Nimi: _____ Päivämäärä: _____ Pisteet: _____

Hotspot Shield -arvostelu

Tekninen analyysi Yhdysvalloissa pääkonttoria pitävästä Hotspot Shield VPN:stä, Pango-konserni

HOTSPOT SHIELD -ARVOSTELUN OPPIMISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: Hotspot Shieldin tekninen arvio. Tutustut Pangon Yhdysvaltain lainkäyttöalueeseen, omiin Catapult Hydra -protokolliin, suorituskykyvertailuihin ja Smart VPN -jaettuun tunnelointiin.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse VPN- ja verkkoturvallisuuden määritykset.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin parhaiden VPN-palvelujen opas

URL: https://www.vpn.com/fi/vpn/hotspot-shield/

Oppimispolkusi: Hotspot Shield

- Analysoi Hotspot Shield -arvioinnin teknistä arkkitehtuuria ja salausstandardeja.
- Määritä asiakasasetukset estämään IP-, DNS- ja WebRTC-liikenteen vuodot.
- Vertaile omia tunnelointiprotokollia tavallisiin toteutuksiin.

HOTSPOT SHIELD -ARVOSTELUN OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: Catapult Hydra -protokolla ja Aura-tietoturvapaketin integrointi. Lopuksi bonustehtävä Nopeat vastaukset.

CATAPULT HYDRAN OPTIMOINTI JA YHDYSVALTAIN LAINKÄYTTÖALUE (JOHDANTO)

Hotspot Shieldin taustalla on Pangon oma Catapult Hydra -protokolla, joka käyttää mukautettuja siirtoalgoritmeja nopeuksien optimointiin pitkillä etäisyyksillä. Toiminta Yhdysvalloista kuitenkin herättää kysymyksiä valvonnasta ja lainkäyttövallan vaikutuksista yksityisyyteen.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. 1. Mitä omaa protokollaa Hotspot Shield käyttää tiedonsiirtonopeuksien optimointiin?
   - A) Catapult Hydra
   - B) Lightway
   - C) NordLynx
   - D) OpenVPN

2. 2. Missä maassa Hotspot Shieldin takana oleva yritys Pango on päämajoitettuna?
   - A) Yhdysvallat
   - B) Yhdistynyt kuningaskunta
   - C) Romania
   - D) Sveitsi

3. 3. Mikä salausstandardi suojaa tietoja Hotspot Shieldin Catapult Hydra -tunneleissa?
   - A) AES-256
   - B) ChaCha20
   - C) Blowfish-128
   - D) Triple DES

4. 4. Mitkä ominaisuudet Hotspot Shield tarjoaa, jotta valitut sovellukset voivat ohittaa VPN:n?
   - A) Smart VPN (jaettu tunnelointi)
   - B) Kaksoishyppy
   - C) Oma IP-osoite
   - D) Tor VPN:n päällä

5. 5. Mikä rajoitus koskee Hotspot Shield -sovelluksen ilmaistason käyttäjiä?
   - A) Vain yksi laite
   - B) Rajaton määrä laitteita
   - C) Kaikki premium-sijainnit
   - D) Ei mainoksia mobiilissa

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Catapult Hydra on rakennettu tavallisen IPSec-tietoturvaprotokollan päälle.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Hotspot Shield toimii Yhdysvaltojen, Five Eyes -liiton jäsenen, lainkäyttövallan alaisuudessa.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Riippumaton tietoturva-auditointi on varmistanut Hotspot Shieldin lokittomuusinfrastruktuurin.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Hotspot Shieldin ilmaistaso antaa pääsyn jokaiseen premium-palvelinsijaintiin.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Hotspot Shield Premium sallii rajattoman määrän samanaikaisia laitteita.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Pangon oma, pitkien etäisyyksien yhteysnopeuksia optimoimaan suunniteltu protokolla on _____ .

2. _____ piilottaa VPN-liikenteen kuviot, mutta Hotspot Shield ei mainosta sellaista.

