Imię i nazwisko: _____ Data: _____ Wynik: _____

WireGuard a OpenVPN Karta pracy

Porównanie protokołów WireGuard i OpenVPN, rozmiarów kodu, szybkości i standardów kryptograficznych

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

- Porównaj złożoność kodu i szybkość audytowania protokołów.
- Przeanalizuj korzyści wydajnościowe wynikające z działania w przestrzeni jądra.
- Porównaj szyfry OpenSSL z nowoczesną kryptografią WireGuard.
- Skonfiguruj pary kluczy publicznych i prywatnych do uzgadniania połączeń między peerami.
- Kieruj ruch VPN przez porty zapory sieciowej TCP i UDP.

INSTRUKCJE DO KARTY PRACY: PORÓWNANIE PROTOKOŁÓW

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 audytowania nowoczesnych protokołów. Zakończ zadaniem dodatkowym Myśl szybko.

WIREGUARD A OPENVPN (WPROWADZENIE)

Wybór protokołu VPN wymaga zrównoważenia prędkości i opcji konfiguracji. OpenVPN jest standardem od dziesięcioleci i oferuje elastyczną konfigurację TCP/UDP. WireGuard to nowoczesny zamiennik działający bezpośrednio w przestrzeni jądra i liczący tylko 4,000 wierszy kodu. Zrozumienie różnic między protokołami jest kluczem do optymalizacji bezpiecznych sieci.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. 1. Jaki jest przybliżony rozmiar kodu źródłowego protokołu WireGuard?
   - A. Około 70 000 wierszy
   - B. Ponad 100 000 wierszy
   - C. Mniej niż 1000 wierszy
   - D. Około 4000 wierszy

2. 2. W której przestrzeni systemu operacyjnego działa WireGuard?
   - A. Przestrzeń użytkownika
   - B. Przestrzeń jądra
   - C. Przestrzeń aplikacji
   - D. Przestrzeń wirtualna

3. 3. Na jakiej bibliotece kryptograficznej OpenVPN opiera się głównie?
   - A. ChaCha20-Poly1305
   - B. Biblioteka kryptograficzna OpenSSL
   - C. Framework protokołu Noise
   - D. Kodowanie DES w postaci jawnej

4. 4. Jaka jest kluczowa korzyść wydajnościowa WireGuard w porównaniu z OpenVPN?
   - A. Szybsze uzgadnianie połączenia i niższe opóźnienie
   - B. Obejście potrzeby posiadania publicznych adresów IP
   - C. Wbudowana natywna obsługa starszych połączeń dial-up
   - D. Zerowy narzut na baterię w urządzeniach mobilnych

5. 5. Jak WireGuard uwierzytelnia połączenia partnerów?
   - A. Przez wymianę standardowych haseł użytkowników
   - B. Przez weryfikację certyfikatów rejestracji domen
   - C. Przez użycie statycznych par kluczy publicznych i prywatnych
   - D. Przez sprawdzanie numerów seryjnych sprzętu

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Zwarta baza kodu WireGuard znacznie ułatwia jego audyt.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. OpenVPN jest zazwyczaj szybszy niż WireGuard, ponieważ działa w przestrzeni jądra.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. OpenVPN jest wysoce konfigurowalny i obsługuje zarówno protokoły UDP, jak i TCP.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. WireGuard używa nowoczesnej kryptografii, takiej jak ChaCha20, do szybkiego szyfrowania pakietów.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. WireGuard wymaga skomplikowanej konfiguracji urzędu certyfikacji do uwierzytelniania.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Nowoczesny protokół _____ działa bezpośrednio w jądrze systemu operacyjnego.

