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

VPN dla przedsiębiorstw

Wdrażanie dostępu do sieci w modelu Zero Trust, dedykowanych węzłów bramy i scentralizowanych firmowych narzędzi administracyjnych.

PRZEGLĄD NAUKI: SIECI VPN DLA PRZEDSIĘBIORSTW

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 firmowe sieci VPN. Poznasz architektury Zero Trust, dedykowane bramy ze statycznymi adresami IP, konsole administratora, provisioning i tunele IPsec typu site-to-site.

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/enterprise/

Twoja ścieżka nauki: firmowa sieć VPN

- Wdróż ramy Zero Trust Network Access (ZTNA).
- Skonfiguruj adresy IP bram dedykowanych serwerów dla filtrów białych list.
- Zarządzaj scentralizowanymi firmowymi panelami administracyjnymi i listami miejsc użytkowników.
- Przeprowadź audyt dzienników dostępu do sieci i historii połączeń użytkowników.
- Skonfiguruj reguły jednokrotnego logowania (SSO) i uwierzytelniania wieloskładnikowego.
- Skonfiguruj tunele IPsec typu site-to-site między oddziałami.

INSTRUKCJE: SIECI VPN DLA PRZEDSIĘBIORSTW

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 Zero Trust i IPsec typu site-to-site. Zakończ zadaniem dodatkowym Myśl szybko.

ARCHITEKTURY ZERO TRUST I DEDYKOWANE BRAMY (WPROWADZENIE)

VPN-y dla przedsiębiorstw zabezpieczają zasoby firmy poprzez przejście na ramy Zero Trust Network Access (ZTNA) i tworzenie białych list dedykowanych statycznych bram IP. Menedżerowie IT korzystają ze scentralizowanych konsol administracyjnych, aby orkiestrować tunele IPsec typu site-to-site i łącza jednokrotnego logowania (SSO).

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. 1. Jaki model bezpieczeństwa zastępuje starsze korporacyjne VPN-y?
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Pojedyncza brama

2. 2. Jaka funkcja jest wymagana, aby ograniczyć dostęp do bazy danych do serwerów firmy?
   - A) Dedykowany IP
   - B) Routing dynamiczny
   - C) Tunel podzielony
   - D) Proxy DNS

3. 3. Który protokół jest standardem dla korporacyjnych tuneli typu site-to-site?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. 4. Które centralne narzędzie pozwala administratorom zarządzać miejscami pracowników?
   - A) Konsola administratora
   - B) Klucz rejestru
   - C) Oprogramowanie układowe routera
   - D) Dziennik systemowy

5. 5. Jaki standard uwierzytelniania pozwala logować się przez Okta lub Microsoft Entra ID?
   - A) Jednokrotne logowanie (SSO)
   - B) Współdzielony sekret
   - C) Uwierzytelnianie EPP
   - D) Klucz WEP

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Zero Trust Network Access przyznaje dostęp do sieci dopiero po zweryfikowaniu ciągłego zaufania do urządzenia.

Prawda Fałsz

7 Pytanie 7

7. Bramy z dedykowanym IP kierują ruch pracowników razem z przypadkowymi publicznymi użytkownikami indywidualnymi.

Prawda Fałsz

8 Pytanie 8

8. Scentralizowane konsole administracyjne umożliwiają menedżerom IT natychmiastowe cofnięcie dostępu poszczególnym pracownikom.

Prawda Fałsz

9 Pytanie 9

9. IPsec to lekki protokół, który nie obsługuje tuneli sieciowych między lokalizacjami (site-to-site).

Prawda Fałsz

10 Pytanie 10

10. Jednokrotne logowanie (SSO) umożliwia bezpieczne uwierzytelnianie pracowników przy użyciu firmowych dostawców tożsamości.

Prawda Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Nowoczesne architektury bezpieczeństwa zastępują starsze tunele dostępem w modelu _____ .

