Naam: _____ Datum: _____ Score: _____

Zakelijke VPN

Zero Trust-netwerktoegang, speciale gatewaynodes en gecentraliseerd bedrijfsbeheer voor beheerders implementeren.

LEEROVERZICHT VPN-NETWERKEN VOOR BEDRIJVEN

LEERLING
STUDENTENSTATUS
Network Defender-traject

VEILIG
VERBINDINGSSTATUS
Gegevenspakketten afschermen

ACTIEF
LEKBESCHERMING
Bescherming tegen DNS- en IPv6-lekken

Welkom! Dit activiteitenpakket leidt je door VPN-netwerken voor ondernemingen. Je verkent Zero Trust-architecturen, dedicated gateways met statisch IP, beheerconsoles, provisioning en site-to-site IPsec-tunnels.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers VPN- en netwerkbeveiligingsconfiguraties.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-gids met de beste VPN's

URL: https://www.vpn.com/nl/vpn/beste-vpn-bedrijven/enterprise/

Jouw leertraject: VPN-netwerk voor ondernemingen

- Voer Zero Trust Network Access-kaders (ZTNA) in.
- Configureer IP-adressen van dedicated servergateways voor whitelistfilters.
- Gecentraliseerde beheerpanelen van bedrijven en lijsten met gebruikersplaatsen beheren.
- Audit de toegangslogs van het netwerk en de verbindingsgeschiedenis van gebruikers.
- Configureer Single Sign-On (SSO) en regels voor meervoudige authenticatie.
- Site-to-site-IPsec-tunnels tussen vestigingen instellen.

INSTRUCTIES VPN-NETWERKEN VOOR BEDRIJVEN

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op Zero Trust en site-to-site-IPsec. Sluit af met de bonusopdracht Snel denken.

ZERO TRUST-ARCHITECTUREN EN DEDICATED GATEWAYS (INLEIDING)

Zakelijke VPN's beveiligen bedrijfsmiddelen door over te stappen op Zero Trust Network Access (ZTNA)-frameworks en dedicated statische IP-gateways op een whitelist te zetten. IT-managers gebruiken gecentraliseerde beheerconsoles om site-to-site-IPsec-tunnels en single sign-on (SSO)-koppelingen te orkestreren.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. Welk beveiligingsmodel vervangt de verouderde VPN's voor ondernemingen?

- A) Zero Trust
- B) Multi-hop
- C) Peer-to-peer
- D) Eén gateway

2. Welke functie is vereist om databasetoegang te beperken tot bedrijfsservers?

- A) Dedicated IP
- B) Dynamische routering
- C) Gesplitste tunnel
- D) DNS-proxy

3. Welk protocol is de standaard voor zakelijke site-to-site-tunnels?

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4. Welk centraal hulpmiddel stelt beheerders in staat om medewerkerslicenties te beheren?

- A) Beheerconsole
- B) Registersleutel
- C) Routerfirmware
- D) Systeemlog

5. Welke authenticatiestandaard maakt inloggen via Okta of Microsoft Entra ID mogelijk?

- A) Single Sign-On
- B) Gedeeld geheim
- C) EPP-authenticatie
- D) WEP-sleutel

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Zero Trust Network Access verleent alleen netwerktoegang nadat het apparaatvertrouwen continu is geverifieerd.

○ Waar ○ Onwaar

7 Vraag 7

7. Dedicated IP-gateways routeren werknemersverkeer samen met willekeurige openbare consumentengebruikers.

○ Waar ○ Onwaar

8 Vraag 8

8. Via centrale beheerconsoles kunnen IT-beheerders de seats van individuele medewerkers direct intrekken.

○ Waar ○ Onwaar

9 Vraag 9

9. IPsec is een lichtgewicht protocol dat geen site-to-site-netwerktunnels ondersteunt.

○ Waar ○ Onwaar

10 Vraag 10

10. Single Sign-On maakt veilige authenticatie van medewerkers mogelijk via bedrijfsidentiteitsproviders.

○ Waar ○ Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Moderne beveiligingsarchitecturen vervangen verouderde tunnels door _____ -toegang.

