Imię i nazwisko: _____ **Data:** _____ **Wynik:** _____

VPN dostępu zdalnego

Zabezpieczanie punktów końcowych zdalnych pracowników, uwierzytelnianie wieloskładnikowe i konfiguracje tuneli IPsec.

PRZEGLĄD NAUKI O VPN DOSTĘPU ZDALNEGO

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 sieci VPN ze zdalnym dostępem. Poznasz tunele klient–serwer, logowanie wieloskładnikowe, kontrole stanu punktów końcowych, limity przepustowości i audyt bezpieczeństwa syslog.

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/najlepszy-vpn-dla-firm/zdalny-dostep/

Twoja ścieżka nauki: VPN do dostępu zdalnego

- Zabezpieczanie punktów końcowych zdalnych pracowników, które mają dostęp do węzłów sieci lokalnej.
- Skonfiguruj zasady uwierzytelniania wieloskładnikowego dla zdalnych logowań.
- Skonfiguruj konfiguracje IPsec i OpenVPN typu klient-do-sieci (client-to-site).
- Przeprowadź audyt dzienników połączeń zdalnych pod kątem naruszeń kontroli dostępu.
- Wdróż kontrole stanu urządzeń przed udzieleniem dostępu do sieci.
- Zoptymalizuj przepustowość serwera, aby zapobiec dławieniu pasma przy pracy zdalnej.

INSTRUKCJE O VPN DOSTĘPU ZDALNEGO

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 kontroli stanu zabezpieczeń urządzenia (posture checks) i logowania wieloskładnikowego. Zakończ zadaniem dodatkowym Myśl szybko.

TUNELE KLIENT-DO-SIECI I ZGODNOŚĆ PUNKTÓW KOŃCOWYCH (WPROWADZENIE)

VPN dostępu zdalnego tworzą bezpieczne tunele klient–sieć dla pracowników spoza siedziby. Zabezpieczenie tych połączeń wymaga wymuszenia logowania z uwierzytelnianiem wieloskładnikowym (MFA), przeprowadzania kontroli zgodności stanu punktów końcowych i audytowania logów za pomocą centralnych kolektorów syslog.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **1. Jaki standard uwierzytelniania powinny wymagać portale VPN do dostępu zdalnego?**
   - A) Wieloskładnikowe
   - B) Pojedynczy czynnik
   - C) Nieszyfrowane
   - D) Lokalny gość

2. **2. Który protokół jest standardem zabezpieczania połączeń klient-sieć w pracy zdalnej?**
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. **3. Jakie sprawdzenie potwierdza, że zdalny laptop jest czysty, zanim się połączy?**
   - A) Kontrola stanu zabezpieczeń
   - B) Test szybkości
   - C) Test ping
   - D) Liczba pamięci

4. **4. Gdzie przechowywane są dzienniki połączeń pracowników zdalnych na potrzeby audytu bezpieczeństwa?**
   - A) Serwer Syslog
   - B) Klucz rejestru
   - C) Pamięć klienta
   - D) Przeglądarka internetowa

5. **5. Jaki problem występuje, gdy liczba pracowników zdalnych przekracza przepustowość bramy?**
   - A) Dławienie przepustowości
   - B) Wyciek DNS
   - C) Przepustka uzgadniania
   - D) Ujawnienie IP

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Uwierzytelnianie wieloskładnikowe dodaje dodatkowy token weryfikacyjny, aby zabezpieczyć zdalne logowania.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Kontrole stanu zabezpieczeń zezwalają urządzeniom zdalnym z wyłączonymi zaporami sieciowymi na dostęp do serwerów prywatnych.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Logi VPN dostępu zdalnego są niezbędne do wykrywania nieautoryzowanego wejścia do sieci firmowej.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. OpenVPN i IPsec to przestarzałe protokoły, które nie szyfrują danych zdalnych klientów.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Wąskie gardło przepustowości bramy występuje, gdy ruch zdalny przekracza pojemność karty połączenia.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Aby chronić portale firmowe, zdalne logowania muszą wymagać uwierzytelniania, które jest _____ .

