Naam: _____ Datum: _____ Score: _____

VPN.com VPN-gids Werkblad

Praktische oefeningen met netwerkprotocollen, tunneling en beveiligingsmaatregelen.

LEEROVERZICHT VPN

LEERLING
STUDENTENSTATUS
Network Defender-traject

VEILIG
VERBINDINGSSTATUS
Gegevenspakketten afschermen

ACTIEF
LEKBESCHERMING
Bescherming tegen DNS- en IPv6-lekken

Welkom! Dit activiteitenpakket leidt je door de basisprincipes van virtuele privénetwerken (VPN's). Je verkent hoe versleutelde tunnels je gegevens beveiligen, hoe netwerkprotocollen werken en hoe je privacylekken herkent en beperkt.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers VPN-begrippen en -protocollen.**
- [ ] **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-VPN-gids

URL: https://www.vpn.com/nl/vpn/

Jouw leertraject: VPN

- Leg het concept van datatunneling en inkapseling uit.
- Standaardprotocolconfiguraties en bandbreedte-eisen herkennen.
- Analyseer de rol van firewalls en geoblokkering bij internetroutering.
- Begrijp hoe internetproviders onversleutelde browse-activiteit volgen en hoe een VPN dat voorkomt.
- Maak onderscheid tussen de operationele grenzen van serverlocatie en jurisdictie.

INSTRUCTIES VPN-GIDS

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 praktijkscenario's in het gedeelte met casestudy's. Sluit af met de bonusopdracht Snel denken.

WAT IS EEN VPN? (INLEIDING)

Een Virtual Private Network is meer dan een privacyschakelaar. Het is een versleutelde tunnel die je internetverkeer via een externe server leidt. Dit verbergt je IP-adres, voorkomt dat je internetprovider logboeken van je online activiteiten opbouwt en beveiligt je gegevens op openbare netwerken. Het begrijpen van de terminologie is essentieel om digitaal veilig te blijven.

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

Controlepunt 1: Meerkeuzeopdracht

1. **1. Wat is een VPN-protocol?**
   - A. Een hardwareapparaat waarmee kabels worden aangesloten.
   - B. Een reeks regels die bepaalt hoe gegevens worden versleuteld en verzonden.
   - C. Een browserplug-in die advertenties blokkeert.
   - D. Een internetprovider.

2. **2. Als je VPN-verbinding traag aanvoelt, wat is dan de meest waarschijnlijke oorzaak?**
   - A. De VPN-server staat te ver weg of is overbelast.
   - B. De resolutie van je monitor is te hoog ingesteld.
   - C. Je hebt de cookies van je webbrowser uitgeschakeld.
   - D. De indeling van je toetsenbord is onjuist ingesteld.

3. **3. Waarom wordt een VPN sterk aanbevolen bij verbinding met openbare wifi?**
   - A. Het maakt de wifiverbinding gratis.
   - B. Het vergroot het bereik van de router.
   - C. Het versleutelt verkeer om hackers op hetzelfde netwerk te blokkeren.
   - D. Het verwijdert ongewenste e-mails automatisch.

4. **4. Welke van de volgende beschrijvingen past bij een geoblokkade?**
   - A. Een hulpmiddel dat de fysieke afstand tot een server meet.
   - B. Een beperking die de toegang tot een site blokkeert op basis van locatie.
   - C. Een protocol voor het comprimeren van lokale bestanden.
   - D. Een opslagmechanisme voor back-ups.

5. **5. Wat kan je internetprovider (ISP) zien als je een VPN gebruikt?**
   - A. Zoekwoorden en webpaginacontent die je bekijkt.
   - B. Dat je met een VPN bent verbonden, maar niet de details van het verkeer.
   - C. Geen enkele informatie, zelfs niet dat je online bent.
   - D. Je bestanden en foto's op je lokale harde schijf.

