Nimi: _____ Päivämäärä: _____ Pisteet: _____

ExpressVPN:n tietoturva

ExpressVPN:n tietoturvainfrastruktuurin, oman avoimen lähdekoodin Lightway-protokollan, vain RAM-muistia käyttävän TrustedServer-teknologian, riippumattomien tietoturvatarkastusten ja Network Lock -kill switchin arviointi.

EXPRESSVPN-TIETOTURVA: YLEISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: ExpressVPN:n tietoturvaominaisuudet. Tutustut avoimen lähdekoodin protokolliin, vain RAM-muistia käyttäviin palvelinsolmuihin, salaimiin ja Internet Kill Switchiin.

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/expressvpn/tietoturva/

Oppimispolkusi: ExpressVPN:n tietoturva

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

EXPRESSVPN-TIETOTURVAOPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: avoimen lähdekoodin protokollat ja pelkästään RAM-muistia käyttävät palvelinsolmut. Lopuksi bonustehtävä Nopeat vastaukset.

PELKKÄÄ RAM-MUISTIA KÄYTTÄVÄT PALVELINRYHMÄT JA AVOIMEN LÄHDEKOODIN YHTEYSPROTOKOLLAT

ExpressVPN käyttää vain RAM-muistia hyödyntävää TrustedServer-teknologiaa paikallisten lokien estämiseksi yhdessä oman avoimen lähdekoodin Lightway-protokollansa ja Internet Kill Switchin kanssa tarjotakseen päästä päähän ulottuvan käyttäjätietojen turvan.

(JOHDANTO)

ExpressVPN käyttää vain RAM-muistia hyödyntävää TrustedServer-teknologiaa paikallisten lokien estämiseksi yhdessä oman avoimen lähdekoodin Lightway-protokollansa ja Internet Kill Switchin kanssa tarjotakseen päästä päähän ulottuvan käyttäjätietojen turvan.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Mikä on ExpressVPN:n oma avoimen lähdekoodin protokolla?**
   - A) Lightway
   - B) WireGuard
   - C) OpenVPN
   - D) Chameleon

2. **2. Mikä palvelinteknologia toimii yksinomaan haihtuvassa RAM-muistissa?**
   - A) TrustedServer
   - B) RAM-Core
   - C) SecureRAM
   - D) NoSpy-palvelin

3. **3. Mitä tapahtuu, jos VPN-yhteys katkeaa odottamatta?**
   - A) Kill switch estää liikenteen
   - B) Liikenne vuotaa internetoperaattorille
   - C) Järjestelmä käynnistyy uudelleen
   - D) Tiedot jäävät salaamattomiksi

4. **4. Missä ExpressVPN on rekisteröity yksityisyyden suojaamiseksi?**
   - A) Brittiläiset Neitsytsaaret
   - B) Sveitsi
   - C) Panama
   - D) Romania

5. **5. Mitä symmetristä salausalgoritmia käytetään oletuksena?**
   - A) AES-256-GCM
   - B) Blowfish
   - C) DES-64
   - D) RC4

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. TrustedServer-teknologia tallentaa palvelinlokit kiintolevyille.

○ Tosi ○ Epätosi

7 Kysymys 7

7. ExpressVPN on käynyt läpi kolmannen osapuolen tietoturvatarkastuksia.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Lightway-protokolla on rakennettu OpenVPN-koodipohjan päälle.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Kill switch on oletuksena päällä pöytäkonesovelluksissa.

○ Tosi ○ Epätosi

10 Kysymys 10

10. ExpressVPN ylläpitää yksityistä DNS:ää jokaisella palvelimella.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. ExpressVPN:n itse kehittämä nopea protokolla on _____ .

2. Tietojen säilytyksen estämiseksi palvelinverkko perustuu vain RAM-muistia käyttäviin solmuihin, joiden tekniikka on _____ .