2. Zdalni klienci szyfrują ładunki tunelu za pomocą standardowych protokołów, takich jak _____ .

3. Przed uzyskaniem połączeń z siecią urządzenia muszą przejść sprawdzenie bezpieczeństwa, czyli _____ .

4. Rejestry wejść, które można audytować, są stale przesyłane do centralnego serwera _____ .

5. Duży ruch w godzinach pracy może prowadzić do zatorów w bramie, a przyczyną jest ograniczona _____ .

6. Sterowniki wirtualnych adapterów w Windows i macOS obsługują połączenia klient–sieć (client-to-site), czyli _____ .

BANK SŁÓW

KONTROLA STANU OPENVPN PRZEPUSTOWOŚĆ SYSLOG SZYFROWANIE
TUNELOWANIE WIELOSKŁADNIKOWE ZAPORA SIECIOWA

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie kluczowych pojęć

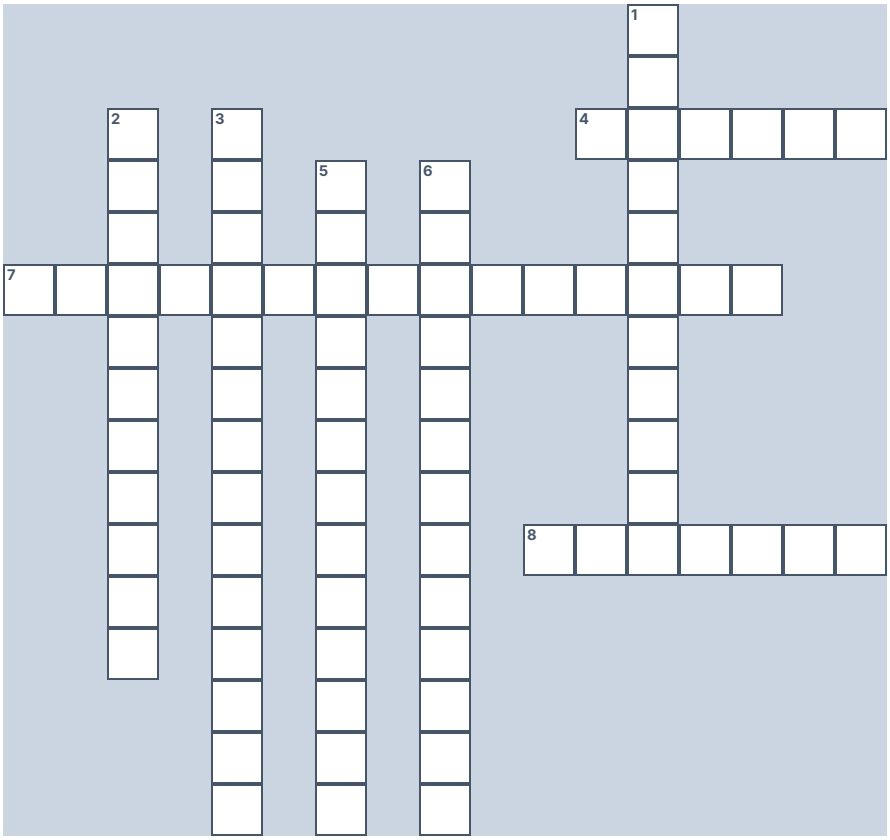
DOPASOWYWANIE DEFINICJI

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

☐	1. WIELOSKŁADNIKOWE	A	Enkapsulacja danych w bezpiecznej ścieżce.
☐	2. OPENVPN	B	Centralny kolektor dzienników zdarzeń bezpieczeństwa.
☐	3. STAN ZABEZPIECZEŃ	C	Limit przepustowości sieci.
☐	4. SYSLOG	D	Standardowy protokół klient-do-sieci (client-to-site).
☐	5. PRZEPUSTOWOŚĆ	E	Zdalna weryfikacja stanu urządzenia.
☐	6. SZYFROWANIE	F	Reguły systemu filtrowania ruchu.
☐	7. TUNELOWANIE	G	Kryptograficzne zniekształcanie pakietów.
☐	8. ZAPORA SIECIOWA	H	Zabezpieczenie logowania wymagające dodatkowych tokenów.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