Controlepunt 2: Waar-of-onwaar-opdracht

6 Locatie maskeren

6. Een VPN verbergt het openbare IP-adres van je apparaat, zodat websites van derden je fysieke locatie niet gemakkelijk kunnen vaststellen.

- ◯ Waar
- ◯ Onwaar

7 Invloed van VPN op de snelheid

7. Door een VPN in te schakelen wordt je basissnelheid op internet twee keer zo snel als je verbinding zonder VPN.

- ◯ Waar
- ◯ Onwaar

8 Sniffen op openbaar wifi

8. Als je een onbeveiligd openbaar wifi-netwerk gebruikt zonder VPN, kunnen andere gebruikers op datzelfde netwerk mogelijk je onversleutelde verkeer onderscheppen.

- ◯ Waar
- ◯ Onwaar

9 Firewalls en geblokkeerde verbindingen

9. Netwerkbeheerders kunnen firewalls zo instellen dat ze uitgaande VPN-tunnelverbindingen herkennen en blokkeren.

- ◯ Waar
- ◯ Onwaar

10 Strikte no-logsbeleidsregels

10. Een strikt "no-logs"-beleid betekent dat de VPN-aanbieder wettelijk verplicht is je zoekopdrachten en bezochte links ten minste 30 dagen op te slaan.

- ◯ 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 je verkeer te beveiligen, verpakt de VPN je datapakketten in een ander protocol, een proces dat _____ heet.

2. Als je tijdens het streamen trage downloadsnelheden ervaart, kan dat komen door een beperkte _____ van het netwerk.

3. Een streamingdienst die alleen in een bepaald land beschikbaar is, gebruikt een _____ om gebruikers wereldwijd te beperken.

4. De verbindingsregels die de versleuteling en de verbindingsparameters bepalen, heten het _____ van de VPN.

5. Je computer gebruikt een lokale _____ om netwerkverkeer te bewaken en onveilige verbindingen te blokkeren.

6. Wanneer je verbinding maakt met een VPN, wordt je data geleid via een externe _____ om je openbare IP-adres te verbergen.

WOORDENBANK

BANDBREEDTE FIREWALL GEOBLOKKADE PRIVACY PROTOCOL PROVIDER SERVER TUNNELING

Schrijf hier je antwoorden:

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

Controlepunt 4: Netwerkbegrippen koppelen

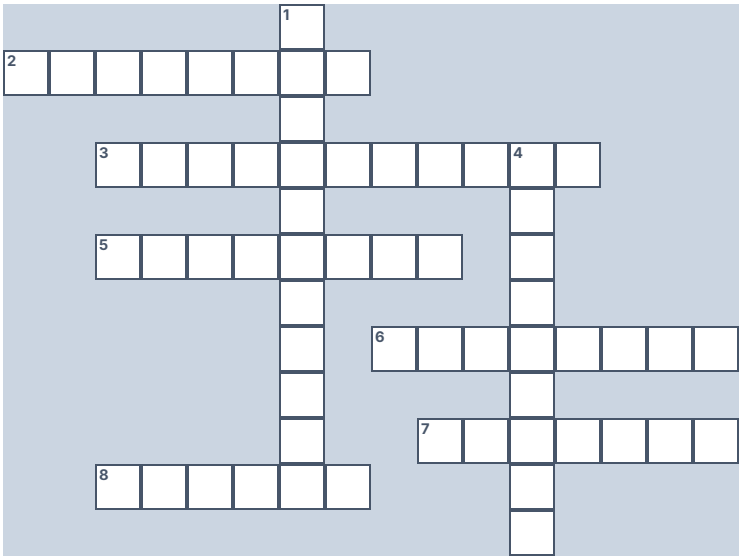
DEFINITIES KOPPELEN

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. Tunneling	A	Een reeks regels die bepaalt hoe gegevens over het netwerk worden verzonden.
☐	2. Protocol	B	De maximale snelheid van gegevensoverdracht via een verbinding.
☐	3. Bandbreedte	C	Een beperking die webtoegang verhindert op basis van de fysieke locatie.
☐	4. Server	D	Een beveiligingssysteem dat ongeoorloofd verkeer bewaakt en blokkeert.
☐	5. Geoblokkade	E	Een externe computer die je verkeer routeert en je IP-adres verbergt.
☐	6. Firewall	F	De staat van vrij zijn van tracking of openbaar toezicht.
☐	7. Privacy	G	Internetprovider die je verkeer vervoert en onversleutelde activiteit kan zien.
☐	8. Internetprovider	H	Het verpakken van datapakketten in een ander pakket voor veilig transport.

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

2. Internetprovider (ISP), die je verkeer logt tenzij het is versleuteld (8)

3. De maximale snelheid van gegevensoverdracht via een verbinding (11)

5. Een set regels die bepaalt hoe data over het netwerk wordt verzonden (8)

6. Een beveiligingssysteem dat ongeautoriseerd verkeer bewaakt en blokkeert (8)

7. De staat waarin je vrij bent van tracking of openbaar toezicht (7)

8. Een externe computer die je verkeer routeert en je IP-adres maskeert (6)

VERTICAAL

1. Een beperking die webtoegang verhindert op basis van de fysieke locatie (11)

4. Datapakketten in een ander pakket verpakken voor veilig transport (9)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

2 horizontaal: Internetprovider (ISP), die je verkeer logt tenzij het is versleuteld (8 letters):

3 horizontaal: De maximale snelheid van gegevensoverdracht via een verbinding (11 letters):

5 horizontaal: Een set regels die bepaalt hoe data over het netwerk wordt verzonden (8 letters):

6 horizontaal: Een beveiligingssysteem dat ongeautoriseerd verkeer bewaakt en blokkeert (8 letters):

7 horizontaal: De staat waarin je vrij bent van tracking of openbaar toezicht (7 letters):

8 horizontaal: Een externe computer die je verkeer routeert en je IP-adres maskeert (6 letters):

VERTICAAL

1 verticaal: Een beperking die webtoegang verhindert op basis van de fysieke locatie (11 letters):

4 verticaal: Datapakketten in een ander pakket verpakken voor veilig transport (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.

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

WOORDENLIJST

TUNNELING PROTOCOL BANDBREEDTE SERVER GEOBLOKKADE FIREWALL PRIVACY PROVIDER

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. TUNNELING**
- **B. PROTOCOL**
- **C. BANDBREEDTE**
- **D. SERVER**
- **E. GEOBLOKKADE**
- **F. FIREWALL**
- **G. PRIVACY**
- **H. PROVIDER**

DEFINITIES EN KOPPELVELDEN

1. De staat waarin je vrij bent van tracking of openbaar toezicht.
2. Een beperking die webtoegang verhindert op basis van de fysieke locatie.
3. Een set regels die bepaalt hoe data over het netwerk wordt verzonden.
4. Een beveiligingssysteem dat ongeautoriseerd verkeer bewaakt en blokkeert.
5. De maximale snelheid van gegevensoverdracht via een verbinding.
6. Een externe computer die je verkeer routeert en je IP-adres maskeert.
7. Internetprovider (ISP), die je verkeer logt tenzij het is versleuteld.
8. Datapakketten in een ander pakket verpakken voor veilig transport.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van VPN's te onthullen. Schrijf je antwoorden in de invulvelden.

