Nimi: _____ Päivämäärä: _____ Pisteet: _____

Turvallisimman VPN:n opas

Tekninen analyysi korkean tietoturvan VPN-suunnittelusta, vain RAM-muistissa toimivista haihtuvan muistin palvelimista, Zero Trust -pääsyturvasta, yksityisistä salatuista DNS-vuotojen torjunnoista ja tarkastetuista WireGuard-määrityksistä.

TURVALLISIMMAN VPN:N OPAS: OPPIMISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: erittäin turvallisten VPN-palvelujen tekniset standardit. Tutustut vain RAM-muistia käyttäviin palvelinlaitteistoihin, Zero Trust -pääsyturvallisuuteen, yksityisiin salattuihin DNS-selvittäjiin ja auditoituihin WireGuard-määrityksiin.

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/turvallisin-vpn/

Oppimispolkusi: turvallisin VPN

- Analysoi Most Secure VPN Guide -oppaan teknistä arkkitehtuuria ja salausstandardeja.
- Määritä asiakasasetukset estämään IP-, DNS- ja WebRTC-liikenteen vuodot.
- Vertaile omia tunnelointiprotokollia tavallisiin toteutuksiin.

TURVALLISIMMAN VPN:N OPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: pelkästään RAM-muistia käyttävä palvelinlaitteisto ja Zero Trust -järjestelmät. Lopuksi bonustehtävä Nopeat vastaukset.

PELKKÄÄ RAM-MUISTIA KÄYTTÄVÄT INFRASTRUKTUURIT JA ZERO TRUST -VERKOT (JOHDANTO)

Todella turvallinen VPN perustuu nollaluottamuskehykseen, vain RAM-muistia käyttäviin palvelimiin, jotka estävät levyjen takavarikoinnin paljastamasta lokeja, yksityisiin salattuihin DNS-selvittimiin ja auditoituihin protokolliin, kuten WireGuard. Nämä yhdistetyt hallintakeinot suojaavat arvokkaita digitaalisia omaisuuseriä sieppausuhilta.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mikä arkkitehtuuri on keskeinen korkeimman turvallisuuden varmistamiseksi nykyaikaisilla VPN-palvelimilla?**

- A) Vain RAM-muistia käyttävä palvelininfrastruktuuri
- B) Levypohjainen tallennus
- C) Dynaaminen DNS-reititys
- D) Portinohjauksen käyttöönotto

2 **2. Mitä protokollaa suositellaan laajasti turvallisimpiin ja nykyaikaisimpiin VPN-määrityksiin?**

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3 **3. Mikä tietoturvakehys edellyttää jokaisen yhteyden jatkuvaa varmennusta poikkeuksetta?**

- A) Nollaluottamusarkkitehtuuri
- B) Reunapalomuurit
- C) Dynaaminen reititys
- D) Jaetut salaiset avaimet

4 **4. Mikä on VPN-asiakasohjelman DNS-vuotosuojauksen ensisijainen tehtävä?**

- A) Reititä kaikki DNS-pyynnöt yksityisten salattujen selvittimien kautta
- B) Hämää IP-paketteja
- C) Välimuistita DNS-kyselyt paikallisesti
- D) Poista nimipalvelimet käytöstä

5 **5. Miten monihyppyreititys (Multi-Hop) lisää VPN-tunnelin kokonaisturvallisuutta?**

- A) Reitittää tiedot kahden erillisen palvelimen kautta peräkkäin
- B) Nopeuttaa pakkausta
- C) Salaa datan heikoilla salausmenetelmillä
- D) Ohittaa palomuurit

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Pelkkää RAM-muistia käyttävät palvelimet tallentavat lokitiedostot tilapäiseen muistiin, joka tyhjenee uudelleenkäynnistyksessä.

○ Tosi ○ Epätosi

7 Kysymys 7

7. WireGuard käyttää nykyaikaisia salausalgoritmeja, jotka ovat vähemmän alttiita nopeuden pullonkauloille.

○ Tosi ○ Epätosi

8 Kysymys 8

8. VPN:n kill switch toimii estämällä kaiken verkkoliikenteen, jos tunneli katkeaa.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Riippumattomilla kolmannen osapuolen auditoinneilla ei ole merkitystä tietoturvasitoumusten todentamisessa.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Zero Trust -mallit olettavat kaikkien sisäisen verkon yhteyksien olevan oletuksena turvallisia.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Ylläpitäjät noudattavat tietoturvassa tiukkaa kehystä, jonka nimi on _____ .