2. Om de toegang tot databases te beperken, stellen bedrijven een _____ als gatewayadres in.

3. Kantoren op andere locaties worden veilig verbonden met site-to-site- _____ -tunnels.

4. In de centrale _____ wijzen IT-beheerders gebruikerslicenties toe aan medewerkers.

5. Dankzij Okta-integratie kunnen medewerkers zich authenticeren via zakelijke _____ .

6. Om logins te beschermen eisen bedrijfsportalen _____ -authenticatie.

WOORDENBANK

ADMIN CONSOLE GATEWAY IPSEC MULTIFACTOR SINGLE SIGN-ON TOEWIJZING VAST IP-ADRES ZERO TRUST

Schrijf hier je antwoorden:

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

Controlepunt 4: Kernbegrippen koppelen

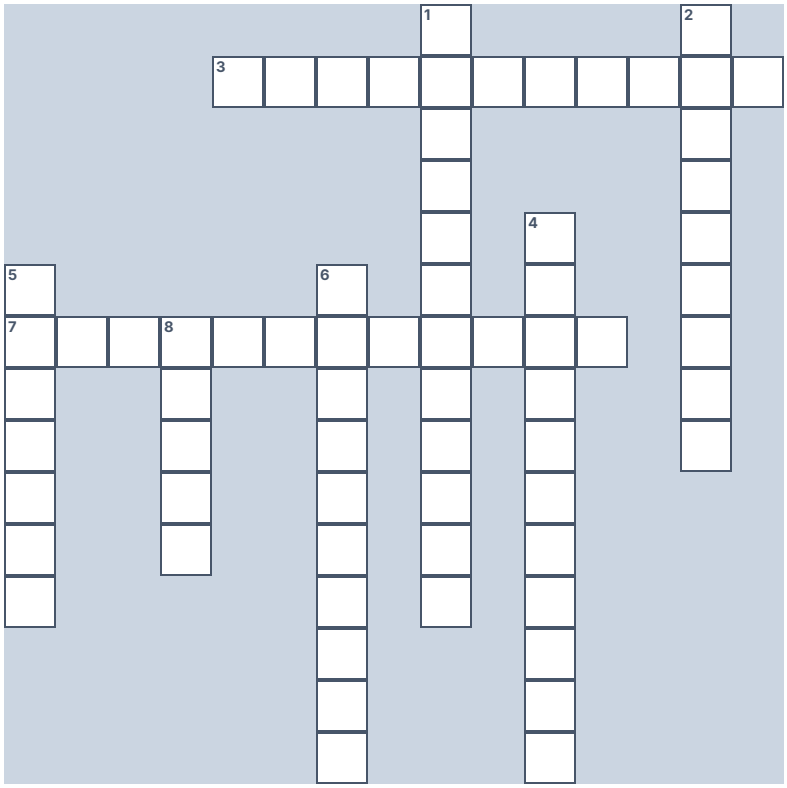
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. ZERO TRUST	A	Licenties voor VPN-toegang van medewerkers toewijzen.
☐	2. DEDICATED IP	B	Identiteitskoppeling van Okta en Entra ID.
☐	3. IPSEC	C	Aanmeldbeveiliging waarvoor extra tokens nodig zijn.
☐	4. BEHEERCONSOLE	D	Statisch adres van de gateway op de whitelist.
☐	5. SINGLE SIGN-ON	E	Standaard voor site-to-site-tunnels.
☐	6. MULTIFACTOR	F	Routeringsnode bij de netwerkingang.
☐	7. GATEWAY	G	Centraal portaal voor de seats van de IT-beheerder.
☐	8. PROVISIONING	H	Raamwerk voor continue verificatie van vertrouwen.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

3. Statisch gatewayadres op de whitelist (11)

7. Centraal portaal voor IT-beheerders (12)

VERTICAAL

1. Identiteitskoppeling met Okta en Entra ID (12)

2. Kader voor continue verificatie van vertrouwen (9)

4. Inlogbeveiliging die extra tokens vereist (11)

5. Routeringsknooppunt aan de toegang tot het netwerk (7)

6. VPN-toegangslicenties voor medewerkers toekennen (10)

8. Standaard voor site-to-site-tunnels (5)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

3 horizontaal: Statisch gatewayadres op de whitelist (11 letters):

