Naam: _____ Datum: _____ Score: _____

WireGuard versus OpenVPN Werkblad

De protocollen WireGuard en OpenVPN vergelijken, inclusief omvang van de codebase, snelheid en cryptografische standaarden

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 de complexiteit van de codebase en de auditsnelheid van protocollen.
- Analyseer de prestatiewinst van het draaien in kernelruimte.
- Vergelijk OpenSSL-ciphers met de moderne cryptografie van WireGuard.
- Publieke en privésleutelparen instellen voor handshakes tussen peers.
- VPN-verkeer routeren via TCP- en UDP-firewallpoorten.

INSTRUCTIES VOOR HET WERKBLAD PROTOCOLVERGELIJKING

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 auditen van moderne protocollen. Sluit af met de bonusopdracht Snel denken.

WIREGUARD VERSUS OPENVPN (INLEIDING)

Het kiezen van een VPN-protocol vereist een afweging tussen snelheid en configuratiemogelijkheden. OpenVPN is al tientallen jaren de standaard en biedt flexibele TCP/UDP-configuraties. WireGuard is een moderne vervanger die rechtstreeks in de kernelruimte draait met slechts 4,000 regels code. Inzicht in de verschillen tussen protocollen is essentieel om je beveiligde netwerken te optimaliseren.

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

Controlepunt 1: Meerkeuzeopdracht

1. Wat is de geschatte omvang van de codebase van het WireGuard-protocol?

- A. Ongeveer 70.000 regels
- B. Meer dan 100.000 regels
- C. Minder dan 1.000 regels
- D. Ongeveer 4.000 regels

2. In welk deel van het besturingssysteem draait WireGuard?

- A. Gebruikersruimte
- B. Kernelruimte
- C. Toepassingsruimte
- D. Virtuele ruimte

3. Op welke cryptografische bibliotheek vertrouwt OpenVPN voornamelijk?

- A. ChaCha20-Poly1305
- B. De cryptografische bibliotheek OpenSSL
- C. Het Noise-protocolframework
- D. Platte DES-codering

4. Wat is een belangrijk prestatievoordeel van WireGuard ten opzichte van OpenVPN?

- A. Snellere verbindingshandshakes en lagere latentie
- B. Het omzeilen van de noodzaak van openbare IP-adressen
- C. Ingebouwde native ondersteuning voor oude inbelverbindingen
- D. Geen enkele accubelasting op mobiele apparaten

5. Hoe authenticeert WireGuard peerverbindingen?

- A. Door standaardwachtwoorden van gebruikers uit te wisselen
- B. Door domeinregistratiecertificaten te verifiëren
- C. Door statische paren van openbare en privésleutels te gebruiken
- D. Door serienummers van hardware te controleren

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. De compacte codebase van WireGuard maakt controle aanzienlijk eenvoudiger.

Waar Onwaar

7 Vraag 7

7. OpenVPN is over het algemeen sneller dan WireGuard omdat het in de kernelruimte draait.

Waar Onwaar

8 Vraag 8

8. OpenVPN is zeer configureerbaar en ondersteunt zowel UDP als TCP.

Waar Onwaar

9 Vraag 9

9. WireGuard gebruikt moderne cryptografie zoals ChaCha20 voor snelle versleuteling van pakketten.

Waar Onwaar

10 Vraag 10

10. WireGuard vereist complexe opstellingen met een certificeringsinstantie om te authenticeren.

Waar Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Het moderne protocol _____ werkt rechtstreeks in de kernel van het besturingssysteem.