3. ExpressVPN:n kill switchin entinen nimi oli Network _____ .

4. ExpressVPN on rekisteröity Brittiläisten _____ lainsäädännön mukaan.

5. Tietosisältö suojataan vahvalla symmetrisellä salauksella nimeltä _____ .

6. Nollalokipolitiikka on todennettu, ja sen ovat riippumattomasti _____ johtavat yritykset.

SANASTON SANAPANKKI

AES-256 LIGHTWAY LOCK NEITSYTSAARET NIMIPALVELIN TARKASTETTU TRUSTED SERVER VUOTO

Kirjoita vastauksesi tähän:

1.
2.
3.
4.
5.
6.

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

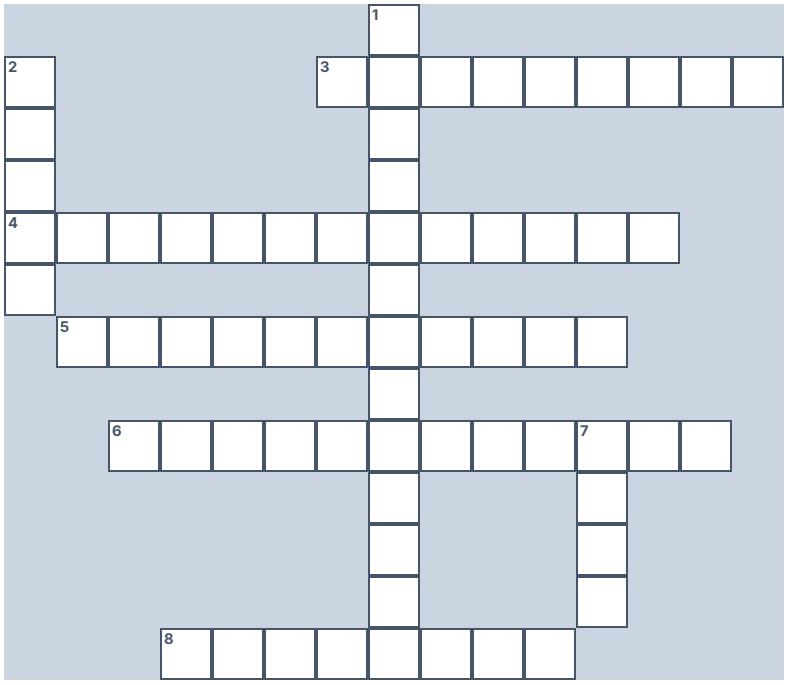
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. LIGHTWAY	A	Brittiläisten Neitsytsaarten lainkäyttöalue, joka tarjoaa vahvan yksityisyyden suojan
☐	2. TRUSTED SERVER	B	Yksityisen IP-, DNS- tai WebRTC-datan tahaton paljastuminen
☐	3. LUKKO	C	Verkkotunnusjärjestelmän ratkaisijat toimivat yksityisesti jokaisessa palvelinsolmussa
☐	4. SAARET	D	Kolmannen osapuolen tietoturvayritysten riippumattomasti varmentama
☐	5. AES-256	E	Pelkkää RAM-muistia käyttävä palvelinarkkitehtuuri, joka estää tietojen tallentamisen levylle
☐	6. AUDITOITU	F	Network Lockin, kill switchin entisen nimen, viimeinen sana
☐	7. VUOTO	G	ExpressVPN:n kevyt, avoimen lähdekoodin yhteysprotokolla
☐	8. DNS	H	Symmetrinen salausstandardi, joka suojaa tiedonsiirtoa

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

3. Symmetrinen salausstandardi, joka suojaa tiedonsiirtoa (9)

4. Vain RAM-muistia käyttävä palvelinarkkitehtuuri, joka estää tietojen tallentamisen levylle (13)

5. Riippumattomien tietoturvayritysten todentama (11)

6. Verkkotunnusjärjestelmän (DNS) nimipalvelimet toimivat yksityisesti jokaisessa palvelinsolmussa (12)

8. ExpressVPN:n kevyt, avoimen lähdekoodin yhteysprotokolla (8)

PYSTYSUORAAN

1. Brittiläisten Neitsytsaarten lainkäyttöalue, joka tarjoaa vahvan yksityisyyden suojan (13)

2. Yksityisen IP-, DNS- tai WebRTC-tiedon tahaton paljastuminen (5)

7. Network Lock -nimen viimeinen sana; kill switchin entinen nimi (4)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