2. Starszy protokół _____ opiera się na bibliotece kryptograficznej OpenSSL.

3. Kod wykonywany w obszarze systemu zwanym: _____ zmniejsza narzut przełączania kontekstu.

4. OpenVPN działa w trybie, który nazywa się: _____ , i kieruje pakiety przez wirtualne interfejsy.

5. Do identyfikowania węzłów połączenia WireGuard używa publicznego i prywatnego klucza; razem tworzą one tzw. _____ .

6. Mały rozmiar bazy kodu poprawia cechę bezpieczeństwa oprogramowania, jaką jest _____ .

BANK SŁÓW

AUDYTOWALNOŚĆ KOMPAKTOWY KOD OPENSSL OPENVPN PARA KLUCZY TRYB JĄDRA TRYB UŻYTKOWNIKA WIREGUARD

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć sieciowych

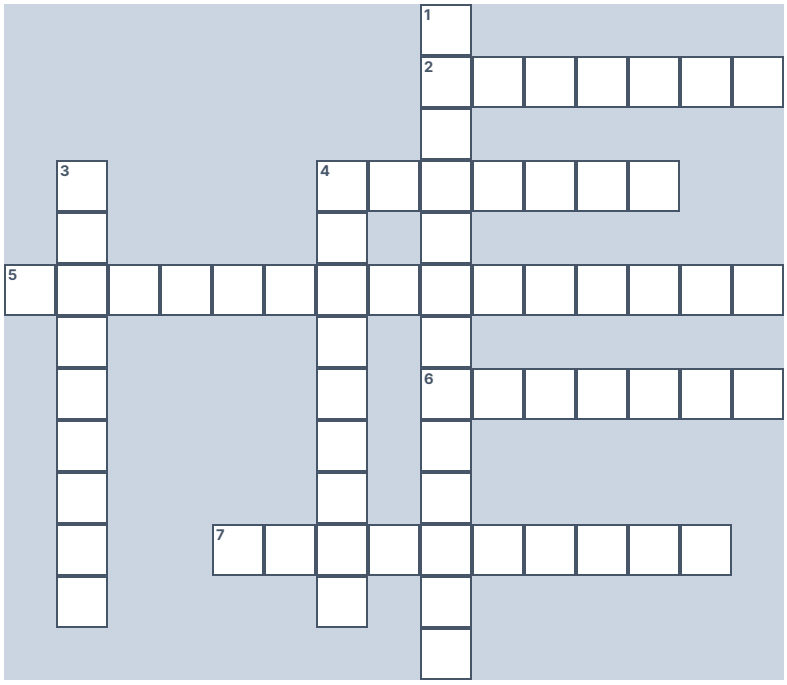
DOPASOWYWANIE DEFINICJI

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

☐	1. WireGuard	A	Obszar wykonywania, w którym działa OpenVPN, powodujący narzut przełączania kontekstu.
☐	2. OpenVPN	B	Niewielki rozmiar bazy kodu WireGuard, który znacznie ułatwia audyt.
☐	3. Przestrzeń jądra	C	Biblioteka kryptograficzna, na której OpenVPN opiera się w zakresie algorytmów szyfrowania.
☐	4. Przestrzeń użytkownika	D	Protokoły transportowe obsługiwane przez OpenVPN; sam WireGuard działa wyłącznie przez UDP.
☐	5. 4,000 wierszy	E	Obszar wykonywania systemu operacyjnego, w którym WireGuard działa dla szybkości.
☐	6. OpenSSL	F	Tokeny asymetryczne używane przez WireGuard do weryfikacji połączeń z peerami.
☐	7. Para kluczy	G	Nowoczesny protokół VPN zaprojektowany z myślą o dużej szybkości i prostym audycie kodu.
☐	8. TCP/UDP	H	Solidny starszy protokół wykorzystujący duży, złożony kod konfiguracyjny.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

2. Biblioteka kryptograficzna, na której OpenVPN opiera się w zakresie algorytmów szyfrowania (7)

4. Protokoły transportowe obsługiwane przez OpenVPN; sam WireGuard działa wyłącznie przez UDP (7)

5. Obszar wykonywania, w którym działa OpenVPN, co powoduje narzut związany z przełączaniem kontekstu (15)

6. Solidny starszy protokół z dużą, złożoną bazą kodu konfiguracji (7)

7. Asymetryczne tokeny używane przez WireGuard do weryfikacji połączeń między węzłami (10)

PIONOWO

1. Niewielki rozmiar bazy kodu WireGuard, który znacznie ułatwia audyt (13)

3. Nowoczesny protokół VPN zaprojektowany z myślą o dużej szybkości i prostym audycie kodu (9)

4. Obszar wykonywania w systemie operacyjnym, w którym działa WireGuard, dla szybkości (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