2. Het oudere protocol _____ vertrouwt op de cryptobibliotheek OpenSSL.

3. Code uitvoeren in de _____ verkleint de overhead van contextwisselingen.

4. OpenVPN draait in de _____ en routeert pakketten via virtuele interfaces.

5. WireGuard gebruikt per peer een openbare en een privésleutel, samen een _____ , om verbindingspeers te identificeren.

6. Een kleine codebase verbetert de _____ van de software, wat de beveiliging ten goede komt.

WOORDENBANK

AUDITEERBAARHEID COMPACTE CODE KERNEL SPACE OPENSSL OPENVPN
SLEUTELPAAR USER SPACE WIREGUARD

Schrijf hier je antwoorden:

1. **2.**

3. **4.**

5. **6.**

Controlepunt 4: Netwerkbegrippen koppelen

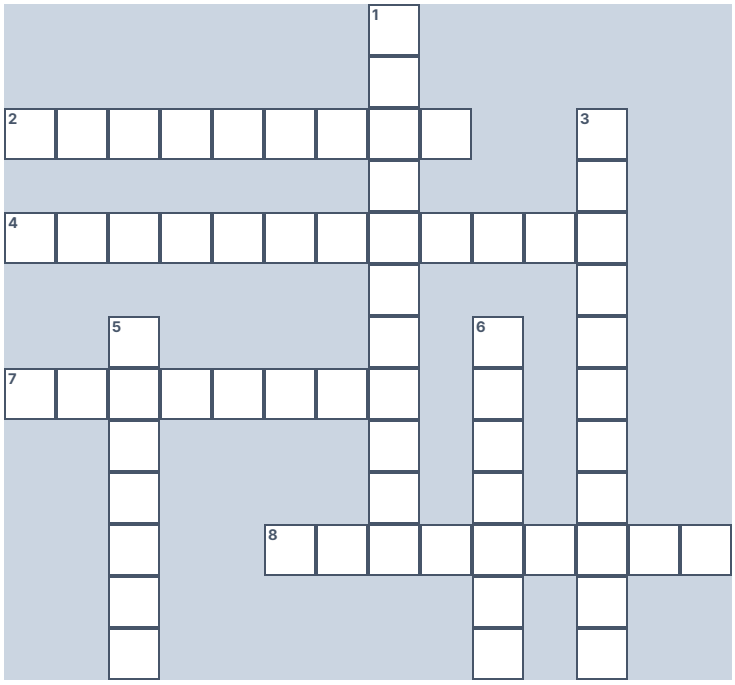
DEFINITIES KOPPELEN

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. WireGuard	A	Uitvoeringsgebied waar OpenVPN draait, wat overhead door contextwisselingen veroorzaakt.
☐	2. OpenVPN	B	De compacte omvang van de WireGuard-codebase, waardoor auditing veel eenvoudiger is.
☐	3. Kernelruimte	C	Cryptografische bibliotheek waarop OpenVPN vertrouwt voor cipheralgoritmen.
☐	4. Gebruikersruimte	D	Transportprotocollen die OpenVPN ondersteunt; WireGuard zelf draait alleen over UDP.
☐	5. 4,000 regels	E	Uitvoeringsgebied van het besturingssysteem waarin WireGuard draait voor snelheid.
☐	6. OpenSSL	F	Asymmetrische tokens die WireGuard gebruikt om verbindingen tussen peers te verifiëren.
☐	7. Sleutelpaar	G	Modern VPN-protocol, ontworpen voor hoge snelheid en eenvoudige code-audits.
☐	8. TCP/UDP	H	Robuust ouder protocol met een grote, complexe configuratiecodebasis.

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. Modern VPN-protocol, ontworpen voor hoge snelheid en eenvoudige code-audits (9)

4. De compacte omvang van de WireGuard-codebase, waardoor auditing veel eenvoudiger is (12)

7. Transportprotocollen die OpenVPN ondersteunt; WireGuard zelf werkt alleen via UDP (8)

8. Uitvoeringsgebied waarin OpenVPN draait, wat overhead door contextwisselingen veroorzaakt (9)

VERTICAAL

1. Uitvoeringsgebied van het besturingssysteem waarin WireGuard voor de snelheid draait (11)

3. Asymmetrische sleutels die WireGuard gebruikt om verbindingen met peers te verifiëren (11)

5. Robuust ouder protocol met een grote, complexe configuratiecodebase (7)

6. Cryptografische bibliotheek waarop OpenVPN vertrouwt voor versleutelingsalgoritmen (7)

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: Modern VPN-protocol, ontworpen voor hoge snelheid en eenvoudige code-audits (9 letters):