4. Centralny kolektor dzienników bezpieczeństwa (6)

7. Zabezpieczenie logowania wymagające dodatkowych tokenów (15)

8. Standardowy protokół typu klient–sieć (client-to-site) (7)

PIONOWO

1. Kryptograficzne przekształcanie pakietów w nieczytelną postać (11)

2. Enkapsulacja danych w bezpiecznej ścieżce (11)

3. Reguły systemu filtrowania ruchu (14)

5. Limit pojemności danych w sieci (13)

6. Weryfikacja kondycji zdalnego urządzenia (13)

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

4 poziomo: Centralny kolektor dzienników bezpieczeństwa (6 liter):

7 poziomo: Zabezpieczenie logowania wymagające dodatkowych tokenów (15 liter):

8 poziomo: Standardowy protokół typu klient–sieć (client-to-site) (7 liter):

PIONOWO

1 pionowo: Kryptograficzne przekształcanie pakietów w nieczytelną postać (11 liter):

2 pionowo: Enkapsulacja danych w bezpiecznej ścieżce (11 liter):

3 pionowo: Reguły systemu filtrowania ruchu (14 liter):

5 pionowo: Limit pojemności danych w sieci (13 liter):

6 pionowo: Weryfikacja kondycji zdalnego urządzenia (13 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 A Ę O K Ń Ć W N C Ć G I Ą Ą
N Ó R Ł P W T I I Ź Z Ę Ź S G
A Y X H Ę G R E T Ń A U Ć K R
T Ć T S S O Ł L P Ł P N Ś Ś H
S L T P Z L H O Ź Ó O Ł O X V
A Ń U Z Y S Q C Q Ą R A W Ł O
L Ó N N F Y Ą Z Ł I A Ę O J P
O Ń E Z R S B Y Ż Ż S Ź T B E
R N L V O Y M N C Ę I Ó S X N
T P O Q W Y G N D Ź E B U X V
N Ł W E A G G I Ż X C C P O P
O Q A K N Y Y K R L I Ż E A N
K N N R I Ż R O M F O Ś Z W F
Ł X I J E B Ź W C B W Ź R O V
Ż O E Ż U T Ą E H W A P P Y C

LISTA SŁÓW

WIELOCZYNNIKOWE OPENVPN KONTROLASTANU SYSLOG PRZEPUSTOWOŚĆ SZYFROWANIE TUNELOWANIE ZAPORASIECIOWA

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. WIELOCZYNNIKOWE**
- **B. OPENVPN**
- **C. KONTROLASTANU**
- **D. SYSLOG**
- **E. PRZEPUSTOWOŚĆ**
- **F. SZYFROWANIE**
- **G. TUNELOWANIE**
- **H. ZAPORASIECIOWA**

DEFINICJE I POLA DOPASOWANIA

1. Centralny kolektor dzienników bezpieczeństwa.
2. Reguły systemu filtrowania ruchu.
3. Enkapsulacja danych w bezpiecznej ścieżce.
4. Kryptograficzne przekształcanie pakietów w nieczytelną postać.
5. Standardowy protokół typu klient–sieć (client-to-site).
6. Limit pojemności danych w sieci.
7. Weryfikacja kondycji zdalnego urządzenia.
8. Zabezpieczenie logowania wymagające dodatkowych tokenów.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z pośrednictwem domenowym. Wpisz odpowiedzi w przygotowanych polach.