2 poziomo: Biblioteka kryptograficzna, na której OpenVPN opiera się w zakresie algorytmów szyfrowania (7 liter):

4 poziomo: Protokoły transportowe obsługiwane przez OpenVPN; sam WireGuard działa wyłącznie przez UDP (7 liter):

5 poziomo: Obszar wykonywania, w którym działa OpenVPN, co powoduje narzut związany z przełączaniem kontekstu (15 liter):

6 poziomo: Solidny starszy protokół z dużą, złożoną bazą kodu konfiguracji (7 liter):

7 poziomo: Asymetryczne tokeny używane przez WireGuard do weryfikacji połączeń między węzłami (10 liter):

PIONOWO

1 pionowo: Niewielki rozmiar bazy kodu WireGuard, który znacznie ułatwia audyt (13 liter):

3 pionowo: Nowoczesny protokół VPN zaprojektowany z myślą o dużej szybkości i prostym audycie kodu (9 liter):

4 pionowo: Obszar wykonywania w systemie operacyjnym, w którym działa WireGuard, dla szybkości (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.

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

LISTA SŁÓW

WIREGUARD OPENVPN TRYBJĄDRA TRYBUŻYTKOWNIKA KOMPAKTOWYKOD OPENSSL PARAKLUCZY TCPIUDP

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. WIREGUARD**
- **B. OPENVPN**
- **C. TRYBJĄDRA**
- **D. TRYBUŻYTKOWNIKA**
- **E. KOMPAKTOWYKOD**
- **F. OPENSSL**
- **G. PARAKLUCZY**
- **H. TCPIUDP**

DEFINICJE I POLA DOPASOWANIA

1. Biblioteka kryptograficzna, na której OpenVPN opiera się w zakresie algorytmów szyfrowania.
2. Obszar wykonywania w systemie operacyjnym, w którym działa WireGuard, dla szybkości.
3. Solidny starszy protokół z dużą, złożoną bazą kodu konfiguracji.
4. Asymetryczne tokeny używane przez WireGuard do weryfikacji połączeń między węzłami.
5. Protokoły transportowe obsługiwane przez OpenVPN; sam WireGuard działa wyłącznie przez UDP.
6. Niewielki rozmiar bazy kodu WireGuard, który znacznie ułatwia audyt.
7. Nowoczesny protokół VPN zaprojektowany z myślą o dużej szybkości i prostym audycie kodu.
8. Obszar wykonywania, w którym działa OpenVPN, co powoduje narzut związany z przełączaniem kontekstu.

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. UGEIWARDR
2. ATRBRĄDJY
3. OKOYWODMT AKKP
4. LZKYACUPAR
5. VNNEOPP
6. NYIYŻTOKAW TRKBU
7. OSSLPNE
8. CIPTDUP

Zadanie dodatkowe: Myśl szybko

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

1	Powody, dla których warto wybrać WireGuard			
2	Obietnice, które składa dobry dostawca VPN			
3	Powody, dla których warto wybrać OpenVPN			
4	Powody, dla których warto używać VPN podczas podróży			
5	Rzeczy, które może zobaczyć twój dostawca internetu			
6	Sposoby na rozpoznanie fałszywej sieci Wi-Fi			
7	Mity o VPN			
8	Miejsca, w których używałbyś VPN			
9	Szybkie rzeczy w codziennym życiu			
10	Rzeczy, przed którymi VPN cię nie ochroni			
11	Rzeczy, które ułatwiają sprawdzanie kodu			
12	Rzeczy, które VPN może ukryć			
13	Różnice między WireGuard a OpenVPN			
14	Słowa związane z prywatnością			
15	Nazwy szyfrowania, które znasz			

Punkt kontrolny 8: Studia przypadków dotyczących VPN

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

SARAH (STUDENTKA W KAWIARNI)

👩‍💻 „Hej! Jestem w kawiarni na Wi-Fi, a moja aplikacja VPN pozwala wybrać WireGuard lub OpenVPN. Moje rozmowy wideo ciągle się urywają, gdy przechodzę między siecią kawiarni a hotspotem z telefonu. Jaki protokół powinienem wybrać i dlaczego lepiej poradziłby sobie z tą zmianą?”

