Nimi: _____ Päivämäärä: _____ Pisteet: _____

CyberGhostin turvallisuus

CyberGhostin tietoturvainfrastruktuurin, Romaniassa sijaitsevien omien NoSpy-palvelinryhmien, levyttömien vain RAM-muistia käyttävien palvelinsolmujen, AES-256-salauksen ja automaattisen kill switch -suojauksen arviointi.

CYBERGHOSTIN TURVALLISUUDEN OPPIMISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: CyberGhostin tietoturvaominaisuudet. Tutustut itse omistettuihin NoSpy-palvelinryhmiin, levyttömään vain RAM-muistia käyttävään laitteistoon, salauksiin ja kill switcheihin.

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/cyberghost/tietoturva/

Oppimispolkusi: CyberGhostin tietoturva

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

CYBERGHOSTIN TURVALLISUUSOPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: salaus ja NoSpy-palvelimet. Lopuksi bonustehtävä Nopeat vastaukset.

OMAT NOSPY-PALVELININFRASTRUKTUURIT JA LEVYTTÖMÄT SOLMUT (JOHDANTO)

CyberGhost ylläpitää yksityisesti hallinnoituja NoSpy-palvelimia Bukarestin, Romanian, pääkonttorissaan ohittaen kaupallisten isännöintipalvelujen riskit. Turvallisuus varmistetaan AES-256-salauksilla, levyttömällä vain RAM-muistia käyttävällä laitteistolla ja automaattisilla kill switcheilla.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mitä protokollaa CyberGhost tarjoaa kaikilla suurilla alustoilla?

- A) WireGuard
- B) OpenVPN
- C) IKEv2
- D) L2TP

2. Mitä salausalgoritmia CyberGhostin OpenVPN- ja IKEv2-yhteydet käyttävät?

- A) AES-256
- B) Blowfish-128
- C) DES-56
- D) RC4

3. Missä CyberGhostin itse ylläpitämät NoSpy-palvelimet sijaitsevat?

- A) Romania
- B) Saksa
- C) Yhdysvallat
- D) Sveitsi

4. Minkä tyyppinen infrastruktuuri ei tallenna lokeja levylle virran katkaisun jälkeen?

- A) Vain RAM-muistia käyttävät palvelimet
- B) HDD-palvelimet
- C) Virtuaalipalvelimet
- D) Hybridipalvelimet

5. Mikä ominaisuus estää yhteydet VPN-katkosten aikana?

- A) Kill switch
- B) Jaettu tunnelointi
- C) Smart DNS
- D) Portinohjaus

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. CyberGhostin pääkonttori on Romaniassa, 14 Eyes -ryhmän ulkopuolella.

○ Tosi ○ Epätosi

7 Kysymys 7

7. NoSpy-palvelimet vuokrataan kolmannen osapuolen kaupallisista konesaleista.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Pelkkää RAM-muistia käyttävät palvelimet kirjoittavat käyttäjien istuntotiedot pysyville SSD-levyille.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Asiakassovelluksessa on sisäänrakennettu suoja DNS-vuotoja vastaan.

○ Tosi ○ Epätosi

10 Kysymys 10

10. CyberGhostin zero-logs-käytäntö on varmennettu riippumattomilla auditoinneilla.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. **Mobiiliyhteyksille suositeltu suorituskykyinen protokolla on _____ .**

2. **Hyötykuorman liikenne salataan erittäin turvallisella symmetrisellä salausalgoritmilla nimeltä _____ .**

3. **Yhtiön pääkonttori sijaitsee maassa nimeltä _____ , jonka lainkäyttöalueen säännöt pätevät.**

4. **Yhtiön omistamia itse hallinnoituja korkean turvallisuustason palvelimia kutsutaan nimellä _____ .**

5. **Jottei data säily virrankatkaisun jälkeen, käytetään levyttömiä palvelimia, joita kutsutaan nimellä _____ .**

6. **Salaamattoman liikenteen paljastuminen yhteyden katketessa estetään vikasuojakytkimellä nimeltä _____ .**

