Imię i nazwisko: _____ Data: _____ Wynik: _____

Najlepszy VPN dla firm

Praktyczna recenzja bezpieczeństwa, skalowalności i centralnej administracji VPN dla firm.

PRZEGLĄD WIEDZY: NAJLEPSZY VPN DLA FIRM

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 Business VPN i sieci zdalnego dostępu. Poznasz architektury Zero Trust, tunele IPsec typu site-to-site, ramy SASE, wieloskładnikowe logowanie i kontrole bezpieczeństwa punktów końcowych.

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/

Twoja ścieżka nauki: VPN dla firm

- Poznaj czołowych dostawców VPN dla firm i ich funkcje dla zespołów.
- Przeanalizuj różnice między prywatnością konsumenckich VPN a biznesowymi kontrolami administracyjnymi.
- Rozróżnij VPN-y zdalnego dostępu od firmowych tuneli typu site-to-site.

INSTRUKCJE DO PRZEWODNIKA PO VPN DLA FIRM

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 konfiguracji zdalnego dostępu w przedsiębiorstwach. Zakończ zadaniem dodatkowym Myśl szybko.

ZDALNY DOSTĘP DLA PRZEDSIĘBIORSTW I BEZPIECZNA KRAWĘDŹ SIECI (WPROWADZENIE)

Zabezpieczenie zdalnego dostępu do zasobów firmy wymaga przejścia od tradycyjnych modeli VPN opartych na obwodzie do architektur Zero Trust. Wymuszanie silnego uwierzytelniania wieloskładnikowego (MFA) oraz frameworków Secure Access Service Edge (SASE) chroni wrażliwe zasoby przed przejętymi punktami końcowymi.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **Który typ biznesowego VPN łączy ze sobą całe sieci biurowe?**
   - A. VPN typu site-to-site
   - B. VPN zdalnego dostępu
   - C. VPN konsumencki
   - D. Smart DNS

2. **Który wybór jest wskazany jako najlepszy ogólnie dla zespołów biznesowych?**
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. **Czemu zapobiega dedykowany statyczny adres IP w zespołach firmowych?**
   - A. Umieszczanie adresów IP na czarnej liście
   - B. Spada szybkość routera
   - C. Kompresja danych
   - D. Aktualizacje klienta

4. **Który dostawca jest wskazany jako najlepszy dla dedykowanej infrastruktury?**
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. **Jaka funkcja zapewnia scentralizowany panel administracyjny do zarządzania użytkownikami?**
   - A. Kontrola administracyjna
   - B. Przekierowywanie portów
   - C. Emulacja routera
   - D. Dzielone tunelowanie

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. VPN dostępu zdalnego pozwalają poszczególnym pracownikom łączyć się z dowolnego miejsca.

Prawda Fałsz

7 Pytanie 7

7. VPN-y konsumenckie chronią całą organizację za pomocą jednego panelu administracyjnego.

Prawda Fałsz

8 Pytanie 8

8. Dedykowane adresy IP oddzielają ruch firmowy od ruchu publicznego.

Prawda Fałsz

9 Pytanie 9

9. Private Internet Access jest wskazywany jako najlepszy dla dużych przedsiębiorstw.

Prawda Fałsz

10 Pytanie 10

10. SASE integruje routing WAN z frameworkami bezpieczeństwa dostarczanymi z chmury.

Prawda Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Najwyżej oceniany dostawca dla zespołów biznesowych to _____ .
2. Połączenie wielu oddziałów firmy odbywa się przez tunel typu _____ .
3. Aby zapobiec umieszczeniu adresu na czarnej liście, zespoły wdrażają _____ .
4. Administratorzy zarządzają uprawnieniami urządzeń, korzystając z centralnego narzędzia, czyli _____ .
5. Dynamiczne dodawanie stanowisk w celu obsługi rosnących zespołów to _____ .
6. Podstawą spełniania wymogów regulacyjnych i audytu danych jest _____ .

