Nimi: _____ Päivämäärä: _____ Pisteet: _____

ProtonVPN:n tietoturva

ProtonVPN:n tietoturva-arkkitehtuurin analysointi, mukaan lukien Secure Core -palvelimet, NetShield-DNS-suodatus, Sveitsin yksityisyyslainsäädäntö, avoimen lähdekoodin auditoidut sovellukset ja Stealth-protokolla.

PROTONVPN:N TIETOTURVA, OPPIMISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: Proton VPN:n tietoturva-arkkitehtuuri. Tutustut Secure Core -kaksoishyppypalvelimiin, NetShield-DNS-estoon, Sveitsin yksityisyyslakeihin ja Stealth-häivytykseen.

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/protonvpn/tietoturva/

Oppimispolkusi: ProtonVPN:n tietoturva

- Analysoi ProtonVPN:n tietoturvan teknistä arkkitehtuuria ja määräyksiä.
- Määritä asiakasasetukset estämään IP-, DNS- ja WebRTC-liikenteen vuodot.
- Vertaile mukautettua hinnoittelua, kokeilua ja suorituskykyominaisuuksia vakiomalleihin.

PROTONVPN:N TIETOTURVAOPAS, OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: Secure Core -kaksoishyppyreititys ja sveitsiläinen yksityisyyden hallinnointi. Lopuksi bonustehtävä Nopeat vastaukset.

SECURE CORE -KAKSOISHYPPYARKKITEHTUURI JA SVEITSILÄINEN YKSITYISYYSLAINKÄYTTÖALUE

Proton VPN suojaa käyttäjien liikennettä Protonin omistamilla Secure Core -palvelimilla Sveitsissä, Islannissa ja Ruotsissa, avoimen lähdekoodin tarkastetuilla sovelluksilla ja Stealth-hämäysprotokollalla, joka on suunniteltu ohittamaan syväpakettitarkastus.

(JOHDANTO)

Proton VPN suojaa käyttäjien liikennettä Protonin omistamilla Secure Core -palvelimilla Sveitsissä, Islannissa ja Ruotsissa, avoimen lähdekoodin tarkastetuilla sovelluksilla ja Stealth-hämäysprotokollalla, joka on suunniteltu ohittamaan syväpakettitarkastus.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Millaisissa tiloissa Protonin Secure Core -palvelimet sijaitsevat?**
   - A) Julkisten pilvipalvelujen virtuaalikoneet
   - B) Korkean turvallisuuden toimipaikat
   - C) Julkiset konesalit
   - D) Jaetut telineet

2. **2. Mikä protokolla auttaa ohittamaan tiukan valtiollisen sensuurin?**
   - A) PPTP
   - B) Stealth-protokolla
   - C) OpenVPN UDP
   - D) IKEv2

3. **3. Mikä on Proton VPN:n NetShield-ominaisuuden tehtävä?**
   - A) Speed Booster
   - B) DNS-mainosten ja haittaohjelmien esto
   - C) Pilvitallennus
   - D) Portinohjaus

4. **4. Minkä maan tietosuojalakien alaisena Proton AG toimii?**
   - A) Yhdysvallat
   - B) Yhdistynyt kuningaskunta
   - C) Sveitsi
   - D) Panama

5. **5. Miten asiantuntijat varmentavat Proton VPN -asiakassovellukset?**
   - A) Salainen koodi
   - B) Avoimen lähdekoodin auditoinnit
   - C) Suljettu lisenssi
   - D) Viranomaistarkastus

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Secure Core reitittää liikenteen tietosuojamyönteisten maiden kautta ennen poistumista.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Sveitsi on 14 Eyes -tiedustelu- ja valvontaliittouman jäsen.

○ Tosi ○ Epätosi

8 Kysymys 8

8. NetShield estää mainokset ja haitalliset verkkotunnukset suoraan DNS-tasolla.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Proton VPN:n sovellukset ovat 100-prosenttisesti avointa lähdekoodia ja julkisesti tarkastettuja.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Stealth-protokolla käyttää tavallisia WireGuard-otsikoita ilman häivytystä.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Monihyppyreititys Protonin omistamien palvelinten kautta yksityisyysystävällisissä maissa on nimeltään _____ -arkkitehtuuri.