SANASTON SANAPANKKI

AES-256 AUDITOINTI KILL SWITCH NOSPY ROMANIA VAIN RAM VUOTO WIREGUARD

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

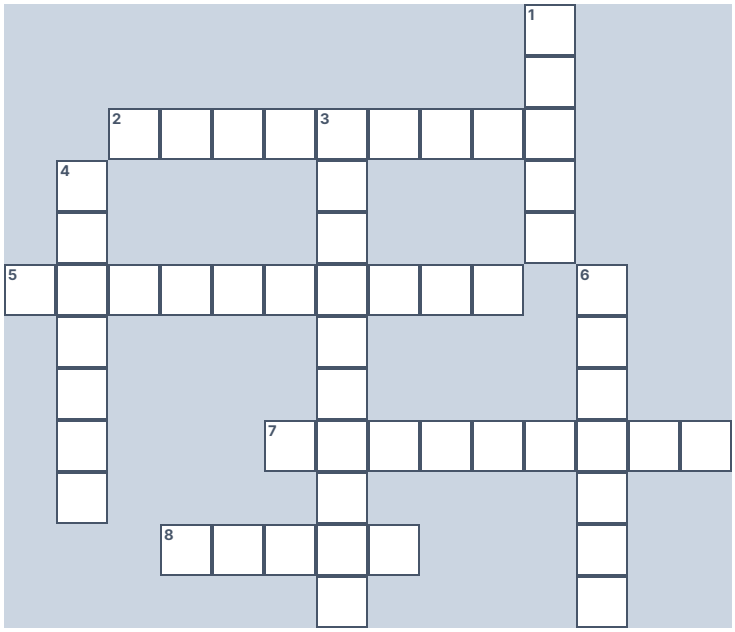
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. WIREGUARD	A	Kansallinen yksityisyyden lainkäyttöalue 14 Eyes -liittoumien ulkopuolella.
☐	2. AES-256	B	Levytön palvelininfrastruktuuri, joka ei kirjoita lainkaan pysyviä lokeja.
☐	3. ROMANIA	C	Selainkyselyjen tahaton paljastuminen VPN:n ulkopuolelle.
☐	4. NOSPY	D	Nopea avoimen lähdekoodin protokolla, joka on saatavilla CyberGhostin sovelluksissa.
☐	5. VAIN RAM	E	Kolmannen osapuolen validointi, joka tarkastelee lokittomuutta koskevien väitteiden noudattamista.
☐	6. KILL SWITCH	F	Symmetrinen salausstandardi, joka suojaa hyötykuormien kulkua tunneleiden läpi.
☐	7. VUOTO	G	Täysin omistettu, erittäin turvallinen palvelinjoukko, jota ylläpidetään Romaniassa.
☐	8. AUDITOINTI	H	Vikaturva-asiakasohjelman apuohjelma, joka katkaisee internetliikenteen yhteyden katketessa.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Symmetrinen salausstandardi, joka suojaa tunneleiden hyötykuormaliikenteen (9)

5. Vikasuojattu asiakastyökalu, joka katkaisee internetliikenteen yhteyden pudotessa (10)

7. Nopea avoimen lähdekoodin protokolla, joka on saatavilla CyberGhostin sovelluksissa (9)

8. Selvityspyyntöjen tahaton paljastuminen VPN:n ulkopuolelle (5)

PYSTYSUORAAN

1. Täysin omistettu korkean turvallisuuden palvelinryhmä, jota ylläpidetään Romaniassa (5)

3. Kolmannen osapuolen tarkistus, joka arvioi väitteitä lokittomuuden noudattamisesta (10)

4. Levytön palvelininfrastruktuuri, joka ei kirjoita lainkaan pysyviä lokeja (7)

6. Kansallinen yksityisyyden lainkäyttöalue 14 Eyes -liittoumien ulkopuolella (7)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Symmetrinen salausstandardi, joka suojaa tunneleiden hyötykuormaliikenteen (9 kirjainta):

5 vaakasuoraan: Vikasuojattu asiakastyökalu, joka katkaisee internetliikenteen yhteyden pudotessa (10 kirjainta):

7 vaakasuoraan: Nopea avoimen lähdekoodin protokolla, joka on saatavilla CyberGhostin sovelluksissa (9 kirjainta):

8 vaakasuoraan: Selvityspyyntöjen tahaton paljastuminen VPN:n ulkopuolelle (5 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Täysin omistettu korkean turvallisuuden palvelinryhmä, jota ylläpidetään Romaniassa (5 kirjainta):