1. LENUTINGN
2. BEABTRNDEED
3. GKOKOEDELAB
4. YRAVCPI
5. OCRLTPOO
6. EVSRRE
7. FLWALIER
8. VRIRPEDO

Bonusopdracht: Snel denken

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

1	Dingen die je met het woord 'tunnel' associeert			
2	Dingen die je je familie over VPN's zou leren			
3	Dingen op een website die je kunnen volgen			
4	Mythes over VPN's			
5	Woorden uit dit werkblad die je wilt onthouden			
6	Apparaten die een VPN kunnen gebruiken			
7	Dingen waartegen een VPN je niet kan beschermen			
8	Landen die je online graag zou 'bezoeken'			
9	Beloften van een goede VPN-aanbieder			
10	Manieren om een nep-wifinetwerk te herkennen			
11	Vragen die je over VPN's hebt			
12	VPN-diensten die je kent			
13	Woorden die met privacy te maken hebben			
14	Dingen die een VPN kan verbergen			
15	Redenen om een VPN te gebruiken in een café			

Controlepunt 8: Casestudy's VPN

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

SARAH (STUDENTE IN EEN KOFFIEZAAK)

👷 "Hoi! Ik zit bij Coffee & Bytes. Er is een onbeveiligd openbaar netwerk met de naam 'Free_Wi-Fi_No_Password'. Ik wil inloggen op mijn school-e-mail en mijn opdracht uploaden, maar ik ben bang voor hackers. Wat zijn de risico's van dit netwerk zonder VPN, en hoe beveiligt een VPN mijn gegevens?"

ALEX (REIZENDE STUDENT)

👷 "Oh nee! Ik ben voor een project in het buitenland en probeer een documentaire over biologie te kijken die op een server in mijn thuisland wordt gehost. Maar de site zegt 'Deze video is niet beschikbaar op je huidige locatie.' Waarom word ik geblokkeerd, en hoe kan een VPN me helpen om hem te kijken?"

Controlepunt 9: De code ontcijferen

Een VPN versleutelt je verkeer om het te beveiligen. Gebruik de onderstaande letter-naar-cijfersleutel om het cyberbeveiligingsbericht 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

2	5	19	3	8	5	18	13	10	5	16	18	9	22	1	3	25

13	5	20	5	5	14	22	5	9	12	9	7	5

20	21	14	14	5	12

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 die potentiële klanten hebben over het gebruik van virtuele privénetwerken.

Q1: Wat is een VPN en hoe werkt het?

Een Virtual Private Network (VPN) versleutelt je internetverbinding en leidt je verkeer via een beveiligde externe server. Dit verbergt je openbare IP-adres en beperkt wat lokale netwerkwaarnemers en je internetprovider kunnen zien van het verkeer dat via de VPN-tunnel loopt.

Q2: Waarom zou ik een VPN gebruiken?

Een VPN beschermt je digitale privacy, beveiligt je verbinding op openbare wifinetwerken (zoals in koffiebars of op luchthavens), kan throttling op basis van activiteit verminderen wanneer de internetprovider het type versleuteld verkeer niet kan herkennen, omzeilt geoblokkades om toegang te krijgen tot wereldwijde content en helpt bronnen voor werken op afstand te beveiligen.

Q3: Maakt een VPN me online volledig anoniem?

Nee. Een VPN verbergt je IP-adres en versleutelt verkeer, maar je kunt nog steeds worden gevolgd via browsercookies, actieve accounts (zoals Google of Facebook), browser-fingerprinting, of als je VPN-aanbieder je gegevens logt.

Q4: Zal een VPN mijn internetsnelheid vertragen?

Ja, een klein beetje. Het versleutelingsproces en de fysieke afstand tot de VPN-server zorgen voor extra latentie en overhead. De invloed verschilt per aanbieder, protocol, serverafstand, apparaat en netwerkomstandigheden.

Q5: Is het gebruik van een VPN legaal?

VPN-gebruik is in veel landen legaal, maar sommige rechtsgebieden beperken, reguleren of blokkeren VPN-diensten. Gebruikers moeten de actuele lokale wetgeving controleren voordat ze een VPN gebruiken. Raadpleeg voor meer informatie de gidsen over legaliteit op VPN.com.

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

Bekijk de meestgestelde vragen en antwoorden die potentiële klanten hebben over het gebruik van virtuele privénetwerken.

Q6: Kan ik een gratis VPN gebruiken?

