Naam: _____ Datum: _____ Score: _____

VPN voor externe toegang

Eindpunten van medewerkers op afstand beveiligen, multifactorauthenticatie en configuratie van IPsec-tunnels.

LEEROVERZICHT: REMOTE ACCESS-VPN'S

LEERLING
STUDENTENSTATUS
Network Defender-traject

VEILIG
VERBINDINGSSTATUS
Gegevenspakketten afschermen

ACTIEF
LEKBESCHERMING
Bescherming tegen DNS- en IPv6-lekken

Welkom! Dit activiteitenpakket leidt je door externe toegang tot VPN-netwerken. Je verkent client-naar-site-tunnels, multifactorinlogs, controles van de apparaatstatus, bandbreedtelimieten en beveiligingsaudits via syslog.

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-zakelijk/externe-toegang/

Jouw leertraject: VPN voor toegang op afstand

- Eindpunten van medewerkers op afstand beveiligen die toegang hebben tot lokale netwerkknooppunten.
- Configureer beleid voor meervoudige authenticatie voor externe aanmeldingen.
- Client-to-site-configuraties voor IPsec en OpenVPN instellen.
- Audit de logs van externe verbindingen op schendingen van de toegangscontrole.
- Voer controles van de apparaatstatus uit voordat netwerkverbindingen worden toegestaan.
- Optimaliseer de serverdoorvoer om bandbreedteknelpunten bij telewerken te voorkomen.

INSTRUCTIES VOOR REMOTE ACCESS-VPN'S

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 postuurcontroles en inloggen met meerdere factoren. Sluit af met de bonusopdracht Snel denken.

CLIENT-TO-SITE-TUNNELS EN ENDPOINTCOMPLIANCE (INLEIDING)

VPN's voor externe toegang zetten beveiligde client-naar-sitetunnels op voor medewerkers buiten kantoor. Om deze verbindingen te beveiligen moet je aanmeldingen met meervoudige verificatie (MFA) afdwingen, controles van de endpointstatus uitvoeren en logs controleren via centrale syslog-collectors.

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

Controlepunt 1: Meerkeuzeopdracht

1. **1. Welke authenticatiestandaard moeten VPN-portalen voor externe toegang verplicht stellen?**
   - A) Multifactor
   - B) Eén factor
   - C) Onversleuteld
   - D) Lokale gast

2. **2. Welk protocol is de standaard voor het beveiligen van client-naar-site-verbindingen bij werken op afstand?**
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. **3. Welke controle valideert of een laptop op afstand schoon is voordat er verbinding wordt gemaakt?**
   - A) Houdingscontrole
   - B) Snelheidstest
   - C) Pingtest
   - D) Aantal geheugens

4. **4. Waar worden de verbindingslogs van medewerkers op afstand opgeslagen voor beveiligingsaudits?**
   - A) Syslog-server
   - B) Registersleutel
   - C) Clientgeheugen
   - D) Webbrowser

5. **5. Welk probleem ontstaat wanneer het aantal thuiswerkers de bandbreedtecapaciteit van de gateway overschrijdt?**
   - A) Bandbreedteknelpunt
   - B) DNS-lek
   - C) Handshake-pas
   - D) Blootstelling van het IP-adres

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Multifactorauthenticatie voegt een tweede validatietoken toe om externe aanmeldingen te beveiligen.

- ◯ Waar
- ◯ Onwaar

7 Vraag 7

7. Statuscontroles laten externe apparaten met uitgeschakelde firewalls toegang krijgen tot privéservers.

- ◯ Waar
- ◯ Onwaar

8 Vraag 8

8. Logs van VPN's voor externe toegang zijn essentieel om ongeautoriseerde toegang tot het bedrijfsnetwerk op te sporen.

- ◯ Waar
- ◯ Onwaar

9 Vraag 9

9. OpenVPN en IPsec zijn verouderde protocollen die de gegevens van externe clients niet versleutelen.

- ◯ Waar
- ◯ Onwaar

10 Vraag 10

10. Bandbreedteknelpunten op de gateway ontstaan wanneer extern verkeer de capaciteit van de netwerkkaart overschrijdt.

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Om bedrijfsportalen te beschermen moet inloggen op afstand _____ -authenticatie vereisen.