ALEX (STUDENT PODRÓŻNIK)

👩‍💻 „Jestem za granicą w sieci hotelowej, która wydaje się blokować większość ruchu VPN. WireGuard w ogóle się nie łączy, a muszę uzyskać dostęp do zasobów mojej szkoły w kraju. Co prawdopodobnie jest blokowane i jak OpenVPN mógłby mi pomóc to obejść?”

Punkt kontrolny 9: Odszyfruj szyfr

Aby ukończyć szkolenie z audytowania protokołów, odszyfruj tę ukrytą wiadomość o wykonywaniu w przestrzeni jądra.

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 15 7 22 25 33 20 22 7 18 29 22 18

25 33 32 3 25 33 32 17 27 28 18 7 15 7 17

30 12 24 7 10 28 1 24 6

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 protokoły mają znaczenie?

Protokół decyduje o tym, jak VPN buduje tunel, jaka kryptografia chroni Twoje dane oraz jak szybko się łączy i ponownie łączy. WireGuard i OpenVPN to dwa protokoły open source, które oferuje większość aplikacji VPN, i różnią się kompromisami między prostotą, szybkością i możliwościami konfiguracji.

Q3: Czy któryś z nich jest bardziej prywatny od drugiego?

Żaden z tych protokołów nie czyni cię anonimowym. Oba szyfrują ruch w tunelu silnymi szyframi; twoja prywatność zależy głównie od tego, co dostawca VPN rejestruje i jak zarządza kluczami, kontami i serwerami.

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 oba są open source?

Tak. WireGuard i społecznościowa edycja OpenVPN publikują swój kod źródłowy, więc niezależni badacze mogą je sprawdzać. Niewielka baza kodu WireGuarda sprawia, że pełny przegląd jest znacznie szybszy.

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: Który jest szybszy?

WireGuard jest zazwyczaj szybszy: działa w jądrze, używa lekkiego szyfrowania ChaCha20-Poly1305 i szybko kończy uzgadnianie. OpenVPN ma większy narzut, ale rzeczywiste prędkości zależą też od obciążenia serwera i odległości.

Q7: Czy oba mogą działać przez TCP i UDP?

Nie. OpenVPN może działać przez UDP lub TCP, a tryb TCP pomaga w sieciach blokujących UDP. WireGuard wysyła swoje pakiety wyłącznie przez UDP, więc może nie działać w sieciach, które dopuszczają tylko TCP. [4]

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 WireGuard i OpenVPN na telefonie?

Tak. WireGuard jest wieloplatformowy, z aplikacjami na Windows, macOS, Linux, iOS i Androida, a klienty OpenVPN istnieją dla tych samych systemów. Większość aplikacji VPN pozwala wybrać jeden z nich. [1]

Q10: Dlaczego WireGuard jest tak mały?

WireGuard obsługuje jeden stały zestaw nowoczesnych szyfrów zamiast wielu opcji. Jego implementacja dla Linuksa wymaga mniej niż 4000 wierszy kodu, co ułatwia audyt w porównaniu z większymi bazami kodu VPN. [3]

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.

Q2: Jakich szyfrów używa WireGuard?

WireGuard używa ChaCha20 z Poly1305 do szyfrowania, Curve25519 do wymiany kluczy, BLAKE2s do haszowania i frameworka Noise do uzgadniania. Nie ma negocjacji szyfrów, więc użytkownicy nie mogą wybrać słabej opcji. [2]

Q3: Jakich szyfrów i bibliotek może używać OpenVPN?

