Naam: _____ Datum: _____ Score: _____

Proxy versus VPN Werkblad

Proxyservers en virtuele privénetwerken vergelijken, verschillen in versleuteling en routering per toepassing versus systeembreed

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

- Vergelijk applicatieproxy's met systeembrede VPN-versleuteling.
- SOCKS5-mogelijkheden herkennen in vergelijking met eenvoudige HTTP-proxy's.
- Analyseer hoe browsergebaseerde proxy's achtergrondapps onbeschermd laten.
- Begrijp hoe internetproviders onversleuteld verkeer via proxytunnels loggen.
- Kies de juiste routeringstool op basis van de behoefte aan snelheid en beveiliging.

INSTRUCTIES VOOR HET WERKBLAD PROXYVERGELIJKING

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 het vergelijken van proxy's en VPN's. Sluit af met de bonusopdracht Snel denken.

PROXY VERSUS VPN (INLEIDING)

Proxy's en VPN's hebben verschillende functies voor digitale privacy. Een proxyserver fungeert als doorverwijzing op toepassingsniveau en maskeert je IP-adres voor specifieke programma's zonder de gegevens te versleutelen. Een VPN werkt op netwerkniveau en beveiligt al het systeemverkeer met versleuteling. Welk hulpmiddel het beste past, hangt af van je beveiligingsbehoeften.

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

Controlepunt 1: Meerkeuzeopdracht

1. Op welke laag van het OSI-model werkt een standaard HTTP-proxy?

- A. Fysieke laag
- B. Netwerklaag
- C. Toepassingslaag
- D. Datalinklaag

2. Wat is een belangrijk protocolvoordeel van SOCKS5 ten opzichte van standaard HTTP-proxy's?

- A. Het dwingt volledige versleuteling van de inhoud af
- B. Het ondersteunt elke vorm van TCP/UDP-routering
- C. Het is immuun voor DNS-lekken
- D. Het werkt rechtstreeks in de kernelruimte

3. Waarom is een VPN over het algemeen veiliger dan een proxyserver?

- A. Het draait op snellere externe hardware
- B. Het versleutelt al het netwerkverkeer op systeemniveau
- C. Het vereist geen lokale routeringstabellen
- D. Het elimineert netwerklatentie volledig

4. Welk type proxy leidt verkeer standaard om zonder enige versleuteling?

- A. Een eenvoudige HTTP-proxy
- B. Een versleutelde HTTPS-proxy
- C. Een beveiligde WireGuard-client
- D. Een geobfusceerde VPN-server

5. Wat gebeurt er met achtergrondverkeer van applicaties wanneer je een browserproxy gebruikt?

- A. Het wordt automatisch versleuteld
- B. Het wordt geblokkeerd door de proxyserver
- C. Het wordt gerouteerd via de proxytunnel
- D. Het omzeilt de proxy en maakt je IP-adres zichtbaar

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Een SOCKS5-proxy versleutelt alle pakketinhoud die via de server loopt.

- ( ) Waar
- ( ) Onwaar

7 Vraag 7

7. Een VPN werkt op de netwerklaag om al het systeemverkeer te beveiligen.

- ( ) Waar
- ( ) Onwaar

8 Vraag 8

8. Proxy's zijn over het algemeen sneller dan VPN's omdat ze diepgaande pakketversleuteling uitvoeren.

- ( ) Waar
- ( ) Onwaar

9 Vraag 9

9. Het configureren van een proxy vereist dat je verkeersomleidingen instelt binnen specifieke apps.

- ( ) Waar
- ( ) Onwaar

10 Vraag 10

10. Een proxy gebruiken beveiligt je dataverkeer niet tegen tracking door de lokale internetprovider.

- ( ) Waar
- ( ) Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Een _____ op applicatielaag leidt specifiek browserverkeer om zonder andere apps te beveiligen.

2. Een robuuste _____ verpakt en versleutelt alle datapakketten van het apparaat.

3. Het proxyprotocol _____ zit tussen de applicatie- en transportlaag.

4. HTTP-proxy's werken op de _____ van het OSI-model.

5. Standaard proxyservers missen _____ van de payload, waardoor data kwetsbaar blijft.

6. Een VPN biedt bescherming die _____ werkt voor alle netwerkadapters.

WOORDENBANK

HTTP-PROXY SOCKS5 SYSTEEMBREED TOEPASSINGSLAAG UDP-RELAY
VERSLEUTELING VPN-TUNNEL ZICHTBAARHEID

Schrijf hier je antwoorden:

1. 2.