3 vaakasuoraan: Symmetrinen salausstandardi, joka suojaa tiedonsiirtoa (9 kirjainta):

4 vaakasuoraan: Vain RAM-muistia käyttävä palvelinarkkitehtuuri, joka estää tietojen tallentamisen levylle (13 kirjainta):

5 vaakasuoraan: Riippumattomien tietoturvayritysten todentama (11 kirjainta):

6 vaakasuoraan: Verkkotunnusjärjestelmän (DNS) nimipalvelimet toimivat yksityisesti jokaisessa palvelinsolmussa (12 kirjainta):

8 vaakasuoraan: ExpressVPN:n kevyt, avoimen lähdekoodin yhteysprotokolla (8 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Brittiläisten Neitsytsaarten lainkäyttöalue, joka tarjoaa vahvan yksityisyyden suojan (13 kirjainta):

2 pystysuoraan: Yksityisen IP-, DNS- tai WebRTC-tiedon tahaton paljastuminen (5 kirjainta):

7 pystysuoraan: Network Lock -nimen viimeinen sana; kill switchin entinen nimi (4 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

LIGHTWAY TRUSTEDSERVER LOCK NEITSYTSAARET AESSALAUS
TARKASTETTU VUOTO NIMIPALVELIN

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. LIGHTWAY**
- **B. TRUSTEDSERVER**
- **C. LOCK**
- **D. NEITSYTSAARET**
- **E. AESSALAUS**
- **F. TARKASTETTU**
- **G. VUOTO**
- **H. NIMIPALVELIN**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

_____ 1. Yksityisen IP-, DNS- tai WebRTC-tiedon tahaton paljastuminen.

_____ 2. Brittiläisten Neitsytsaarten lainkäyttöalue, joka tarjoaa vahvan yksityisyyden suojan.

_____ 3. Verkkotunnusjärjestelmän (DNS) nimipalvelimet toimivat yksityisesti jokaisessa palvelinsolmussa.

_____ 4. ExpressVPN:n kevyt, avoimen lähdekoodin yhteysprotokolla.

_____ 5. Network Lock -nimen viimeinen sana; kill switchin entinen nimi.

_____ 6. Symmetrinen salausstandardi, joka suojaa tiedonsiirtoa.

_____ 7. Vain RAM-muistia käyttävä palvelinarkkitehtuuri, joka estää tietojen tallentamisen levylle.

_____ 8. Riippumattomien tietoturvayritysten todentama.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. AHTLWIYG
2. LCKO
3. ALAEASSUS
4. OOTVU
5. EVRUSTRERDTES
6. SATYRIEANESTT
7. EATATUTTRSK
8. VMPLLNNAIIEI

Bonustehtävä: Nopeat vastaukset

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

1	Ominaisuuksia, joita etsit palvelusta ExpressVPN			
2	Julkisen Wi-Fin uhkia			
3	VPN-vuotojen tyyppejä			
4	Tapoja tehdä vahva salasana			
5	Painikkeita tai valikkoja VPN-sovelluksessa			
6	Asioita, joita teet verkossa joka päivä			
7	Ihmisiä, joille suosittelisit palvelua ExpressVPN			
8	Maita, jotka tunnetaan vahvoista tietosuojalaeistaan			
9	VPN-protokollia, jotka tunnet			
10	Asioita, joita tarkastus voi tutkia			
11	Palvelun ExpressVPN tietoturvaominaisuuksia			
12	Asioita, jotka kannattaa tarkistaa ennen VPN:n ostamista			
13	Asetuksia, jotka otat käyttöön lisäturvaksi			
14	Asioita, joita salaus suojaa			
15	Asioita, jotka ExpressVPN voi piilottaa verkostasi			

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: RAM-VAIN-SUOJAUSTEN TOTEUTTAMINEN



Tilanne: Valtion virasto takavarikoi ExpressVPN-palvelimen poimiakseen käyttäjälokeja ja yhteyshistoriaa.

Keskustelukysymys: Mitä tietoja he löytävät palvelimelta, ja miksi?