1. CZNNIIYEKO WWLEO
2. NROONKALUS TAT
3. RPTWOŚĆZSP UOE
4. WIEONLNATU E
5. VNNEOPP
6. OLSSGY
7. ARSZWENIYO F
8. OIOAECAAZS PWIR

Zadanie dodatkowe: Myśl szybko

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

1	Mity o VPN			
2	Słowa opisujące Zero Trust			
3	Programy biurowe, które znasz			
4	Zasady bezpiecznej pracy zdalnej			
5	Rzeczy, które może zobaczyć twój dostawca internetu			
6	Usługi VPN, które znasz			
7	Miejsca, z których pracują pracownicy			
8	Narzędzia, których firma używa codziennie			
9	Role w dziale IT			
10	Urządzenia, które może mieć pracownik			
11	Dane, które firma musi chronić			
12	Rzeczy do zrobienia po naruszeniu bezpieczeństwa			
13	Rzeczy, które mogą zakłócić spotkanie wideo			
14	Sposoby na bezpieczne logowanie			
15	Powody, dla których warto dać pracownikom VPN			

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: EGZEKWOWANIE MFA



Scenariusz: Analityk biznesowy próbuje zalogować się do firmowej bazy danych podczas pracy zdalnej. Wpisuje poprawną nazwę użytkownika i hasło, ale portal VPN blokuje dostęp i żąda kodu z fizycznego tokena.

Pytanie do dyskusji: Jaka polityka bezpieczeństwa wymusza ten krok podwójnej weryfikacji?

STUDIUM PRZYPADKU 2: ZGODNOŚĆ Z POSTAWĄ BEZPIECZEŃSTWA



Scenariusz: Wykonawca łączy swojego prywatnego laptopa ze zdalną siecią firmową. Klient VPN natychmiast zrywa połączenie, informując użytkownika, że jego definicje antywirusowe są nieaktualne.

Pytanie do dyskusji: Jaka wyspecjalizowana kontrola bramy VPN zablokowała tę próbę połączenia?

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

33	6	1	15	18	32		6	20	25	27	8	22		29	22	18				
4	11	24	20	18	12		24	20	33	22	24	20	25	33	20	18	7			
						28	24	33	2	6	33	7	18	12	1					

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 VPN do dostępu zdalnego?

Bezpieczna metoda połączenia umożliwiająca pracownikom pracującym poza biurem bezpośrednie łączenie się z prywatnymi serwerami firmowymi.

Q2: Czym różni się połączenie klient–sieć od połączenia sieć–sieć (site-to-site)?

Klient-do-sieci łączy poszczególne urządzenia użytkowników, natomiast sieć-do-sieci łączy całe fizyczne lokalizacje biur.

Q3: Czym jest kontrola stanu urządzenia (device posture check)?

Skan sprawdzający stan bezpieczeństwa urządzenia zdalnego (antywirus, poziom poprawek systemu) przed przyznaniem dostępu.

Q4: Dlaczego OpenVPN jest używany do dostępu zdalnego?

Ze względu na silny protokół bezpieczeństwa, zgodność z wieloma platformami i możliwość obsługi pojedynczych połączeń.

Q5: Jak MFA chroni dostęp zdalny?

Dodaje dodatkowy token weryfikacyjny, który uniemożliwia dostęp nawet wtedy, gdy hasła pracowników wyciekły lub zostały skradzione.

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

Przejrzyj najczęstsze pytania i odpowiedzi dotyczące wirtualnych sieci prywatnych (VPN) i tunelowania.

Q6: Czym jest serwer syslog?

Scentralizowane repozytorium logów, które przechowuje zdarzenia połączeń, logowania i alerty systemowe na potrzeby audytów zgodności.

Q7: Co powoduje dławienie przepustowości?

Gdy łączne zapotrzebowanie pracowników zdalnych na przepustowość przekracza limit prędkości internetu bramy firmowej.