2. Clients op afstand versleutelen de payload van datatunnels met standaard _____ -protocollen.

3. Apparaten moeten een beveiligingscontrole op _____ doorstaan voordat ze een netwerkverbinding krijgen.

4. Controleerbare toegangslogs worden continu doorgestuurd naar een centrale _____ -server.

5. Veel verkeer tijdens kantooruren kan leiden tot congestie van de _____ gateway.

6. Virtuele adapterstuurprogramma's regelen de client-naar-site- _____ onder Windows en macOS.

WOORDENBANK

BANDBREEDTE BEVEILIGINGSSTATUS FIREWALL MULTIFACTOR OPENVPN SYSLOG TUNNELING VERSLEUTELING

Schrijf hier je antwoorden:

1. **2.**

3. **4.**

5. **6.**

Controlepunt 4: Kernbegrippen koppelen

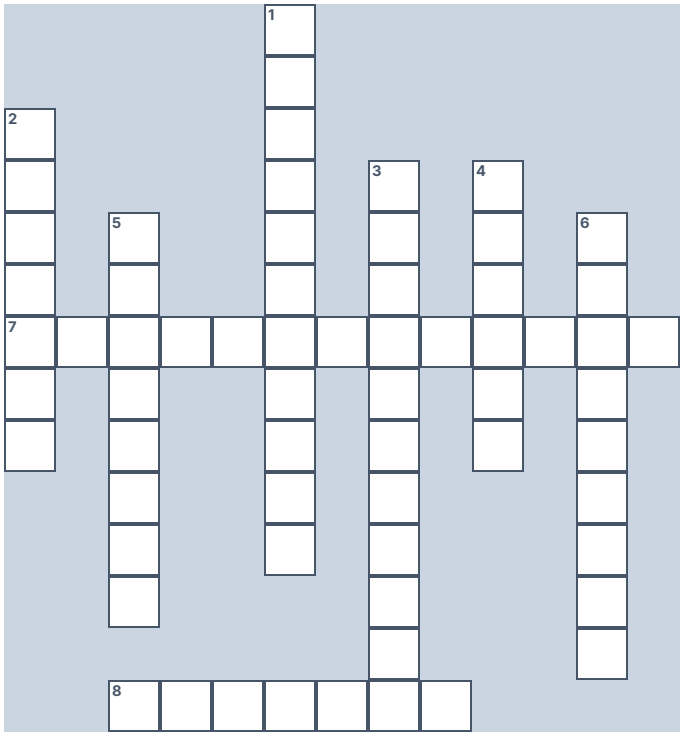
DEFINITIES KOPPELEN

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. MULTIFACTOR	A	Gegevens inkapselen in een beveiligd pad.
☐	2. OPENVPN	B	Centrale verzamelaar van beveiligingslogs.
☐	3. BEVEILIGINGSSTATUS	C	Limiet voor netwerkdatacapaciteit.
☐	4. SYSLOG	D	Standaard client-to-site-protocol.
☐	5. BANDBREEDTE	E	Validatie van de gezondheid van externe apparaten.
☐	6. VERSLEUTELING	F	Regels van het verkeersfiltersysteem.
☐	7. TUNNELING	G	Cryptografisch door elkaar halen van pakketten.
☐	8. FIREWALL	H	Aanmeldbeveiliging waarvoor extra tokens nodig zijn.