4 horizontaal: De compacte omvang van de WireGuard-codebase, waardoor auditing veel eenvoudiger is (12 letters):

7 horizontaal: Transportprotocollen die OpenVPN ondersteunt; WireGuard zelf werkt alleen via UDP (8 letters):

8 horizontaal: Uitvoeringsgebied waarin OpenVPN draait, wat overhead door contextwisselingen veroorzaakt (9 letters):

VERTICAAL

1 verticaal: Uitvoeringsgebied van het besturingssysteem waarin WireGuard voor de snelheid draait (11 letters):

3 verticaal: Asymmetrische sleutels die WireGuard gebruikt om verbindingen met peers te verifiëren (11 letters):

5 verticaal: Robuust ouder protocol met een grote, complexe configuratiecodebase (7 letters):

6 verticaal: Cryptografische bibliotheek waarop OpenVPN vertrouwt voor versleutelingsalgoritmen (7 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.

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

WOORDENLIJST

WIREGUARD OPENVPN KERNELSPACE USERSPACE COMPACTECODE
OPENSSL SLEUTELPAAR TCPENUDP

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. WIREGUARD

B. OPENVPN

C. KERNELSPACE

D. USERSPACE

E. COMPACTECODE

F. OPENSSL

G. SLEUTELPAAR

H. TCPENUDP

DEFINITIES EN KOPPELVELDEN

1. Cryptografische bibliotheek waarop OpenVPN vertrouwt voor versleutelingsalgoritmen.

2. Uitvoeringsgebied van het besturingssysteem waarin WireGuard voor de snelheid draait.

3. Robuust ouder protocol met een grote, complexe configuratiecodebase.

4. Asymmetrische sleutels die WireGuard gebruikt om verbindingen met peers te verifiëren.

5. Transportprotocollen die OpenVPN ondersteunt; WireGuard zelf werkt alleen via UDP.

6. De compacte omvang van de WireGuard-codebase, waardoor auditing veel eenvoudiger is.

7. Modern VPN-protocol, ontworpen voor hoge snelheid en eenvoudige code-audits.

8. Uitvoeringsgebied waarin OpenVPN draait, wat overhead door contextwisselingen veroorzaakt.

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. UGEIWARDR
2. EEEKCLRAPSN
3. COETDCMCEAOP
4. LAREETAPSLU
5. VNNEOPP
6. CRSAPUSEE
7. OSSLPNE
8. ECNPTDUP

Bonusopdracht: Snel denken

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

1	Redenen om voor WireGuard te kiezen			
2	Beloften van een goede VPN-aanbieder			
3	Redenen om voor OpenVPN te kiezen			
4	Redenen om een VPN te gebruiken tijdens het reizen			
5	Dingen die je internetprovider kan zien			
6	Manieren om een nep-wifinetwerk te herkennen			
7	Mythes over VPN's			
8	Plekken waar je een VPN zou gebruiken			
9	Snelle dingen in het dagelijks leven			
10	Dingen waartegen een VPN je niet kan beschermen			
11	Dingen die code makkelijker te controleren maken			
12	Dingen die een VPN kan verbergen			
13	Verschillen tussen WireGuard en OpenVPN			
14	Woorden die met privacy te maken hebben			
15	Namen van versleutelingen die je kent			

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 op de wifi van het café en met mijn VPN-app kan ik kiezen tussen WireGuard en OpenVPN. Mijn videogesprekken vallen steeds weg als ik tussen het netwerk van het café en de hotspot van mijn telefoon loop. Welk protocol moet ik kiezen, en waarom zou dat de overgang beter aankunnen?"