3. 4.

5. 6.

Controlepunt 4: Netwerkbegrippen koppelen

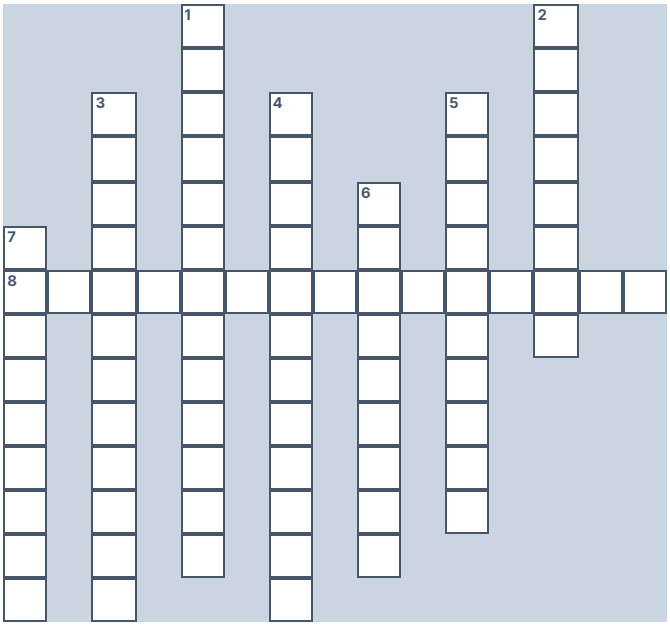
DEFINITIES KOPPELEN

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. HTTP-proxy	A	Routering op besturingssysteemniveau die al het toepassingsverkeer versleutelt.
☐	2. SOCKS5-proxy	B	De applicatielaag, waarop standaard webproxyprotocollen werken.
☐	3. VPN-tunnel	C	Het vermogen van SOCKS5 om naast TCP ook UDP door te sturen, anders dan gewone HTTP-proxy's.
☐	4. Systeembrede	D	Clientextensie die verkeer alleen verbergt binnen de sandbox van de browser.
☐	5. OSI-laag 7	E	Versleuteling en inkapseling van al het achtergrondverkeer van het apparaat.
☐	6. UDP-ondersteuning	F	Verkeerstoestand waarin onversleutelde proxygegevens zichtbaar blijven voor internetproviders.
☐	7. Browserproxy	G	Proxy op toepassingslaag die specifiek browserverkeer omleidt.
☐	8. Zichtbaarheid voor de internetprovider	H	Proxyprotocol tussen de applicatie- en transportlaag, zonder versleuteling.

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

8. De applicatielaag waarop standaard webproxyprotocollen werken (15)

VERTICAAL

1. Verkeerstoestand waarin onversleutelde proxydata zichtbaar blijft voor internetproviders (13)

2. Het vermogen van SOCKS5 om naast TCP ook UDP door te sturen, in tegenstelling tot gewone HTTP-proxy's (8)

3. Routering op besturingssysteemniveau die al het applicatieverkeer versleutelt (12)

4. Clientextensie die alleen verkeer binnen de browsersandbox verbergt (12)

5. Proxyprotocol tussen de applicatie- en transportlaag, zonder versleuteling (10)

6. Versleuteling en inkapseling van al het achtergrondverkeer van een apparaat (9)

7. Proxy op applicatielaag die specifiek webbrowserverkeer omleidt (9)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

8 horizontaal: De applicatielaag waarop standaard webproxyprotocollen werken (15 letters):

VERTICAAL

1 verticaal: Verkeerstoestand waarin onversleutelde proxydata zichtbaar blijft voor internetproviders (13 letters):

2 verticaal: Het vermogen van SOCKS5 om naast TCP ook UDP door te sturen, in tegenstelling tot gewone HTTP-proxy's (8 letters):

3 verticaal: Routering op besturingssysteemniveau die al het applicatieverkeer versleutelt (12 letters):

4 verticaal: Clientextensie die alleen verkeer binnen de browsersandbox verbergt (12 letters):

5 verticaal: Proxyprotocol tussen de applicatie- en transportlaag, zonder versleuteling (10 letters):

6 verticaal: Versleuteling en inkapseling van al het achtergrondverkeer van een apparaat (9 letters):

7 verticaal: Proxy op applicatielaag die specifiek webbrowserverkeer omleidt (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.

