Nimi: _____ Päivämäärä: _____ Pisteet: _____

VyprVPN-arvostelu

Tekninen analyysi Yhdysvalloissa pääkonttoria pitävästä VyprVPN:stä, Chameleon-protokollasta

VYPRVPN-ARVOSTELU, OPPIMISEN YLEISKATSAUS

OPPIJA

OPISKELIJASTATUS

Verkon puolustajan polku

TURVALLINEN

YHTEYDEN TILA

Datapakettien suojaaminen

AKTIIVINEN

VUOTOSUOJA

DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: VyprVPN:n tekninen arvio. Tutustut Certidan Yhdysvaltain lainkäyttöalueeseen, Chameleon-metatietojen sekoitukseen, omiin palvelinverkkoihin ja yksityisiin VyprDNS-selvittäjiin.

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/vyprvpn/

Oppimispolkusi: VyprVPN

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

VYPRVPN-ARVOSTELU, OHJEET

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

CHAMELEON-PROTOKOLLAN METADATAN SEKOITUS JA PALVELINTEN OMISTUSMALLIT

VyprVPN käyttää omaa Chameleon-protokollaansa syvän pakettitarkastuksen (DPI) sensuurin ohittamiseen. Se on texasilaisen Certidan omistama, käyttää palvelimia omissa konesalitiloissaan ja reitittää pyynnöt yksityisten, salattujen VyprDNS-nimipalvelimien kautta.

(JOHDANTO)

VyprVPN käyttää omaa Chameleon-protokollaansa syvän pakettitarkastuksen (DPI) sensuurin ohittamiseen. Se on texasilaisen Certidan omistama, käyttää palvelimia omissa konesalitiloissaan ja reitittää pyynnöt yksityisten, salattujen VyprDNS-nimipalvelimien kautta.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. **1. Mitä omaa protokollaa VyprVPN käyttää DPI-sensuurin ohittamiseen?**
   - A) Chameleon-protokolla
   - B) Stealth-tunneli
   - C) GhostBear
   - D) Catapult Hydra

2. **2. Missä VyprVPN:n perustaja Golden Frog toimi ennen Certidaa?**
   - A) Sveitsi
   - B) Panama
   - C) Brittiläiset Neitsytsaaret
   - D) Kypros

3. **3. Mikä on VyprVPN:n yksityisen DNS-selvityspalvelun nimi?**
   - A) VyprDNS
   - B) SafeDNS
   - C) NetShield
   - D) CleanWeb

4. **4. Mikä emoyhtiö perusti ja ylläpiti VyprVPN:ää alun perin?**
   - A) Golden Frog
   - B) Kape Technologies
   - C) protected.net
   - D) Aura Group

5. **5. Mitä VyprVPN:n emoyhtiö kertoo palvelininfrastruktuuristaan?**
   - A) Se ylläpitää omia konesalitilojaan
   - B) Se toimii kokonaan vuokratuilla virtuaalipalvelimilla
   - C) Se tukeutuu kolmannen osapuolen julkisiin välityssolmuihin
   - D) Se reitittää liikenteen vain Yhdysvaltain palvelinryhmien kautta

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Chameleon-protokolla sekoittaa OpenVPN-pakettien metatiedot, jotta ne näyttävät tavalliselta liikenteeltä.

Tosi Epätosi

7 Kysymys 7

7. VyprDNS on kolmannen osapuolen DNS-palvelu, joka on vuokrattu julkisilta nimipalvelimilta.

Tosi Epätosi

8 Kysymys 8

8. VyprVPN:n emoyhtiön Certidan pääkonttori on Texasissa, Yhdysvalloissa.

Tosi Epätosi

9 Kysymys 9

9. VyprVPN:n zero-logs-käytäntö on varmennettu riippumattomilla auditoinneilla.

Tosi Epätosi

10 Kysymys 10

10. Palveluntarjoaja käyttää virtuaalisia sijaintipalvelimia kaikissa Euroopan solmuissa.

Tosi Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Sensuurin kiertämisestä vastaa oma _____ -protokolla.
2. Ennen Certidaa VyprVPN:n perustaja Golden Frog sijaitsi maassa _____ .
3. Sisäiset DNS-kyselyt selvitetään turvallisesti _____ -palvelimilla.
4. VPN:n loi emoyhtiö _____ , ennen kuin Certida otti sen haltuunsa.
5. VyprVPN on pitkään mainostanut käyttävänsä omia palvelinlaitteita, joiden omistusmalli on _____ .
6. Työpöytäohjelmisto muodostaa oletuksena perinteiset tunnelit _____ -reitityksellä.