Q8: Czy mogę połączyć swój domowy komputer z firmowym VPN?

Tylko jeśli urządzenie przechodzi audyty kontroli stanu zabezpieczeń firmy i jest autoryzowane przez administratorów IT.

Q9: Czym jest enkapsulacja sieciowa?

Opakowywanie przesyłanych pakietów danych w szyfrowane nagłówki protokołu w celu zabezpieczenia transmisji.

Q10: Jak tunelowanie dzielone optymalizuje dostęp zdalny?

Pozwala pracownikom korzystać z lokalnego dostawcy internetu do zwykłego przeglądania, a pliki związane z pracą kierować przez 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: Jak uwierzytelnianie oparte na certyfikatach wzmacnia dostęp zdalny?

Wiąże uprawnienia do połączeń z zainstalowanymi lokalnie certyfikatami cyfrowymi, blokując niezarządzane lub nieautoryzowane urządzenia.

Q2: Jakie jest ryzyko dla bezpieczeństwa związane z tunelowaniem dzielonym w pracy zdalnej?

Tworzy potencjalny most, przez który przejęte urządzenie lokalne może kierować zewnętrzne zagrożenia do sieci prywatnej.

Q3: Jak kontrole stanu urządzenia sprawdzają ustawienia rejestru?

Klient VPN uruchamia lokalne skrypty, które odpytują ścieżki rejestru, aby sprawdzić, czy firmowe oprogramowanie zabezpieczające jest aktywne.

Q4: Dlaczego syslog domyślnie używa portu UDP 514?

Aby szybko przesyłać logi przy minimalnym narzucie, choć bezpieczne konfiguracje wymagają obecnie enkapsulacji TLS przez TCP.

Q5: Jak firmy rozwiązują problemy z wąskimi gardłami przepustowości bramy?

Przez wdrożenie load balancerów i rozdzielanie ruchu zdalnego między regionalne węzły serwerowe.

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: Jaką funkcję pełnią wirtualne adaptery TAP/TUN na klientach zdalnych?

Działają jak wirtualne karty sieciowe, kierując ruch TCP/IP na poziomie urządzenia bezpośrednio do szyfrowanego tunelu VPN.

Q7: Jak IKEv2 MOBIKE wspiera mobilność pracowników zdalnych?

Dynamicznie aktualizuje powiązania adresów IP, utrzymując aktywny VPN, gdy użytkownik przechodzi między Wi-Fi a danymi komórkowymi.

Q8: Czym różni się routing dzielony od routingu z pełnym tunelem?

Pełny routing kieruje cały ruch internetowy urządzenia przez VPN, podczas gdy routing dzielony wysyła przez VPN tylko ruch do firmowych adresów IP.

Q9: Jak urządzenia NAT obsługują zdalne połączenia VPN?

Przez mapowanie lokalnych zakresów portów na publiczne adresy IP bramy w celu kierowania powracających zaszyfrowanych pakietów danych.

Q10: Jakie standardy zgodności nakazują audytowanie dostępu zdalnego?

Standardy takie jak HIPAA, SOC 2 i PCI DSS wymagają rejestrowania i monitorowania wszystkich sesji połączeń zdalnych.

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

VPN dostępu zdalnego tworzą bezpieczne tunele klient–sieć dla pracowników spoza siedziby.

2. WGLĄD W VPN

Uwierzytelnianie wieloskładnikowe jest wymagane przez przepisy dotyczące zgodności, aby chronić zdalne portale biznesowe.

3. WGLĄD W VPN

Kontrole stanu zabezpieczeń weryfikują lokalne ustawienia bezpieczeństwa klienta, zanim przyznany zostanie dostęp do sieci prywatnej.

4. WGLĄD W VPN

Serwery syslog agregują logi połączeń, aby audytować i wykrywać nieautoryzowane próby dostępu.