ALEX (REIZENDE STUDENT)

👩‍💻 "Ik ben in het buitenland op een hotelnetwerk dat de meeste VPN-verkeer lijkt te blokkeren. WireGuard maakt helemaal geen verbinding, maar ik moet bij de bronnen van mijn school thuis kunnen. Wat wordt waarschijnlijk geblokkeerd, en hoe kan OpenVPN me erdoorheen helpen?"

Controlepunt 9: De code ontcijferen

Ontcijfer om je training protocolaudits af te ronden dit verborgen bericht over uitvoering in kernelruimte.

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

21	16	7	18	1	4	5		10	5		15	16	5	14	22	16	14
13	5	20		5	5	14		19	14	5	12	12	5	18	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 zijn protocollen belangrijk?

Het protocol bepaalt hoe je VPN zijn tunnel opbouwt, welke cryptografie je gegevens beschermt en hoe snel hij verbinding maakt en opnieuw verbindt. WireGuard en OpenVPN zijn de twee open-sourceprotocollen die de meeste VPN-apps aanbieden, en ze maken verschillende afwegingen tussen eenvoud, snelheid en configureerbaarheid.

Q3: Is een van beide privater dan de andere?

Geen van beide protocollen maakt je anoniem. Beide versleutelen het tunnelverkeer met sterke coderingen; je privacy hangt vooral af van wat de VPN-aanbieder logt en hoe die sleutels, accounts en servers beheert.

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: Zijn beide open source?

Ja. WireGuard en de OpenVPN Community Edition publiceren allebei hun broncode, zodat onafhankelijke onderzoekers ze kunnen controleren. Doordat WireGuard een kleine codebase heeft, is een volledige controle veel sneller te doen.

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: Welke is sneller?

WireGuard is meestal sneller: het draait in de kernel, gebruikt lichte ChaCha20-Poly1305-versleuteling en rondt handshakes snel af. OpenVPN heeft meer overhead, maar de werkelijke snelheden hangen ook af van de serverbelasting en de afstand.

Q7: Kunnen beide via TCP en UDP draaien?

Nee. OpenVPN kan over UDP of TCP draaien, en TCP-modus helpt op netwerken die UDP blokkeren. WireGuard verstuurt zijn pakketten alleen via UDP, dus het kan mislukken op netwerken die alleen TCP toestaan. [4]

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 WireGuard en OpenVPN op mijn telefoon gebruiken?

Ja. WireGuard is platformonafhankelijk, met apps voor Windows, macOS, Linux, iOS en Android, en er bestaan OpenVPN-clients voor dezelfde systemen. In de meeste VPN-apps kun je kiezen tussen beide. [1]

Q10: Waarom is WireGuard zo klein?

WireGuard ondersteunt één vaste set moderne algoritmen in plaats van veel opties. De Linux-implementatie heeft minder dan 4.000 regels code nodig, waardoor het gemakkelijker te controleren is dan grotere VPN-codebases. [3]

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.

Q2: Welke coderingen gebruikt WireGuard?

WireGuard gebruikt ChaCha20 met Poly1305 voor versleuteling, Curve25519 voor sleuteluitwisseling, BLAKE2s voor hashing en het Noise-framework voor de handshake. Er is geen onderhandeling over algoritmen, zodat gebruikers geen zwakke optie kunnen kiezen. [2]

Q3: Welke coderingen en bibliotheken kan OpenVPN gebruiken?

OpenVPN is nauw geïntegreerd met de OpenSSL-bibliotheek en gebruikt TLS om sleutels uit te wisselen. Beheerders kunnen coderingen voor het datakanaal kiezen, zoals AES-256-GCM, wat flexibiliteit biedt maar ook ruimte voor zwakke instellingen. [4]

Q4: Hoe authenticeert elk protocol peers?