3. Pangon Hotspot Shieldin ydintunnelointiprotokolla on virallisesti nimeltään _____ Hydra.

4. Kaikkea tunnelin läpi kulkevaa liikennettä suojaa edistyneiden standardien mukainen _____ .

5. Yksinkertainen _____ peittää sijaintisi, mutta ei välttämättä salaa liikennettäsi kuten VPN.

6. Laaja maailmanlaajuinen, useissa maissa sijaitsevien palvelinten muodostama kokonaisuus on Hotspot Shieldin _____ .

SANASTON SANAPANKKI

CATAPULT | HYDRA-PROTOKOLLA | HÄIVETILA | KILL SWITCH | PALVELINVERKKO | TIETOJEN SALAUS | TUNNELOINTI | VÄLITYSPALVELU

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

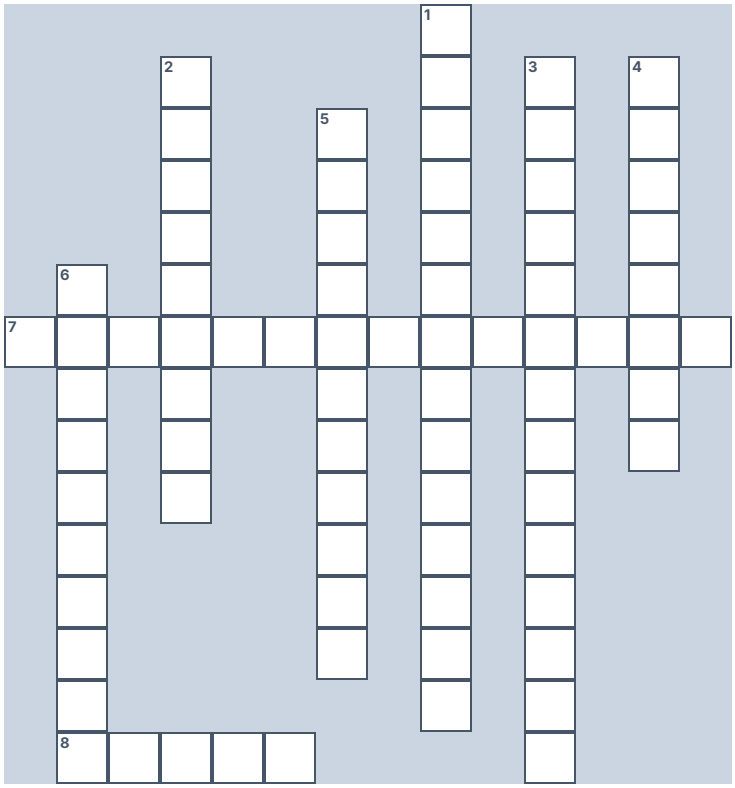
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. Hydra-protokolla	A	Yksinkertainen reitityspalvelu, joka peittää todelliset sijaintipäätepisteet.
☐	2. Stealth-tila	B	Nimi, joka on pariksi Hydran kanssa Pangon omassa tunnelointiprotokollassa.
☐	3. Catapult	C	Vikaturvamekanismi, joka estää liikenteen, jos VPN pettää.
☐	4. Tietojen salaus	D	Maailmanlaajuinen joukko palvelinsolmuja, jotka sijaitsevat useissa maissa.
☐	5. Välityspalvelinpalvelu	E	Pakettien liikenteen salaamiseen käytetty kryptografinen standardi.
☐	6. Palvelinverkko	F	Hämäystekniikka VPN-otsikoiden piilottamiseen rajoitetuilla alueilla.
☐	7. Kill switch	G	Datapakettien kapselointi niiden kuljettamiseksi verkkojen yli.
☐	8. Tunnelointi	H	Pangon oma TLS-pohjainen protokolla, joka on rakennettu lisäämään VPN:n nopeutta.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

7. Kryptografinen standardi, jolla liikennepaketit salataan (14)

8. Pangon oma TLS-pohjainen protokolla, joka on rakennettu nopeuttamaan VPN-yhteyttä (5)

PYSTYSUORAAN

1. Yksinkertainen reititys, joka peittää todelliset sijaintipisteet (14)

2. Hämäystekniikka, joka piilottaa VPN-otsikot rajoitetuilla alueilla (9)

3. Useissa maissa sijaitsevien palvelinsolmujen maailmanlaajuinen joukko (14)

4. Hydran pari Pangon omassa tunnelointiprotokollassa (8)

5. Datapakettien kapselointi niiden kuljettamiseksi verkkojen yli (11)

6. Suojamekanismi, joka estää liikenteen, jos VPN-yhteys pettää (10)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