3 pystysuoraan: Kolmannen osapuolen tarkistus, joka arvioi väitteitä lokittomuuden noudattamisesta (10 kirjainta):

4 pystysuoraan: Levytön palvelininfrastruktuuri, joka ei kirjoita lainkaan pysyviä lokeja (7 kirjainta):

6 pystysuoraan: Kansallinen yksityisyyden lainkäyttöalue 14 Eyes -liittoumien ulkopuolella (7 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

WIREGUARD AESSALAUS ROMANIA NOSPY VAINRAM KILLSWITCH
VUOTO AUDITOINTI

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. WIREGUARD**
- **B. AESSALAUS**
- **C. ROMANIA**
- **D. NOSPY**
- **E. VAINRAM**
- **F. KILLSWITCH**
- **G. VUOTO**
- **H. AUDITOINTI**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Selvityspyyntöjen tahaton paljastuminen VPN:n ulkopuolelle.
2. Nopea avoimen lähdekoodin protokolla, joka on saatavilla CyberGhostin sovelluksissa.
3. Täysin omistettu korkean turvallisuuden palvelinryhmä, jota ylläpidetään Romaniassa.
4. Vikasuojattu asiakastyökalu, joka katkaisee internetliikenteen yhteyden pudotessa.
5. Symmetrinen salausstandardi, joka suojaa tunneleiden hyötykuormaliikenteen.
6. Kansallinen yksityisyyden lainkäyttöalue 14 Eyes -liittoumien ulkopuolella.
7. Kolmannen osapuolen tarkistus, joka arvioi väitteitä lokittomuuden noudattamisesta.
8. Levytön palvelininfrastruktuuri, joka ei kirjoita lainkaan pysyviä lokeja.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. **UGEIWARDR** _____

2. **RMAINAO** _____

3. **NVRMIAA** _____

4. **OOTVU** _____

5. **AAESLSAUS** _____

6. **PNSYO** _____

7. **ILKIWTCHSL** _____

8. **TIOIATUIND** _____

Bonustehtävä: Nopeat vastaukset

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

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

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: LAINKÄYTTÖALUEEN YKSITYISYYSTARKASTUS



Tilanne: Mediayritys haluaa varmistaa, ettei ulkomainen lainvalvonta voi haastaa yrityksen tiedusteluaineistoa oikeuteen.

Keskustelukysymys: Miten CyberGhostin romanialainen pääkonttori suojaa yritystä valvontamääräyksiltä?

TAPAUSTUTKIMUS 2: LAITTEISTON TAKAVARIKOINNIN TURVALLISUUS



Tilanne: Palvelinkeskukseen tehdään luvaton fyysinen tunkeutuminen, ja VPN-palvelinkaappi takavarikoidaan.

Keskustelukysymys: Mikä laitteistosuunnittelu estää tunkeilijoita poimimasta istuntoavaimia tai käyttäjähistoriaa?

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

14	15	19	16	25		16	1	12	22	5	12	9	13	5	20

20	1	11	1	1	22	1	20		20	9	5	20	15	10	5	14

25	11	19	9	20	25	9	19	25	25	4	5	14

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: Onko CyberGhost turvallinen?

Kyllä, se käyttää AES-256-salausta ja turvallisia protokollia, ja sen toimintaan sovelletaan Romanian tietosuojalakeja.

Q2: Mitä ovat NoSpy-palvelimet?

NoSpy-palvelimet ovat yksinomaan CyberGhostin omistamia, rakentamia ja hallinnoimia sen Romanian pääkonttorissa maksimaalisen turvallisuuden vuoksi.

Q3: Tallentaako CyberGhost lokeja?

Ei, se noudattaa tiukkaa lokittomuuskäytäntöä, eli selaushistoriaa tai yhteyslokeja ei tallenneta.

Q4: Missä CyberGhost toimii?

CyberGhost sijaitsee Bukarestissa, Romaniassa, jonka perustuslakituomioistuin kumosi yleiset tietojen säilytyslait vuosina 2009 ja 2014, vaikka vuoden 2015 laki velvoittaa jälleen sähköisen viestinnän tarjoajia säilyttämään tiettyjä liikennetietoja.

Q5: Mitä protokollia se käyttää?