7 horizontaal: Centraal portaal voor IT-beheerders (12 letters):

VERTICAAL

1 verticaal: Identiteitskoppeling met Okta en Entra ID (12 letters):

2 verticaal: Kader voor continue verificatie van vertrouwen (9 letters):

4 verticaal: Inlogbeveiliging die extra tokens vereist (11 letters):

5 verticaal: Routeringsknooppunt aan de toegang tot het netwerk (7 letters):

6 verticaal: VPN-toegangslicenties voor medewerkers toekennen (10 letters):

8 verticaal: Standaard voor site-to-site-tunnels (5 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

N I Q T I P V U O U U K A E P
O M K A N V G G P Q M X Y J K
N V J Y W Y P J I Z U I J N A
G E I A S A J F W E L K Z K E
I G N I Z J I W E O T K Q V N
S J A F O K N D N C I D H A I
E B A P R L P W T I F Y F S Y
L S G X W H F R T N A U K T R
G D T S L P L M S H C K P I H
N Y P L W U N Y Q Q T B A P L
I A D M I N C O N S O L E A P
S M B G A T E W A Y R L I D F
I N Z E R O T R U S T Y B R Z
Z Y B N V X M C F P W Q Q E X
H E Y C C E S P I W L F G S H

WOORDENLIJST

ZEROTRUST VASTIPADRES IPSEC ADMINCONSOLE SINGLESIGNON
MULTIFACTOR GATEWAY TOEWIJZING

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN

- **A. ZEROTRUST**
- **B. VASTIPADRES**
- **C. IPSEC**
- **D. ADMINCONSOLE**
- **E. SINGLESIGNON**
- **F. MULTIFACTOR**
- **G. GATEWAY**
- **H. TOEWIJZING**

DEFINITIES EN KOPPELVELDEN

1. Statisch gatewayadres op de whitelist.
2. Routeringsknooppunt aan de toegang tot het netwerk.
3. VPN-toegangslicenties voor medewerkers toekennen.
4. Inlogbeveiliging die extra tokens vereist.
5. Standaard voor site-to-site-tunnels.
6. Kader voor continue verificatie van vertrouwen.
7. Identiteitskoppeling met Okta en Entra ID.
8. Centraal portaal voor IT-beheerders.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen uit dit werkblad te onthullen. Schrijf je antwoorden in de invulvelden.

1. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. YAWEAGT
5. RADASSIPVET
6. ENSOCLNADOMI
7. CIMUARTOLFT
8. NWJGTIOZIE

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Tools die een bedrijf elke dag gebruikt			
2	Dingen die een VPN kan verbergen			
3	Functies binnen een IT-afdeling			
4	Woorden die Zero Trust beschrijven			
5	Manieren om veilig in te loggen			
6	Redenen om werknemers een VPN te geven			
7	Dingen die je doet na een beveiligingsincident			
8	Redenen om een VPN te gebruiken tijdens het reizen			
9	Regels voor veilig thuiswerken			
10	Gegevens die een bedrijf moet beschermen			
11	Dingen die een videovergadering kunnen verstoren			
12	Apparaten die een VPN kunnen gebruiken			
13	Kantoorprogramma's die je kent			
14	Plekken waar werknemers werken			
15	Apparaten die een werknemer kan hebben			

Controlepunt 8: Casestudy's VPN en netwerk

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

CASESTUDY 1: MIGRATIE NAAR ZERO TRUST

👷

Scenario: Een onderneming wil haar lokale servers beveiligen door voortdurend de compliancecertificaten van apparaten, de firewallstatus en de locatie van gebruikers te controleren, in plaats van iedereen binnen het netwerk te vertrouwen.

Discussievraag: Welk raamwerk moet de IT-beveiligingsdirecteur invoeren om dit te bereiken?