2. Aby ograniczyć dostęp do bazy danych, firmy konfigurują adres bramy w postaci: _____ .

3. Oddziały łączy się bezpiecznie za pomocą tuneli typu site-to-site opartych na _____ .

4. Administratorzy IT przydzielają licencje użytkowników pracowników w centralnym narzędziu, którym jest _____ .

5. Integracja z Okta pozwala pracownikom uwierzytelniać się za pomocą firmowego _____ .

6. Aby chronić logowania, portale korporacyjne wymuszają uwierzytelnianie, które jest _____ .

BANK SŁÓW

BRAMA SIECIOWA DEDYKOWANY IP IPSEC KONSOLA ADMINA PRZYDZIELANIE SINGLE SIGN-ON WIELOSKŁADNIKOWE ZERO TRUST

Wpisz tutaj swoje odpowiedzi:

1. 2.

3. 4.

5. 6.

Punkt kontrolny 4: Dopasowywanie kluczowych pojęć

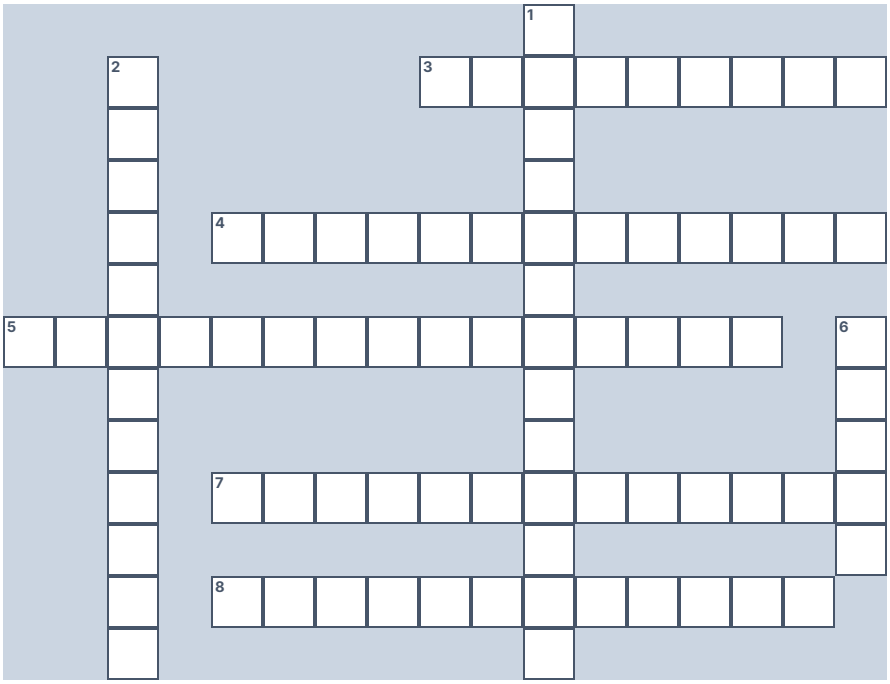
DOPASOWYWANIE DEFINICJI

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

☐	1. ZERO TRUST	A	Przydzielanie licencji na dostęp pracowników do VPN.
☐	2. DEDYKOWANY ADRES IP	B	Połączenie tożsamości Okta i Entra ID.
☐	3. IPSEC	C	Zabezpieczenie logowania wymagające dodatkowych tokenów.
☐	4. KONSOLA ADMINISTRATORA	D	Adres bramy na statycznej białej liście.
☐	5. JEDNOKROTNE LOGOWANIE	E	Standard tunelu site-to-site.
☐	6. WIELOSKŁADNIKOWE	F	Węzeł routingu wejścia do sieci.
☐	7. BRAMA	G	Portal centralny do zarządzania stanowiskami przez menedżera IT.
☐	8. PRZYDZIAŁ ZASOBÓW	H	Ramy ciągłej weryfikacji zaufania.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