BANK SŁÓW

BRAMA NORDLAYER PANEL ADMINA ROUTING SITE-TO-SITE
SKALOWALNOŚĆ STAŁY ADRES IP ZGODNOŚĆ

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie kluczowych pojęć

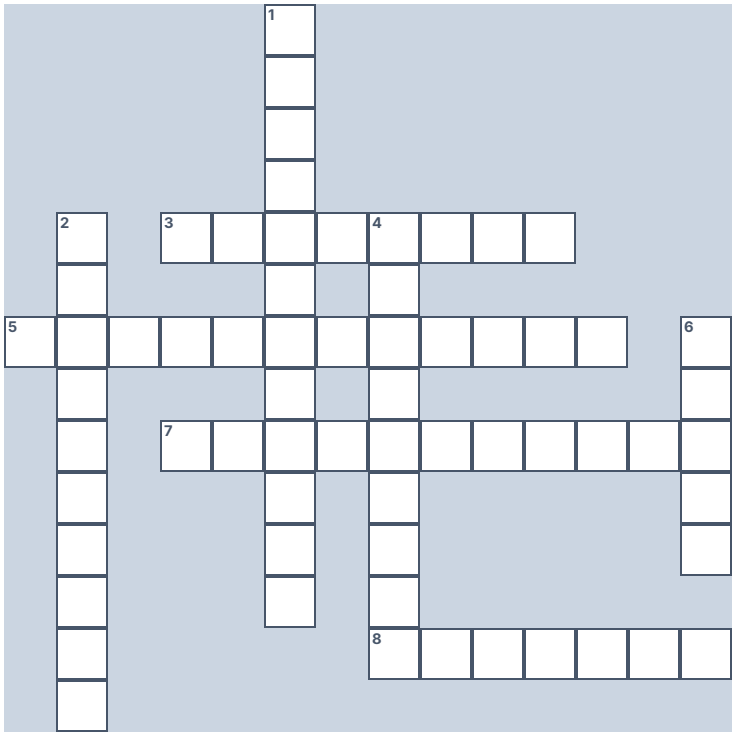
DOPASOWYWANIE DEFINICJI

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

	1. NORDLAYER	A	Dynamiczny wzrost zespołu z wieloma stanowiskami.
	2. SITE-TO-SITE	B	Najlepszy ogólny wybór dla firm.
	3. STAŁY ADRES IP	C	Kontrola ruchu w tunelowaniu dzielonym.
	4. PANEL	D	Standardowy audyt regulacyjny.
	5. SKALOWALNOŚĆ	E	Zdalny węzeł wejściowy uwierzytelniania.
	6. ZGODNOŚĆ	F	Dedykowany adres spoza czarnych list.
	7. ROUTING	G	Tunel łączący sieci biurowe.
	8. BRAMA	H	Centralna konsola administracyjna.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

3. Standard zgodności z wymogami regulacyjnymi i audytu (8)

5. Dedykowany adres spoza czarnej listy (12)

7. Centralna konsola sterowania administratora (11)

8. Kontrola ruchu w ramach tunelowania dzielonego (split tunneling) (7)

PIONOWO

1. Dynamiczne powiększanie zespołu o kolejne stanowiska (12)

2. Tunel łączący sieci biur (10)

4. Najlepszy wybór ogólny dla firm (9)

6. Zdalny węzeł wejściowy do uwierzytelniania (5)

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

3 poziomo: Standard zgodności z wymogami regulacyjnymi i audytu (8 liter):

5 poziomo: Dedykowany adres spoza czarnej listy (12 liter):

7 poziomo: Centralna konsola sterowania administratora (11 liter):

8 poziomo: Kontrola ruchu w ramach tunelowania dzielonego (split tunneling) (7 liter):

PIONOWO

1 pionowo: Dynamiczne powiększanie zespołu o kolejne stanowiska (12 liter):

2 pionowo: Tunel łączący sieci biur (10 liter):

4 pionowo: Najlepszy wybór ogólny dla firm (9 liter):

6 pionowo: Zdalny węzeł wejściowy do uwierzytelniania (5 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

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

Ć A D O D Ę G S I Ć R Q M E I

Ś Ć S Ż Ś Ę Q I V E N A A Q Ó

O Ś A M A R B T N P O T Y Q K

N O R T S Ć N E Ź B R Ę S Y X

L N J A R Ż Z T Z Ł D F I P N

A D R K M M T O O G L P Q A G

W O Ż Ą O V F S V B A Ź S N Ź

O G B G M Ż G I K O Y P Ń E X

L Z C M Ż Ź F T Z O E X U L L

A V Ó B Ń W T E M G R V Ć A Z

K S T A Ł Y A D R E S I P D V

S L R Ą Y Ż Z M S Q Y I Ó M D

A Ć R O U T I N G K Q W X I X

L J H T H F Ą E I L Ś S W N Q

Ź E H E S C A Ł P C Ż M L A W

LISTA SŁÓW

NORDLAYER SITETOSITE STAŁYADRESIP PANELADMINA SKALOWALNOŚĆ ZGODNOŚĆ ROUTING BRAMA

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. NORDLAYER**
- **B. SITETOSITE**
- **C. STAŁYADRESIP**
- **D. PANELADMINA**
- **E. SKALOWALNOŚĆ**
- **F. ZGODNOŚĆ**
- **G. ROUTING**
- **H. BRAMA**

DEFINICJE I POLA DOPASOWANIA

1. Kontrola ruchu w ramach tunelowania dzielonego (split tunneling).
2. Centralna konsola sterowania administratora.
3. Zdalny węzeł wejściowy do uwierzytelniania.
4. Dedykowany adres spoza czarnej listy.
5. Standard zgodności z wymogami regulacyjnymi i audytu.
6. Tunel łączący sieci biur.
7. Najlepszy wybór ogólny dla firm.
8. Dynamiczne powiększanie zespołu o kolejne stanowiska.