CASESTUDY 2: GATEWAYBEPERKING

👷

Scenario: Een bedrijf host privé-financiële databases in de cloud. Het wil alle openbare internettoegang tot de beheerpanelen blokkeren en alleen inloggen toestaan vanaf geverifieerde bedrijfsapparaten.

Discussievraag: Welke netwerkconfiguratie moet de databasebeheerder op de cloudfirewall instellen?

Controlepunt 9: De code ontcijferen

Een netwerkingenieur beveiligt routeringskanalen en clienttunnels. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

26	5	18	15		20	18	21	19	20		22	5	18	9	6	9	5	5	18	20
5	12	11		22	5	18	2	15	14	4	5	14								
1	16	16	1	18	1	1	20													

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

Controlepunt 10: Veelgestelde vragen over VPN – basis (Deel A)

Bekijk de meestgestelde vragen en antwoorden over virtuele privénetwerken (VPN's) en tunneling.

Q1: Wat is een enterprise-VPN?

Een beveiligde netwerktunnel voor bedrijven, waarmee externe medewerkers met gecentraliseerd beheer toegang krijgen tot bedrijfsnetwerken.

Q2: Waarin verschilt Zero Trust van traditionele VPN's?

Traditionele VPN's vertrouwen iedereen binnen de tunnel, terwijl Zero Trust elk apparaat en elke gebruikersverbinding voortdurend verifieert.

Q3: Wat is een dedicated IP in zakelijke VPN's?

Een statisch IP-adres dat uitsluitend voor jouw bedrijf is gereserveerd, zodat je het kunt whitelisten voor veilige toegang tot clouddatabases.

Q4: Waarom is SSO belangrijk voor zakelijke VPN's?

Met Single Sign-On kunnen medewerkers hun bedrijfsgegevens (zoals Okta of Microsoft Entra ID) gebruiken om veilig in te loggen.

Q5: Wat is een site-to-site-VPN?

Een tunnel die via IPsec twee fysieke kantoren (zoals een filiaal en het hoofdkantoor) verbindt via het openbare internet.

Controlepunt 10: Veelgestelde vragen over VPN – basis (Deel B)

Bekijk de meestgestelde vragen en antwoorden over virtuele privénetwerken (VPN's) en tunneling.

Q6: Wat is de functie van een beheerconsole?

Een dashboard voor IT-beheerders om medewerkerslicenties toe te voegen of te verwijderen, gateways toe te wijzen en actieve verbindingen te bewaken.

Q7: Hoe beveiligt MFA zakelijke VPN's?

Door een tweede code te eisen (zoals een token van een authenticator-app) om ongeoorloofde toegang met gecompromitteerde wachtwoorden te voorkomen.

Q8: Kan ik de verbindingsgeschiedenis van medewerkers controleren?

Ja, bedrijfs-VPN's registreren tijdstippen van verbindingen, de duur en toegewezen IP-adressen voor nalevingscontroles.

Q9: Wat is ZTNA?

Zero Trust Network Access, een beveiligingsmodel dat alleen toegang verleent tot specifieke toepassingen in plaats van tot het hele netwerk.

Q10: Wat is de rol van gatewayknooppunten?

Ze dienen als beveiligde toegangspunten voor extern verkeer en routeren gegevens rechtstreeks naar privé-bedrijfsservers.

Controlepunt 10: Veelgestelde vragen over VPN – gevorderd (Deel C)

Verken geavanceerde technische aspecten van VPN-tunnelprotocollen, integraties van mobiele clients en implementatie in bedrijven.

Q1: Hoe beschermt IPsec communicatie tussen bedrijfslocaties (site-to-site)?

IPsec versleutelt verkeer op netwerklaag met Encapsulating Security Payload (ESP) om vertrouwelijkheid en integriteit van gegevens te waarborgen.

Q2: Waarom schiet verouderde beveiliging op basis van een netwerkperimeter tekort voor medewerkers op afstand?

Omdat medewerkers vanaf meerdere locaties en apparaten toegang hebben tot gegevens, waardoor één enkele netwerkfirewall als perimeter achterhaald is.