7 vaakasuoraan: Kryptografinen standardi, jolla liikennepaketit salataan (14 kirjainta):

8 vaakasuoraan: Pangon oma TLS-pohjainen protokolla, joka on rakennettu nopeuttamaan VPN-yhteyttä (5 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Yksinkertainen reititys, joka peittää todelliset sijaintipisteet (14 kirjainta):

2 pystysuoraan: Hämäystekniikka, joka piilottaa VPN-otsikot rajoitetuilla alueilla (9 kirjainta):

3 pystysuoraan: Useissa maissa sijaitsevien palvelinsolmujen maailmanlaajuinen joukko (14 kirjainta):

4 pystysuoraan: Hydran pari Pangon omassa tunnelointiprotokollassa (8 kirjainta):

5 pystysuoraan: Datapakettien kapselointi niiden kuljettamiseksi verkkojen yli (11 kirjainta):

6 pystysuoraan: Suojamekanismi, joka estää liikenteen, jos VPN-yhteys pettää (10 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

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

SANASTOLISTA

HYDRA HÄIVETILA CATAPULT TIETOJENSALAUS VÄLITYSPALVELU
PALVELINVERKKO KILLSWITCH TUNNELOINTI

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. HYDRA**
- **B. HÄIVETILA**
- **C. CATAPULT**
- **D. TIETOJENSALAUS**
- **E. VÄLITYSPALVELU**
- **F. PALVELINVERKKO**
- **G. KILLSWITCH**
- **H. TUNNELOINTI**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Datapakettien kapselointi niiden kuljettamiseksi verkkojen yli.
2. Yksinkertainen reititys, joka peittää todelliset sijaintipisteet.
3. Pangon oma TLS-pohjainen protokolla, joka on rakennettu nopeuttamaan VPN-yhteyttä.
4. Hydran pari Pangon omassa tunnelointiprotokollassa.
5. Suojamekanismi, joka estää liikenteen, jos VPN-yhteys pettää.
6. Hämäystekniikka, joka piilottaa VPN-otsikot rajoitetuilla alueilla.
7. Useissa maissa sijaitsevien palvelinsolmujen maailmanlaajuinen joukko.
8. Kryptografinen standardi, jolla liikennepaketit salataan.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä virtuaalisen yksityisverkon (VPN) käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. RDHAY
2. ACTALUPT
3. VAÄLPULVLS TYEI
4. WCSHLTIKIL
5. IEÄATVHLI
6. JELOEANUATI SST
7. RKEPVALOLK NVIE
8. NOILNTEUTIN

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Asioita, jotka Hotspot Shield voi piilottaa verkostasi			
2	Paikkoja, joissa ottaisit palvelun Hotspot Shield käyttöön			
3	Muita VPN-palveluja kuin Hotspot Shield			
4	Kysymyksiä palvelun Hotspot Shield asiakastuelle			
5	Sanoja, jotka kuvaavat hyvää VPN-sovellusta			
6	Sovelluksia, joita käyttäisit yhdessä palvelun Hotspot Shield kanssa			
7	Syitä valita Hotspot Shield			
8	Ominaisuuksia, joita etsit palvelusta Hotspot Shield			
9	Tietoturvasanoja, jotka opit tässä tehtävämonisteessa			
10	Merkkejä siitä, että VPN-yhteytesi on hidas			
11	Tilanteita, joissa kill switch auttaa			
12	Asioita, jotka kannattaa tarkistaa ennen VPN:n ostamista			
13	Maita, joissa haluaisit palvelun Hotspot Shield palvelimia			
14	Painikkeita tai valikkoja VPN-sovelluksessa			
15	Asioita, joita teet verkossa joka päivä			

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: ETÄTYÖN OPTIMOINTI

👷

Tilanne: Yrityksen on optimoitava etätyöntekijöiden yhteysnopeudet. He päättävät ottaa käyttöön Hotspot Shieldin sen omalla Hydra-protokollalla.