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. ALDONYERR
2. PTYASSIARED Ł
3. SKLAŚNAWĆO OL
4. GOITNRU
5. IOEIESTSTT
6. LAAMNIPADN E
7. ZĆNOŚGDO
8. ABAMR

Zadanie dodatkowe: Myśl szybko

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

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

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: BLOKOWANIE WSPÓŁDZIELONEGO PUBLICZNEGO IP

👷

Scenariusz: Zespół sprzedaży uzyskuje dostęp do firmowych baz danych za pomocą konsumenckiego VPN, ale zostaje zablokowany, ponieważ współdzielony wyjściowy adres IP trafił na czarną listę systemów antyfraudowych.

Pytanie do dyskusji: Zaproponuj konfigurację biznesowej infrastruktury VPN, która rozwiąże tę blokadę.

STUDIUM PRZYPADKU 2: POŁĄCZENIE BIUR FIRMY

👷

Scenariusz: Duża firma z biurami w Monachium i Bostonie musi bezpiecznie udostępniać lokalne serwery plików bez kierowania ruchu przez publiczne przestrzenie sieciowe.

Pytanie do dyskusji: Wybierz odpowiednią topologię VPN dla firmy.

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	7	24	20		27	24	28	25	27		4	11	24	20	18	12

18	20	30	20	4	33	7	25	18	7		25	12	7	4	12

9	12	24	17	20	30	7

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 biznesowy?

Bezpieczne połączenie sieciowe umożliwiające zdalnym pracownikom i biurom bezpieczny dostęp do prywatnych danych firmowych.

Q2: Czym różnią się VPN konsumenckie i biznesowe?

VPN-y konsumenckie ukrywają osobiste przeglądanie; firmowe VPN-y chronią systemy firmowe za pomocą centralnych konsol administracyjnych.

Q3: Czym jest VPN typu site-to-site?

Tunel, który łączy ze sobą całe fizyczne sieci biurowe przez internet.

Q4: Czym jest VPN dostępu zdalnego (Remote Access VPN)?

Tunel umożliwiający poszczególnym zdalnym pracownikom bezpieczne połączenie z siecią firmową.

Q5: Jaka jest korzyść z dedykowanego statycznego adresu IP?

Utrzymuje ruch firmowy oddzielnie od pul publicznych i unika wspólnego umieszczania adresów IP na czarnych listach.

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

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

Q6: Który dostawca jest najlepszy dla małych firm?

Private Internet Access (PIA), znany z przystępnej ceny dla małych zespołów i prostoty konfiguracji.

Q7: Który biznesowy VPN zajmuje 1. miejsce w ogólnym rankingu?

NordLayer, oceniony przez VPN.com na 92/100 za funkcje i narzędzia administracyjne.

Q8: Czym jest skalowalność zespołu w VPN-ach?

Możliwość dynamicznego dodawania stanowisk użytkowników, licencji i bram w miarę rozwoju firmy.

Q9: Dlaczego centralne zarządzanie jest kluczowe?

Pozwala administratorom egzekwować polityki bezpieczeństwa i cofać dostęp pracowników w jednym panelu.

Q10: Czym jest SASE?

Secure Access Service Edge, który łączy routing WAN z usługami bezpieczeństwa dostarczanymi z chmury.

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 tunelowanie dzielone zabezpiecza zespoły?

Utrzymuje prywatny ruch SaaS wewnątrz bezpiecznego tunelu, a publiczny dostęp do sieci kieruje lokalnie.

Q2: Co Proton VPN oferuje firmom?

Infrastruktura serwerów dedykowanych, oceniona na 88/100 przez VPN.com (z siedzibą w Szwajcarii).

Q3: Jakie normy zgodności wymagają użycia VPN?

PCI DSS wymaga silnego szyfrowania w sieciach publicznych; HIPAA i RODO (GDPR) oczekują go jako zabezpieczenia.

Q4: Czy biznesowe VPN-y można uruchamiać na routerach?

Tak, skonfigurowanie tuneli VPN na routerach automatycznie chroni wszystkie urządzenia w biurze.