Se tukee WireGuardia, OpenVPN:ää (TCP/UDP) ja IKEv2-protokollia laitetyypeistä riippuen.

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

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

Q6: Estääkö se mainoksia?

Kyllä, asiakassovelluksessa on sisäänrakennettu sisällönesto mainoksille, seurantaskripteille ja haittaohjelmien verkkotunnuksille.

Q7: Onko kill switchiä?

Kyllä, siinä on automaattinen kill switch, joka estää internetyhteyden, jos VPN-yhteys katkeaa.

Q8: Suojaako CyberGhost vuodoilta?

Kyllä, sovelluksissa on sisäänrakennettu DNS- ja IP-vuotosuoja, joka piilottaa todellisen IP-osoitteesi.

Q9: Tarkastetaanko palvelimet?

Kyllä, Deloitte auditoi CyberGhostin zero-logs-käytännön ja infrastruktuurin riippumattomasti. [2]

Q10: Käyttääkö se RAM-palvelimia?

Kyllä, CyberGhost kuvaa palvelinverkkonsa toimivan levyttömällä, pelkästään RAM-muistia käyttävällä laitteistolla.

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

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

Q1: Mitä protokollaa käytetään oletuksena?

Sovellus valitsee parhaan protokollan automaattisesti, mutta voit vaihtaa sitä milloin tahansa.

Q2: Miten jaettu tunnelointi toimii?

Se antaa sinun valita, mitkä sovellukset ja sivustot käyttävät VPN:ää ja mitkä ohittavat tunnelin.

Q3: Minne DNS-kyselyt menevät?

Ne lähetetään VPN-tunnelin kautta CyberGhostin omille DNS-palvelimille, ei palveluntarjoajasi palvelimille.

Q4: Kuka omistaa CyberGhostin?

CyberGhost on Kape Technologiesin omistuksessa, joka omistaa myös ExpressVPN:n ja Private Internet Accessin. [7]

Q5: Mitä salausalgoritmia WireGuardin kanssa käytetään?

WireGuard käyttää nykyaikaista ChaCha20-Poly1305-symmetristä salausstandardia. [9]

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

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

Q6: Miten NoSpy-palvelimet eroavat?

Niissä on suuremman kaistanleveyden laitteisto, dedikoidut yhteydet ja ne sijaitsevat yksityisessä datakeskuksessa.

Q7: Ovatko Dedicated IP -osoitteet anonyymejä?

Kyllä, IP-osoite yhdistetään satunnaiseen tunnisteeseen tilisi sijaan, ja tunniste poistetaan.

Q8: Kuka tarkastaa lokittomuuskäytännön?

Deloitte Audit Romania, joka suoritti CyberGhostin kolmannen lokittomuustarkastuksen vuonna 2025.

Q9: Purkaako mainosesto HTTPS-salauksen?

Ei, mainosesto toimii DNS-tasolla ja ohjaa mainosverkkotunnukset mustiin aukkoihin.

Q10: Voinko käyttää CyberGhostia reitittimessä?

Kyllä, asenna CyberGhost VPN-yhteensopivaan reitittimeen, niin suojaus kattaa kaikki kodin laitteet.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

CyberGhostin pääkonttori on Romaniassa, Five Eyes -tiedustelutietojen jakamisliiton ulkopuolella. [1]

2. VPN-OIVALLUS

OpenVPN ja IKEv2 käyttävät AES-256:ta, kun taas WireGuard käyttää ChaCha20-Poly1305:ä. [5]

3. VPN-OIVALLUS

NoSpy-palvelimet ovat CyberGhostin henkilökunnan omistamia ja talon sisällä hallinnoimia. [3]

4. VPN-OIVALLUS

Deloitte tarkastaa ja todentaa säännöllisesti niiden lokittomat toimintakäytännöt. [2]

5. VPN-OIVALLUS

Levyttömät, vain RAM-muistia käyttävät palvelinryhmät estävät tietojen säilymisen virran katkaisun jälkeen. [1]

6. VPN-OIVALLUS

Asiakassovelluksessa on automaattinen kill switch VPN-yhteyden katkeamisen varalta.

7. VPN-TIETOA

Sisäänrakennettu DNS- ja IP-vuotosuoja auttaa pitämään todellisen IP-osoitteesi piilossa.