Keskustelukysymys: Selitä, miten Catapult Hydra -protokolla saavuttaa nopeammat yhteysnopeudet verrattuna tavallisiin OpenVPN-määrityksiin.

TAPAUSTUTKIMUS 2: JULKISTEN PÄÄTTEIDEN SUOJAAMINEN

👷

Tilanne: Organisaatio haluaa suojata kenttäagenttien julkisissa hotspoteissa käyttämät mobiililaitteet automaattisilla salaussäädöillä.

Keskustelukysymys: Kuvaa AES-256-salauksen ja Kill Switchin rooli tietojen paljastumisen estämisessä julkisissa verkoissa.

Tarkistuspiste 9: Salakirjoituksen purkaminen

Verkkoinsinööri suojaa reititysreittejä ja asiakastunneleita. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

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 Å=27 Ä=28 Ö=29

8	25	4	18	1		16	18	15	20	15	11	15	12	12	1
20	1	18	10	15	1	1		14	15	16	5	1	20		22	16	14
							25	8	20	5	25	4	5	20	

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa A)

Tutustu yleisimpiin kysymyksiin ja vastauksiin virtuaalisista yksityisverkoista (VPN) ja tunneloinnista.

Q1: Mitä protokollaa Hotspot Shield käyttää?

Catapult Hydra, oma TLS-pohjainen protokolla, sekä WireGuard ja IKEv2.

Q2: Onko Hotspot Shieldistä ilmaisversiota?

Kyllä, ilmainen mainosrahoitteinen taso kattaa yhden laitteen rajoitetuilla sijainneilla ja nopeudella.

Q3: Tallentaako Hotspot Shield yhteyslokeja?

Tietosuojakäytäntönsä mukaan se kirjaa kaistanleveyden käytön ja aikaleimat, mutta ei selaushistoriaa tai IP-osoitteita.

Q4: Voinko käyttää Hotspot Shieldiä useilla laitteilla?

Kyllä, Premium tukee jopa 10 laitetta samanaikaisesti (syyskuusta 2026 alkaen). [7]

Q5: Mitä salausstandardia se hyödyntää?

Se käyttää AES-256-salausta kaikkien verkkoliikenteen hyötykuormien suojaamiseen.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa B)

Tutustu yleisimpiin kysymyksiin ja vastauksiin virtuaalisista yksityisverkoista (VPN) ja tunneloinnista.

Q6: Tukeeko Hotspot Shield jaettua tunnelointia?

Kyllä, sen Smart VPN -toiminnolla käyttäjät voivat jättää tietyt sovellukset VPN-reitityksen ulkopuolelle.

Q7: Missä yrityksen pääkonttori sijaitsee?

Sitä pyörittää Pango, yhdysvaltalainen yritys, joka on nyt osa Point Wildia. [4]

Q8: Sisältääkö se Kill Switchin?

Kyllä, siinä on kill switch, joka estää liikenteen automaattisesti, jos yhteys katkeaa.

Q9: Sopiiko se median suoratoistoon?

Kyllä, Hydra on erittäin optimoitu nopeisiin videosuoratoistonopeuksiin.

Q10: Voinko asentaa Hotspot Shieldin reitittimeen?

Kyllä, premium-tilit voivat määrittää sen yhteensopiviin reitittimiin.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa C)

Tutustu VPN-tunnelointiprotokollien, mobiiliasiakasohjelmien integraatioiden ja yrityskäyttöönoton edistyneisiin teknisiin puoliin.

Q1: Miten Catapult Hydra eroaa OpenVPN:stä?

Hydra toimii UDP:n päällä, käyttää omaa siirron optimointia ja minimoi viiveen.

Q2: Vaikuttaako Yhdysvaltojen lainkäyttöalue käyttäjien yksityisyyteen?

Kyllä, toiminta Yhdysvaltojen Five Eyes -lainkäyttöalueella sallii viranomaisten antaa vaikenemismääräyksiä ja haasteita.

Q3: Miten kill switch toimii Windowsissa?