WireGuard-peers identificeren elkaar met statische publieke sleutels, vergelijkbaar met het uitwisselen van SSH-sleutels, en elke sleutel verwijst naar toegestane tunnel-IP-adressen. OpenVPN vertrouwt meestal op een certificeringsinstantie met X.509-certificaten, vaak gecombineerd met een gebruikersnaam en wachtwoord.

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 gebeurt er als ik van wifi naar mobiel overschakel?

WireGuard is verbindingsloos: het verstuurt pakketten vanaf het nieuwe adres en de tunnel gaat na een snelle handshake gewoon door. OpenVPN houdt de sessiestatus bij, waardoor een netwerkwijziging een iets langer durende herverbinding kan vereisen.

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: Is OpenVPN nog steeds een goede keuze als WireGuard sneller is?

Ja. OpenVPN is beproefd en wijdverbreid, werkt via TCP wanneer UDP wordt geblokkeerd en ondersteunt zakelijke opstellingen op basis van certificaten. Veel aanbieders bieden beide protocollen aan, zodat gebruikers kunnen wisselen als het ene wordt geblokkeerd of traag is.

Q9: Welke poorten gebruiken ze?

De standaardpoort van OpenVPN is 1194, maar die kan worden verplaatst naar elke UDP- of TCP-poort, inclusief 443. WireGuard luistert op een UDP-poort die in de configuratie is ingesteld; 51820 is de poort die in de officiële voorbeelden wordt gebruikt.

Q10: Welk protocol is gemakkelijker handmatig in te stellen?

WireGuard is meestal eenvoudiger: genereer een sleutelpaar, wissel publieke sleutels uit en geef de toegestane IP-adressen op. OpenVPN heeft certificaten, een CA en meer opties nodig, hoewel .ovpn-profielen die in één bestand bundelen.

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. TWEE TRANSPORTEN

OpenVPN kan zijn tunnel over UDP of TCP laten lopen, en in TLS-modus delen het controle- en het datakanaal één poort. [4]

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. MODERNE CRYPTOGRAFIE

WireGuard combineert ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 en HKDF binnen het Noise-protocolframework, zonder dat gebruikers algoritmen kunnen kiezen waarbij ze iets fout kunnen doen. [2]

5. OPENSSL IN OPENVPN

OpenVPN is nauw geïntegreerd met de OpenSSL-bibliotheek en ontleent er veel van zijn cryptografische mogelijkheden aan, waaronder de TLS die wordt gebruikt om sleutels uit te wisselen. [4]

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. SSH-ACHTIGE SLEUTELS

WireGuard-verbindingen worden opgezet door eenvoudige publieke sleutels uit te wisselen, vergelijkbaar met het uitwisselen van SSH-sleutels, zonder dat een certificeringsinstantie nodig is. [1]

8. PLATFORMOVERSTIJGEND

WireGuard werd voor het eerst uitgebracht voor de Linux-kernel en is nu beschikbaar voor Windows, macOS, BSD, iOS en Android, zodat hetzelfde protocol op de meeste apparaten werkt. [1]

9. FORWARD SECRECY

WireGuard herhaalt zijn Noise_IK-handshake om de paar minuten om de symmetrische sessiesleutels te vernieuwen, wat perfect forward secrecy geeft, ook als een langetermijnsleutel later lekt. [2]

10. TUN/TAP-INTERFACES

OpenVPN is ontworpen om te werken met de virtuele netwerkinterface TUN/TAP, die op de meeste platforms beschikbaar is en de pakketten van de tunnel vervoert. [4]

Technische referenties en bronnen

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

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Antwoordsleutel: WireGuard- en OpenVPN-protocollen vergelijken: codebasisgrootte, snelheid en cryptografische standaarden

1 **Omvang van de WireGuard-code** PROTOCOLLEN — **Juist antwoord: D**

DOCENTENNOTITIE

WireGuard is uiterst compact en draait op ongeveer 4.000 regels code. Dat houdt het aanvalsoppervlak klein en maakt controle eenvoudiger. Bron: WireGuard Project.