TAPAUSTUTKIMUS 2: EPÄVAKAIDEN WI-FI-YHTEYKSIEN TUNNELIT



Tilanne: Etätyöntekijä käyttää julkista hotellin Wi-Fi-verkkoa, joka katkeaa muutaman minuutin välein asiakirjoja muokatessa.

Keskustelukysymys: Miten ExpressVPN suojaa heidän tietonsa vuotamiselta katkosten aikana?

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

20	18	21	19	20	5	4	19	5	18	22	5	18

20	25	8	10	5	14	20	28	28

11	28	25	20	20	28	10	28	12	15	11	9	20

16	28	9	22	9	20	20	28	9	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: Mitä salausta ExpressVPN käyttää?

ExpressVPN käyttää oletuksena AES-256-GCM-symmetristä salausta.

Q2: Mikä on Lightway-protokolla?

Lightway on ExpressVPN:n oma protokolla, joka on rakennettu nopeutta, turvallisuutta ja vakautta varten.

Q3: Kirjaako ExpressVPN hakuhistoriani?

Ei, ExpressVPN noudattaa tiukkaa, riippumattomasti auditoitua lokittomuuskäytäntöä.

Q4: Mikä on Internet Kill Switch?

Se on ExpressVPN:n natiivi kill switch, joka estää internetliikenteen, jos yhteys katkeaa.

Q5: Onko Lightway-protokolla avointa lähdekoodia?

Kyllä, Lightway-protokollan ydinkoodi on avointa lähdekoodia ja saatavilla GitHubissa. [9]

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

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

Q6: Ylläpitääkö ExpressVPN yksityistä DNS:ää?

Kyllä, ExpressVPN ylläpitää omaa yksityistä, salattua DNS:ää jokaisella palvelimella. [7]

Q7: Mikä on TrustedServer-teknologia?

Se on palvelinasetelma, jossa käyttöjärjestelmä ja sovellukset toimivat kokonaan haihtuvassa RAM-muistissa.

Q8: Onko ExpressVPN tarkastettu?

Kyllä, ExpressVPN:n ovat auditoineet muun muassa PwC, Cure53 ja F-Secure. [1]

Q9: Suojaako ExpressVPN DNS- ja IPv6-vuodoilta?

Kyllä, Internet Kill Switch estää IPv4-, IPv6- ja DNS-liikenteen tunnelin ulkopuolella.

Q10: Missä ExpressVPN sijaitsee?

ExpressVPN on rekisteröity Brittiläisille Neitsytsaarille (BVI).

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

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

Q1: Miten pelkkään RAM-muistiin perustuva arkkitehtuuri parantaa tietoturvaa?

Tietoja ei kirjoiteta kiintolevyille, ja muistissa olevat tiedot pyyhitään aina, kun palvelimesta katkaistaan virta.

Q2: Miksi BVI:n lainkäyttöalue on tärkeä yksityisyyden kannalta?

ExpressVPN on sijoittunut BVI:lle, joten tietopyyntöihin sovelletaan BVI:n lakeja.

Q3: Tukeeko ExpressVPN täydellistä eteenpäin salassapitoa (perfect forward secrecy)?

Kyllä, Lightway käyttää dynaamisia avaimia, jotka tyhjennetään ja luodaan uudelleen säännöllisesti.

Q4: Miten Network Lock estää IP-vuodot?

Se estää kaiken liikenteen järjestelmätasolla aina, kun VPN-yhteys katkeaa.

Q5: Suojaako Lightway kvanttihyökkäyksiltä?

Kyllä, Lightwayssa on kvanttiturva NISTin ML-KEM-standardilla.

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

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

Q6: Voivatko viranomaiset siepata Lightway-liikennettä?

Ne voivat siepata sen, mutta eivät voi purkaa sitä AES-256/ChaCha20-salauksen vuoksi.

Q7: Miten yksityinen DNS suojaa käyttäjien hakulokeja?

Se käsittelee kaikki DNS-kyselyt salatun tunnelin sisällä ja estää palveluntarjoajan seurannan.

Q8: Mihin Lightway Turboa käytetään?