8. VPN-TIETOA

WireGuard-, OpenVPN- ja IKEv2-protokollat ovat tuettuina natiivisti asiakasohjelmassa. [4]

9. VPN-TIETOA

Omat IP-osoitteet myönnetään suojatulla, nollatietoon perustuvalla token-järjestelmällä. [8]

10. VPN-OIVALLUS

Sisäänrakennetut haittaohjelmasuodattimet tarkistavat verkkotunnushaut ja estävät haitalliset kohteet. [6]

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] CyberGhost VPN. (n.d.). No-Logs VPN: Secure & Private VPN with Zero Tracking.
https://www.cyberghostvpn.com/features/no-logs-vpn

[2] CyberGhost VPN. (2025). Third Deloitte Romania Audit Verifies Our Commitment to Privacy.
https://www.cyberghostvpn.com/privacyhub/privacy-audit-2025/

[3] CyberGhost VPN. (n.d.). CyberGhost's NoSpyServers: Complete Privacy & Anonymity.
https://www.cyberghostvpn.com/features/nospy

[4] CyberGhost VPN Support Center. (n.d.). Which VPN Protocols Do You Support?
https://support.cyberghostvpn.com/hc/en-us/articles/213983829-Which-VPN-Protocols-Do-You-Support

[5] CyberGhost VPN. (n.d.). VPN Encryption: How VPNs Help Secure Your Browsing.
https://www.cyberghostvpn.com/features/vpn-encryption

[6] CyberGhost VPN. (n.d.). VPN Features and Use Cases.
https://www.cyberghostvpn.com/features

[7] Kape Technologies. (n.d.). Our Brands.
https://www.kape.com/our-brands/

[8] CyberGhost VPN. (n.d.). Dedicated IP VPN | Get a Secure Static IP Address.
https://www.cyberghostvpn.com/dedicated-ip-vpn

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

[10] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[11] National Institute of Standards and Technology. (n.d.). FIPS 197: Advanced Encryption Standard (AES).
https://csrc.nist.gov/pubs/fips/197/final

[12] European Digital Rights (EDRi). (2014). Romania: The aftermath of the second CCR data retention ruling.
https://edri.org/our-work/romania-aftermath-of-second-ccr-data-retention-ruling/

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Kysymys 1** — **Oikea vastaus: A**

OPETTAJALLE

Mitä protokollaa CyberGhost tarjoaa kaikilla suurilla alustoilla? → A) WireGuard

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

OPETTAJALLE

Mitä salausalgoritmia CyberGhostin OpenVPN- ja IKEv2-yhteydet käyttävät? → A) AES-256

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

OPETTAJALLE

Missä CyberGhostin itse ylläpitämät NoSpy-palvelimet sijaitsevat? → Romania

4 **Kysymys 4** — **Oikea vastaus: A**

OPETTAJALLE

Minkä tyyppinen infrastruktuuri ei tallenna lokeja levylle virran katkaisun jälkeen? → Vain RAM-muistia käyttävät palvelimet

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

OPETTAJALLE

Mikä ominaisuus estää yhteydet VPN-katkosten aikana? → Kill switch

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 Kysymys 6

Oikea vastaus: Tosi

OPETTAJALLE

CyberGhostin pääkonttori on Romaniassa, 14 Eyes -ryhmän ulkopuolella. [1]

7 Kysymys 7

Oikea vastaus: Epätosi

OPETTAJALLE

NoSpy-palvelimet vuokrataan kolmannen osapuolen kaupallisista konesaleista.

8 Kysymys 8

Oikea vastaus: Epätosi

OPETTAJALLE

Pelkkää RAM-muistia käyttävät palvelimet kirjoittavat käyttäjien istuntotiedot pysyville SSD-levyille.

9 Kysymys 9

Oikea vastaus: Tosi

OPETTAJALLE

Asiakassovelluksessa on sisäänrakennettu suoja DNS-vuotoja vastaan.