Gratis VPN's kunnen vertrouwen op advertenties, beperkte functies, gebruiksanalyses, datalimieten of andere verdienmodellen. Gebruikers moeten het privacybeleid, het eigendom, de audits en het bedrijfsmodel van de aanbieder bekijken voordat ze de dienst gebruiken.

Q7: Wat is een "no-logs"-beleid?

Een no-logsbeleid beschrijft welke activiteits- en verbindingsgegevens een aanbieder zegt niet te bewaren. De exacte reikwijdte verschilt, dus lezers moeten het beleid en de bevindingen van onafhankelijke audits doornemen.

Q8: Hoe kies ik de beste VPN?

Let op auditeerde no-logsbeleid, sterke protocollen (WireGuard, OpenVPN), veilige serverlocaties, hoge snelheden, servers die alleen RAM gebruiken, een kill switch en een rechtsgebied buiten inlichtingenallianties (zoals de 5/9/14 Eyes).

Q9: Kan ik een VPN op mijn telefoon en smart-tv gebruiken?

Ja. Moderne VPN-aanbieders bieden speciale apps voor iOS, Android, macOS, Windows, Linux en smart-tv's, evenals routerinstellingen om alle apparaten in je thuisnetwerk te beschermen.

Q10: Wat is een kill switch?

Een kill switch is een beveiligingsfunctie die je apparaat automatisch van het internet loskoppelt als de VPN-verbinding wegvalt. Zo voorkom je dat je onversleutelde gegevens of je echte IP-adres lekken.

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

Verken technische en structurele aspecten van virtuele privénetwerken en beveiligde tunnelprotocollen.

Q1: Wat is het verschil tussen WireGuard, OpenVPN en IKEv2?

WireGuard is een modern, lichtgewicht protocol (slechts ongeveer 4.000 regels code) met hoge snelheden en snelle verbindingstijden. OpenVPN is een zeer veilig, beproefd open-sourceprotocol. IKEv2 is uitstekend voor mobiele apparaten, omdat het snel opnieuw verbinding kan maken bij het wisselen van netwerk. [3]

Q2: Wat is dubbele VPN- of multihoprouting?

Multihop routeert je verkeer achtereenvolgens via twee of meer VPN-servers. Dit voegt een tweede laag versleuteling toe en helpt je echte IP-adres verborgen te houden voor de tweede hop als een server wordt gecompromitteerd.

Q3: Wat is WebRTC-lekken en hoe voorkomt een VPN dat?

WebRTC is een browserprotocol dat je echte lokale en openbare IP-adres kan onthullen, zelfs als een VPN actief is. Premium-VPN's blokkeren of vervalsen WebRTC-verzoeken in hun desktop-/mobiele apps en browserextensies.

Q4: Wat zijn servers die alleen RAM gebruiken en waarom zijn ze belangrijk?

Traditionele servers schrijven gegevens naar harde schijven, die in beslag genomen of gecompromitteerd kunnen worden. Servers met alleen RAM (schijfloos) draaien volledig in vluchtig geheugen (RAM). Wanneer de server opnieuw wordt opgestart of uitgeschakeld, worden de gegevens in het geheugen gewist.

Q5: Hoe omzeilt obfuscatie VPN-blokkades?

Obfuscatie (of "stealth-VPN") laat VPN-verkeer eruitzien als gewoon HTTPS-verkeer (poort 443). Dat kan helpen om langs Deep Packet Inspection (DPI) te komen, die overheden of school- en kantoornetwerken gebruiken om VPN's te blokkeren.

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

Verken technische en structurele aspecten van virtuele privénetwerken en beveiligde tunnelprotocollen.

Q6: Wat is split tunneling en wanneer moet ik het gebruiken?

Met split tunneling kies je welke apps via de versleutelde VPN-tunnel lopen en welke rechtstreeks verbinding maken met internet. Gebruik het om gevoelige bank-apps via de VPN te laten lopen terwijl lokale games rechtstreeks verbinden, zodat je latentie door de VPN vermijdt.