5. WGLĄD W VPN

Wąskie gardła przepustowości bramy występują, gdy łączne zapotrzebowanie na ruch zdalny przekracza limity internetowe serwera.

6. WGLĄD W VPN

Wirtualne karty sieciowe enkapsulują zapytania sieciowe systemu operacyjnego w bezpiecznych protokołach.

7. WGLĄD W VPN

Obsługa MOBIKE pozwala zdalnym klientom przełączać sieci bez zrywania tunelu VPN.

8. WGLĄD W VPN

Routing pełnego tunelu zabezpiecza cały ruch internetowy pracowników, ale zwiększa obciążenie firmowej bramy.

9. WGLĄD W VPN

Uwierzytelnianie certyfikatem wiąże autoryzację połączenia VPN bezpośrednio ze sprzętem zarządzanym przez firmę.

10. WGLĄD W VPN

Ramy takie jak SOC 2 i PCI DSS oczekują rejestrowania i monitorowania sesji dostępu zdalnego.

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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 **Tokeny logowania** BEZPIECZEŃSTWO MFA — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Uwierzytelnianie wieloskładnikowe wymusza dodatkową weryfikację przy logowaniu. Źródło: MFA Implementation.

2 **Tunel OpenVPN** KLIENT-DO-SIECI — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

OpenVPN to standardowy protokół zabezpieczania tuneli klient–sieć. Źródło: OpenVPN Client.

3 **Audyty stanu zabezpieczeń** SPRAWDZANIE URZĄDZENIA — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Kontrole stanu zabezpieczeń skanują punkty końcowe pod kątem aktywnych zapór sieciowych i narzędzi antywirusowych. Źródło: Posture Compliance.

4 **Agregator logów** SERWER SYSLOG — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Serwery syslog zbierają logi zdarzeń bezpieczeństwa, aby monitorować naruszenia dostępu. Źródło: Syslog Standard.

5 **Przepełnienie karty** WĄSKIE GARDŁO BRAMY — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Wąskie gardło przepustowości bramy występuje, gdy ruch użytkowników przekracza limity serwera. Źródło: Capacity Planning.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Tokeny logowania** KONTROLE MFA — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Uwierzytelnianie wieloskładnikowe wymusza dodatkową weryfikację przy logowaniu. Źródło: MFA Implementation.

7 **Pytanie 7** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Kontrole stanu urządzenia (posture checks) blokują urządzenia z wyłączoną zaporą sieciową lub antywirusem, więc takie urządzenia są odrzucane.

8 **Agregator logów** SERWER SYSLOG — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Serwery syslog zbierają logi zdarzeń bezpieczeństwa, aby monitorować naruszenia dostępu. Źródło: Syslog Standard.

9 **Pytanie 9** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

OpenVPN i IPsec to aktualne protokoły, które szyfrują ruch zdalnych klientów.

10 **Przepełnienie karty** WĄSKIE GARDŁO BRAMY — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Wąskie gardło przepustowości bramy występuje, gdy ruch użytkowników przekracza limity serwera. Źródło: Capacity Planning.

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. WIELOSKŁADNIKOWE	D 2. OPENVPN	E 3. STAN ZABEZPIECZEŃ	B 4. SYSLOG
C 5. PRZEPUSTOWOŚĆ	G 6. SZYFROWANIE	A 7. TUNELOWANIE	F 8. ZAPORA SIECIOWA

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 WIELOSKŁADNIKOWE	2 OPENVPN	3 KONTROLA STANU	4 SYSLOG
5 PRZEPUSTOWOŚĆ	6 TUNELOWANIE		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 D – SYSLOG	2 H – ZAPORASIECIOWA	3 G – TUNELOWANIE	4 F – SZYFROWANIE
5 B – OPENVPN	6 E – PRZEPUSTOWOŚĆ	7 C – KONTROLASTANU	8 A – WIELOCZYNNIKOWE

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia WIELOSKŁADNIKOWE, OPENVPN i STAN ZABEZPIECZEŃ oraz podać przykład każdego z nich.