Q5: Czym jest uwierzytelnianie wieloskładnikowe?

Wymaganie wielu poświadczeń (takich jak karty inteligentne lub kody SMS) do uwierzytelniania logowań.

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: Dlaczego współdzielone adresy IP trafiają na czarne listy?

Ponieważ korzystają z nich tysiące użytkowników, z których niektórzy mogą dopuszczać się złośliwych działań.

Q7: Jak brama uwierzytelnia użytkowników?

Przez weryfikację certyfikatów klienta, haseł i kodów wieloskładnikowych względem aktywnych katalogów.

Q8: Co Surfshark oferuje zespołom?

Najlepszy wybór VPN.com dla pakietów zabezpieczeń, oceniony na 84/100, z serwerami wyłącznie RAM.

Q9: Jak przeprowadza się audyt połączeń biznesowego VPN?

Przez sprawdzanie dzienników połączeń, metryk użycia danych i historii logowania w konsoli administracyjnej.

Q10: Czym jest kontrola dostępu Zero Trust?

Paradygmat, w którym zakłada się, że wszystkie urządzenia są niezaufane i wymagają weryfikacji w każdej sesji.

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 biznesowy szyfruje ruch i chroni systemy firmy przed podsłuchiwaniem w sieciach publicznych.

2. WGLĄD W VPN
VPN typu site-to-site bezpiecznie łączą ze sobą całe sieci oddziałów bez ujawniania lokalnych hostów.

3. WGLĄD W VPN
VPN-y konsumenckie maskują osobiste przeglądanie, natomiast firmowe VPN-y chronią bramy do zasobów przedsiębiorstwa.

4. WGLĄD W VPN
VPN.com ocenia NordLayer na 92/100, jako swój najlepszy ogólny VPN dla firm.

5. WGLĄD W VPN
VPN.com ocenia Proton VPN na 88/100 i wskazuje go jako najlepszy pod względem dedykowanej infrastruktury.

6. WGLĄD W VPN
VPN.com ocenia Private Internet Access na 76/100 i uznaje go za najlepszy dla zespołów małych firm.

7. WGLĄD W VPN
Centralne panele administracyjne umożliwiają specjalistom ds. bezpieczeństwa zarządzanie uprawnieniami użytkowników i regułami dostępu.

8. WGLĄD W VPN
Dedykowane statyczne adresy IP chronią zespoły przed blokowaniem przez systemy wykrywania nadużyć, które współdzielą adresy IP.

9. WGLĄD W VPN
RODO (GDPR) wymienia szyfrowanie jako odpowiedni środek ochrony danych osobowych.

10. WGLĄD W VPN
Architektury Zero Trust weryfikują wszystkie zdalne punkty końcowe niezależnie od lokalizacji czy poświadczeń.

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/

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 **Topologia tunelu** SITE-TO-SITE — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

VPN typu site-to-site bezpiecznie łączą ze sobą całe zdalne oddziały firmy. Źródło: NIST Zero Trust.

2 **Pytanie 2** — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

VPN.com ocenia NordLayer na 92/100 i uznaje go za najlepszy ogółem dla zespołów biznesowych.

3 **Biała lista IP** DEDYKOWANY ADRES IP — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Dedykowane statyczne adresy IP chronią zespoły przed utratą dostępu z powodu wspólnych czarnych list adresów IP. Źródło: NIST Remote Access.

4 **Pytanie 4** — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

VPN.com ocenia Proton VPN na 88/100 i uznaje go za najlepszy pod względem dedykowanej infrastruktury.

5 **Konsola centralna** KONTROLA ADMINISTRACYJNA — **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Scentralizowane panele umożliwiają specjalistom ds. bezpieczeństwa zarządzanie uprawnieniami użytkowników i stanowiskami. Źródło: NIST Remote Access.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Połączenia zdalne** DOSTĘP ZDALNY — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

VPN dostępu zdalnego pozwalają poszczególnym pracownikom zdalnym łączyć się z prywatnymi serwerami. Źródło: NIST Remote Access.

7 **Tunele dla przedsiębiorstw** LIMITY DLA KONSUMENTÓW — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

VPN-y konsumenckie nie mają scentralizowanych kontroli administracyjnych i nie nadają się do audytów organizacji. Źródło: CISA Infrastructure.

8 **Izolacja bramy** DEDYKOWANY TUNEL — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Dedykowane adresy IP oddzielają ruch firmowy od szumu publicznego, aby zabezpieczyć bazy danych. Źródło: NIST Zero Trust.