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

WOORDENLIJST

HTTPPROXY SOCKSPROXY VPNTUNNEL SYSTEEMBREED TOEPASSINGSLAAG
UDPRELAY BROWSERPROXY ZICHTBAARHEID

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. HTTPPROXY**
- **B. SOCKSPROXY**
- **C. VPNTUNNEL**
- **D. SYSTEEMBREED**
- **E. TOEPASSINGSLAAG**
- **F. UDPRELAY**
- **G. BROWSERPROXY**
- **H. ZICHTBAARHEID**

DEFINITIES EN KOPPELVELDEN

1. De applicatielaag waarop standaard webproxyprotocollen werken.
2. Het vermogen van SOCKS5 om naast TCP ook UDP door te sturen, in tegenstelling tot gewone HTTP-proxy's.
3. Proxy op applicatielaag die specifiek webbrowserverkeer omleidt.
4. Clientextensie die alleen verkeer binnen de browsersandbox verbergt.
5. Versleuteling en inkapseling van al het achtergrondverkeer van een apparaat.
6. Routering op besturingssysteemniveau die al het applicatieverkeer versleutelt.
7. Verkeerstoestand waarin onversleutelde proxydata zichtbaar blijft voor internetproviders.
8. Proxyprotocol tussen de applicatie- en transportlaag, zonder versleuteling.

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. RPPTHOXYT
2. LVETPNNUN
3. TEGOASNSLPIGSAA
4. XPSORYEORBRW
5. OPYOKRSSXC
6. DEREEEBSYMST
7. UYELADRP
8. RCTBEADZAIIHH

Bonusopdracht: Snel denken

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

1	Verschillen tussen een proxy en een VPN			
2	Dingen die zonder VPN onversleuteld blijven			
3	Manieren om een nep-wifinetwerk te herkennen			
4	Dingen die een tussenpersoon in het dagelijks leven doet			
5	Situaties waarin een proxy genoeg is			
6	Apparaten die een VPN kunnen gebruiken			
7	Soorten proxy's die je kent			
8	Dingen die een VPN kan verbergen			
9	Mythes over VPN's			
10	Beloften van een goede VPN-aanbieder			
11	Dingen waartegen een VPN je niet kan beschermen			
12	Woorden uit dit werkblad die je wilt onthouden			
13	Redenen om een VPN te gebruiken tijdens het reizen			
14	Situaties waarin je een VPN wilt			
15	Plekken waar je een VPN zou gebruiken			

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 op een open netwerk met de naam 'Free_Wi-Fi_No_Password'. Ik moet inloggen op mijn school-e-mail, en een vriend zegt dat een gratis browserproxy genoeg is om veilig te blijven. Beschermt een proxy mijn inlog en bestanden, of heb ik een VPN nodig?"

ALEX (REIZENDE STUDENT)

👷 "Ik ben in het buitenland en een documentaire over biologie die in mijn thuisland wordt gehost, zegt 'Deze video is niet beschikbaar op je huidige locatie.' Een klasgenoot gebruikt een proxy en ik heb een VPN. Waarom word ik geblokkeerd, en welke tool werkt beter?"

Controlepunt 9: De code ontcijferen

Ontcijfer om je training proxyvergelijking af te ronden dit geheime bericht over veilig tunnelen.

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

12	5	9	4		10	5		22	5	18	11	5	5	18		15	13		22	9	1

5	5	14		16	18	15	24	25

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: Wat is een proxyserver?

Een proxyserver is een tussenpersoon die verzoeken doorstuurt tussen je applicatie en de bestemmingsserver. De website ziet het IP-adres van de proxy in plaats van het jouwe, maar alleen verkeer van apps die zijn ingesteld om de proxy te gebruiken, wordt omgeleid, en een eenvoudige proxy versleutelt dat verkeer niet.

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 een proxy een VPN?

Nee. Een proxy stuurt verkeer door voor specifieke apps, meestal zonder versleuteling. Een VPN bouwt een versleutelde tunnel op de netwerklaag die al het verkeer van het apparaat draagt, inclusief apps op de achtergrond.

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 proxy gebruiken?

Dat kan, maar gratis proxy's worden vaak beheerd door onbekende exploitanten. Omdat een eenvoudige proxy het verkeer niet versleutelt, kan de exploitant niet-versleutelde pagina's zien en zelfs aanpassen. Controleer wie de dienst beheert voordat je hem gebruikt.

Q7: Bewaart een proxy logs?