Se päivittää dynaamisesti palomuurin suodatussäännöt estääkseen salaamattoman liikenteen yhteyden katketessa.

Q4: Mitä protokollia tuetaan Hydran lisäksi?

Se tarjoaa myös WireGuardin ja IKEv2/IPSecin alustasta riippuen.

Q5: Miten Smart VPN käsittelee selainliikenteen?

Se antaa käyttäjien valita selaimet tai sovellukset, jotka reititetään suoraan tavallisen palveluntarjoajan yhteyden kautta.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa D)

Tutustu VPN-tunnelointiprotokollien, mobiiliasiakasohjelmien integraatioiden ja yrityskäyttöönoton edistyneisiin teknisiin puoliin.

Q6: Suojaako Hotspot Shield DNS-vuodoilta?

Kyllä, se reitittää kaikki DNS-kyselyt omien salattujen yksityisten DNS-palvelimiensa kautta.

Q7: Tukeeko se IPv6-liikennettä natiivisti?

Kyllä, se estää tai tunneloi IPv6-paketteja aktiivisesti, jotta todelliset IP-osoitteet eivät vuoda.

Q8: Miten Hydra optimoi pitkän matkan yhteyksiä?

Se toteuttaa mukautettuja ikkunoiden skaalaus- ja ruuhkanhallinta-algoritmeja UDP-tunneleissa.

Q9: Voiko se ohittaa tiukan DPI-sensuurin?

Ei luotettavasti; Hotspot Shield ei mainosta erillistä hämäys- tai piilotilaa.

Q10: Miten sen no-logs-käytäntö varmistetaan?

Sen lokittomuusasetukset auditoitiin riippumattomasti vuonna 2023; Aon auditoi Hydran vuonna 2022. [5]

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

Tutustu todellisiin tosiasioihin VPN-salauksen nopeuksista, protokollien auditoinneista, mobiiliyhteyksistä ja yritysten etätyöstä.

1. VPN-OIVALLUS

Pango lisensoi Catapult Hydra -kumppani-VPN-alustansa muille tietoturvabrändeille, myös Bitdefender VPN:lle. [5]

2. VPN-OIVALLUS

Hotspot Shieldin valmistaja Pango erotettiin Aurasta vuonna 2024 ja liittyi sitten Point Wildiin. [3]

3. VPN-OIVALLUS

Hydra-protokolla käyttää useita rinnakkaisia kanavia estääkseen pakettihävikin pysäyttämästä koko yhteyttä.

4. VPN-OIVALLUS

Sitä käytettiin laajasti arabikevään kansannousuissa hallitusten internetestojen kiertämiseen ja sosiaalisen median tavoittamiseen.

5. VPN-OIVALLUS

Yhdysvaltojen lainkäyttöalueella viranomaiset voivat pyytää yhteyden metatietoja mutta eivät salattuja sisältötietoja.

6. VPN-OIVALLUS

Hotspot Shield ylläpitää palvelimia yli 80 maassa maailmanlaajuisesti (syyskuun 2026 tilanteen mukaan). [2]

7. VPN-TIETOA

Ilmaista tasoa tukee mobiilisovelluksen käyttöliittymässä näytettävä asiayhteyteen perustuva mainonta. [2]

8. VPN-TIETOA

Maksullisiin Hotspot Shield -paketteihin sisältyy 45 päivän rahat takaisin -takuu (syyskuussa 2026). [1]

9. VPN-TIETOA

Windows-asiakasohjelmat käyttävät ydintason verkko-ohjaimia (TAP-sovittimia) reititystaulujen tehokkaaseen hallintaan.

10. VPN-OIVALLUS

Se tukee automaattisia käynnistyssääntöjä, jotka muodostavat VPN-tunnelin automaattisesti aina, kun suojaamaton Wi-Fi-verkko havaitaan.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista teknisistä standardeista, määrittelyistä ja sääntelykehyksistä.