2 **Snelheid in de kernelruimte** LATENTIE — **Juist antwoord: B**

DOCENTENNOTITIE

Doordat WireGuard rechtstreeks in de kernelruimte draait, wordt de extra belasting van contextwisselingen vermeden, wat een hoge doorvoer mogelijk maakt. Bronvermelding: WireGuard Project.

3 **Vraag 3** — **Juist antwoord: B**

DOCENTENNOTITIE

OpenVPN is nauw geïntegreerd met OpenSSL, dat versleutelingen zoals AES-GCM levert en het zeer configureerbaar maar ook complexer maakt.

4 **Protocolprestaties** ROUTERINGSBEHEER — **Juist antwoord: A**

DOCENTENNOTITIE

WireGuard legt handshakes in milliseconden vast en reageert direct op netwerkroaming (bijvoorbeeld bij het overschakelen van wifi naar mobiel). Bron: Microsoft Native Gateway, Apple Support.

5 **Asymmetrische cryptografie** PRIVACY — **Juist antwoord: C**

DOCENTENNOTITIE

WireGuard gebruikt Cryptokey Routing, waarbij publieke sleutels worden gekoppeld aan toegestane tunnel-IP-adressen, vergelijkbaar met SSH-configuraties. Bron: WireGuard Project.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Waar

DOCENTENNOTITIE

De Linux-implementatie van WireGuard telt minder dan 4.000 regels, dus beveiligingsteams kunnen die veel sneller beoordelen dan veel grotere VPN-codebases zoals die van OpenVPN.

7 Latentie in gebruikersruimte SNELHEDEN

Juist antwoord: Onwaar

DOCENTENNOTITIE

OpenVPN werkt in de gebruikersruimte en geeft pakketten heen en weer door aan de virtuele kernelinterface, wat overhead door contextwisselingen veroorzaakt (tenzij kerneloffload zoals OpenVPN DCO wordt gebruikt). Bron: DD-WRT custom firmware.

8 OpenVPN-configuratie SNIFFINGRISICO

Juist antwoord: Waar

DOCENTENNOTITIE

OpenVPN kan via TCP (voor betrouwbaarheid en het omzeilen van firewalls) of UDP (voor snelheid) draaien, waardoor het compatibel is met complexe bedrijfsfirewalls. Bron: IETF Cryptographic Protocols.

9 Moderne cryptografie FIREWALLS

Juist antwoord: Waar

DOCENTENNOTITIE

WireGuard laat verouderde algoritmen vallen ten gunste van moderne, veilige bouwstenen zoals ChaCha20 en Poly1305, die snel draaien op mobiele cpu's. Bron: WireGuard Project.

10 Vereenvoudiging van sleutelparen NO-LOGS

Juist antwoord: Onwaar

DOCENTENNOTITIE

WireGuard gebruikt geen certificaten of complexe CA-hiërarchieën; het vertrouwt op eenvoudige publieke/private sleutelparen die tussen peers worden uitgewisseld. Bron: WireGuard Project.

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. WireGuard	H 2. OpenVPN	E 3. Kernelruimte	A 4. Gebruikersruimte
B 5. 4,000 regels	C 6. OpenSSL	F 7. Sleutelpaar	D 8. TCP/UDP

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 WIREGUARD	2 OPENVPN	3 KERNEL SPACE	4 USER SPACE
5 SLEUTELPAAR	6 AUDITEERBAARHEID		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 F – OPENSSL	2 C – KERNELSPACE	3 B – OPENVPN	4 G – SLEUTELPAAR
5 H – TCPENUDP	6 E – COMPACTECODE	7 A – WIREGUARD	8 D – USERSPACE

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen WireGuard, OpenVPN en Kernelruimte 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.