Q7: Hoe werkt Forward Secrecy (Perfect Forward Secrecy)?

PFS zorgt ervoor dat voor elke sessie een unieke, tijdelijke versleutelingssleutel wordt gegenereerd. Zelfs als een privésleutel in de toekomst wordt gecompromitteerd, kan die niet worden gebruikt om eerdere of toekomstige sessies te ontsleutelen, omdat die onafhankelijke sleutels gebruikten.

Q8: Wat zijn de 5/9/14 Eyes-bondgenootschappen en waarom zou ik dat belangrijk vinden?

Jurisdictie kan van invloed zijn op de juridische procedure waarmee een aanbieder te maken kan krijgen, maar het praktische privacyrisico hangt ook af van welke gegevens de aanbieder bewaart, zijn technische architectuur, eigendom, transparantierapportages en auditgeschiedenis.

Q9: Wat is bescherming tegen DNS-lekken?

DNS-lekbescherming zorgt ervoor dat je apparaat opzoekverzoeken voor websites (DNS-verzoeken) verstuurt via de privé, versleutelde DNS-servers van de VPN in plaats van via de servers van je isp. Zo kan je isp niet volgen welke sites je bezoekt.

Q10: Kan een VPN het afknijpen van het internet door de internetprovider omzeilen?

Soms. Een VPN kan helpen wanneer een ISP selectief herkenbare activiteiten vertraagt, maar het lost congestie, datalimieten, snelheidslimieten op accountniveau of een slechte netwerkkwaliteit niet op.

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

Bekijk deze waardevolle feiten en inzichten uit de praktijk over de geschiedenis, de markt en de technologie van VPN's.

1. EERSTE VPN-PROTOCOL

PPTP (Point-to-Point Tunneling Protocol) is ontwikkeld door een groep leveranciers, waaronder Microsoft, en in juli 1999 gepubliceerd als RFC 2637 om VPN's voor toegang op afstand te ondersteunen. [6]

2. MARKTWAARDERING

De wereldwijde VPN-markt is snel gegroeid, aangedreven door de toenemende behoefte aan thuiswerken en de beveiligingseisen van bedrijven.

3. DE WIREGUARD-REVOLUTIE

WireGuard heeft een sterk gestroomlijnde codebase die is ontworpen voor efficiëntie, waardoor het gemakkelijker te controleren is op beveiligingslekken dan traditionele protocollen. [3]

4. STRIKTE AUDITSTANDAARDEN

Toonaangevende VPN-aanbieders huren externe auditors in (zoals Cure53 of PwC) voor onafhankelijke code-reviews en om te verifiëren dat ze geen gebruikersactiviteit loggen.

5. OORSPRONG VAN DE 5-EYES-ALLIANTIE

De Five Eyes-alliantie is ontstaan uit de UKUSA-overeenkomst voor signalenspionage uit 1946 tussen de VS en het VK, waarbij later Canada, Australië en Nieuw-Zeeland zich aansloten.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) onderzoekt de inhoud van pakketten en verkeerspatronen, niet alleen headers, en sommige firewalls gebruiken het om veelgebruikte VPN-protocollen te detecteren en te blokkeren.

7. ZAKELIJK GEBRUIK

Een groot percentage van de werknemers van ondernemingen wereldwijd gebruikt beveiligde VPN's om in te loggen op interne databases, waardoor het een belangrijke beveiligingsstandaard is.

8. GEDECENTRALISEERDE VPN'S

Gedecentraliseerde VPN's (dVPN's) verdelen verkeer over een netwerk van nodes die door peers worden beheerd, waardoor er minder afhankelijkheid is van één gecentraliseerde aanbieder.