2. Pakettien reititys usean sisääntulopisteen kautta edellyttää turvallista _____ -määritystä.

3. Varastetuilta levyiltä tapahtuvien tietovuotojen estämiseksi käytetään rakennetta, jossa on _____ .

4. Operaattorin tekemän kaappauksen estämiseksi määritetään natiivi _____ .

5. Liikenteen estämiseksi yhteyskatkoissa ota käyttöön _____ -mekanismi.

6. Tallennettujen tietokantalokien minimoimiseksi valitse täysin _____ palveluntarjoaja.

SANASTON SANAPANKKI

DNS-SUOJAUS KILL SWITCH MULTIHOP NOLLALUOTTAMUS PROTOKOLLA
RAM-PALVELIN SALAUS TARKASTETTU

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: VPN- ja verkkokäsitteiden yhdistäminen

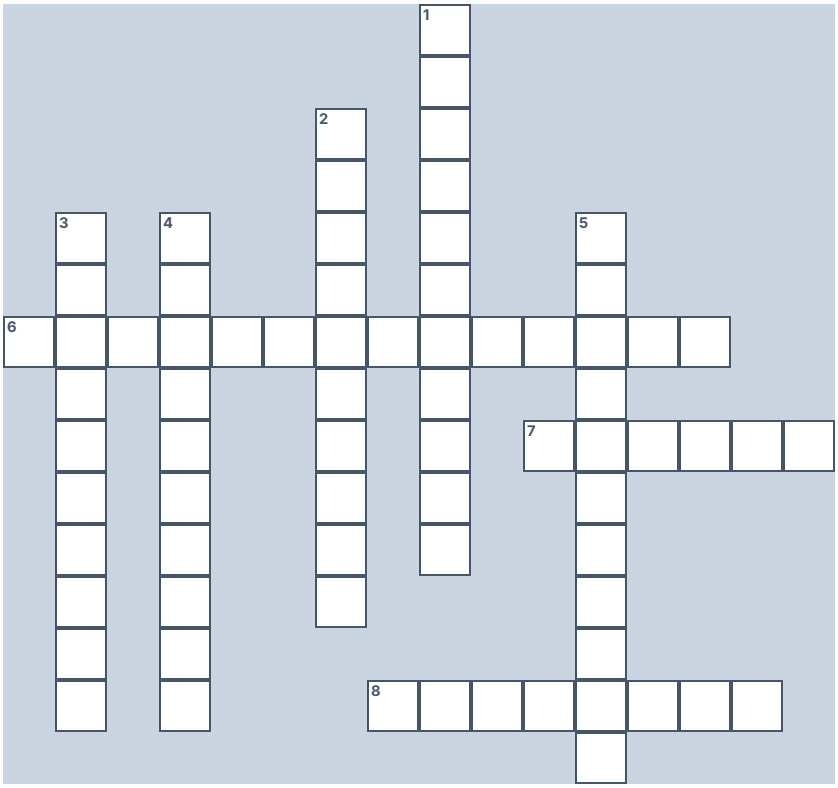
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. Zero Trust	A	Riippumattomasti tarkastettu ratkaisu, joka vahvistaa, ettei lokeja tallenneta.
☐	2. Multi-Hop	B	Datan hyötykuormien kryptografinen sekoittaminen siirron suojaamiseksi.
☐	3. Vain RAM -palvelin	C	Tietoturvakehys, joka edellyttää kaikkien käyttäjien jatkuvaa tunnistautumista.
☐	4. DNS-suojaus	D	Joukko teknisiä sääntöjä, jotka määrittävät, miten data paketoidaan ja lähetetään.
☐	5. Kill switch	E	Kaskadoitu VPN-reititys, joka ketjuttaa kaksi palvelinsolmua yhteen.
☐	6. Auditoitu järjestelmä	F	Palvelinarkkitehtuuri, joka käyttää haihtuvaa muistia datan tallentamiseen.
☐	7. Salaus	G	Yksityisten DNS-kyselyjen pakottaminen nimipalvelinhakujen suojaamiseksi.
☐	8. Protokolla	H	Vikaturvamekanismi, joka estää liikenteen, jos VPN pettää.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

6. Tietoturvakehys, joka edellyttää kaikkien käyttäjien jatkuvaa todennusta (14)

7. Datasisältöjen kryptografinen sekoittaminen siirron turvaamiseksi (6)

8. Porrastettu VPN-reititys, joka ketjuttaa kaksi palvelinsolmua yhteen (8)

PYSTYSUORAAN

1. Riippumattomasti tarkastettu järjestelmä, joka vahvistaa, ettei lokeja tallenneta (11)

2. Yksityisten DNS-kyselyjen valvominen nimipalvelinhakujen suojaamiseksi (10)

3. Tekniset säännöt, jotka määrittävät, miten data paketoidaan ja lähetetään (10)

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

5. Palvelinarkkitehtuuri, joka käyttää haihtuvaa muistia datasisältöjen tallentamiseen (11)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