TIETEELLISET JA ALAN VIITTEET

[1] VPN.com. (2026). Hotspot Shield Review: Pricing, Privacy & Hydra Protocol.

https://www.vpn.com/vpn/hotspot-shield/

[2] Security.org. (n.d.). Hotspot Shield VPN Review.

https://www.security.org/vpn/hotspot-shield/review/

[3] Point Wild. (2024). Aura Splits Into Two World-Class Online Safety Companies.

https://www.pointwild.com/news/aura-splits-into-two-world-class-online-safety-companies/

[4] Point Wild. (2024). Pango Group Merges With Total Security, Combined Company Rebranded Point Wild.

https://www.pointwild.com/news/pango-group-merges-with-total-security-combined-company-rebranded-point-wild/

[5] Bitdefender. (2023). VPN Audit Pango 2023.

https://www.bitdefender.com/en-us/company/VPN-Audit-Pango-2023

[6] Bitdefender. (n.d.). Bitdefender VPN - Fast & Secure VPN Service.

https://www.bitdefender.com/en-us/consumer/vpn

[7] AnchorFree Inc. (n.d.). Hotspot Shield VPN—Wifi Proxy App [App Store listing].

https://apps.apple.com/us/app/hotspot-shield-vpn-wifi-proxy/id771076721

[8] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2). IETF.

https://www.rfc-editor.org/rfc/rfc7296

[9] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[10] National Institute of Standards and Technology. (2023). FIPS 197, Advanced Encryption Standard (AES).

https://csrc.nist.gov/pubs/fips/197/final

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Hydra-protokolla** CATAPULT HYDRA — **Oikea vastaus: A**

OPETTAJALLE

Catapult Hydra -protokolla optimoi yhteysnopeuksia pitkän matkan yhteyksillä. Lähde: Hotspot Shield Support.

2 **Kysymys 2** — **Oikea vastaus: A**

OPETTAJALLE

Pango, Hotspot Shieldia pyörittävä yritys, toimii Yhdysvalloista.

3 **Kysymys 3** — **Oikea vastaus: A**

OPETTAJALLE

Hotspot Shieldin Catapult Hydra -tunnelit suojataan AES-256-salauksella.

4 **Smart VPN** JAETTU TUNNELOINTI — **Oikea vastaus: A**

OPETTAJALLE

Smart VPN antaa käyttäjien valita sovelluksia, jotka ohittavat VPN-tunnelin. Lähde: Hotspot Shield Support.

5 **Kysymys 5** — **Oikea vastaus: A**

OPETTAJALLE

Ilmaistaso on rajattu yhteen laitteeseen, näyttää mainoksia ja tarjoaa vain vähän sijainteja.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **IPSec-pohja** MUKAUTETTU YDIN **Oikea vastaus: Epätosi**

OPETTAJALLE

Catapult Hydra on oma siirtoprotokolla, jota ei ole rakennettu IPSecin päälle. Lähde: Hotspot Shield Support.

7 **Kysymys 7** **Oikea vastaus: Tosi**

OPETTAJALLE

Tosi: Hotspot Shieldin operaattori toimii Yhdysvalloista, ja Yhdysvallat on Five Eyes -liittouman jäsen.

8 **Kysymys 8** **Oikea vastaus: Tosi**

OPETTAJALLE

Tosi: Hotspot Shieldin lokittomuusjärjestelmä tarkastettiin riippumattomasti vuonna 2023.

9 **Kysymys 9** **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: ilmaiskäyttäjät saavat rajoitetun määrän sijainteja; Premium avaa koko verkon.

10 **Kysymys 10** **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: Hotspot Shield Premium kattaa enintään 10 laitetta kerrallaan, ei rajattomasti.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

H 1. Hydra-protokolla	F 2. Stealth-tila	B 3. Catapult	E 4. Tietojen salaus
A 5. Välityspalvelinpalvelu	D 6. Palvelinverkko	C 7. Kill switch	G 8. Tunnelointi

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 HYDRA-PROTOKOLLA	2 HÄIVETILA	3 CATAPULT	4 TIETOJEN SALAUS
5 VÄLITYSPALVELU	6 PALVELINVERKKO		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 H – TUNNELOINTI	2 E – VÄLITYSPALVELU	3 A – HYDRA	4 C – CATAPULT
5 G – KILLSWITCH	6 B – HÄIVETILA	7 F – PALVELINVERKKO	8 D – TIETOJENSALAUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Hydra-protokolla, Stealth-tila ja Catapult omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