SANASTON SANAPANKKI

CHAMELEON FYYSINEN GOLDEN FROG LOKITTOMUUS OPENVPN SVEITSI VYPRDNS WIREGUARD

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

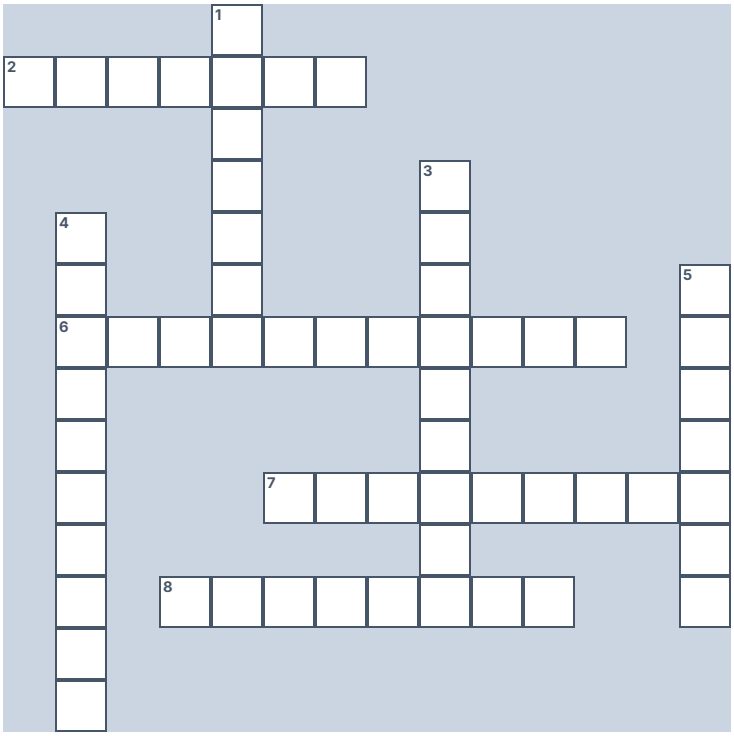
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. KAMELEONTTI	A	Perustajan Golden Frogin kotimaa ennen Certidaa.
☐	2. SVEITSI	B	Seuraavan sukupolven protokolla, joka on toteutettu nopeaa reititystä varten.
☐	3. VYPRDNS	C	Käytössä olevan palvelininfrastruktuurin omistusmalli.
☐	4. GOLDEN FROG	D	Perinteinen avoimen lähdekoodin protokolla, jota käytetään työpöytäasiakasohjelmissa.
☐	5. FYYSINEN	E	Oma protokolla, joka on suunniteltu ohittamaan syväpakettitarkastus.
☐	6. OPENVPN	F	Yksityinen DNS-selvitysverkko, joka ei tallenna lokeja.
☐	7. WIREGUARD	G	Lokiluokitus, joka varmistaa, ettei käyttäjien IP-osoitteita tallenneta.
☐	8. EI LOKEJA	H	Alkuperäinen emoyhtiö, joka perusti VyprVPN:n ennen Certidaa.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Työpöytäasiakkaissa käytetty perinteinen avoimen lähdekoodin protokolla (7)

6. Lokiluokitus, joka vahvistaa, ettei käyttäjien IP-osoitteita tallenneta (11)

7. Suurinopeuksiseen reititykseen käyttöön otettu seuraavan sukupolven protokolla (9)

8. Käytössä oleva palvelininfrastruktuurin omistusmallin tyyppi (8)

PYSTYSUORAAN

1. Perustajan Golden Frogin kotimaa ennen Certidaa (7)

3. Oma protokolla, joka on suunniteltu ohittamaan syväpakettitarkastus (9)

4. Alkuperäinen emoyhtiö, joka perusti VyprVPN:n ennen Certidaa (10)

5. Yksityinen DNS-selvitysverkko, joka ei kirjaa lokeja (7)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Työpöytäasiakkaissa käytetty perinteinen avoimen lähdekoodin protokolla (7 kirjainta):

6 vaakasuoraan: Lokiluokitus, joka vahvistaa, ettei käyttäjien IP-osoitteita tallenneta (11 kirjainta):