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

7. Cryptografisch versleutelen van pakketten (13)

8. Controle van de gezondheid van apparaten op afstand (7)

VERTICAAL

1. Limiet op de datacapaciteit van het netwerk (11)

2. Standaard client-naar-site-protocol (7)

3. Inlogbeveiliging die extra tokens vereist (11)

4. Centrale verzamelaar van beveiligingslogs (6)

5. Regels van een systeem dat verkeer filtert (8)

6. Gegevens inpakken in een beveiligd pad (9)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

7 horizontaal: Cryptografisch versleutelen van pakketten (13 letters):

8 horizontaal: Controle van de gezondheid van apparaten op afstand (7 letters):

VERTICAAL

1 verticaal: Limiet op de datacapaciteit van het netwerk (11 letters):

2 verticaal: Standaard client-naar-site-protocol (7 letters):

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

4 verticaal: Centrale verzamelaar van beveiligingslogs (6 letters):

5 verticaal: Regels van een systeem dat verkeer filtert (8 letters):

6 verticaal: Gegevens inpakken in een beveiligd pad (9 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.

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

WOORDENLIJST

MULTIFACTOR OPENVPN POSTURE SYSLOG BANDBREEDTE VERSLEUTELING TUNNELING FIREWALL

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. MULTIFACTOR
B. OPENVPN
C. POSTURE
D. SYSLOG
E. BANDBREEDTE
F. VERSLEUTELING
G. TUNNELING
H. FIREWALL

DEFINITIES EN KOPPELVELDEN

1. Centrale verzamelaar van beveiligingslogs. ____
2. Regels van een systeem dat verkeer filtert. ____
3. Gegevens inpakken in een beveiligd pad. ____
4. Cryptografisch versleutelen van pakketten. ____
5. Standaard client-naar-site-protocol. ____
6. Limiet op de datacapaciteit van het netwerk. ____
7. Controle van de gezondheid van apparaten op afstand. ____
8. Inlogbeveiliging die extra tokens vereist. ____

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. IAOUFCMTLRT
2. PSERUTO
3. BERENATEBDD
4. EGNNILTUN
5. VNNEOPP
6. OLSSGY
7. LITEVEELGNRUS
8. EIWLFLAR

Bonusopdracht: Snel denken

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

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

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: AFDWINGEN VAN MFA



Scenario: Een bedrijfsanalist probeert tijdens het werken op afstand in te loggen op de zakelijke database. Hij voert zijn juiste gebruikersnaam en wachtwoord in, maar het VPN-portaal blokkeert de toegang en vraagt om een code van een fysiek token.

Discussievraag: welk beveiligingsbeleid dwingt deze dubbele verificatiestap af?

CASESTUDY 2: POSTURE-COMPLIANCE



Scenario: Een freelancer verbindt zijn persoonlijke laptop met het zakelijke netwerk op afstand. De VPN-client verbreekt de verbinding meteen en meldt de gebruiker dat zijn antivirusdefinities verouderd zijn.

Discussievraag: Welke gespecialiseerde controle van de VPN-gateway blokkeerde deze verbindingspoging?

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

22 16 14 15 16 1 6 19 20 1 14 4

2 5 19 3 8 5 18 13 20 22 5 18 19 16 18 5 9 4 5

5 9 14 4 16 21 14 20 5 14

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 VPN voor toegang op afstand?

Een beveiligde verbindingsmethode waarmee medewerkers die op een externe locatie werken rechtstreeks verbinding kunnen maken met privéservers van het bedrijf.

Q2: Waarom verschilt client-naar-site van site-naar-site?

Client-to-site verbindt individuele gebruikersapparaten, terwijl site-to-site volledige fysieke kantoorlocaties aan elkaar koppelt.

Q3: Wat is een apparaat-posture check?

Een scan die de beveiligingsstatus van een extern apparaat controleert (antivirus, patchniveau van het besturingssysteem) voordat toegang wordt verleend.

Q4: Waarom wordt OpenVPN gebruikt voor toegang op afstand?