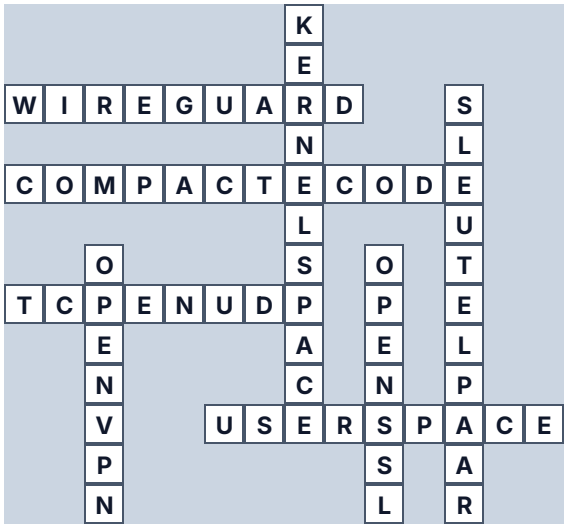
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

2 horizontaal: WIREGUARD Modern VPN-protocol, ontworpen voor hoge snelheid en eenvoudige code-audits (9 letters)

4 horizontaal: COMPACTECODE De compacte omvang van de WireGuard-codebase, waardoor auditing veel eenvoudiger is (12 letters)

7 horizontaal: TCPENUDP Transportprotocollen die OpenVPN ondersteunt; WireGuard zelf werkt alleen via UDP (8 letters)

8 horizontaal: USERSPACE Uitvoeringsgebied waarin OpenVPN draait, wat overhead door contextwisselingen veroorzaakt (9 letters)

VERTICAAL

1 verticaal: KERNELSPACE Uitvoeringsgebied van het besturingssysteem waarin WireGuard voor de snelheid draait (11 letters)

3 verticaal: SLEUTELPAAR Asymmetrische sleutels die WireGuard gebruikt om verbindingen met peers te verifiëren (11 letters)

5 verticaal: OPENVPN Robuust ouder protocol met een grote, complexe configuratiecodebase (7 letters)

6 verticaal: OPENSSL Cryptografische bibliotheek waarop OpenVPN vertrouwt voor versleutelingsalgoritmen (7 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. UGEIWARDR — **WIREGUARD**
2. EEEKCLRAPSN — **KERNELSPACE**
3. COETDCMCEAOP — **COMPACTECODE**
4. LAREETAPSLU — **SLEUTELPAAR**
5. VNNEOPP — **OPENVPN**
6. CRSAPUSEE — **USERSPACE**
7. OSSLPNE — **OPENSSL**
8. ECNPTDUP — **TCPENUDP**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"UPGRADE JE OPENVPN MET EEN SNELLERE TUNNEL"

Antwoordsleutel casestudy's

A Scenario A: Een protocol kiezen

SNIFFING EN VERSLEUTELING | Het dilemma van Sarah

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Aanbeveling: WireGuard. Door het lichtgewicht, verbindingsloze ontwerp herstelt de tunnel snel wanneer haar netwerk verandert, en ChaCha20-Poly1305 houdt de versleuteling snel.
- Beveiliging: Beide protocollen versleutelen haar verkeer op de wifi van het café, dus beide beschermen haar logins als ze correct zijn geconfigureerd; de keuze beïnvloedt vooral snelheid en stabiliteit.

B Scenario B: VPN-blokkades omzeilen

GEOBLOKKADES EN IP-ADRESSEN | Het dilemma van Alex

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Reden van blokkade: WireGuard gebruikt alleen UDP, en de firewall van het hotel blokkeert waarschijnlijk UDP of herkent WireGuard-pakketten via filtering of deep packet inspection.
- Hoe OpenVPN helpt: Het kan via TCP draaien, ook via poort 443 die HTTPS gebruikt, en die hotelfirewalls zelden volledig blokkeren omdat surfen op het web ervan afhangt.