7 vaakasuoraan: Suurinopeuksiseen reititykseen käyttöön otettu seuraavan sukupolven protokolla (9 kirjainta):

8 vaakasuoraan: Käytössä oleva palvelininfrastruktuurin omistusmallin tyyppi (8 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Perustajan Golden Frogin kotimaa ennen Certidaa (7 kirjainta):

3 pystysuoraan: Oma protokolla, joka on suunniteltu ohittamaan syväpakettitarkastus (9 kirjainta):

4 pystysuoraan: Alkuperäinen emoyhtiö, joka perusti VyprVPN:n ennen Certidaa (10 kirjainta):

5 pystysuoraan: Yksityinen DNS-selvitysverkko, joka ei kirjaa lokeja (7 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

CHAMELEON, SVEITSI, VYPRDNS, GOLDENFROG, FYYSINEN, OPENVPN, WIREGUARD, LOKITTOMUUS

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. CHAMELEON**
- **B. SVEITSI**
- **C. VYPRDNS**
- **D. GOLDENFROG**
- **E. FYYSINEN**
- **F. OPENVPN**
- **G. WIREGUARD**
- **H. LOKITTOMUUS**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Suurinopeuksiseen reititykseen käyttöön otettu seuraavan sukupolven protokolla.
2. Työpöytäasiakkaissa käytetty perinteinen avoimen lähdekoodin protokolla.
3. Käytössä oleva palvelininfrastruktuurin omistusmallin tyyppi.
4. Oma protokolla, joka on suunniteltu ohittamaan syväpakettitarkastus.
5. Lokiluokitus, joka vahvistaa, ettei käyttäjien IP-osoitteita tallenneta.
6. Yksityinen DNS-selvitysverkko, joka ei kirjaa lokeja.
7. Alkuperäinen emoyhtiö, joka perusti VyprVPN:n ennen Certidaa.
8. Perustajan Golden Frogin kotimaa ennen Certidaa.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. LEMHCEONA
2. VPSNDRY
3. SYFINNEY
4. GDREAUWIR
5. TIIESSV
6. OEDFRGONGL
7. OPVNPNE
8. UOSTKLTOUMI

Bonustehtävä: Nopeat vastaukset

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

1	Suoratoistopalveluja, joita katsot			
2	Maita, joissa haluaisit palvelun VyprVPN palvelimia			
3	Paikkoja, joissa ottaisit palvelun VyprVPN käyttöön			
4	Ihmisiä, joille suosittelisit palvelua VyprVPN			
5	Tilanteita, joissa kill switch auttaa			
6	Syitä valita VyprVPN			
7	Kysymyksiä palvelun VyprVPN asiakastuelle			
8	Sovelluksia, joita käyttäisit yhdessä palvelun VyprVPN kanssa			
9	Asioita, jotka VyprVPN voi piilottaa verkostasi			
10	Merkkejä siitä, että VPN-yhteytesi on hidas			
11	Asioita, joita teet verkossa joka päivä			
12	VPN-protokollia, jotka tunnet			
13	Muita VPN-palveluja kuin VyprVPN			
14	Tietoturvasanoja, jotka opit tässä tehtävämonisteessa			
15	Ominaisuuksia, joita etsit palvelusta VyprVPN			

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: SYVÄPAKETTITARKASTUKSEN OHITTAMINEN



Tilanne: Kansallisen palomuurin omaavan maan läpi matkustava yritysjohtaja huomaa, että tavalliset OpenVPN-yhteydet on estetty.

Keskustelukysymys: Mikä VyprVPN-protokolla tulisi valita onnistuneen tunnelin muodostamiseksi?

TAPAUSTUTKIMUS 2: KOLMANNEN OSAPUOLEN LAITTEISTON TURVALLISUUS



Tilanne: Yritys haluaa estää isännöintipalveluntarjoajia tai kolmannen osapuolen konesalin ylläpitäjiä kirjaamasta sen VPN-liikennettä.

Keskustelukysymys: Miten VyprVPN:n palvelininfrastruktuurimalli lieventää tätä uhkaa?

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

3	8	1	13	5	12	5	15	14		20	15	18	10	21	21

16	1	11	5	20	20	9	20	1	18	11	1	19	20	21	11	19	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: Mikä on VyprVPN?