2. Syväpakettitarkastuksen ja verkkopalomuurien voittamiseksi käyttäjät aktivoivat _____ -tilan.

3. Haittaohjelmia sisältävät verkkotunnukset, seurantaohjelmat ja mainoskoodit suodattaa _____ -DNS.

4. Protonin mukaan sen ei tarvitse säilyttää lokeja käyttäjien toiminnasta, koska voimassa on _____ .

5. Jos VPN-tunneli katkeaa odottamatta, internetliikenne estetään _____ -suojauksella.

6. Riippumattomat tietoturvatutkijat varmistavat asiakasohjelman eheyden, koska sovellukset noudattavat mallia nimeltä _____ .

SANASTON SANAPANKKI

AES-GCM | AVOIN KOODI | KILL SWITCH | NETSHIELD | SECURE CORE | STEALTH | SVEITSIN LAKI | WIREGUARD

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

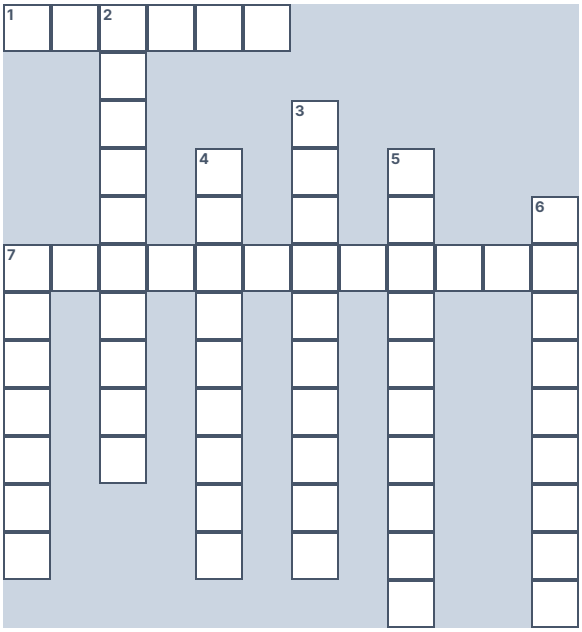
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. SECURE CORE	A	Julkisesti saatavilla oleva ja riippumattomasti tarkastettu asiakassovellusohjelmisto.
☐	2. STEALTH	B	Symmetrinen salausstandardi, joka salaa VPN:n datapaketit.
☐	3. NETSHIELD	C	Sveitsin tiukat tietosuojalait 14 Eyes -lainkäyttöalueen ulkopuolella.
☐	4. SVEITSIN LAKI	D	Hämärretty tunnelointiprotokolla, joka on naamioitu tavalliseksi HTTPS-verkkoliikenteeksi.
☐	5. KILL SWITCH	E	Moderni kevyt protokolla, joka tarjoaa vahvan salauksen ja nopeat nopeudet.
☐	6. AVOIN KOODI	F	DNS-pohjainen suodatin, joka estää mainokset, telemetriaseurannat ja haittaohjelmat.
☐	7. WIREGUARD	G	Monihyppyrakenne, joka reitittää liikenteen Protonin omistamien ensimmäisen hypyn palvelinten kautta.
☐	8. AES-GCM	H	Suojausmekanismi, joka pysäyttää verkkoliikenteen yhteyden katketessa.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

1. Sotilastason symmetrinen salaus, joka suojaa kaikki kapseloidut VPN-datapaketit (6)

7. Sveitsin tiukat yksityisyyslait 14 Eyes -lainkäyttöalueiden ulkopuolella (12)

PYSTYSUORAAN

2. Monihyppyarkkitehtuuri, joka reitittää liikenteen Protonin omistamien ensimmäisen hypyn palvelinten kautta (10)

3. Julkisesti saatavilla oleva ja riippumattomasti tarkastettu asiakassovellus (10)

4. DNS-pohjainen suodatin, joka estää mainokset, telemetriaseurannat ja haittaohjelmat (9)

5. Suojaominaisuus, joka pysäyttää verkkoliikenteen yhteyden katketessa (10)

6. Moderni kevyt protokolla, joka tarjoaa vankan salauksen ja nopeat yhteydet (9)

7. Hämäävä tunnelointiprotokolla, joka on naamioitu tavalliseksi HTTPS-verkkoliikenteeksi (7)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