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

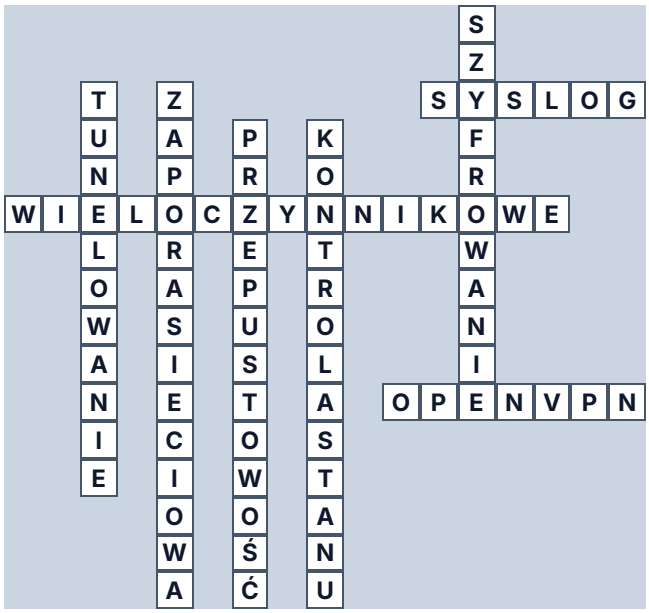
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

4 poziomo: SYSLOG Centralny kolektor dzienników bezpieczeństwa (6 liter)

7 poziomo: WIELOCZYNNIKOWE Zabezpieczenie logowania wymagające dodatkowych tokenów (15 liter)

8 poziomo: OPENVPN Standardowy protokół typu klient–sieć (client-to-site) (7 liter)

PIONOWO

1 pionowo: SZYFROWANIE Kryptograficzne przekształcanie pakietów w nieczytelną postać (11 liter)

2 pionowo: TUNELOWANIE Enkapsulacja danych w bezpiecznej ścieżce (11 liter)

3 pionowo: ZAPORASIECIOWA Reguły systemu filtrowania ruchu (14 liter)

5 pionowo: PRZEPUSTOWOŚĆ Limit pojemności danych w sieci (13 liter)

6 pionowo: KONTROLASTANU Weryfikacja kondycji zdalnego urządzenia (13 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. CZNNIIYEKOWWLEO — **WIELOCZYNNIKOWE**
2. NROONKALUSTAT — **KONTROLASTANU**
3. RPTWOŚĆZSPUOE — **PRZEPUSTOWOŚĆ**
4. WIEONLNATUE — **TUNELOWANIE**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. ARSZWENIYOF — **SZYFROWANIE**
8. OIOAECAAZSPWIR — **ZAPORASIECIOWA**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"ZDALNY DOSTĘP VPN CHRONI ROZPROSZONE URZĄDZENIA"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Egzekwowanie MFA

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Analityk biznesowy próbuje zalogować się do firmowej bazy danych podczas pracy zdalnej. Wpisuje poprawną nazwę użytkownika i hasło, ale portal VPN blokuje dostęp i żąda kodu z fizycznego tokena.
- Zalecana strategia i rozwiązanie: Firmowy portal VPN wymusza ścisłą politykę uwierzytelniania wieloskładnikowego (MFA), aby zabezpieczyć zdalne logowania.

B Studium przypadku 2: Zgodność z postawą bezpieczeństwa

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Wykonawca łączy swojego prywatnego laptopa ze zdalną siecią firmową. Klient VPN natychmiast rozłącza połączenie, informując użytkownika, że jego definicje antywirusowe są nieaktualne.
- Zalecana strategia i rozwiązanie: Brama dostępu zdalnego przeprowadziła kontrolę stanu punktu końcowego i zablokowała urządzenie z powodu przestarzałej konfiguracji zabezpieczeń.