Q3: Hoe voeren IT-managers geautomatiseerde provisioning in?

Door SCIM-protocollen tussen identiteitsproviders (Okta) en de VPN-beheerconsole te koppelen om gebruikersmappen te synchroniseren.

Q4: Wat is het voordeel van split tunneling in bedrijfsomgevingen?

Het routeert lokaal SaaS-verkeer (zoals Microsoft 365) buiten de VPN-tunnel, zodat bandbreedte van de bedrijfsgateway beschikbaar blijft voor privédatabases.

Q5: Hoe valideren posture checks van apparaten de beveiliging van eindpunten?

De VPN-client scant het apparaat vóór het verbinden om te controleren of de firewall actief is, het antivirusprogramma draait en de besturingssysteempatches up-to-date zijn.

Controlepunt 10: Veelgestelde vragen over VPN – gevorderd (Deel D)

Verken geavanceerde technische aspecten van VPN-tunnelprotocollen, integraties van mobiele clients en implementatie in bedrijven.

Q6: Welke rol speelt NAT-traversal bij zakelijke VPN-opstellingen?

NAT-T verpakt IPsec-pakketten in UDP, zodat ze zonder verbindingsverlies door routers en firewalls thuis kunnen.

Q7: Hoe voorkomen bedrijven een knelpunt in de gatewaybandbreedte?

Door meerdere regionale gatewayknooppunten in te zetten en het binnenkomende gebruikersverkeer daarover te verdelen met load balancers.

Q8: Waarom hebben statische IP-whitelists de voorkeur boven dynamische?

Statische whitelists voorkomen dat ongeautoriseerde externe IP-adressen proberen handshakes voor verbindingen uit te voeren, waardoor het aanvalsoppervlak drastisch kleiner wordt.

Q9: Welke rol speelt certificaatgebaseerde authenticatie in zakelijke VPN's?

Het valideert unieke digitale certificaten die op door het bedrijf beheerde apparaten zijn geïnstalleerd en blokkeert onbeheerde persoonlijke computers.

Q10: Hoe verkleint ZTNA het risico op laterale beweging?

Door gebruikerssessies te isoleren tot specifieke geautoriseerde bronnen, zodat hackers zich niet door het netwerk kunnen bewegen als één knooppunt wordt gecompromitteerd.

Deel 11: 10 VPN-feiten en inzichten uit de praktijk

Bekijk feiten uit de praktijk over VPN-versleutelingssnelheden, protocolaudits, mobiele connectiviteit en zakelijk werken op afstand.

1. VPN-INZICHT

Zero Trust-architecturen controleren continu de beveiligingsstatus van elk apparaat dat een netwerkverbinding probeert te maken.

2. VPN-INZICHT

Met dedicated IP-gateways kunnen bedrijven cloud-databases afschermen door statische adressen op een whitelist te zetten.

3. VPN-INZICHT

IPsec is het standaardprotocol in de sector voor het instellen van beveiligde site-to-site-tunnels tussen kantoornetwerken.

4. VPN-INZICHT

Met beheerconsoles kunnen IT-afdelingen VPN-toegangslicenties voor medewerkers inrichten, beheren en controleren.

5. VPN-INZICHT

Single Sign-On integreert VPN-toegang met bedrijfsidentiteitsproviders zoals Okta en Entra ID.

6. VPN-INZICHT

Multifactorauthenticatie blokkeert onbevoegde verbindingspogingen die afkomstig zijn van gestolen wachtwoordsleutels.

7. VPN-INZICHT

Split tunneling optimaliseert de bedrijfsbandbreedte door openbaar SaaS-verkeer uit te sluiten van de versleutelde tunnel.

8. VPN-INZICHT

Apparaatcontroles controleren lokale beveiligingsinstellingen voordat toegang tot bedrijfsservers wordt verleend.

9. VPN-INZICHT

SCIM-directorysynchronisatie automatiseert de toegangscontroles voor het in- en uitdienst treden van medewerkers.