1 vaakasuoraan: Sotilastason symmetrinen salaus, joka suojaa kaikki kapseloidut VPN-datapaketit (6 kirjainta):

7 vaakasuoraan: Sveitsin tiukat yksityisyyslait 14 Eyes -lainkäyttöalueiden ulkopuolella (12 kirjainta):

PYSTYSUORAAN

2 pystysuoraan: Monihyppyarkkitehtuuri, joka reitittää liikenteen Protonin omistamien ensimmäisen hypyn palvelinten kautta (10 kirjainta):

3 pystysuoraan: Julkisesti saatavilla oleva ja riippumattomasti tarkastettu asiakassovellus (10 kirjainta):

4 pystysuoraan: DNS-pohjainen suodatin, joka estää mainokset, telemetriaseurannat ja haittaohjelmat (9 kirjainta):

5 pystysuoraan: Suojaominaisuus, joka pysäyttää verkkoliikenteen yhteyden katketessa (10 kirjainta):

6 pystysuoraan: Moderni kevyt protokolla, joka tarjoaa vankan salauksen ja nopeat yhteydet (9 kirjainta):

7 pystysuoraan: Hämäävä tunnelointiprotokolla, joka on naamioitu tavalliseksi HTTPS-verkkoliikenteeksi (7 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

SECURECORE STEALTH NETSHIELD SVEITSINLAKI KILLSWITCH AVOINKOODI WIREGUARD AESGCM

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. SECURECORE**
- **B. STEALTH**
- **C. NETSHIELD**
- **D. SVEITSINLAKI**
- **E. KILLSWITCH**
- **F. AVOINKOODI**
- **G. WIREGUARD**
- **H. AESGCM**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Hämäävä tunnelointiprotokolla, joka on naamioitu tavalliseksi HTTPS-verkkoliikenteeksi.
2. Moderni kevyt protokolla, joka tarjoaa vankan salauksen ja nopeat yhteydet.
3. Sveitsin tiukat yksityisyyslait 14 Eyes -lainkäyttöalueiden ulkopuolella.
4. Monihyppyarkkitehtuuri, joka reitittää liikenteen Protonin omistamien ensimmäisen hypyn palvelinten kautta.
5. Sotilastason symmetrinen salaus, joka suojaa kaikki kapseloidut VPN-datapaketit.
6. Suojaominaisuus, joka pysäyttää verkkoliikenteen yhteyden katketessa.
7. DNS-pohjainen suodatin, joka estää mainokset, telemetriaseurannat ja haittaohjelmat.
8. Julkisesti saatavilla oleva ja riippumattomasti tarkastettu asiakassovellus.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. ITLASKNSVIEI
7. VIAOKODINO
8. SMACGE

Bonustehtävä: Nopeat vastaukset

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

1	Asioita, joita teet verkossa joka päivä			
2	Maita, jotka tunnetaan vahvoista tietosuojalaeistaan			
3	Palvelun Proton VPN tietoturvaominaisuuksia			
4	VPN-vuotojen tyyppejä			
5	Tilanteita, joissa kill switch auttaa			
6	Asioita, joita tarkastus voi tutkia			
7	Asetuksia, jotka otat käyttöön lisäturvaksi			
8	Asioita, joita salaus suojaa			
9	Sanoja, jotka kuvaavat hyvää VPN-sovellusta			
10	Syitä valita Proton VPN			
11	Painikkeita tai valikkoja VPN-sovelluksessa			
12	Suoratoistopalveluja, joita katsot			
13	Julkisen Wi-Fin uhkia			
14	Tapoja tehdä vahva salasana			
15	Maita, joissa haluaisit palvelun Proton VPN palvelimia			

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: RAJOITTAVIEN PALOMUURIEN OHITTAMINEN



Tilanne: Käyttäjä matkustaa maahan, jossa tavallinen VPN-liikenne, kuten OpenVPN ja WireGuard, estetään syväpakettitarkastuksella.