VyprVPN on VPN, jota nykyisin pyörittää yhdysvaltalainen Certida ja joka tunnetaan omista palvelinlaitteistaan ja Chameleon-protokollastaan.

Q2: Mikä on Chameleon-protokolla?

Chameleon on oma protokolla, joka sekoittaa OpenVPN-pakettien metadataa DPI-estojen ohittamiseksi.

Q3: Onko VyprVPN edelleen Sveitsissä?

Ei. Sen emoyhtiö Certida LLC:n pääkonttori on Teksasissa Yhdysvalloissa; perustaja Golden Frog oli sveitsiläinen. [2]

Q4: Tallentaako VyprVPN lokeja?

Ei, se noudattaa riippumattomasti auditoitua lokittomuuskäytäntöä eikä tallenna käyttäjien liikennettä tai IP-tietueita. [3]

Q5: Mikä on VyprDNS?

VyprDNS on VyprVPN:n oma yksityinen DNS-palvelu, joka suojaa DNS-kyselyjä sensuurilta ja vuodoilta.

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

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

Q6: Omistaako VyprVPN palvelimensa?

Sen emoyhtiö Certida kertoo ylläpitävänsä omia konesalitilojaan eri puolilla maailmaa.

Q7: Tukeeko VyprVPN WireGuardia?

Kyllä, WireGuard on integroitu heidän asiakassovelluksiinsa nopeaa yhteyttä varten.

Q8: Voinko käyttää VyprVPN:ää mobiilissa?

Kyllä, sovelluksia on saatavilla sekä Android-että iOS-laitteille, ja ne tukevat WireGuardia ja Chameleonia.

Q9: Onko siinä kill switch?

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

Q10: Kuka omistaa VyprVPN:n?

VyprVPN:n perusti Golden Frog, ja sen omistaa ja ylläpitää nykyisin Certida. [1]

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

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

Q1: Miten Chameleon hämää dataa?

Se poistaa OpenVPN-pakettien metatiedot ja muuttaa pakettikokoja ja -tiheyksiä heikentämättä salauksen vahvuutta.

Q2: Mitä lainkäyttöaluetta VyprVPN:ään sovelletaan nyt?

Yhdysvaltojen lainsäädäntö, koska emoyhtiö Certida sijaitsee Texasissa; VyprVPN luottaa sen sijaan auditoituun lokittomuuskäytäntöönsä.

Q3: Miten VyprDNS estää vuotoja?

Se pakottaa yksityisen DNS-tunnelin ja estää paikallisia verkkoja tai palveluntarjoajia sieppaamasta raakakyselyjä.

Q4: Estääkö laitteiston omistus lokien tallentamisen?

Kyllä. Se pitää kolmannen osapuolen isäntäyhtiöiden ylläpitäjät poissa fyysisten palvelimiensa hypervisoreista ja verkoista, mikä pienentää tätä riskiä.

Q5: Kuinka vahva salaus on?

VyprVPN käyttää AES-256-GCM-salausta ja 2048-bittisiä RSA-avaimia kättelyn suojaamiseen.

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

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

Q6: Onko nollalokitarkastus julkinen?

Kyllä, VyprVPN kuvaa itseään riippumattomasti auditoiduksi No Log -VPN:ksi, joka ei säilytä käyttäjien toimintalokeja. [3]

Q7: Tukeeko VyprVPN jaettua tunnelointia?

Kyllä, toiminnolla (Connection Per App) voi valita, mitkä sovellukset ohittavat salauksen Androidilla ja Macilla.

Q8: Voinko ajaa sitä reitittimissä?

Kyllä, ne tarjoavat reitittimen sovelman ja manuaaliset OpenVPN-määritykset DD-WRT-reitittimille.

Q9: Tukeeko se IPv6:ta?

Kyllä, VyprVPN sisältää IPv6-vuotosuojauksen estämällä IPv6-liikenteen asiakasohjelman sovitintasolla.

Q10: Miten palvelimen viive minimoidaan?

Omistamalla verkkonsa ne reitittävät liikenteen suoraan nopeiden tier-1-kaistapalveluntarjoajien kautta.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

VyprVPN:n loi sveitsiläinen Golden Frog, ja sen omistaa vuodesta 2023 lähtien texasilainen Certida LLC. [5]

2. VPN-OIVALLUS

Chameleon-protokolla estää VPN:n estämisen sekoittamalla OpenVPN-metadatapakettien rakenteita.