6 vaakasuoraan: Tietoturvakehys, joka edellyttää kaikkien käyttäjien jatkuvaa todennusta (14 kirjainta):

7 vaakasuoraan: Datasisältöjen kryptografinen sekoittaminen siirron turvaamiseksi (6 kirjainta):

8 vaakasuoraan: Porrastettu VPN-reititys, joka ketjuttaa kaksi palvelinsolmua yhteen (8 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Riippumattomasti tarkastettu järjestelmä, joka vahvistaa, ettei lokeja tallenneta (11 kirjainta):

2 pystysuoraan: Yksityisten DNS-kyselyjen valvominen nimipalvelinhakujen suojaamiseksi (10 kirjainta):

3 pystysuoraan: Tekniset säännöt, jotka määrittävät, miten data paketoidaan ja lähetetään (10 kirjainta):

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

5 pystysuoraan: Palvelinarkkitehtuuri, joka käyttää haihtuvaa muistia datasisältöjen tallentamiseen (11 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

NOLLALUOTTAMUS | MULTIHOP TARKASTETTU | RAMPALVELIN SALAUS | DNSSUOJAUS PROTOKOLLA | KILLSWITCH

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. NOLLALUOTTAMUS**
- **B. MULTIHOP**
- **C. RAMPALVELIN**
- **D. DNSSUOJAUS**
- **E. KILLSWITCH**
- **F. TARKASTETTU**
- **G. SALAUS**
- **H. PROTOKOLLA**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Suojamekanismi, joka estää liikenteen, jos VPN-yhteys pettää.
2. Yksityisten DNS-kyselyjen valvominen nimipalvelinhakujen suojaamiseksi.
3. Porrastettu VPN-reititys, joka ketjuttaa kaksi palvelinsolmua yhteen.
4. Tekniset säännöt, jotka määrittävät, miten data paketoidaan ja lähetetään.
5. Datasisältöjen kryptografinen sekoittaminen siirron turvaamiseksi.
6. Palvelinarkkitehtuuri, joka käyttää haihtuvaa muistia datasisältöjen tallentamiseen.
7. Riippumattomasti tarkastettu järjestelmä, joka vahvistaa, ettei lokeja tallenneta.
8. Tietoturvakehys, joka edellyttää kaikkien käyttäjien jatkuvaa todennusta.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. ALOTULOTMNUSAL
2. ANARILMLEVP
3. KWCIISHLTL
4. SALUSA
5. IHUPTMOL
6. UUSJADNOSS
7. EATATUTTRSK
8. LTKAPOROLO

Bonustehtävä: Nopeat vastaukset

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

1	Lukkoja tai avaimia, joita käytät joka päivä			
2	Asioita, jotka VPN voi piilottaa			
3	Asioita, jotka tekevät VPN:stä turvallisen			
4	Myyttejä VPN:istä			
5	Syitä käyttää VPN:ää matkustaessa			
6	Turvallisia paikkoja tosielämässä			
7	Sanoja, jotka tarkoittavat "suojattu"			
8	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
9	Yksityisyyteen liittyviä sanoja			
10	Tarkastuksen tai tutkinnan tyyppejä			
11	Sanoja tästä tehtävämonisteesta, jotka haluat muistaa			
12	Asioita, jotka hakkeri haluaa varastaa			
13	Tapoja tunnistaa väärennetty Wi-Fi-verkko			
14	Paikkoja, joissa käyttäisit VPN:ää			
15	Asioita, jotka internetoperaattorisi näkee			

Tarkistuspiste 8: VPN:n ja verkon tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: YRITYSINFRASTRUKTUURIN KOVENTAMINEN



Tilanne: Yrityspankki suunnittelee etäyhteystopologiansa uudelleen. Se vaatii Zero Trust -arkkitehtuurin, joka yhdistää kaikki asiakaslaitteet suojattuihin palvelimiin.

Keskustelukysymys: Mikä on verkon mikrosegmentoinnin ensisijainen hyöty Zero Trust -VPN-mallissa?

TAPAUSTUTKIMUS 2: RAM-VAIN-PALVELINTEN SUOJAUKSET



Tilanne: Tietoturvaan keskittyvä VPN-palveluntarjoaja päivittää palvelimiaan estääkseen fyysisen palvelintakavarikon paljastamasta käyttäjälokihistoriaa.