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

UWAGA DLA NAUCZYCIELA

VPN.com umieszcza PIA (76/100) jako najlepszy dla małych firm, a nie dla dużych przedsiębiorstw.

10 **Bezpieczeństwo łączy się** STANDARD SASE — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

SASE łączy firmowy routing WAN z bezpieczeństwem zero trust dostarczanym z chmury. Źródło: Cloudflare Zero Trust.

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

B 1. NORDLAYER	G 2. SITE-TO-SITE	F 3. STAŁY ADRES IP	H 4. PANEL
A 5. SKALOWALNOŚĆ	D 6. ZGODNOŚĆ	C 7. ROUTING	E 8. BRAMA

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 NORDLAYER	2 SITE-TO-SITE	3 STAŁY ADRES IP	4 PANEL ADMINA
5 SKALOWALNOŚĆ	6 ZGODNOŚĆ		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 G – ROUTING	2 D – PANELADMINA	3 H – BRAMA	4 C – STAŁYADRESIP
5 F – ZGODNOŚĆ	6 B – SITETOSITE	7 A – NORDLAYER	8 E – SKALOWALNOŚĆ

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia NORDLAYER, SITE-TO-SITE i STAŁY ADRES IP oraz podać przykład każdego z nich.

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

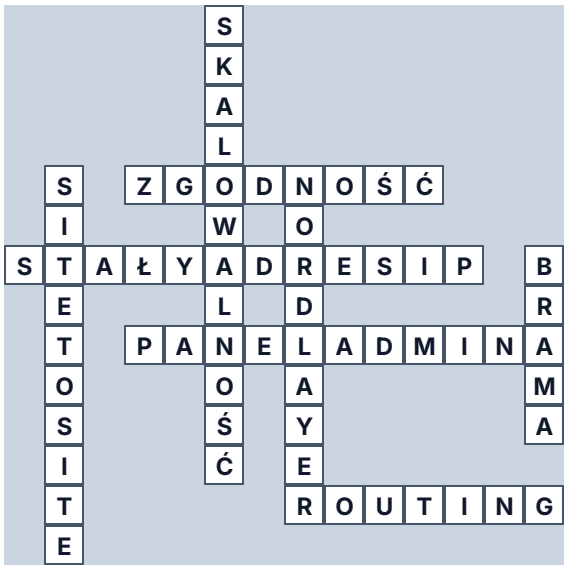
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

3 poziomo: ZGODNOŚĆ Standard zgodności z wymogami regulacyjnymi i audytu (8 liter)

5 poziomo: STAŁYADRESIP Dedykowany adres spoza czarnej listy (12 liter)

7 poziomo: PANELADMINA Centralna konsola sterowania administratora (11 liter)

8 poziomo: ROUTING Kontrola ruchu w ramach tunelowania dzielonego (split tunneling) (7 liter)

PIONOWO

1 pionowo: SKALOWALNOŚĆ Dynamiczne powiększanie zespołu o kolejne stanowiska (12 liter)

2 pionowo: SITETOSITE Tunel łączący sieci biur (10 liter)

4 pionowo: NORDLAYER Najlepszy wybór ogólny dla firm (9 liter)

6 pionowo: BRAMA Zdalny węzeł wejściowy do uwierzytelniania (5 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. ALDONYERR — **NORDLAYER**
2. PTYASSIAREDŁ — **STAŁYADRESIP**
3. SKLAŚNAWĆOOL — **SKALOWALNOŚĆ**
4. GOITNRU — **ROUTING**
5. IOEIESTSTT — **SITETOSITE**
6. LAAMNIPADNE — **PANELADMINA**
7. ZĆNOŚGDO — **ZGODNOŚĆ**
8. ABAMR — **BRAMA**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"ZERO TRUST CHRONI NOWOCZESNE SIECI FIRMOWE"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Blokowanie współdzielonego publicznego IP

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Zespół sprzedaży korzysta z firmowych baz danych przez konsumencki VPN, ale zostaje zablokowany, ponieważ współdzielony wyjściowy adres IP trafił na czarną listę systemów antyfraudowych.
- Zalecana strategia i rozwiązanie: Wdróż dedykowane serwery biznesowe w połączeniu ze statycznym adresem IP, aby oddzielić ruch firmowy od publicznych pul.

B Studium przypadku 2: Połączenie biur firmy

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firma z biurami w Monachium i Bostonie musi bezpiecznie udostępniać lokalne serwery plików bez przesyłania ruchu przez publiczne przestrzenie internetu.
- Zalecana strategia i rozwiązanie: Skonfiguruj tunel VPN typu site-to-site, aby bezpiecznie połączyć dwie lokalne sieci biurowe przez internet.