3. VPN-OIVALLUS

VyprDNS on VyprVPN:n oma no-logs-DNS-verkko, joka estää kolmansien osapuolten DNS-seurannan.

4. VPN-OIVALLUS

Certidan mukaan sillä on omia datakeskustiloja kasvavassa määrässä maita. [2]

5. VPN-OIVALLUS

VyprVPN kertoo olevansa riippumattomasti auditoitu No Log -palvelu, joka ei säilytä käyttäjien toimintalokeja. [6]

6. VPN-OIVALLUS

Palvelu tukee WireGuard-, OpenVPN-, IKEv2- ja Chameleon-protokollia.

7. VPN-TIETOA

Asiakassovelluksissa on sisäänrakennettu IPv6- ja WebRTC-vuotosuoja.

8. VPN-TIETOA

Työpöydän ja mobiilin kill switch estää kaikki lähtevät pistokkeet yhteyden katketessa.

9. VPN-TIETOA

Koska Certida on yhdysvaltalainen, VyprVPN kuuluu nyt Yhdysvaltojen lainsäädännön, Five-Eyes-maan, piiriin. [5]

10. VPN-OIVALLUS

Palveluntarjoaja ei käytä virtuaalisia palvelinsijainteja eikä simuloitua maantieteellistä reititystä.

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] VyprVPN Support. (2023). Certida FAQ.

https://support.vyprvpn.com/hc/en-us/articles/15903991797645-Certida-FAQ

[2] VyprVPN Support. (2023). What jurisdiction does VyprVPN operate in?

https://support.vyprvpn.com/hc/en-us/articles/360040528292-What-jurisdiction-does-VyprVPN-operate-in

[3] VyprVPN Support. (2023). Does VyprVPN store logs of my VPN activity?

https://support.vyprvpn.com/hc/en-us/articles/360038096191-Does-VyprVPN-store-logs-of-my-VPN-activity

[4] Golden Frog, Inc. (n.d.). VyprVPN: VPN Secure & Private - App Store.

https://apps.apple.com/us/app/-/id577635689

[5] VPN Compare. (n.d.). VyprVPN ownership change brings US jurisdiction move.

https://www.vpncompare.co.uk/vyprvpn-ownership-change-brings-us-jurisdiction-move/

[6] VPN Compare. (2018). VyprVPN now a No Log VPN with an audit to prove it.

https://www.vpncompare.co.uk/vyprvpn-no-log-vpn-audit/

[7] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

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

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

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

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

[10] NIST. (2001, updated 2023). FIPS 197, Advanced Encryption Standard (AES).

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

Vastausavain: Tarkistuspiste 1 – Monivalinta

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

OPETTAJALLE

Mitä omaa protokollaa VyprVPN käyttää DPI-sensuurin ohittamiseen? → Chameleon-protokolla

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

OPETTAJALLE

VyprVPN:n perustaja Golden Frog oli sveitsiläinen yritys; VyprVPN:n omistaa nyt texasilainen Certida. [5]

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

OPETTAJALLE

Mikä on VyprVPN:n yksityisen DNS-selvityspalvelun nimi? → VyprDNS

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

OPETTAJALLE

Mikä emoyhtiö perusti ja ylläpiti VyprVPN:ää alun perin? → Golden Frog

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

OPETTAJALLE

Certida kertoo ylläpitävänsä VyprVPN:lle omia konesalitilojaan monissa maissa.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Tosi**

OPETTAJALLE

Chameleon-protokolla sekoittaa OpenVPN-pakettien metatiedot, jotta ne näyttävät tavalliselta liikenteeltä.

7 **Kysymys 7** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: VyprDNS on VyprVPN:n oma lokiton DNS-palvelu.

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

OPETTAJALLE

Tosi: VyprVPN:n emoyhtiön Certida LLC:n pääkonttori on Texasissa.

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

OPETTAJALLE

VyprVPN:n zero-logs-käytäntö on varmennettu riippumattomilla auditoinneilla.

