpiecznego przesyłu.
7. Zdalny komputer, który kieruje twój ruch i maskuje twój adres IP.
8. Maksymalna szybkość transferu danych w połączeniu.

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. L W I U O A T N N E E

2. O Z K E O M S S Ś A P A Ć R

3. G O D K E L A B A O

4. T Ś A Ć W O N P R Y

5. O K R Ł T P Ó O

6. E W S R R E

7. I W C Z E A P A A O I O S R

8. I C P W S D A O S A T

Zadanie dodatkowe: Myśl szybko

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

1	Rzeczy, które może ujawnić adres IP			
2	Mity o VPN			
3	Rzeczy, które podróżują przez internet			
4	Obietnice, które składa dobry dostawca VPN			
5	Sekrety, które byś zaszyfrował			
6	Rzeczy, przed którymi VPN cię nie ochroni			
7	Sposoby na rozpoznanie fałszywej sieci Wi-Fi			
8	Słowa związane z prywatnością			
9	Urządzenia, które mogą korzystać z VPN			
10	Rzeczy, które się dzieją, gdy naciskasz „Połącz”			
11	Miejsca, w których używałbyś VPN			
12	Powody, dla których warto używać VPN podczas podróży			
13	Rzeczy z prawdziwego życia, które wyglądają jak tunel			
14	Słowa z tej karty pracy, które chcesz zapamiętać			
15	Słowa do wyjaśnienia VPN dziecku			

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

VPN szyfruje Twój ruch, aby go zabezpieczyć. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość o cyberbezpieczeństwie, 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

4	11	24	20	19		25	30	20	13	2

22	24	32	30	1	27	18	20	26	5

3	7	33	22	12	7	4	33	18	32	17		27	28	18	7	15	7	17

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 VPN spowolni moje połączenie z internetem?

Tak, nieznacznie. Proces szyfrowania i fizyczna odległość od serwera VPN dodają opóźnienie i narzut. Wpływ zależy od dostawcy, protokołu, odległości serwera, urządzenia i warunków sieciowych.

Q5: Czy korzystanie z VPN jest legalne?

Używanie VPN jest legalne w wielu krajach, ale niektóre jurysdykcje ograniczają, regulują lub blokują usługi VPN. Przed użyciem sprawdź aktualne lokalne przepisy. Więcej szczegółów znajdziesz w przewodnikach o legalności na VPN.com.

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 mogę używać darmowego VPN?

Darmowe VPN mogą opierać się na reklamach, ograniczonych funkcjach, analityce użytkowania, limitach danych lub innych modelach zarabiania. Przed użyciem użytkownicy powinni zapoznać się z polityką prywatności dostawcy, jego właścicielem, audytami i modelem biznesowym.

Q7: Czym jest polityka „no-logs" (braku logów)?

Polityka braku logów opisuje, jakich danych o aktywności i połączeniach dostawca deklaruje, że nie przechowuje. Dokładny zakres bywa różny, dlatego czytelnicy powinni sprawdzić politykę i wyniki niezależnych audytów.

Q8: Jak wybrać najlepszy VPN?

Szukaj audytowanych polityk braku logów, silnych protokołów (WireGuard, OpenVPN), bezpiecznych lokalizacji serwerów, dużej szybkości, serwerów działających wyłącznie w pamięci RAM, funkcji kill switch oraz jurysdykcji spoza sojuszy wymiany informacji wywiadowczych (takich jak 5/9/14 Eyes).

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: Jaka jest różnica między WireGuard, OpenVPN i IKEv2?

WireGuard to nowoczesny, lekki protokół (tylko ok. 4000 wierszy kodu), który zapewnia dużą prędkość i szybkie nawiązywanie połączeń. OpenVPN to bardzo bezpieczny, sprawdzony w boju protokół open source. IKEv2 doskonale sprawdza się na urządzeniach mobilnych dzięki możliwości szybkiego ponownego łączenia po zmianie sieci. [4]

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: Czym są serwery działające wyłącznie w pamięci RAM i dlaczego mają znaczenie?

Tradycyjne serwery zapisują dane na dyskach twardych, które mogą zostać zajęte lub naruszone. Serwery wyłącznie RAM (bezdyskowe) działają w całości w pamięci ulotnej (RAM). Gdy serwer zostanie ponownie uruchomiony lub wyłączony, dane przechowywane w pamięci są usuwane.

Q5: Jak obfuskacja omija blokady VPN?

Obfuskacja (lub „Stealth VPN") ukrywa ruch VPN tak, by wyglądał jak zwykły ruch HTTPS (port 443). Może to pomóc 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: Czym jest tunelowanie dzielone (Split Tunneling) i kiedy warto z niego korzystać?