3. Ramy ciągłej weryfikacji zaufania (9)

4. Centralny portal administratora IT do zarządzania stanowiskami (13)

5. Zabezpieczenie logowania wymagające dodatkowych tokenów (15)

7. Przydzielanie pracownikom licencji dostępu do VPN (13)

8. Statyczny adres bramy na białej liście (12)

PIONOWO

1. Węzeł routingu będący wejściem do sieci (13)

2. Powiązanie tożsamości Okta i Entra ID (12)

6. Standard tuneli typu site-to-site (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: Ramy ciągłej weryfikacji zaufania (9 liter):

4 poziomo: Centralny portal administratora IT do zarządzania stanowiskami (13 liter):

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

7 poziomo: Przydzielanie pracownikom licencji dostępu do VPN (13 liter):

8 poziomo: Statyczny adres bramy na białej liście (12 liter):

PIONOWO

1 pionowo: Węzeł routingu będący wejściem do sieci (13 liter):

2 pionowo: Powiązanie tożsamości Okta i Entra ID (12 liter):

6 pionowo: Standard tuneli typu site-to-site (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.

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

LISTA SŁÓW

ZEROTRUST DEDYKOWANYIP IPSEC KONSOLAADMINA SINGLESIGNON
WIELOCZYNNIKOWE BRAMASIECIOWA PRZYDZIELANIE

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. ZEROTRUST**
- **B. DEDYKOWANYIP**
- **C. IPSEC**
- **D. KONSOLAADMINA**
- **E. SINGLESIGNON**
- **F. WIELOCZYNNIKOWE**
- **G. BRAMASIECIOWA**
- **H. PRZYDZIELANIE**

DEFINICJE I POLA DOPASOWANIA

1. Statyczny adres bramy na białej liście.
2. Węzeł routingu będący wejściem do sieci.
3. Przydzielanie pracownikom licencji dostępu do VPN.
4. Zabezpieczenie logowania wymagające dodatkowych tokenów.
5. Standard tuneli typu site-to-site.
6. Ramy ciągłej weryfikacji zaufania.
7. Powiązanie tożsamości Okta i Entra ID.
8. Centralny portal administratora IT do zarządzania stanowiskami.

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. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. SWCAEAAIOIBRM
5. EYAWPDKNODIY
6. OMALINNDKOAAS
7. NIZNWKIEECOWLYO
8. LZDZNEEPIRIAY

Zadanie dodatkowe: Myśl szybko

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

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

Punkt kontrolny 8: Studia przypadków dotyczących VPN i sieci

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

STUDIUM PRZYPADKU 1: MIGRACJA DO ZERO TRUST

👷

Scenariusz: Przedsiębiorstwo chce zabezpieczyć swoje lokalne serwery, stale weryfikując certyfikaty zgodności urządzeń, stan zapory sieciowej i lokalizację użytkownika, zamiast ufać każdemu wewnątrz sieci.

Pytanie do dyskusji: Jakie ramy powinien wdrożyć dyrektor ds. bezpieczeństwa IT, aby to osiągnąć?

STUDIUM PRZYPADKU 2: OGRANICZENIE BRAMY

👷

Scenariusz: Firma hostuje prywatne bazy danych finansowych w chmurze. Chce zablokować cały dostęp z publicznego internetu do paneli administracyjnych, zezwalając na logowanie tylko z zweryfikowanych punktów końcowych firmy.

Pytanie do dyskusji: Jaką konfigurację sieci powinien ustawić administrator baz danych na zaporze sieciowej w chmurze?

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		25	22	24	1	30	6	33	1
14	1	35	6	7		16	2	4	33	2	4	7		25	12	8		
					28	24	33	2	6	33	7	18	12	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 dla przedsiębiorstw?

Bezpieczny tunel sieciowy zaprojektowany dla firm, umożliwiający pracownikom zdalnym dostęp do sieci firmowych ze scentralizowanym zarządzaniem.

Q2: Czym Zero Trust różni się od tradycyjnych VPN?