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

OPETTAJALLE

Epätosi: VyprVPN ei tukeudu virtuaalisijainteihin kaikilla Euroopan palvelimillaan.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

E 1. KAMELEONTTI	A 2. SVEITSI	F 3. VYPRDNS	H 4. GOLDEN FROG
C 5. FYYSINEN	D 6. OPENVPN	B 7. WIREGUARD	G 8. EI LOKEJA

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 CHAMELEON	2 SVEITSI	3 VYPRDNS	4 GOLDEN FROG
5 FYYSINEN	6 OPENVPN		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – WIREGUARD	2 F – OPENVPN	3 E – FYYSINEN	4 A – CHAMELEON
5 H – LOKITTOMUUS	6 C – VYPRDNS	7 D – GOLDENFROG	8 B – SVEITSI

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit KAMELEONTTI, SVEITSI ja VYPRDNS omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

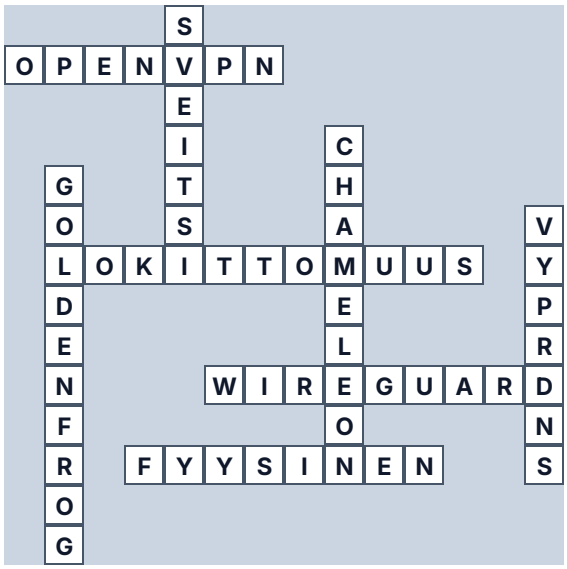
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: OPENVPN Työpöytäasiakkaissa käytetty perinteinen avoimen lähdekoodin protokolla (7 kirjainta)

6 vaakasuoraan: LOKITTOMUUS Lokiluokitus, joka vahvistaa, ettei käyttäjien IP-osoitteita tallenneta (11 kirjainta)

7 vaakasuoraan: WIREGUARD Suurinopeuksiseen reititykseen käyttöön otettu seuraavan sukupolven protokolla (9 kirjainta)

8 vaakasuoraan: FYYSINEN Käytössä oleva palvelininfrastruktuurin omistusmallin tyyppi (8 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: SVEITSI Perustajan Golden Frogin kotimaa ennen Certidaa (7 kirjainta)

3 pystysuoraan: CHAMELEON Oma protokolla, joka on suunniteltu ohittamaan syväpakettitarkastus (9 kirjainta)

4 pystysuoraan: GOLDENFROG Alkuperäinen emoyhtiö, joka perusti VyprVPN:n ennen Certidaa (10 kirjainta)

5 pystysuoraan: VYPRDNS Yksityinen DNS-selvitysverkko, joka ei kirjaa lokeja (7 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. LEMHCEONA — **CHAMELEON**
2. VPSNDRY — **VYPRDNS**
3. SYFINNEY — **FYYSINEN**
4. GDREAUWIR — **WIREGUARD**
5. TIIESSV — **SVEITSI**
6. OEDFRGONGL — **GOLDENFROG**
7. OPVNPNE — **OPENVPN**
8. UOSTKLTOUMI — **LOKITTOMUUS**

SALAKIRJOITUSHAASTEEN AVAIN

"CHAMELEON TORJUU PAKETTITARKASTUKSEN"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: SYVÄPAKETTITARKASTUKSEN OHITTAMINEN

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Maan, jossa on kansallinen palomuuri, kautta matkustava yritysjohtaja huomaa, että tavalliset OpenVPN-yhteydet on estetty.
- Suositeltu strategia ja ratkaisu: Chameleon-protokolla täytyy valita, jotta OpenVPN-pakettien metatiedot sekoitetaan ja DPI-suodattimet ohitetaan.

B TAPAUSTUTKIMUS 2: KOLMANNEN OSAPUOLEN LAITTEISTON TURVALLISUUS

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys haluaa estää hosting-palveluntarjoajia tai kolmannen osapuolen konesalin ylläpitäjiä kirjaamasta VPN-liikennettään.
- Suositeltu strategia ja ratkaisu: VyprVPN käyttää palvelimia emoyhtiönsä omissa konesalitiloissa, mikä vähentää riippuvuutta kolmansien osapuolten hosting-yrityksistä.