Tunelowanie dzielone pozwala wybrać, które aplikacje kierują ruch przez zaszyfrowany tunel VPN, a które łączą się bezpośrednio z internetem. Użyj go, aby kierować wrażliwe aplikacje bankowe przez VPN, podczas gdy lokalne gry łączą się bezpośrednio, co pozwala uniknąć opóźnienia dodawanego przez VPN.

Q7: Jak działa Forward Secrecy (Perfect Forward Secrecy)?

PFS zapewnia, że dla każdej pojedynczej sesji generowany jest unikalny, tymczasowy klucz szyfrowania. Nawet jeśli klucz prywatny zostanie w przyszłości ujawniony, nie można go użyć do odszyfrowania sesji z przeszłości ani przyszłych, ponieważ używały niezależnych kluczy.

Q8: Czym są sojusze 5/9/14 Eyes i dlaczego powinno mnie to interesować?

Jurysdykcja może wpływać na proces prawny, z którym może mierzyć się dostawca, ale praktyczne ryzyko dla prywatności zależy też od tego, jakie dane dostawca przechowuje, jego architektury technicznej, własności, raportów przejrzystości i historii audytów.

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: Czy VPN może ominąć ograniczanie internetu przez dostawcę?

Czasami. VPN może pomóc, gdy dostawca internetu selektywnie spowalnia rozpoznawalne działania, ale nie pokona przeciążenia, limitów danych, ograniczeń prędkości na poziomie konta ani słabej jakości sieci.

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) został opracowany przez grupę dostawców, w tym Microsoft, i opublikowany jako RFC 2637 w lipcu 1999 roku, aby obsługiwać VPN do dostępu zdalnego. [6]

2. WYCENA RYNKOWA

Globalny rynek VPN szybko rośnie, napędzany rosnącymi potrzebami pracy zdalnej i wymaganiami bezpieczeństwa w przedsiębiorstwach.

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]

4. ŚCISŁE STANDARDY AUDYTU

Czołowi dostawcy VPN zatrudniają zewnętrznych audytorów (takich jak Cure53 czy PwC), aby przeprowadzali niezależne przeglądy kodu i weryfikowali, że nie rejestrują aktywności użytkowników.

5. POCHODZENIE SOJUSZU 5 EYES

Sojusz Five Eyes wyrósł z porozumienia UKUSA z 1946 r. o wywiadzie sygnałowym między USA a Wielką Brytanią, do którego później dołączyły Kanada, Australia i Nowa Zelandia.

6. GŁĘBOKA INSPEKCJA PAKIETÓW

Głęboka inspekcja pakietów (DPI) bada zawartość pakietów i wzorce ruchu, a nie tylko nagłówki, a niektóre zapory sieciowe używają jej do wykrywania i blokowania popularnych protokołów VPN.

7. UŻYTKOWANIE KORPORACYJNE

Duży odsetek pracowników przedsiębiorstw na całym świecie korzysta z bezpiecznych VPN, aby logować się do wewnętrznych baz danych, co czyni to kluczowym standardem bezpieczeństwa.

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 i wyjściowy), tak że żaden pojedynczy przekaźnik nie zna obu końców połączenia.

10. KOSZT NARUSZEŃ OCHRONY DANYCH

Zastosowanie modelu bezpiecznego dostępu zero trust z VPN pomaga organizacjom chronić własność intelektualną i łagodzić skutki finansowe naruszeń danych.

Źródła i odnośniki techniczne

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

PUBLIKACJE NAUKOWE I BRANŻOWE

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/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] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Klucz odpowiedzi: Karta pracy „Czym jest VPN”

1 **Główna funkcja** PROTOKOŁY — **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

Głównym zadaniem VPN jest ustanowienie zaszyfrowanego tunelu, który chroni dane ładunku pakietów i maskuje publiczny adres IP użytkownika. Źródło: IETF Tunnel RFC.

2 **Tunelowanie sieciowe** OPÓŹNIENIE — **Poprawna odpowiedź: D**

UWAGA DLA NAUCZYCIELA

Protokoły tunelowania enkapsulują oryginalne pakiety danych w zewnętrznych pakietach nośnych, aby bezpiecznie przechodziły przez sieci publiczne. Źródło: IETF Tunnel RFC.

3 **Pytanie 3** — **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

Jaki standard szyfrowania jest szeroko stosowany do ochrony ruchu VPN? → Nowoczesny standard AES-256

4 **Zaszyfrowane komponenty** KONTROLA ROUTINGU — **Poprawna odpowiedź: C**

UWAGA DLA NAUCZYCIELA

VPN szyfruje cały segment ładunku pakietów danych IP, dzięki czemu zawartość transmisji pozostaje poufna. Źródło: IETF Tunnel RFC.