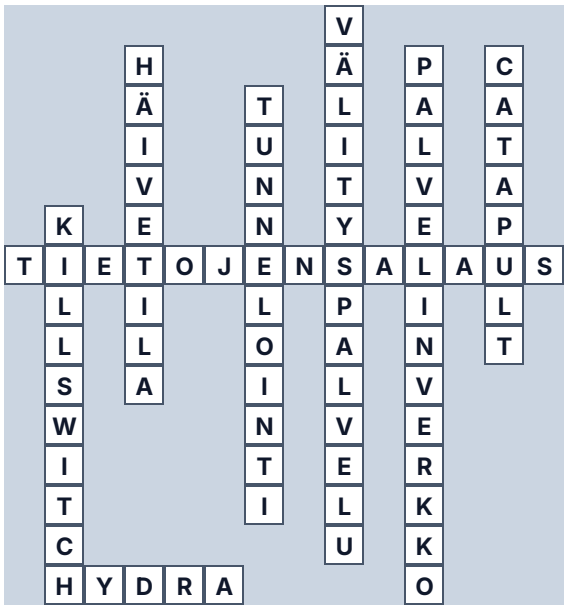
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

7 vaakasuoraan: TIETOJENSALAUS Kryptografinen standardi, jolla liikennepaketit salataan (14 kirjainta)

8 vaakasuoraan: HYDRA Pangon oma TLS-pohjainen protokolla, joka on rakennettu nopeuttamaan VPN-yhteyttä (5 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: VÄLITYSPALVELU Yksinkertainen reititys, joka peittää todelliset sijaintipisteet (14 kirjainta)

2 pystysuoraan: HÄIVETILA Hämäystekniikka, joka piilottaa VPN-otsikot rajoitetuilla alueilla (9 kirjainta)

3 pystysuoraan: PALVELINVERKKO Useissa maissa sijaitsevien palvelinsolmujen maailmanlaajuinen joukko (14 kirjainta)

4 pystysuoraan: CATAPULT Hydran pari Pangon omassa tunnelointiprotokollassa (8 kirjainta)

5 pystysuoraan: TUNNELOINTI Datapakettien kapselointi niiden kuljettamiseksi verkkojen yli (11 kirjainta)

6 pystysuoraan: KILLSWITCH Suojamekanismi, joka estää liikenteen, jos VPN-yhteys pettää (10 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. RDHAY — **HYDRA**
2. ACTALUPT — **CATAPULT**
3. VAÄLPULVLSTYEI — **VÄLITYSPALVELU**
4. WCSHLTIKIL — **KILLSWITCH**
5. IEÄATVHLI — **HÄIVETILA**
6. JELOEANUATISST — **TIETOJENSALAUS**
7. RKEPVALOLKNVIE — **PALVELINVERKKO**
8. NOILNTEUTIN — **TUNNELOINTI**

SALAKIRJOITUSHAASTEEN AVAIN

"HYDRA PROTOKOLLA TARJOAA NOPEAT VPN YHTEYDET"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: ETÄTYÖN OPTIMOINTI

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys tarvitsee optimoida etätyöntekijöiden yhteysnopeudet. Se päättää ottaa käyttöön Hotspot Shieldin omalla Hydra-protokollallaan.
- Suositeltu strategia ja ratkaisu: Arviointiohje: Selitä, että Hydra on Pangon oma TLS-pohjainen protokolla, joka on viritetty nopeampaan yhteyden muodostukseen ja pienempään viiveeseen kuin tavallinen OpenVPN.

B TAPAUSTUTKIMUS 2: JULKISTEN PÄÄTTEIDEN SUOJAAMINEN

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Organisaatio haluaa suojata kenttäagenttien käyttämät mobiililaitteet julkisissa hotspoteissa automaattisilla salauksen hallintakeinoilla.
- Suositeltu strategia ja ratkaisu: Arviointiohje: Kuvaa, että AES-256 salaa kaiken siirrettävän liikenteen ja Kill Switch estää salaamattomat IP-vuodot, jos VPN-yhteys katkeaa.