Vanwege het sterke beveiligingsprotocol, de compatibiliteit met meerdere platforms en het vermogen om individuele verbindingen te verwerken.

Q5: Hoe beschermt MFA toegang op afstand?

Het voegt een tweede verificatietoken toe, waardoor toegang wordt voorkomen, zelfs als wachtwoorden van werknemers zijn gelekt of gestolen.

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 een syslogserver?

Een gecentraliseerde logopslag die verbindingsgebeurtenissen, aanmeldingen en systeemmeldingen bewaart voor compliance-audits.

Q7: Wat veroorzaakt een knelpunt in de bandbreedte?

Wanneer de gezamenlijke bandbreedtebehoefte van medewerkers op afstand de limiet voor de internetsnelheid van de bedrijfsgateway overschrijdt.

Q8: Kan ik mijn thuiscomputer verbinden met een werk-VPN?

Alleen als het apparaat de audits van de bedrijfsstatuscontrole doorstaat en door IT-beheerders is geautoriseerd.

Q9: Wat is netwerkencapsulatie?

Het verpakken van datapakketten tijdens het transport in versleutelde protocolheaders om de overdracht te beveiligen.

Q10: Hoe optimaliseert split tunneling toegang op afstand?

Het laat werknemers hun lokale provider gebruiken voor gewoon surfen, terwijl werkgerelateerde bestanden via de VPN worden gerouteerd.

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 verbetert authenticatie op basis van certificaten de toegang op afstand?

Het koppelt verbindingsrechten aan vooraf geïnstalleerde lokale digitale certificaten, waardoor onbeheerde of ongeautoriseerde apparaten worden geblokkeerd.

Q2: Wat is het beveiligingsrisico van split tunneling voor werken op afstand?

Het creëert een mogelijke brug waarlangs een gecompromitteerd lokaal apparaat externe dreigingen het privénetwerk in kan sturen.

Q3: Hoe controleren posture checks registerinstellingen?

De VPN-client voert lokale scripts uit die registerpaden opvragen om te controleren of bedrijfsbeveiligingssoftware actief draait.

Q4: Waarom gebruiken syslogs standaard UDP-poort 514?

Om logs snel en met minimale overhead te verzenden, hoewel beveiligde opstellingen tegenwoordig TLS-inkapseling over TCP verplicht stellen.

Q5: Hoe lossen bedrijven knelpunten in de gatewaybandbreedte op?

Door load balancers in te zetten en extern verkeer over regionale serverknooppunten te verdelen.

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: Wat is de functie van virtuele TAP/TUN-adapters op clients op afstand?

Ze fungeren als virtuele netwerkkaarten en routeren TCP/IP-verkeer op apparaatniveau rechtstreeks de versleutelde VPN-tunnel in.

Q7: Hoe ondersteunt IKEv2 MOBIKE de mobiliteit van medewerkers op afstand?

Het werkt IP-adresbindingen dynamisch bij, zodat de VPN actief blijft terwijl de gebruiker tussen wifi en mobiele data wisselt.

Q8: Wat is het verschil tussen gesplitste en volledige tunnelroutering?

Bij volledige routering gaat al het internetverkeer van het apparaat via de VPN, terwijl bij gesplitste routering alleen bedrijfs-IP-adressen als bestemming via de VPN gaan.

Q9: Hoe gaan NAT-apparaten om met VPN-verbindingen op afstand?

Door lokale poortbereiken aan openbare gateway-IP-adressen te koppelen om terugkerende versleutelde gegevenspakketten te routeren.

Q10: Welke nalevingsnormen verplichten tot het auditen van toegang op afstand?

Normen zoals HIPAA, SOC 2 en PCI DSS vereisen dat alle sessies voor externe verbindingen worden gelogd en gemonitord.

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

VPN's voor externe toegang zetten beveiligde client-naar-sitetunnels op voor medewerkers buiten kantoor.

2. VPN-INZICHT

Multifactorauthenticatie is volgens nalevingsregels verplicht om externe zakelijke portalen te beschermen.