Tradycyjne VPN ufają każdemu wewnątrz tunelu, podczas gdy Zero Trust stale weryfikuje każde urządzenie i połączenie użytkownika.

Q3: Czym jest dedykowany adres IP w biznesowych VPN-ach?

Stały adres IP zarezerwowany wyłącznie dla Twojej firmy, który pozwala dodać go do białej listy w celu bezpiecznego dostępu do bazy danych w chmurze.

Q4: Dlaczego SSO jest ważne w biznesowych VPN-ach?

Jednokrotne logowanie (SSO) pozwala pracownikom używać firmowych danych logowania (np. Okta lub Microsoft Entra ID) do bezpiecznego logowania.

Q5: Czym jest VPN typu site-to-site?

Tunel łączący dwa fizyczne biura (np. oddział i centralę) przez publiczny internet przy użyciu IPsec.

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

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

Q6: Jaką funkcję pełni konsola administratora?

Panel dla administratorów IT do dodawania lub usuwania miejsc pracowników, przypisywania bram i monitorowania aktywnych połączeń.

Q7: Jak MFA zabezpiecza biznesowe VPN-y?

Przez wymaganie dodatkowego kodu (np. tokenu z aplikacji uwierzytelniającej), aby zapobiec nieautoryzowanemu wejściu przy użyciu przejętych haseł.

Q8: Czy mogę audytować historię połączeń pracowników?

Tak, firmowe sieci VPN rejestrują znaczniki czasu połączeń, czas trwania i przydzielone adresy IP na potrzeby audytów zgodności.

Q9: Czym jest ZTNA?

Zero Trust Network Access, model bezpieczeństwa, który przyznaje dostęp tylko do określonych aplikacji, a nie do całej sieci.

Q10: Jaka jest rola węzłów bramowych?

Służą jako bezpieczne punkty wejścia dla ruchu zdalnego, kierując dane bezpośrednio do prywatnych serwerów firmowych.

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 IPsec chroni komunikację firmową między lokalizacjami (site-to-site)?

IPsec szyfruje ruch w warstwie sieciowej, używając Encapsulating Security Payload (ESP), aby zapewnić poufność i integralność danych.

Q2: Dlaczego tradycyjne zabezpieczenia oparte na obwodzie sieci zawodzą w przypadku pracowników zdalnych?

Ponieważ pracownicy uzyskują dostęp do danych z wielu lokalizacji i urządzeń, przez co pojedynczy obwód zapory sieciowej staje się przestarzały.

Q3: Jak menedżerowie IT wdrażają zautomatyzowane udostępnianie zasobów (provisioning)?

Przez mapowanie protokołów SCIM między dostawcami tożsamości (Okta) a konsolą administracyjną VPN w celu synchronizacji katalogów użytkowników.

Q4: Jaka jest korzyść z tunelowania dzielonego w środowiskach korporacyjnych?

Kieruje lokalny ruch SaaS (np. Microsoft 365) poza tunel VPN, oszczędzając przepustowość firmowej bramy dla prywatnych baz danych.

Q5: Jak kontrole stanu urządzenia weryfikują bezpieczeństwo punktów końcowych?

Klient VPN skanuje urządzenie przed połączeniem, aby sprawdzić, czy zapora sieciowa jest aktywna, antywirus działa, a poprawki systemu operacyjnego są aktualne.

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 rolę odgrywa NAT traversal w konfiguracjach VPN dla firm?

NAT-T enkapsuluje pakiety IPsec w UDP, aby mogły przechodzić przez domowe routery i zapory sieciowe bez zrywania połączeń.

Q7: Jak firmy zapobiegają dławieniu przepustowości bramy?

Przez wdrożenie wielu regionalnych węzłów bramowych i równoważenie przychodzącego ruchu użytkowników między nimi za pomocą load balancerów.

Q8: Dlaczego statyczne listy dozwolonych adresów IP są preferowane nad dynamicznymi?