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

UWAGA DLA NAUCZYCIELA

Szyfrowanie używa algorytmu i klucza, aby zamienić tekst jawny w nieczytelny szyfrogram.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Blokada podsłuchu** MASKOWANIE IP

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Zaszyfrowane tunele sprawiają, że ładunki pakietów pozostają nieczytelne dla osób przechwytujących dane w lokalnych sieciach Wi-Fi. Źródło: Deloitte Advisory.

7 **Zmiany sprzętowe** PRĘDKOŚCI

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

VPN to programowe tunele sieciowe i nie zmieniają fizycznie sprzętu routera bramowego. Źródło: Cure53 Audit.

8 **Pakiety tunelowania** RYZYKO SNIFFINGU

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Tunelowanie polega na opakowywaniu oryginalnych pakietów sieciowych w nagłówki transportowe na czas przesyłania. Źródło: IETF Tunnel RFC.

9 **Klucze symetryczne** ZAPORY SIECIOWE

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Kryptografia symetryczna wykorzystuje wspólny klucz zarówno do szyfrowania, jak i deszyfrowania strumieni sieciowych. Źródło: WireGuard Project.

10 **Odporność mocy** BRAK LOGÓW

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

VPN szyfruje tylko aktywne sygnały połączenia; nie może zapobiec przerwom w usłudze spowodowanym lokalnymi awariami zasilania. Źródło: EDRi Retention Guidelines.

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

H 1. Tunelowanie	E 2. Protokół	G 3. Przepustowość	A 4. Serwer
C 5. Blokada geograficzna	D 6. Zapora sieciowa	F 7. Prywatność	B 8. DOSTAWCA INTERNETU

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 TUNELOWANIE	2 SZEROKOŚĆ PASMA	3 GEOBLOKADA	4 PROTOKÓŁ
5 ZAPORA SIECIOWA	6 SERWER		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 B – PROTOKÓŁ	2 E – GEOBLOKADA	3 F – ZAPORASIECIOWA	4 G – PRYWATNOŚĆ
5 H – DOSTAWCAISP	6 A – TUNELOWANIE	7 D – SERWER	8 C – SZEROKOŚĆPASMA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Tunelowanie, Protokół i Przepustowość 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

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

ROZWIĄZANIE KRZYŻÓWKI

							Z							
				P	R	Y	W	A	T	N	O	Ś	Ć	
							P							
			T	U	N	E	L	O	W	A	N	I	E	
		G					R							
S	Z	E	R	O	K	O	Ś	Ć	P	A	S	M	A	
E		O								S				
R		B								I				
W		L								E				
E		O		D	O	S	T	A	W	C	A	I	S	P
R		K								I				
		A					P	R	O	T	O	K	Ó	Ł
		D								W				
		A								A				

PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: PRYWATNOŚĆ Stan wolności od śledzenia i publicznej inwigilacji (10 liter)

3 poziomo: TUNELOWANIE Opakowywanie pakietów danych w inny pakiet w celu bezpiecznego przesyłu (11 liter)

5 poziomo: SZEROKOŚĆPASMA Maksymalna szybkość transferu danych w połączeniu (14 liter)

6 poziomo: DOSTAWCAISP Dostawca usług internetowych, który rejestruje twój ruch, jeśli nie jest zaszyfrowany (11 liter)

7 poziomo: PROTOKÓŁ Zbiór reguł określających, jak dane są przesyłane w sieci (8 liter)

PIONOWO

1 pionowo: ZAPORASIECIOWA System bezpieczeństwa monitorujący i blokujący nieautoryzowany ruch (14 liter)

4 pionowo: GEOBLOKADA Ograniczenie uniemożliwiające dostęp do sieci w zależności od fizycznej lokalizacji (10 liter)

5 pionowo: SERWER Zdalny komputer, który kieruje twój ruch i maskuje twój adres IP (6 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. L W I U O A T N N E E — **TUNELOWANIE**
2. O Z K E O M S S Ś A P A Ć R — **SZEROKOŚĆPASMA**
3. G O D K E L A B A O — **GEOBLOKADA**
4. T Ś A Ć W O N P R Y — **PRYWATNOŚĆ**
5. O K R Ł T P Ó O — **PROTOKÓŁ**
6. E W S R R E — **SERWER**
7. I W C Z E A P A A O I O S R — **ZAPORASIECIOWA**
8. I C P W S D A O S A T — **DOSTAWCAISP**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"CHROŃ SWOJĄ PRYWATNOŚĆ BEZPIECZNYM TUNELEM"

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.