10 Kysymys 10

Oikea vastaus: Tosi

OPETTAJALLE

CyberGhostin zero-logs-käytäntö on varmennettu riippumattomilla auditoinneilla.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

D 1. WIREGUARD	F 2. AES-256	A 3. ROMANIA	G 4. NOSPY
B 5. VAIN RAM	H 6. KILL SWITCH	C 7. VUOTO	E 8. AUDITOINTI

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 WIREGUARD	2 AES-256	3 ROMANIA	4 NOSPY
5 VAIN RAM	6 KILL SWITCH		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – VUOTO	2 A – WIREGUARD	3 D – NOSPY	4 F – KILLSWITCH
5 B – AESSALAUS	6 C – ROMANIA	7 H – AUDITOINTI	8 E – VAINRAM

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit WIREGUARD, AES-256 ja ROMANIA omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

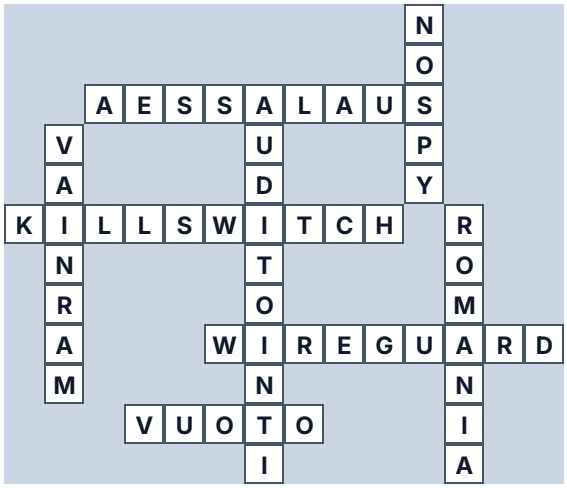
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: AESSALAUS Symmetrinen salausstandardi, joka suojaa tunneleiden hyötykuormaliikenteen (9 kirjainta)

5 vaakasuoraan: KILLSWITCH Vikasuojattu asiakastyökalu, joka katkaisee internetliikenteen yhteyden pudotessa (10 kirjainta)

7 vaakasuoraan: WIREGUARD Nopea avoimen lähdekoodin protokolla, joka on saatavilla CyberGhostin sovelluksissa (9 kirjainta)

8 vaakasuoraan: VUOTO Selvityspyyntöjen tahaton paljastuminen VPN:n ulkopuolelle (5 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: NOSPY Täysin omistettu korkean turvallisuuden palvelinryhmä, jota ylläpidetään Romaniassa (5 kirjainta)

3 pystysuoraan: AUDITOINTI Kolmannen osapuolen tarkistus, joka arvioi väitteitä lokittomuuden noudattamisesta (10 kirjainta)

4 pystysuoraan: VAINRAM Levytön palvelininfrastruktuuri, joka ei kirjoita lainkaan pysyviä lokeja (7 kirjainta)

6 pystysuoraan: ROMANIA Kansallinen yksityisyyden lainkäyttöalue 14 Eyes -liittoumien ulkopuolella (7 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. UGEIWARDR — **WIREGUARD**
2. RMAINAO — **ROMANIA**
3. NVRMIAA — **VAINRAM**
4. OOTVU — **VUOTO**
5. AAESLSAUS — **AESSALAUS**
6. PNSYO — **NOSPY**
7. ILKIWTCHSL — **KILLSWITCH**
8. TIOIATUIND — **AUDITOINTI**

SALAKIRJOITUSHAASTEEN AVAIN

"NOSPY PALVELIMET TAKAAVAT TIETOJEN YKSITYISYYDEN"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: LAINKÄYTTÖALUEEN YKSITYISYYSTARKASTUS

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Mediayritys haluaa varmistaa, että yrityksen tiedusteluaineistoa ei voida haastaa ulkomaisten lainvalvontaviranomaisten toimesta.
- Suositeltu strategia ja ratkaisu: Romaniassa on vahva tietosuojalainsäädäntö, eikä se ole Five Eyes- tai Fourteen Eyes -tiedustelutietoa jakavien verkostojen jäsen.

B TAPAUSTUTKIMUS 2: LAITTEISTON TAKAVARIKOINNIN TURVALLISUUS

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Palvelintilassa tapahtuu luvaton fyysinen tunkeutuminen ja VPN-palvelinkaappi takavarikoidaan.
- Suositeltu strategia ja ratkaisu: Palvelin toimii RAM-only-arkkitehtuurilla, mikä tarkoittaa, että kaikki tiedot häviävät heti, kun virta katkaistaan.