Dat kan. Een proxy verwerkt elk verzoek dat hij doorstuurt, dus de beheerder kan je IP-adres, de sites die je bezoekt en het tijdstip vastleggen. Controleer wie hem beheert en wat zijn privacybeleid zegt.

Q8: Wanneer is een proxy voldoende?

Een proxy kan genoeg zijn voor taken met een laag risico, zoals het wijzigen van de schijnbare locatie van één browser. Voor bankieren, openbare wifi of het beschermen van elke app op een apparaat is een VPN de veiligere keuze, omdat die al het verkeer versleutelt.

Q9: Kan een proxy alle apps op mijn telefoon beschermen?

Nee. Alleen apps die de proxy-instelling respecteren gebruiken die; de rest maakt rechtstreeks verbinding. Een VPN-app routeert in plaats daarvan alle apps van de telefoon via de versleutelde tunnel.

Q10: Wat is een SOCKS5-proxy?

SOCKS5, gedefinieerd in RFC 1928, is een proxyprotocol dat tussen de applicatie- en transportlaag zit. Het kan TCP-verbindingen en UDP-datagrammen doorsturen en ondersteunt authenticatie, maar heeft geen ingebouwde versleuteling. [1]

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

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

Q1: Op welke netwerklagen werken proxy's en VPN's?

Een HTTP-proxy werkt op de applicatielaag (laag 7) en begrijpt webverzoeken. SOCKS5 zit tussen de applicatie- en transportlaag. VPN-protocollen zoals IPsec of WireGuard werken op de netwerklaag, zodat ze al het IP-verkeer van het apparaat kunnen vervoeren.

Q2: Blijft een HTTPS-site versleuteld via een proxy?

Ja. Als je een HTTPS-site opent via een proxy, loopt de TLS-versleuteling end-to-end tussen je browser en de site, zodat de proxy het domein ziet maar niet de inhoud van de pagina. Gewone HTTP-pagina's blijven leesbaar.

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 is een transparante proxy en wie gebruikt die?

Een transparante proxy onderschept verkeer zonder dat er op het apparaat van de gebruiker iets hoeft te worden ingesteld. Scholen, bedrijven en internetproviders gebruiken ze voor caching of contentfiltering. Gebruikers weten vaak niet dat er een actief is, en hij biedt hun geen privacy.

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: Waarom kan een proxy sneller aanvoelen dan een VPN-verbinding?

Een eenvoudige proxy slaat versleuteling over en verwerkt alleen het verkeer van één app, waardoor er minder verwerking nodig is. Een VPN versleutelt elk pakket van het apparaat. Bij moderne protocollen is het verschil vaak klein, en biedt de proxy veel minder bescherming.

Q8: Kunnen websites zien dat ik een proxy of een VPN gebruik?

Vaak wel. Veel websites vergelijken IP-adressen met lijsten van bekende proxy- en VPN-servers, en HTTP-proxy's kunnen headers toevoegen zoals Via of X-Forwarded-For. Streamingdiensten blokkeren vaak allebei.

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 proxy het afknijpen door de internetprovider stoppen?

Zelden. Een gewone proxy versleutelt verkeer niet, dus de ISP kan nog steeds zien om wat voor soort activiteit het gaat. Een VPN verbergt de soorten verkeer, maar geen van beide hulpmiddelen lost congestie of datalimieten 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. SOCKS-STANDAARD

SOCKS Protocol Version 5 is in maart 1996 door de IETF gepubliceerd als RFC 1928 en is nog steeds de referentiespecificatie voor SOCKS5-proxy's die tegenwoordig door browsers en apps worden gebruikt. [1]

2. SHIM-LAAG

RFC 1928 beschrijft SOCKS als een tussenlaag (shim) tussen de applicatielaag en de transportlaag, waardoor het geen verkeer op netwerklaag, zoals ICMP, kan doorsturen. [1]

3. UDP-RELAY

SOCKS5 heeft de opdracht UDP ASSOCIATE toegevoegd, waarmee een proxy UDP-datagrammen kan doorsturen, en niet alleen TCP-verbindingen, iets wat gewone HTTP-proxy's niet aankunnen. [1]

4. STANDAARD SOCKS-POORT

SOCKS5-clients maken standaard verbinding met de proxyserver op TCP-poort 1080, zoals gedefinieerd in RFC 1928; veel proxydiensten laten gebruikers andere poorten kiezen. [1]

5. HTTP-TUSSENSCHAKELS

De HTTP-standaard (RFC 9110) definieert een proxy als een door de client gekozen agent die berichten doorstuurt en verzoeken doorgeeft richting de oorspronkelijke server.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) onderzoekt de inhoud van pakketten en verkeerspatronen; onversleuteld proxyverkeer is er volledig zichtbaar voor, terwijl VPN-verkeer veel minder prijsgeeft.