Se käyttää monikaistaista tunnelointia lähettääkseen enemmän dataa kerralla nopeampaa nopeutta varten.

Q9: Mikä on Lightwayn etu WireGuardiin verrattuna?

Lightway on rakennettu käsittelemään verkonvaihdokset (kuten Wi-Fistä mobiiliverkkoon) nopeasti katkeamatta.

Q10: Kuinka usein palvelinohjelmisto asennetaan uudelleen?

TrustedServerissä koko ohjelmistopino ladataan uudelleen suojatusta vain luku -levykuvasta jokaisen uudelleenkäynnistyksen yhteydessä.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

Lightway käyttää AES-256-GCM:ää tai vähätehoisilla laitteilla ChaCha20/Poly1305:tä. [6]

2. VPN-OIVALLUS

TrustedServer-teknologia on suunniteltu suorittamaan kaikki palvelintoiminnot RAM-muistissa. [4]

3. VPN-OIVALLUS

Brittiläiset Neitsytsaaret (BVI) on yhtiön kotipaikan lainkäyttöalue. [8]

4. VPN-OIVALLUS

Lightway kirjoitettiin uudelleen C:stä Rustille, ja sen ovat auditoineet Cure53 ja Praetorian. [3]

5. VPN-OIVALLUS

Internet Kill Switch estää liikenteen järjestelmätasolla, jos VPN katkeaa. [5]

6. VPN-OIVALLUS

Kaikki DNS-kyselyt selvitetään yksityisten, salattujen DNS-palvelimien kautta. [7]

7. VPN-TIETOA

ExpressVPN on julkaissut yli 20 riippumatonta kolmannen osapuolen tarkastusta. [1]

8. VPN-TIETOA

Palvelu ei kirjaa IP-osoitteita, selaushistoriaa eikä liikenteen metatietoja.

9. VPN-TIETOA

Täydellinen eteenpäin salaisuus säilytetään dynaamisella istuntoavainten kierrätyksellä. [1]

10. VPN-OIVALLUS

Lightway-protokolla tukee sekä UDP-että TCP-siirtokerrosta.

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1 — **Oikea vastaus: A**

OPETTAJALLE

Mikä on ExpressVPN:n oma avoimen lähdekoodin protokolla? → Lightway

2 Kysymys 2 — **Oikea vastaus: A**

OPETTAJALLE

Mikä palvelinteknologia toimii yksinomaan haihtuvassa RAM-muistissa? → TrustedServer

3 Kysymys 3 — **Oikea vastaus: A**

OPETTAJALLE

Mitä tapahtuu, jos VPN-yhteys katkeaa odottamatta? → A) Kill switch estää liikenteen

4 Kysymys 4 — **Oikea vastaus: A**

OPETTAJALLE

Missä ExpressVPN on rekisteröity yksityisyyden suojaamiseksi? → Brittiläiset Neitsytsaaret

5 Kysymys 5 — **Oikea vastaus: A**

OPETTAJALLE

Mitä symmetristä salausalgoritmia käytetään oletuksena? → AES-256-GCM

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Epätosi**

OPETTAJALLE

TrustedServer-teknologia tallentaa palvelinlokit kiintolevyille.

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

OPETTAJALLE

ExpressVPN on käynyt läpi kolmannen osapuolen tietoturvatarkastuksia.

8 **Kysymys 8** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Lightway-protokolla on rakennettu OpenVPN-koodipohjan päälle.

9 **Kysymys 9** — **Oikea vastaus: Tosi**

OPETTAJALLE

Kill switch on oletuksena päällä pöytäkonesovelluksissa.

10 **Kysymys 10** — **Oikea vastaus: Tosi**

OPETTAJALLE

ExpressVPN ylläpitää yksityistä DNS:ää jokaisella palvelimella.