9. TOR TEGENOVER VPN-ANONIMITEIT

Een VPN tunnelt verkeer via één aanbieder, terwijl Tor (The Onion Router) verkeer via drie vrijwilligersrelays stuurt (guard, middle en exit), zodat geen enkele relay beide uiteinden kent.

10. KOSTEN VAN DATALEKKEN

Het hanteren van een zero-trust-toegangsmodel met een VPN helpt organisaties intellectueel eigendom te beschermen en de financiële impact van datalekken te beperken.

Technische referenties en bronnen

Geciteerde publicaties, cryptografische specificaties en officiële documentstandaarden die in dit werkblad worden gebruikt.

ACADEMISCHE LITERATUUR EN BEVEILIGINGSSTANDAARDEN

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

SAMENVATTING VAN TECHNISCHE NORMEN

- Inkapselingsstandaarden: RFC 4301 definieert beveiligde IPsec/L2TP-internetpakketroutering.
- Tracking door de provider: DNS-verzoeken via de versleutelde VPN-tunnel routeren kan de zichtbaarheid van DNS voor de lokale provider verkleinen.
- Firewallbeheerprotocollen: verhulde stealth-pakketten omzeilen deep packet-filters.

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: B

DOCENTENNOTITIE

Een VPN-protocol bepaalt de regels voor het opzetten van de tunnel en het versleutelen van gegevens; de andere opties beschrijven kabels, advertentieblokkeerders en internetproviders.

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Afstand voegt latentie toe en een overbelaste server heeft minder capaciteit om te delen; schermresolutie, cookies en toetsenbordindeling hebben geen invloed op de verbindingssnelheid.

3 Vraag 3

Juist antwoord: C

DOCENTENNOTITIE

Op open netwerken kunnen anderen onversleutelde pakketten onderscheppen; een VPN versleutelt het verkeer, zodat onderschepte gegevens niet kunnen worden gelezen.

4 Vraag 4

Juist antwoord: B

DOCENTENNOTITIE

Geoblokkering koppelt het openbare IP-adres van een bezoeker aan een locatiedatabase en weigert toegang buiten toegestane gebieden.

5 Vraag 5

Juist antwoord: B

DOCENTENNOTITIE

De internetprovider kan zien dat je versleutelde gegevens naar een VPN-server stuurt, maar niet welke sites je bezoekt of waarnaar je zoekt.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Waar

DOCENTENNOTITIE

Websites zien het IP-adres van de VPN-server in plaats van het jouwe, waardoor je ongeveer locatie voor hen verborgen blijft.

7 Vraag 7

Juist antwoord: Onwaar

DOCENTENNOTITIE

Versleuteling en de extra hop naar de VPN-server verlagen de snelheid meestal licht; een VPN kan je basissnelheid niet verdubbelen.

8 Vraag 8

Juist antwoord: Waar

DOCENTENNOTITIE

Op onbeveiligde wifi kunnen packet-sniffingtools onversleuteld verkeer vastleggen, zoals logins die zonder HTTPS worden verstuurd.

9 Vraag 9

Juist antwoord: Waar

DOCENTENNOTITIE

Beheerders kunnen bekende VPN-poorten blokkeren, zoals poort 1194 van OpenVPN, of Deep Packet Inspection gebruiken om VPN-verkeer te detecteren.

10 Vraag 10

Juist antwoord: Onwaar

DOCENTENNOTITIE

Een no-logsbeleid is de belofte van een aanbieder om geen gegevens over je activiteit te bewaren; geen enkele wet verplicht VPN's om zoekopdrachten 30 dagen op te slaan.

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. Tunneling	A 2. Protocol	B 3. Bandbreedte	E 4. Server
C 5. Geoblokkade	D 6. Firewall	F 7. Privacy	G 8. Internetprovider

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 TUNNELING	2 BANDBREEDTE	3 GEOBLOKKADE	4 PROTOCOL
5 FIREWALL	6 SERVER		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 G – PRIVACY	2 E – GEOBLOKKADE	3 B – PROTOCOL	4 F – FIREWALL
5 C – BANDBREEDTE	6 D – SERVER	7 H – PROVIDER	8 A – TUNNELING

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen Tunneling, Protocol en Bandbreedte 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.