3. VPN-INZICHT

Statuscontroles verifiëren de lokale beveiligingsinstellingen van de client voordat toegang tot het privénetwerk wordt verleend.

4. VPN-INZICHT

Syslog-servers verzamelen verbindingslogboeken om pogingen tot ongeoorloofde toegang te auditen en te detecteren.

5. VPN-INZICHT

Bandbreedteknelpunten op de gateway ontstaan wanneer de totale vraag naar extern verkeer de internetlimieten van de server overschrijdt.

6. VPN-INZICHT

Virtuele netwerkadapters kapselen netwerkverzoeken van het besturingssysteem in binnen beveiligde protocollen.

7. VPN-INZICHT

Dankzij MOBIKE-ondersteuning kunnen externe clients van netwerk wisselen zonder dat de VPN-tunnel wegvalt.

8. VPN-INZICHT

Volledige tunnelroutering beveiligt al het internetverkeer van werknemers, maar verhoogt de belasting van de bedrijfsgateway.

9. VPN-INZICHT

Certificaatverificatie koppelt de autorisatie van de VPN-verbinding rechtstreeks aan door het bedrijf beheerde hardware.

10. VPN-INZICHT

Raamwerken zoals SOC 2 en PCI DSS verwachten dat sessies voor toegang op afstand worden vastgelegd en bewaakt.

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/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 **Inlogtokens** MFA-BEVEILIGING **Juist antwoord: A**

DOCENTENNOTITIE

Multifactorauthenticatie dwingt een tweede verificatie af bij aanmeldingen. Bron: MFA Implementation.

2 **OpenVPN-tunnel** CLIENT-TO-SITE **Juist antwoord: A**

DOCENTENNOTITIE

OpenVPN is een standaardprotocol voor het beveiligen van client-naar-sitetunnels. Bron: OpenVPN Client.

3 **Statuscontroles** APPARAATCONTROLE **Juist antwoord: A**

DOCENTENNOTITIE

Statuscontroles scannen eindpunten op actieve firewalls en antivirustools. Bron: Posture Compliance.

4 **Logaggregator** SYSLOG-SERVER **Juist antwoord: A**

DOCENTENNOTITIE

Syslog-servers verzamelen beveiligingsgebeurtenislogboeken om schendingen van toegangsregels te monitoren. Bron: Syslog Standard.

5 **Kaartoverloop** GATEWAY-KNELPUNT **Juist antwoord: A**

DOCENTENNOTITIE

Bandbreedteknelpunten op de gateway ontstaan wanneer gebruikersverkeer de limieten van de server overschrijdt. Bron: Capacity Planning.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Inlogtokens** MFA-CONTROLES **Juist antwoord: Waar**

DOCENTENNOTITIE

Multifactorauthenticatie dwingt een tweede verificatie af bij aanmeldingen. Bron: MFA Implementation.

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

DOCENTENNOTITIE

Posture checks blokkeren apparaten waarvan de firewall of antivirus uit staat, dus zulke apparaten worden geweigerd.

8 **Logaggregator** SYSLOG-SERVER **Juist antwoord: Waar**

DOCENTENNOTITIE

Syslog-servers verzamelen beveiligingsgebeurtenislogboeken om schendingen van toegangsregels te monitoren. Bron: Syslog Standard.

9 **Vraag 9** **Juist antwoord: Onwaar**

DOCENTENNOTITIE

OpenVPN en IPsec zijn gangbare protocollen die het verkeer van externe clients wel versleutelen.

10 **Kaartoverloop** GATEWAY-KNELPUNT **Juist antwoord: Waar**

DOCENTENNOTITIE

Bandbreedteknelpunten op de gateway ontstaan wanneer gebruikersverkeer de limieten van de server overschrijdt. Bron: Capacity Planning.