Keskustelukysymys: Mikä Proton VPN -protokollamääritys antaa käyttäjän ohittaa valtiotason tarkastuksen?

TAPAUSTUTKIMUS 2: EDISTYNYT SUOJAUS VASTUSTAJAA VASTAAN



Tilanne: Tilintarkastaja epäilee, että hänen paikallisen internetoperaattorinsa poistumissolmu voi olla pitkäkestoisten kehittyneiden uhkien vaarantama.

Keskustelukysymys: Miten Secure Core suojaa tarkastajan henkilöllisyyttä poistumissolmun vaarantumiselta?

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

19	5	3	21	18	5		3	15	18	5

16	1	12	22	5	12	9	13	5	20		19	21	15	10	1	1	22	1	20

20	9	5	20	15	19	9

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: Mikä on Proton VPN Secure Core?

Secure Core reitittää liikenteen usean tietosuojamyönteisen maan palvelimien kautta ennen poistumista.

Q2: Mikä on Stealth-protokolla?

Stealth on obfuskoitu protokolla, joka piilottaa VPN-yhteydet tavalliseksi TLS/HTTPS-liikenteeksi.

Q3: Miten NetShield suojaa käyttäjiä?

NetShield on DNS-pohjainen työkalu, joka estää mainokset, seuraimet ja haittaohjelmaverkkotunnukset automaattisesti.

Q4: Onko Proton VPN oikeudellisesti suojattu Sveitsissä?

Kyllä, Sveitsillä on tiukka tietosuojalainsäädäntö, ja se on Yhdysvaltojen sekä EU:n ja 14 Eyes -yhteenliittymän lainkäyttöalueen ulkopuolella. [4]

Q5: Ovatko Proton VPN:n sovellukset avointa lähdekoodia?

Kyllä. Proton VPN:n sovellukset ovat avointa lähdekoodia, ja niille on tehty julkaistuja tietoturva-auditointeja.

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

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

Q6: Mitä salausalgoritmeja käytetään?

Proton VPN käyttää AES-256-GCM:ää tai ChaCha20-Poly1305:tä HMAC-SHA384:n ja RSA-4096-kättelyjen kanssa.

Q7: Onko Proton VPN:ssä Kill Switch?

Kyllä, Proton VPN sisältää tavallisen ja pysyvän Kill Switchin salaamattomien vuotojen estämiseksi.

Q8: Voiko Proton VPN vuotaa DNS-kyselyjä?

Ei, kaikki DNS-kyselyt reititetään Protonin omistamien salattujen yksityisten DNS-palvelimien kautta.

Q9: Tallentaako Proton VPN yhteyslokeja?

Ei, Proton VPN noudattaa tiukkaa lokittomuuskäytäntöä, jonka Securitumin vuosittaiset auditoinnit vahvistavat. [3]

Q10: Onko Proton VPN altis WebRTC-vuodoille?

Ei, Proton-asiakasohjelmissa on sisäänrakennetut palomuurisäännöt ja reitityskäytännöt, jotka estävät WebRTC-vuodot.

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

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

Q1: Missä Secure Core -datakeskukset fyysisesti sijaitsevat?

Ne sijaitsevat Sveitsissä, Islannin entisellä sotilastukikohdalla ja maanalaisessa kohteessa Ruotsissa. [1]

Q2: Miten täydellinen eteenpäin salaisuus (PFS) toimii Proton VPN:ssä?

Jokaiselle istunnolle luodaan yksilöllinen tilapäinen salausavain, mikä estää jälkikäteisen salauksen purkamisen.

Q3: Mikä on Permanent Kill Switch Windowsissa/Linuxissa?

Pysyvä kill switch estää kaiken verkkoliikenteen, vaikka VPN-sovellus suljettaisiin kokonaan tai se kaatuisi.