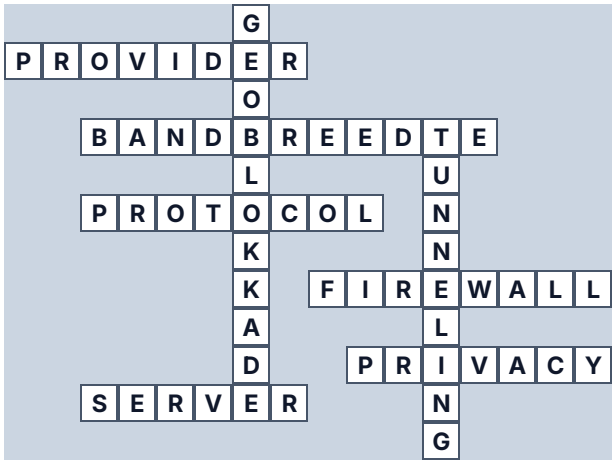
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



HORIZONTAAL

2 horizontaal: PROVIDER Internetprovider (ISP), die je verkeer logt tenzij het is versleuteld (8 letters)

3 horizontaal: BANDBREEDTE De maximale snelheid van gegevensoverdracht via een verbinding (11 letters)

5 horizontaal: PROTOCOL Een set regels die bepaalt hoe data over het netwerk wordt verzonden (8 letters)

6 horizontaal: FIREWALL Een beveiligingssysteem dat ongeautoriseerd verkeer bewaakt en blokkeert (8 letters)

7 horizontaal: PRIVACY De staat waarin je vrij bent van tracking of openbaar toezicht (7 letters)

8 horizontaal: SERVER Een externe computer die je verkeer routeert en je IP-adres maskeert (6 letters)

VERTICAAL

1 verticaal: GEOBLOKKADE Een beperking die webtoegang verhindert op basis van de fysieke locatie (11 letters)

4 verticaal: TUNNELING Datapakketten in een ander pakket verpakken voor veilig transport (9 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. LENUTINGN — **TUNNELING**
2. BEABTRNDEED — **BANDBREEDTE**
3. GKOKOEDELAB — **GEOBLOKKADE**
4. YRAVCPI — **PRIVACY**
5. OCRLTPOO — **PROTOCOL**
6. EVSRRE — **SERVER**
7. FLWALIER — **FIREWALL**
8. VRIRPEDO — **PROVIDER**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"BESCHERM JE PRIVACY MET EEN VEILIGE TUNNEL"

Antwoordsleutel casestudy's

A Scenario A: Beveiliging van openbare netwerken

SNIFFING EN VERSLEUTELING | Het dilemma van Sarah

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Risico's: Packet sniffing, onderschepping van gegevens en man-in-the-middle-aanvallen. Iemand op hetzelfde netwerk van de koffiezaak zou haar inloggegevens of huiswerkbestand kunnen onderscheppen.
- VPN-bescherming: versleutelt de payloads van netwerkpakketten, waardoor onderschept tunnelverkeer onleesbaar is voor passieve afluisteraars op het lokale netwerk wanneer de VPN correct is geconfigureerd.

B Scenario B: Toegang tot geblokkeerde bronnen

GEOBLOKKADES EN IP-ADRESSEN | Het dilemma van Alex

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Reden van blokkade: de streamingdienst gebruikt geoblokkering, waarbij het lokale IP-adres van de reiziger wordt gekoppeld aan zijn fysieke land en op basis van territoriale licenties wordt geblokkeerd.
- Hoe VPN helpt: Zijn echte locatie maskeren door verkeer te routeren via een server in zijn thuisland. De site ziet het IP-adres van het thuisland, waardoor toegang mogelijk is.