OpenVPN jest ściśle zintegrowany z biblioteką OpenSSL i używa TLS do wymiany kluczy. Administratorzy mogą wybierać szyfry kanału danych, takie jak AES-256-GCM, co zwiększa elastyczność, ale też stwarza miejsce na słabe ustawienia. [4]

Q4: Jak każdy protokół uwierzytelnia partnerów połączenia?

Partnerzy WireGuard identyfikują się nawzajem za pomocą statycznych kluczy publicznych, podobnie jak przy wymianie kluczy SSH, a każdy klucz odpowiada dozwolonym adresom IP tunelu. OpenVPN zwykle opiera się na urzędzie certyfikacji z certyfikatami X.509, często w połączeniu z nazwą użytkownika i hasłem.

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: Co się dzieje, gdy przełączam się z Wi-Fi na sieć komórkową?

WireGuard jest bezpołączeniowy: wysyła pakiety z nowego adresu, a tunel działa dalej po szybkim uzgadnianiu. OpenVPN utrzymuje stan sesji, więc zmiana sieci może wymagać ponownego połączenia, które trwa nieco dłużej.

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: Czy OpenVPN nadal jest dobrym wyborem, skoro WireGuard jest szybszy?

Tak. OpenVPN jest dojrzały i szeroko stosowany, działa przez TCP, gdy UDP jest blokowany, i obsługuje firmowe konfiguracje oparte na certyfikatach. Wielu dostawców oferuje oba protokoły, aby użytkownicy mogli się przełączyć, jeśli jeden jest zablokowany lub wolny.

Q9: Jakich portów używają?

Standardowy port OpenVPN to 1194, ale można go przenieść na dowolny port UDP lub TCP, w tym 443. WireGuard nasłuchuje na porcie UDP ustawionym w jego konfiguracji; 51820 to port używany w jego oficjalnych przykładach.

Q10: Który protokół jest łatwiejszy do ręcznej konfiguracji?

WireGuard jest zazwyczaj prostszy: wygeneruj parę kluczy, wymień klucze publiczne i wypisz dozwolone adresy IP. OpenVPN wymaga certyfikatów, urzędu certyfikacji i większej liczby opcji, choć profile .ovpn łączą je w jednym pliku.

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. DWA TRANSPORTY

OpenVPN może przesyłać swój tunel przez UDP lub TCP, a w trybie TLS jego kanały sterowania i danych współdzielą jeden port. [4]

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. [3]

4. NOWOCZESNA KRYPTOGRAFIA

WireGuard łączy ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 i HKDF w ramach protokołu Noise, bez wyboru szyfrów, w którym użytkownicy mogliby się pomylić. [2]

5. OPENSSL W OPENVPN

OpenVPN jest ściśle zintegrowany z biblioteką OpenSSL i czerpie z niej wiele swoich możliwości kryptograficznych, w tym TLS używany do wymiany kluczy. [4]

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. KLUCZE W STYLU SSH

Połączenia WireGuard nawiązuje się przez wymianę prostych kluczy publicznych, podobnie jak przy wymianie kluczy SSH, bez potrzeby korzystania z urzędu certyfikacji. [1]

8. WIELOPLATFORMOWOŚĆ

WireGuard został po raz pierwszy wydany dla jądra Linuksa, a obecnie jest dostępny dla Windows, macOS, BSD, iOS i Androida, więc ten sam protokół działa na większości urządzeń. [1]

9. UTAJNIENIE PRZESYŁANIA DALEJ

WireGuard powtarza uzgadnianie Noise_IK co kilka minut, aby rotować symetryczne klucze sesji, co zapewnia doskonałą poufność przekazywania (perfect forward secrecy), nawet jeśli długoterminowy klucz później wycieknie. [2]

10. INTERFEJSY TUN/TAP

OpenVPN został zaprojektowany do pracy z wirtualnym interfejsem sieciowym TUN/TAP, który jest dostępny na większości platform i przenosi pakiety tunelu. [4]