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. MULTIFACTOR	D 2. OPENVPN	E 3. BEVEILIGINGSSTATUS	B 4. SYSLOG
C 5. BANDBREEDTE	G 6. VERSLEUTELING	A 7. TUNNELING	F 8. FIREWALL

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 MULTIFACTOR	2 OPENVPN	3 BEVEILIGINGSSTATUS	4 SYSLOG
5 BANDBREEDTE	6 TUNNELING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 D – SYSLOG	2 H – FIREWALL	3 G – TUNNELING	4 F – VERSLEUTELING
5 B – OPENVPN	6 E – BANDBREEDTE	7 C – POSTURE	8 A – MULTIFACTOR

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen MULTIFACTOR, OPENVPN en BEVEILIGINGSSTATUS 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.

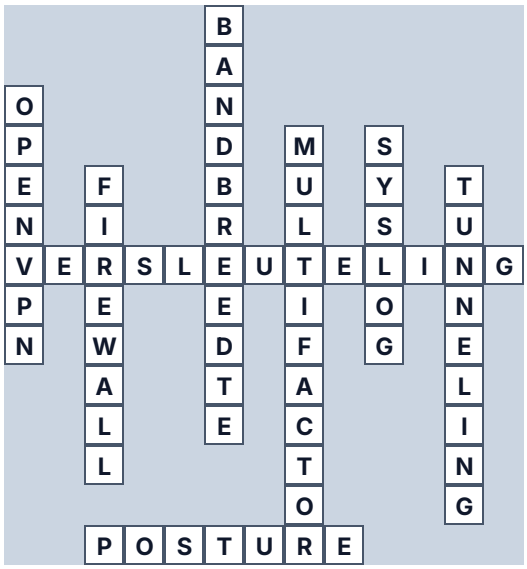
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

7 horizontaal: VERSLEUTELING Cryptografisch versleutelen van pakketten (13 letters)

8 horizontaal: POSTURE Controle van de gezondheid van apparaten op afstand (7 letters)

VERTICAAL

1 verticaal: BANDBREEDTE Limiet op de datacapaciteit van het netwerk (11 letters)

2 verticaal: OPENVPN Standaard client-naar-site-protocol (7 letters)

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

4 verticaal: SYSLOG Centrale verzamelaar van beveiligingslogs (6 letters)

5 verticaal: FIREWALL Regels van een systeem dat verkeer filtert (8 letters)

6 verticaal: TUNNELING Gegevens inpakken in een beveiligd pad (9 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. IAOUFCMTLRT — **MULTIFACTOR**
2. PSERUTO — **POSTURE**
3. BERENATEBDD — **BANDBREEDTE**
4. EGNNILTUN — **TUNNELING**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. LITEVEELGNRUS — **VERSLEUTELING**
8. EIWLFLAR — **FIREWALL**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"VPN OP AFSTAND BESCHERMT VERSPREIDE EINDPUNTEN"

Antwoordsleutel casestudy's

A Casestudy 1: Afdwingen van MFA

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een bedrijfsanalist probeert tijdens het werken op afstand in te loggen op de bedrijfsdatabase. Hij voert zijn juiste gebruikersnaam en wachtwoord in, maar het VPN-portaal blokkeert de toegang en vraagt om een fysieke tokencode.
- Aanbevolen strategie en oplossing: Het zakelijke VPN-portaal past een strikt beleid voor meervoudige verificatie (MFA) toe om externe aanmeldingen te beveiligen.

B Casestudy 2: Posture-compliance

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een externe medewerker verbindt zijn persoonlijke laptop met het bedrijfsnetwerk op afstand. De VPN-client verbreekt de verbinding onmiddellijk en meldt de gebruiker dat zijn antivirusdefinities verouderd zijn.
- Aanbevolen strategie en oplossing: De gateway voor externe toegang voerde een controle van de endpointstatus uit en blokkeerde het apparaat vanwege verouderde beveiligingsconfiguraties.