7. VPN'S OP NETWERKLAAG

IPsec, beschreven in NIST SP 800-77, beschermt verkeer op netwerklaag, zodat de IP-pakketten van elke applicatie kunnen worden beveiligd zonder instellingen per app. [2]

8. ALLEEN BROWSERBEREIK

Een proxy die in één browser is ingesteld, geldt alleen voor die browser; e-mailprogramma's, games en systeemupdates blijven de normale verbinding van het apparaat gebruiken.

9. TOR TEGENOVER PROXY'S

Tor stuurt verkeer via drie relays van vrijwilligers (guard, middle en exit) en wordt meestal bereikt via een lokale SOCKS-proxy, wat lagen toevoegt die één proxy niet kan bieden.

10. SNELHEID ALS COMPROMIS

Proxy's lijken soms sneller omdat ze versleuteling overslaan, maar moderne VPN-protocollen zoals WireGuard voegen weinig overhead toe en beschermen al het verkeer van het apparaat.

Technische referenties en bronnen

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

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Antwoordsleutel: proxyservers en virtuele privénetwerken vergelijken: verschillen in versleuteling en routering per applicatie versus systeembreed

1 **OSI-laag van proxy's** PROTOCOLLEN — **Juist antwoord: C**

DOCENTENNOTITIE

Standaard HTTP/HTTPS-proxy's werken op de applicatielaag (laag 7) en leiden specifiek browserverkeer om. Ze beschikken niet over systeembrede netwerkroutering. Bron: Tor Project Foundation.

2 **Vraag 2** — **Juist antwoord: B**

DOCENTENNOTITIE

SOCKS5 stuurt TCP- en UDP-verkeer door tussen de applicatie- en transportlaag maar versleutelt standaard niet, terwijl HTTP-proxy's webverzoeken afhandelen.

3 **VPN-systeemversleuteling** WIFI-BEVEILIGING — **Juist antwoord: B**

DOCENTENNOTITIE

Een VPN kapselt al het verkeer van het besturingssysteem systeembreed in en versleutelt het, terwijl een proxy alleen het verkeer van specifiek geconfigureerde applicaties omleidt. Bron: Deloitte Advisory.

4 **Ontbrekende proxyversleuteling** ROUTERINGSBEHEER — **Juist antwoord: A**

DOCENTENNOTITIE

HTTP-proxy's sturen browserverkeer door op applicatielaag zonder de payload van pakketten te versleutelen, waardoor je netwerkbeheerder of provider je contentverkeer nog steeds kan herleiden. Bron: IETF Proxy Vulnerabilities.

5 **Kwetsbaarheid bij omzeiling** PRIVACY — **Juist antwoord: D**

DOCENTENNOTITIE

Browserproxy's passen regels alleen toe op de webbrowser zelf. Apps op de achtergrond, updates van het besturingssysteem en e-mailprogramma's omzeilen de proxy, waardoor je eigen IP-adres zichtbaar wordt. Bronvermelding: W3C Consortium.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Onwaar

DOCENTENNOTITIE

SOCKS5 stuurt verkeer door tussen de applicatie- en transportlaag maar versleutelt standaard niet, dus de inhoud van pakketten blijft onderweg leesbaar.

7 Tunnels op netwerklaag SNELHEDEN

Juist antwoord: Waar

DOCENTENNOTITIE

Doordat een VPN op de netwerklaag werkt, routeert en versleutelt het uitgaand verkeer van je apparaat, waardoor het verkeer op systeemniveau beter beschermd is. Bronvermelding: Deloitte Advisory.

8 Beperking van proxyversleuteling SNIFFINGRISICO

Juist antwoord: Onwaar

DOCENTENNOTITIE

Proxy's kunnen soms sneller zijn, maar dat komt doordat ze GEEN versleuteling uitvoeren. Zonder versleuteling zijn gegevens kwetsbaar voor inspectie. Bron: IETF Proxy Vulnerabilities.

9 Omleiding op appniveau FIREWALLS

Juist antwoord: Waar

DOCENTENNOTITIE

In tegenstelling tot systeembrede VPN's vereisen proxyservers handmatige configuratie in de browserinstellingen of in applicatiespecifieke proxyvelden. Bron: W3C Consortium.