Źródła i odnośniki techniczne

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

PUBLIKACJE NAUKOWE I BRANŻOWE

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

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

[3] 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/

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

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

Klucz odpowiedzi: Porównanie protokołów WireGuard i OpenVPN, rozmiarów kodu, szybkości i standardów kryptograficznych

1 **Rozmiar kodu WireGuard** PROTOKOŁY — **Poprawna odpowiedź: D**

UWAGA DLA NAUCZYCIELA

WireGuard jest wyjątkowo zwarty i działa na około 4000 wierszy kodu. Dzięki temu powierzchnia ataku jest mała, a audyt łatwiejszy. Źródło: WireGuard Project.

2 **Prędkość w przestrzeni jądra** OPÓŹNIENIE — **Poprawna odpowiedź: B**

UWAGA DLA NAUCZYCIELA

Wykonując się bezpośrednio w przestrzeni jądra, WireGuard unika narzutu przełączania kontekstu, co umożliwia dużą przepustowość. Źródło: WireGuard Project.

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

UWAGA DLA NAUCZYCIELA

OpenVPN jest ściśle zintegrowany z OpenSSL, który dostarcza szyfry takie jak AES-GCM i sprawia, że jest wysoce konfigurowalny, ale bardziej złożony.

4 **Wydajność protokołu** KONTROLA ROUTINGU — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

WireGuard nawiązuje uzgadnianie w milisekundach i natychmiast reaguje na roaming sieciowy (np. przełączenie z Wi-Fi na sieć komórkową). Źródło: Microsoft Native Gateway, Apple Support.

5 **Kryptografia asymetryczna** PRYWATNOŚĆ — **Poprawna odpowiedź: C**

UWAGA DLA NAUCZYCIELA

WireGuard używa Cryptokey Routing, czyli kojarzenia kluczy publicznych z dozwolonymi adresami IP tunelu, podobnie jak w konfiguracjach SSH. Źródło: WireGuard Project.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 Pytanie 6

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Implementacja WireGuard dla Linuksa liczy mniej niż 4 000 linii, więc zespoły ds. bezpieczeństwa mogą ją przejrzeć znacznie szybciej niż znacznie większe bazy kodu VPN, takie jak OpenVPN.

7 Opóźnienie w przestrzeni użytkownika

PRĘDKOŚCI

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

OpenVPN działa w przestrzeni użytkownika i przekazuje pakiety tam i z powrotem między wirtualnym interfejsem jądra, co dodaje narzut przełączania kontekstu (chyba że używane jest odciążenie jądra, takie jak OpenVPN DCO). Źródło: DD-WRT custom firmware.

8 Konfiguracja OpenVPN

RYZYKO SNIFFINGU

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

OpenVPN obsługuje działanie przez TCP (dla niezawodności i omijania zapór sieciowych) lub UDP (dla szybkości), dzięki czemu jest zgodny ze złożonymi zaporami sieciowymi w przedsiębiorstwach. Źródło: IETF Cryptographic Protocols.

9 Nowoczesna kryptografia

ZAPORY SIECIOWE

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

WireGuard odrzuca przestarzałe szyfry na rzecz nowoczesnych, bezpiecznych prymitywów, takich jak ChaCha20 i Poly1305, które działają szybko na mobilnych procesorach. Źródło: WireGuard Project.

10 Uproszczenie pary kluczy

BRAK LOGÓW

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

WireGuard nie używa certyfikatów ani skomplikowanych hierarchii urzędów certyfikacji; opiera się na prostych parach kluczy publicznych i prywatnych wymienianych między partnerami (peerami). Źródło: WireGuard Project.

Klucze słownictwa i kryteria oceny

Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).

PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

G 1. WireGuard	H 2. OpenVPN	E 3. Przestrzeń jądra	A 4. Przestrzeń użytkownika
B 5. 4,000 wierszy	C 6. OpenSSL	F 7. Para kluczy	D 8. TCP/UDP

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 WIREGUARD	2 OPENVPN	3 TRYB JĄDRA	4 TRYB UŻYTKOWNIKA
5 PARA KLUCZY	6 AUDYTOWALNOŚĆ		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 F – OPENSSL	2 C – TRYBJĄDRA	3 B – OPENVPN	4 G – PARAKLUCZY
5 H – TCPIUDP	6 E – KOMPAKTOWYKOD	7 A – WIREGUARD	8 D – TRYBUŻYTKOWNIKA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia WireGuard, OpenVPN i Przestrzeń jądra 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

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

ROZWIĄZANIE KRZYŻÓWKI

							K							
							O	P	E	N	S	S	L	
							M							
	W				T	C	P	I	U	D	P			
	I				R		A							
T	R	Y	B	U	Ż	Y	T	K	O	W	N	I	K	A
	E				B		T							
	G				J		O	P	E	N	V	P	N	
	U				Ą		W							
	A				D		Y							
	R			P	A	R	A	K	L	U	C	Z	Y	
	D				A		O							
							D							

PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: OPENSSL Biblioteka kryptograficzna, na której OpenVPN opiera się w zakresie algorytmów szyfrowania (7 liter)

4 poziomo: TCPIUDP Protokoły transportowe obsługiwane przez OpenVPN; sam WireGuard działa wyłącznie przez UDP (7 liter)

5 poziomo: TRYBUŻYTKOWNIKA Obszar wykonywania, w którym działa OpenVPN, co powoduje narzut związany z przełączaniem kontekstu (15 liter)

6 poziomo: OPENVPN Solidny starszy protokół z dużą, złożoną bazą kodu konfiguracji (7 liter)

7 poziomo: PARAKLUCZY Asymetryczne tokeny używane przez WireGuard do weryfikacji połączeń między węzłami (10 liter)

PIONOWO

1 pionowo: KOMPAKTOWYKOD Niewielki rozmiar bazy kodu WireGuard, który znacznie ułatwia audyt (13 liter)

3 pionowo: WIREGUARD Nowoczesny protokół VPN zaprojektowany z myślą o dużej szybkości i prostym audycie kodu (9 liter)

4 pionowo: TRYBJĄDRA Obszar wykonywania w systemie operacyjnym, w którym działa WireGuard, dla szybkości (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. UGEIWARDR — **WIREGUARD**
2. ATRBRĄDJY — **TRYBJĄDRA**
3. OKOYWODMTAKKP — **KOMPAKTOWYKOD**
4. LZKYACUPAR — **PARAKLUCZY**
5. VNNEOPP — **OPENVPN**
6. NYIYŻTOKAWTRKBU — **TRYBUŻYTKOWNIKA**
7. OSSLPNE — **OPENSSL**
8. CIPTDUP — **TCPIUDP**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"ULEPSZ OPENVPN SZYBSZYM TUNELEM WIREGUARD"

Klucz odpowiedzi do studiów przypadków

A Scenariusz A: Wybór protokołu

SNIFFING I SZYFROWANIE | Dylemat Sarah

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Rekomendacja: WireGuard. Jego lekka, bezpołączeniowa konstrukcja pozwala tunelowi szybko odzyskać połączenie, gdy zmienia się jej sieć, a ChaCha20-Poly1305 zapewnia szybkie szyfrowanie.
- Bezpieczeństwo: Oba protokoły szyfrują jej ruch w sieci Wi-Fi w kawiarni, więc każdy z nich chroni jej loginy, jeśli jest poprawnie skonfigurowany; wybór wpływa głównie na prędkość i stabilność.

B Scenariusz B: Omijanie blokad VPN

GEOBLOKADY I ADRESY IP | Dylemat Alexa

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Powód blokady: WireGuard używa wyłącznie UDP, a zapora sieciowa hotelu prawdopodobnie blokuje UDP lub rozpoznaje pakiety WireGuard przez filtrowanie albo głęboką inspekcję pakietów (DPI).
- Jak pomaga OpenVPN: może działać przez TCP, w tym port 443 używany przez HTTPS, którego zapory sieciowe w hotelach rzadko blokują całkowicie, ponieważ przeglądanie stron od niego zależy.