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. LIGHTWAY	E 2. TRUSTED SERVER	F 3. LUKKO	A 4. SAARET
H 5. AES-256	D 6. AUDITOITU	B 7. VUOTO	C 8. DNS

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 LIGHTWAY	2 TRUSTED SERVER	3 LOCK	4 NEITSYTSAARET
5 AES-256	6 TARKASTETTU		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – VUOTO	2 D – NEITSYTSAARET	3 H – NIMIPALVELIN	4 A – LIGHTWAY
5 C – LOCK	6 E – AESSALAUS	7 B – TRUSTEDSERVER	8 F – TARKASTETTU

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit LIGHTWAY, TRUSTED SERVER ja LUKKO omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

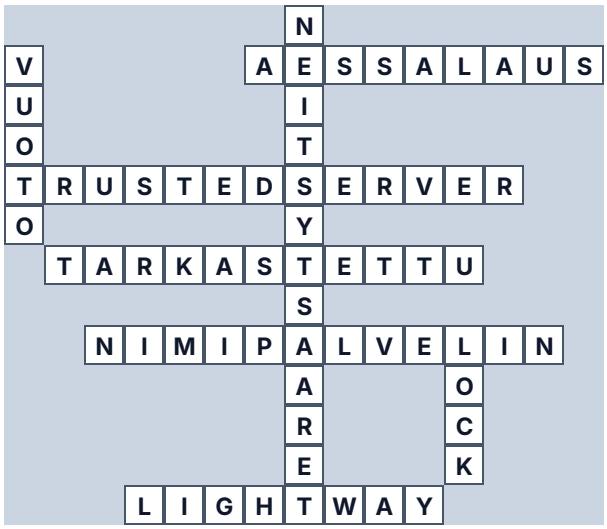
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: AESSALAUS Symmetrinen salausstandardi, joka suojaa tiedonsiirtoa (9 kirjainta)

4 vaakasuoraan: TRUSTEDSERVER Vain RAM-muistia käyttävä palvelinarkkitehtuuri, joka estää tietojen tallentamisen levylle (13 kirjainta)

5 vaakasuoraan: TARKASTETTU Riippumattomien tietoturvayritysten todentama (11 kirjainta)

6 vaakasuoraan: NIMIPALVELIN Verkkotunnusjärjestelmän (DNS) nimipalvelimet toimivat yksityisesti jokaisessa palvelinsolmussa (12 kirjainta)

8 vaakasuoraan: LIGHTWAY ExpressVPN:n kevyt, avoimen lähdekoodin yhteysprotokolla (8 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: NEITSYTSAARET Brittiläisten Neitsytsaarten lainkäyttöalue, joka tarjoaa vahvan yksityisyyden suojan (13 kirjainta)

2 pystysuoraan: VUOTO Yksityisen IP-, DNS- tai WebRTC-tiedon tahaton paljastuminen (5 kirjainta)

7 pystysuoraan: LOCK Network Lock -nimen viimeinen sana; kill switchin entinen nimi (4 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. AHTLWIYG — LIGHTWAY
2. LCKO — LOCK
3. ALAEASSUS — AESSALAUS
4. OOTVU — VUOTO
5. EVRUSTRERDTES — TRUSTEDSERVER
6. SATYRIEANESTT — NEITSYTSAARET
7. EATATUTTRSK — TARKASTETTU
8. VMPLLNNAIIEI — NIMIPALVELIN

SALAKIRJOITUSHAASTEEN AVAIN

"TRUSTEDSERVER TYHJENTÄÄ KÄYTTÄJÄLOKIT PÄIVITTÄIN"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: RAM-VAIN-SUOJAUSTEN TOTEUTTAMINEN

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Valtion virasto takavarikoi ExpressVPN-palvelimen saadakseen käyttäjälokit ja yhteyshistorian.
- Suositeltu strategia ja ratkaisu: Ei mitään. ExpressVPN:n TrustedServer-teknologia toimii kokonaan RAM-muistissa, joten kaikki tiedot tyhjentyvät heti virran katketessa.

B TAPAUSTUTKIMUS 2: EPÄVAKAIDEN WI-FI-YHTEYKSIEN TUNNELIT

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Etätyöntekijä käyttää hotellin julkista Wi-Fi-verkkoa, joka katkeaa muutaman minuutin välein asiakirjoja muokattaessa.
- Suositeltu strategia ja ratkaisu: Internet Kill Switch estää automaattisesti kaiken internetliikenteen, kunnes VPN-tunneli on muodostettu uudelleen.