10 Trackingrisico via de provider NO-LOGS

Juist antwoord: Waar

DOCENTENNOTITIE

Omdat standaard HTTP-/SOCKS5-proxy's de payload niet versleutelen, houdt je lokale internetprovider volledig zicht op je online activiteiten. Bronvermelding: EDRi Retention Guidelines.

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

G 1. HTTP-proxy	H 2. SOCKS5-proxy	E 3. VPN-tunnel	A 4. Systeembrede
B 5. OSI-laag 7	C 6. UDP-ondersteuning	D 7. Browserproxy	F 8. Zichtbaarheid voor de internetprovider

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 HTTP-PROXY	2 VPN-TUNNEL	3 SOCKS5	4 TOEPASSINGSLAAG
5 VERSLEUTELING	6 SYSTEEMBREED		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 E – TOEPASSINGSLAAG	2 F – UDPRELAY	3 A – HTTPPROXY	4 G – BROWSERPROXY
5 C – VPNTUNNEL	6 D – SYSTEEMBREED	7 H – ZICHTBAARHEID	8 B – SOCKSPROXY

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen HTTP-proxy, SOCKS5-proxy en VPN-tunnel 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.

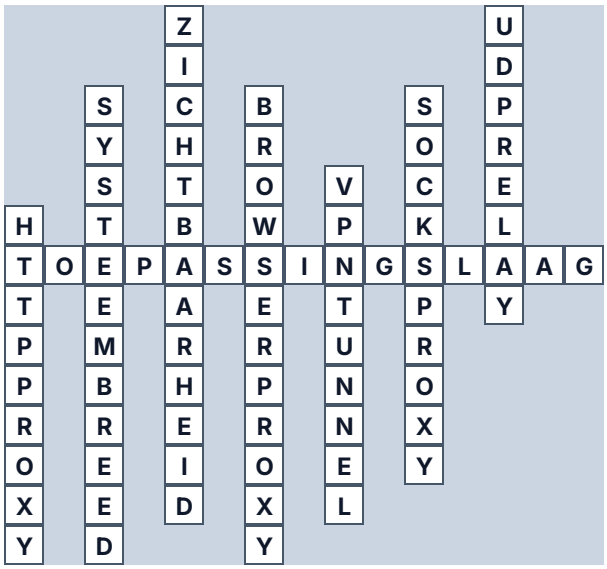
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

8 horizontaal: TOEPASSINGSLAAG De applicatielaag waarop standaard webproxyprotocollen werken (15 letters)

VERTICAAL

1 verticaal: ZICHTBAARHEID Verkeerstoestand waarin onversleutelde proxydata zichtbaar blijft voor internetproviders (13 letters)

2 verticaal: UDPRELAY Het vermogen van SOCKS5 om naast TCP ook UDP door te sturen, in tegenstelling tot gewone HTTP-proxy's (8 letters)

3 verticaal: SYSTEEMBREED Routering op besturingssysteemniveau die al het applicatieverkeer versleutelt (12 letters)

4 verticaal: BROWSERPROXY Clientextensie die alleen verkeer binnen de browsersandbox verbergt (12 letters)

5 verticaal: SOCKSPROXY Proxyprotocol tussen de applicatie- en transportlaag, zonder versleuteling (10 letters)

6 verticaal: VPNTUNNEL Versleuteling en inkapseling van al het achtergrondverkeer van een apparaat (9 letters)

7 verticaal: HTTPPROXY Proxy op applicatielaag die specifiek webbrowserverkeer omleidt (9 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. RPPTHOXYT — HTTPPROXY
2. LVETPNNUN — VPNTUNNEL
3. TEGOASNSLPIGSAA — TOEPASSINGSLAAG
4. XPSORYEORBRW — BROWSERPROXY
5. OPYOKRSSXC — SOCKSPROXY
6. DEREEEBSYMST — SYSTEEMBREED
7. UYELADRP — UDPRELAY
8. RCTBEADZAIIHH — ZICHTBAARHEID

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"LEID JE VERKEER OM VIA EEN PROXY"

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.
- Proxy versus VPN: een gewone browserproxy versleutelt haar verkeer niet. Een VPN versleutelt alles op het apparaat, waardoor onderschepte pakketten onleesbaar zijn voor lokale gluurders.

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.
- Wat werkt beter: beide geven hem een IP-adres uit zijn thuisland, maar een proxy dekt alleen de geconfigureerde app, terwijl een VPN ook al het verkeer van zijn apparaat versleutelt.