Q4: Tukeeko Proton VPN IPv6-reititystä ja vuotosuojausta?

Proton VPN reitittää IPv6-liikenteen kokonaan tunneleiden kautta tai poistaa sen turvallisesti käytöstä vuotojen estämiseksi.

Q5: Miten NetShieldin DNS-suodatus käsittelee HTTPS-tarkastuksen?

NetShield toimii pelkästään DNS-selvityksen tasolla ilman tunkeilevaa TLS-salauksen purkua.

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

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

Q6: Kuka suoritti Proton VPN:n kolmannen osapuolen koodiauditoinnit?

SEC Consult auditoi sovellukset, ja Securitum auditoi sovellukset ja no-logs-käytännön.

Q7: Miten Stealth-protokolla vertautuu OpenVPN XOR:iin tai Shadowsocksiin?

Stealth tunneloi WireGuardin obfuskoidun TLS:n kautta ja suoriutuu paremmin kuin vanhempi OpenVPN-pohjainen obfuskointi. [5]

Q8: Voivatko Sveitsin viranomaiset pakottaa Proton VPN:n tallentamaan liikennettä?

Proton kertoo, ettei Sveitsin lain mukaan sillä ole velvollisuutta säilyttää lokeja käyttäjien toiminnasta tai tiedoista.

Q9: Miten Proton VPN:n palvelimet suojataan takavarikolta?

Kaikki Proton VPN:n palvelimet ovat bare-metal-koneita, joita suojaa koko levyn salaus. [2]

Q10: Tukeeko Proton VPN omia DNS-palvelinmäärityksiä?

Kyllä, maksavat tilaajat voivat määrittää omia ylävirran DNS-palvelimia suoraan sovelluksen asetuksissa.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

1. Proton omistaa ja asentaa Secure Core -palvelimensa itse korkean turvallisuuden kohteissa Sveitsissä, Islannissa ja Ruotsissa. [1]

2. VPN-OIVALLUS

2. Proton VPN:n asiakassovellukset ovat avointa lähdekoodia, ja niille tehdään toistuvia kolmannen osapuolen kooditarkastuksia.

3. VPN-OIVALLUS

3. Stealth-hämärtysprotokolla ohittaa syvän pakettitarkastuksen simuloimalla tavallista TLS-liikennettä.

4. VPN-OIVALLUS

4. Sveitsi on 5-Eyes-, 9-Eyes- ja 14-Eyes-kansainvälisten tiedustelutietojen jakoliittoumien ulkopuolella. [4]

5. VPN-OIVALLUS

5. NetShield toimii DNS-selvittäjän tasolla ja estää mainokset ja haittaohjelmat ennen hyötykuorman latausta.

6. VPN-OIVALLUS

6. Perfect Forward Secrecy varmistaa, etteivät vaarantuneet avaimet pysty purkamaan aiemmin tallennettuja liikenneistuntoja. [7]

7. VPN-TIETOA

7. Proton VPN käyttää bare-metal-palvelimilla koko levyn salausta palvelinmääritysten suojaamiseen. [2]

8. VPN-TIETOA

8. Pysyvä kill switch estää salaamattomien tietojen vuotamisen jopa käyttöjärjestelmän uudelleenkäynnistysten aikana.

9. VPN-TIETOA

9. Securitum on auditoinut ja vahvistanut Proton VPN:n lokittomuuskäytännön viidessä peräkkäisessä vuosiauditoinnissa. [3]

10. VPN-OIVALLUS

10. Proton VPN:n kehittivät tutkijat, jotka tapasivat CERNissä (Euroopan ydintutkimusjärjestö). [4]

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Kysymys 1** **Oikea vastaus: B**

OPETTAJALLE

Secure Core -palvelimet sijaitsevat korkean turvallisuuden toimipaikoissa, kuten entisellä sotilastukikohdalla Islannissa ja maanalaisessa konesalissa Ruotsissa.