10. VPN-INZICHT

Zero Trust Network Access beperkt de toegang van gebruikers tot specifieke geautoriseerde toepassingen, waardoor laterale beweging in het netwerk wordt voorkomen.

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde technische standaarden, specificaties en regelgevend kaders.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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/

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 **Zero Trust** ZTNA-MODEL **Juist antwoord: A**

DOCENTENNOTITIE

Zero Trust-modellen controleren vóór toegang tot het netwerk continu of apparaten aan de regels voldoen. Bron: NIST Zero Trust.

2 **Dedicated IP** STATISCH IP-ADRES **Juist antwoord: A**

DOCENTENNOTITIE

Met dedicated IP-adressen kun je gateways op een whitelist zetten om openbaar verkeer te blokkeren. Bronvermelding: Dedicated IP Guide.

3 **IPsec-standaard** IPSEC-TUNNEL **Juist antwoord: A**

DOCENTENNOTITIE

IPsec is het standaardprotocol voor site-to-site-tunnels tussen filialen. Bron: IPsec Tunneling.

4 **IT-toewijzing** BEHEERCONSOLE **Juist antwoord: A**

DOCENTENNOTITIE

Via gecentraliseerde beheerdashboards kunnen IT-beheerders seatlicenties toewijzen. Bron: CISA Guidelines.

5 **Vraag 5** **Juist antwoord: A**

DOCENTENNOTITIE

Welke authenticatiestandaard maakt inloggen via Okta of Microsoft Entra ID mogelijk? → Single Sign-On

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Zero Trust** ZTNA-CONTROLES — **Juist antwoord: Waar**

DOCENTENNOTITIE

Zero Trust-modellen controleren vóór toegang tot het netwerk continu of apparaten aan de regels voldoen. Bron: NIST Zero Trust.

7 **Vraag 7** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Dedicated IP's zijn gereserveerd voor één bedrijf, dus het verkeer wordt niet vermengd met dat van andere gebruikers.

8 **IT-toewijzing** IT-BEHEERDERSPLEK — **Juist antwoord: Waar**

DOCENTENNOTITIE

Via gecentraliseerde beheerdashboards kunnen IT-beheerders seatlicenties toewijzen. Bron: CISA Guidelines.

9 **IPsec-standaard** SITE-TO-SITE — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

IPsec is het standaardprotocol voor site-to-site-tunnels tussen filialen. Bron: IPsec Tunneling.

10 **Okta SSO-koppeling** SSO-AANMELDING — **Juist antwoord: Waar**

DOCENTENNOTITIE

Single Sign-On integreert VPN-logins met bedrijfsdirectory's zoals Okta. Bron: Okta SSO.

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

H 1. ZERO TRUST	D 2. DEDICATED IP	E 3. IPSEC	G 4. BEHEERCONSOLE
B 5. SINGLE SIGN-ON	C 6. MULTIFACTOR	F 7. GATEWAY	A 8. PROVISIONING

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 ZERO TRUST	2 VAST IP-ADRES	3 IPSEC	4 ADMIN CONSOLE
5 SINGLE SIGN-ON	6 MULTIFACTOR		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 B – VASTIPADRES	2 G – GATEWAY	3 H – TOEWIJZING	4 F – MULTIFACTOR
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – ADMINCONSOLE

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen ZERO TRUST, DEDICATED IP en IPSEC in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

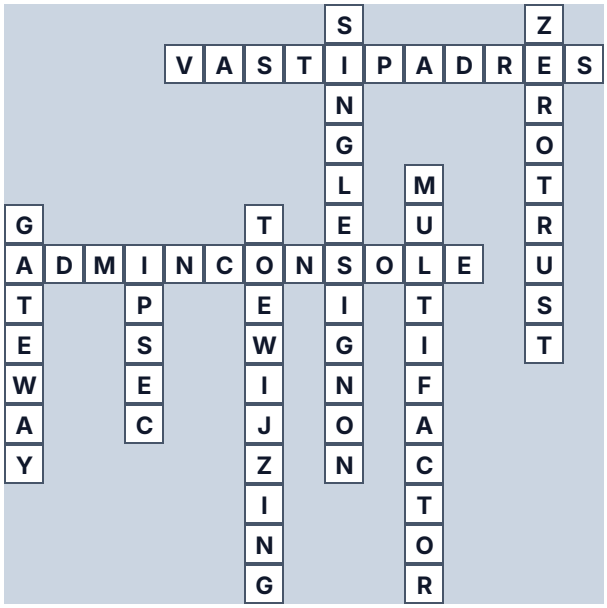
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