Statyczne białe listy zapobiegają próbom nawiązania uzgadniania połączenia przez nieautoryzowane zewnętrzne adresy IP, co drastycznie zmniejsza powierzchnię ataku.

Q9: Jaką rolę odgrywa uwierzytelnianie oparte na certyfikatach w korporacyjnych VPN-ach?

Waliduje unikalne certyfikaty cyfrowe zainstalowane na urządzeniach zarządzanych przez firmę, blokując niezarządzane komputery osobiste.

Q10: Jak ZTNA zmniejsza ryzyko ruchu bocznego?

Przez izolowanie sesji użytkowników do określonych autoryzowanych zasobów, co uniemożliwia hakerom przemieszczanie się po sieci, jeśli jeden węzeł zostanie naruszony.

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

Architektury Zero Trust stale weryfikują stan bezpieczeństwa każdego urządzenia próbującego nawiązać połączenie z siecią.

2. WGLĄD W VPN

Bramy z dedykowanym IP pozwalają firmom zabezpieczyć bazy danych w chmurze dzięki białym listom statycznych adresów.

3. WGLĄD W VPN

IPsec to branżowy standardowy protokół do konfigurowania bezpiecznych tuneli sieciowych site-to-site między biurami.

4. WGLĄD W VPN

Konsole administracyjne pozwalają działom IT przydzielać, zarządzać i audytować miejsca dostępu pracowników do VPN.

5. WGLĄD W VPN

Jednokrotne logowanie (SSO) integruje dostęp do VPN z firmowymi dostawcami tożsamości, takimi jak Okta i Entra ID.

6. WGLĄD W VPN

Uwierzytelnianie wieloskładnikowe blokuje nieautoryzowane próby połączenia pochodzące z użyciem skradzionych haseł.

7. WGLĄD W VPN

Tunelowanie dzielone optymalizuje przepustowość firmową przez wyłączenie publicznego ruchu SaaS z zaszyfrowanego tunelu.

8. WGLĄD W VPN

Kontrole stanu urządzenia sprawdzają lokalne ustawienia bezpieczeństwa przed udzieleniem dostępu do serwerów firmowych.

9. WGLĄD W VPN

Synchronizacja katalogów SCIM automatyzuje kontrolę dostępu przy przyjmowaniu i odchodzeniu pracowników.

10. WGLĄD W VPN

Zero Trust Network Access ogranicza dostęp użytkowników do określonych autoryzowanych aplikacji, zapobiegając ruchowi bocznemu w sieci.

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 **Zero Trust** MODEL ZTNA **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Modele Zero Trust stale weryfikują zgodność urządzenia przed wejściem do sieci. Źródło: NIST Zero Trust.

2 **Dedykowany adres IP** STAŁY ADRES IP **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Dedykowane adresy IP pozwalają tworzyć białe listy bram, aby blokować ruch publiczny. Źródło: Dedicated IP Guide.

3 **Standard IPsec** TUNEL IPSEC **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

IPsec to standardowy protokół używany w tunelach site-to-site między oddziałami. Źródło: IPsec Tunneling.

4 **Alokacja IT** KONSOLA ADMINISTRATORA **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Scentralizowane panele administracyjne umożliwiają menedżerom IT przydzielanie licencji na stanowiska. Źródło: CISA Guidelines.

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

UWAGA DLA NAUCZYCIELA

Jaki standard uwierzytelniania pozwala logować się przez Okta lub Microsoft Entra ID? → Jednokrotne logowanie (SSO)

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Zero Trust** KONTROLE ZTNA **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Modele Zero Trust stale weryfikują zgodność urządzenia przed wejściem do sieci. Źródło: NIST Zero Trust.

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

UWAGA DLA NAUCZYCIELA

Dedykowane adresy IP są zarezerwowane dla jednej firmy, więc jej ruch nie miesza się z ruchem innych użytkowników.