2 **Stealth-obfuskointiprotokolla** SENSUURIN TORJUNTA **Oikea vastaus: B**

OPETTAJALLE

Protonin Stealth-protokolla naamioi WireGuard-yhteydet tavalliseksi TLS/HTTPS-liikenteeksi syväpakettitarkastuksen (DPI) palomuurien ohittamiseksi. Lähde: Proton Stealth Protocol Whitepaper.

3 **NetShieldin DNS-mainosesto** DNS-SUODATUS **Oikea vastaus: B**

OPETTAJALLE

NetShield käyttää DNS-tason suodatusta haittaohjelmaverkkotunnusten, vakoiluohjelmien, häiritsevän mainonnan ja telemetriaseuraimien estämiseen ennen verkkosivujen latautumista. Lähde: NetShield Security Specs.

4 **Sveitsin oikeudellinen lainkäyttöalue** LAINKÄYTTÖVALTA **Oikea vastaus: C**

OPETTAJALLE

Proton AG:n pääkonttori on Genevessä Sveitsissä, mikä tuo vahvan Sveitsin yksityisyyslainsäädännön suojan Yhdysvaltojen ja EU:n 14 Eyes -valvontaliittoumien ulkopuolella. Lähde: Swiss Federal Data Protection Act.

5 **Kysymys 5** **Oikea vastaus: B**

OPETTAJALLE

Kaikki Proton VPN -sovellukset ovat avoimen lähdekoodin sovelluksia; SEC Consult ja myöhemmin Securitum ovat tarkastaneet ne.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Secure Core: usean lainkäyttöalueen reititys** REITITYSARKKITEHTUURI Oikea vastaus: Tosi

OPETTAJALLE

Secure Core reitittää liikenteen vahvan tietosuojan lainkäyttöalueiden kautta ennen poistumista kohdemaahan, mikä voi auttaa suojautumaan vaarantuneelta poistumispalvelimelta. Lähde: Secure Core Architecture.

7 **Sveitsin valvontaliittouma** VALVONTALIITOT Oikea vastaus: Epätosi

OPETTAJALLE

Sveitsi ei ole 5 Eyes-, 9 Eyes- tai 14 Eyes -tiedustelutietojen jakosopimusten jäsen, mikä säilyttää itsenäisen oikeudellisen suvereniteetin. Lähde: International Surveillance Treaties.

8 **Kysymys 8** Oikea vastaus: Tosi

OPETTAJALLE

NetShield käyttää Protonin DNS-palvelimia tarkistaakseen verkkotunnukset tunnettujen mainos-, seuranta- ja haittaohjelmatunnusten luetteloita vasten.

9 **Avoimen lähdekoodin asiakasohjelman tarkastus** TIETOTURVAN LÄPINÄKYVYYS Oikea vastaus: Tosi

OPETTAJALLE

Proton on tehnyt työpöytä- ja mobiilisovelluksistaan avoimen lähdekoodin ja julkaisee kolmansien osapuolten tarkastusraportit. Lähde: SEC Consult Security Report.

10 **Kysymys 10** Oikea vastaus: Epätosi

OPETTAJALLE

Epätosi: Stealth tunneloi WireGuardin obfuskoidun TLS:n sisällä TCP:n yli, jolloin liikenne näyttää tavalliselta HTTPS-liikenteeltä.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

G 1. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. SVEITSIN LAKI
H 5. KILL SWITCH	A 6. AVOIN KOODI	E 7. WIREGUARD	B 8. AES-GCM

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 SVEITSIN LAKI
5 KILL SWITCH	6 AVOIN KOODI		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 B – STEALTH	2 G – WIREGUARD	3 D – SVEITSINLAKI	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – AVOINKOODI

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit SECURE CORE, STEALTH ja NETSHIELD omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

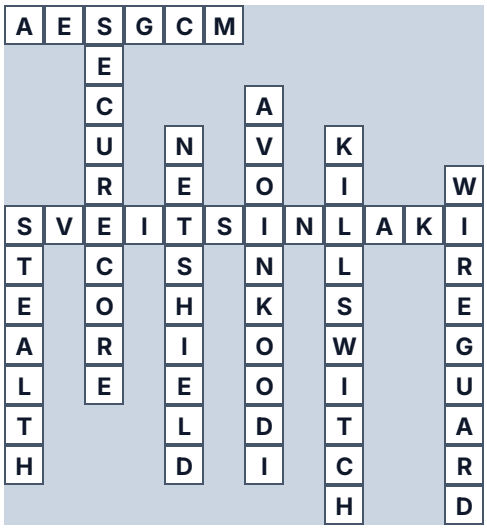
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