N	I	Q	T	I	P	V	U	O	U	U	K	A	E	P
O	M	K	A	N	V	G	G	P	Q	M	X	Y	J	K
N	V	J	Y	W	Y	P	J	I	Z	U	I	J	N	A
G	E	I	A	S	A	J	F	W	E	L	K	Z	K	E
I	G	N	I	Z	J	I	W	E	O	T	K	Q	V	N
S	J	A	F	O	K	N	D	N	C	I	D	H	A	I
E	B	A	P	R	L	P	W	T	I	F	Y	F	S	Y
L	S	G	X	W	H	F	R	T	N	A	U	K	T	R
G	D	T	S	L	P	L	M	S	H	C	K	P	I	H
N	Y	P	L	W	U	N	Y	Q	Q	T	B	A	P	L
I	A	D	M	I	N	C	O	N	S	O	L	E	A	P
S	M	B	G	A	T	E	W	A	Y	R	L	I	D	F
I	N	Z	E	R	O	T	R	U	S	T	Y	B	R	Z
Z	Y	B	N	V	X	M	C	F	P	W	Q	Q	E	X
H	E	Y	C	C	E	S	P	I	W	L	F	G	S	H

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

3 horizontaal: VASTIPADRES Statisch gatewayadres op de whitelist (11 letters)

7 horizontaal: ADMINCONSOLE Centraal portaal voor IT-beheerders (12 letters)

VERTICAAL

1 verticaal: SINGLESIGNON Identiteitskoppeling met Okta en Entra ID (12 letters)

2 verticaal: ZEROTRUST Kader voor continue verificatie van vertrouwen (9 letters)

4 verticaal: MULTIFACTOR Inlogbeveiliging die extra tokens vereist (11 letters)

5 verticaal: GATEWAY Routeringsknooppunt aan de toegang tot het netwerk (7 letters)

6 verticaal: TOEWIJZING VPN-toegangslicenties voor medewerkers toekennen (10 letters)

8 verticaal: IPSEC Standaard voor site-to-site-tunnels (5 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1.	RTOEZUSTR	ZEROTRUST	5.	RADASSIPVET	VASTIPADRES
2.	ICESP	IPSEC	6.	ENSOCLNADOMI	ADMINCONSOLE
3.	SIISOGNENLNG	SINGLESIGNON	7.	CIMUARTOLFT	MULTIFACTOR
4.	YAWEAGT	GATEWAY	8.	NWJGTIOZIE	TOEWIJZING

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"ZERO TRUST VERIFIEERT ELK VERBONDEN APPARAAT"

Antwoordsleutel casestudy's

A Casestudy 1: Migratie naar zero trust

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een groot bedrijf wil zijn lokale servers beveiligen door continu de compliancecertificaten van apparaten, de firewallstatus en de locatie van gebruikers te controleren in plaats van iedereen binnen het netwerk te vertrouwen.
- Aanbevolen strategie en oplossing: De directeur moet overstappen op een Zero Trust Network Access-model (ZTNA), dat continu contextgebaseerde beveiligingscontroles afdwingt.

B Casestudy 2: Gatewaybeperking

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een bedrijf host privé-financiële databases in de cloud. Het wil alle openbare internettoegang tot de beheerpanelen blokkeren en aanmeldingen alleen toestaan vanaf geverifieerde endpoints van het bedrijf.
- Aanbevolen strategie en oplossing: De beheerder moet een Dedicated IP-gateway configureren op de zakelijke VPN en dit statische adres op de whitelist van de firewall van de clouddatabase zetten.