8 **Alokacja IT** STANOWISKO ADMINISTRATORA IT **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Scentralizowane panele administracyjne umożliwiają menedżerom IT przydzielanie licencji na stanowiska. Źródło: CISA Guidelines.

9 **Standard IPsec** SITE-TO-SITE **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

IPsec to standardowy protokół używany w tunelach site-to-site między oddziałami. Źródło: IPsec Tunneling.

10 **Łącze Okta SSO** LOGOWANIE SSO **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Jednokrotne logowanie (SSO) integruje logowanie do VPN z katalogami firmowymi, takimi jak Okta. Źródło: Okta SSO.

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. ZERO TRUST	D 2. DEDYKOWANY ADRES IP	E 3. IPSEC	G 4. KONSOLA ADMINISTRATORA
B 5. JEDNOKROTNE LOGOWANIE	C 6. WIELOSKŁADNIKOWE	F 7. BRAMA	A 8. PRZYDZIAŁ ZASOBÓW

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 ZERO TRUST	2 DEDYKOWANY IP	3 IPSEC	4 KONSOLA ADMINA
5 SINGLE SIGN-ON	6 WIELOSKŁADNIKOWE		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 B – DEDYKOWANYIP	2 G – BRAMASIECIOWA	3 H – PRZYDZIELANIE	4 F – WIELOCZYNNIKOWE
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – KONSOLAADMINA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia ZERO TRUST, DEDYKOWANY ADRES IP i IPSEC oraz podać przykład każdego z nich.

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

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

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI

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

PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

3 poziomo: ZEROTRUST Ramy ciągłej weryfikacji zaufania (9 liter)

4 poziomo: KONSOLAADMINA Centralny portal administratora IT do zarządzania stanowiskami (13 liter)

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

7 poziomo: PRZYDZIELANIE Przydzielanie pracownikom licencji dostępu do VPN (13 liter)

8 poziomo: DEDYKOWANYIP Statyczny adres bramy na białej liście (12 liter)

PIONOWO

1 pionowo: BRAMASIECIOWA Węzeł routingu będący wejściem do sieci (13 liter)

2 pionowo: SINGLESIGNON Powiązanie tożsamości Okta i Entra ID (12 liter)

6 pionowo: IPSEC Standard tuneli typu site-to-site (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. RTOEZUSTR — **ZEROTRUST**
2. ICESP — **IPSEC**
3. SIISOGNENLNG — **SINGLESIGNON**
4. SWCAEAAIOIBRM — **BRAMASIECIOWA**
5. EYAWPDKNODIY — **DEDYKOWANYIP**
6. OMALINNDKOAAS — **KONSOLAADMINA**
7. NIZNWKIEECOWLYO — **WIELOCZYNNIKOWE**
8. LZDZNEEPIRIAY — **PRZYDZIELANIE**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"ZERO TRUST SPRAWDZA KAŻDE ŁĄCZĄCE SIĘ URZĄDZENIE"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Migracja do Zero Trust

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firma chce zabezpieczyć swoje lokalne serwery, stale weryfikując certyfikaty zgodności urządzeń, stan zapory sieciowej i lokalizację użytkownika, zamiast ufać każdemu wewnątrz sieci.
- Zalecana strategia i rozwiązanie: Dyrektor powinien przejść na model Zero Trust Network Access (ZTNA), który wymusza ciągłe kontrole bezpieczeństwa oparte na kontekście.

B Studium przypadku 2: Ograniczenie bramy

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firma przechowuje prywatne bazy danych finansowych w chmurze. Chce zablokować cały publiczny dostęp z internetu do paneli administracyjnych, zezwalając na logowanie tylko ze zweryfikowanych firmowych punktów końcowych.
- Zalecana strategia i rozwiązanie: Administrator powinien skonfigurować bramę Dedicated IP w firmowym VPN i dodać ten statyczny adres do białej listy na zaporze sieciowej bazy danych w chmurze.