1 vaakasuoraan: AESGCM Sotilastason symmetrinen salaus, joka suojaa kaikki kapseloidut VPN-datapaketit (6 kirjainta)

7 vaakasuoraan: SVEITSINLAKI Sveitsin tiukat yksityisyyslait 14 Eyes -lainkäyttöalueiden ulkopuolella (12 kirjainta)

PYSTYSUORAAN

2 pystysuoraan: SECURECORE Monihyppyarkkitehtuuri, joka reitittää liikenteen Protonin omistamien ensimmäisen hypyn palvelinten kautta (10 kirjainta)

3 pystysuoraan: AVOINKOODI Julkisesti saatavilla oleva ja riippumattomasti tarkastettu asiakassovellus (10 kirjainta)

4 pystysuoraan: NETSHIELD DNS-pohjainen suodatin, joka estää mainokset, telemetriaseurannat ja haittaohjelmat (9 kirjainta)

5 pystysuoraan: KILLSWITCH Suojaominaisuus, joka pysäyttää verkkoliikenteen yhteyden katketessa (10 kirjainta)

6 pystysuoraan: WIREGUARD Moderni kevyt protokolla, joka tarjoaa vankan salauksen ja nopeat yhteydet (9 kirjainta)

7 pystysuoraan: STEALTH Hämäävä tunnelointiprotokolla, joka on naamioitu tavalliseksi HTTPS-verkkoliikenteeksi (7 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. RCERESOEUC — **SECURECORE**
2. DNLSEIEHT — **NETSHIELD**
3. KWCIISHLTL — **KILLSWITCH**
4. GDREAUWIR — **WIREGUARD**
5. LHAESTT — **STEALTH**
6. ITLASKNSVIEI — **SVEITSINLAKI**
7. VIAOKODINO — **AVOINKOODI**
8. SMACGE — **AESGCM**

SALAKIRJOITUSHAASTEEN AVAIN

"SECURE CORE PALVELIMET SUOJAAVAT TIETOSI"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: RAJOITTAVIEN PALOMUURIEN OHITTAMINEN

Opettajan ratkaisu

ARVIOINTIKRITEERIT JA RATKAISUOHJEET

- Tilanneanalyysi: Käyttäjä matkustaa maahan, jossa tavallinen VPN-liikenne, kuten OpenVPN ja WireGuard, on estetty DPI:llä.
- Pohdintakysymys: Mikä Proton VPN -protokollan asetus antaa käyttäjän ohittaa valtiotason tarkastuksen?
- Suositeltu strategia ja ratkaisu: Käyttäjän tulisi aktivoida Stealth-protokolla, joka hämärtää VPN-pakettien otsikot tavalliseksi TLS/HTTPS-verkkoliikenteeksi ja livahtaa DPI-suodattimien ohi.

B TAPAUSTUTKIMUS 2: EDISTYNYT SUOJAUS VASTUSTAJAA VASTAAN

Opettajan ratkaisu

ARVIOINTIKRITEERIT JA RATKAISUOHJEET

- Tilanneanalyysi: Taloustarkastaja epäilee, että hänen paikallisen palveluntarjoajansa ulostulosolmu saattaa olla kehittyneiden jatkuvien uhkien (APT) vaarantama.
- Pohdintakysymys: Miten Secure Core suojaa auditoijan henkilöllisyyttä poistumissolmun vaarantumiselta?
- Suositeltu strategia ja ratkaisu: Secure Core reitittää liikenteen ensin Protonin omistamien Sveitsin, Islannin tai Ruotsin palvelinten kautta, joten vaarantunut ulostulopalvelin ei voi jäljittää käyttäjän IP-osoitetta.