Keskustelukysymys: Selitä, miten vain RAM-muistia käyttävät laitteistomääritykset estävät oikeuslääketieteellisen tiedonpoiminnan fyysisten palvelintakavarikkojen 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

22	16	14		19	21	15	10	1	1		1	18	22	15	11	11	1	1	20

4	9	7	9	15	13	1	9	19	21	21	4	5	20

Purettu viesti:

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

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

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

Q1: Mikä tekee VPN:stä "turvallisimman"?

Nollaluottamuksen, vain RAM-muistia käyttävien palvelimien ja auditoitujen protokollien yhdistelmä.

Q2: Mitä ovat pelkkää RAM-muistia käyttävät palvelimet?

Haihtuvassa muistissa toimivat palvelimet, jotka on suunniteltu olemaan tallentamatta lokeja levylle.

Q3: Mikä on Zero Trust -VPN?

Kehys, joka varmistaa jatkuvasti jokaisen käyttöpyynnön ja yhteyden.

Q4: Miksi WireGuardia pidetään turvallisena?

Siinä on pieni, helposti auditoitava koodikanta, ja se käyttää nykyaikaisia salauksia.

Q5: Miten turvalliset VPN:t estävät DNS-vuodot?

Reitittämällä kaikki kyselyt yksityisten, salattujen DNS-ratkaisijoiden kautta.

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

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

Q6: Vaatiiko turvallinen VPN tarkastuksia?

Kyllä, riippumattomat auditoinnit varmistavat, että väitteet lokien puuttumisesta ja koodin turvallisuudesta pitävät paikkansa.

Q7: Mikä rooli kill switchillä on?

Se pysäyttää verkkoliikenteen välittömästi, jos VPN-yhteys katkeaa.

Q8: Mitä salausta turvallisissa VPN:issä käytetään?

AES-256 ja ChaCha20 ovat alan salausstandardit.

Q9: Onko Multi-Hop-reititys turvallista?

Kyllä, se ketjuttaa vähintään kaksi palvelinta liikenneanalyysin estämiseksi.

Q10: Miten offshore-lainkäyttöalue auttaa?

Se voi rajata sovellettavia lakeja, mutta ei tarjoa ehdotonta koskemattomuutta.

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

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

Q1: Miten pelkästään RAM-muistissa toimivat palvelimet ehkäisevät tietojen takavarikoinnin riskejä?

Koska ne toimivat RAM-muistissa, pistokkeen irrottaminen tyhjentää muistissa olevan datan.

Q2: Miten Zero Trust korvaa tavallisen perimetriturvan?

Se kohtelee jokaista asiakasta vihamielisenä ja vaatii jatkuvaa todennusta.

Q3: Mikä tekee WireGuardin koodikannasta helpommin tarkastettavan?

Sen Linux-koodi on alle 4 000 riviä, selvästi pienempi kuin tyypilliset VPN-pinot. [4]

Q4: Miten DNSSEC suojaa DNS-kyselyjä?

Se allekirjoittaa DNS-tietueet, jotta selvittäjät voivat havaita väärennetyt tai peukaloidut vastaukset.

Q5: Miten Multi-Hop vaikeuttaa liikenteen korrelaatiota?

Erottamalla saapuvat ja lähtevät IP-osoitteet eri isännöintipalveluntarjoajille.

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

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

Q6: Miksi Five Eyes -lainkäyttöalueet ovat riskialttiita VPN:ille?

Jäsenvaltiot jakavat tiedustelutietoa ja voivat käyttää oikeudellisia määräyksiä pyytääkseen käyttäjätietoja.

Q7: Miten kill switch toteutetaan ydintasolla?

Se käyttää järjestelmän palomuurisääntöjä (kuten iptables tai WFP) lähtevän liikenteen estämiseen.

Q8: Mitä eteenpäin salassapito on VPN-kättelyissä?

Se luo yksilölliset istuntoavaimet, joten aiempia istuntoja ei voi purkaa.

Q9: Miten turvalliset VPN:t vähentävät WebRTC-vuotoja?

Estämällä WebRTC-pyynnöt tai reitittämällä ne tunnelin kautta.

Q10: Miten riippumattomat tarkastukset varmistavat yksityisyyden noudattamisen?

Auditoijat tekevät tunkeutumistestausta ja tarkastavat palvelinmääritykset.

Osa 11: 10 tosielämän VPN-faktaa ja havaintoa

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

1. VPN-OIVALLUS

Pelkkää RAM-muistia käyttävät palvelimet lataavat käyttöjärjestelmänsä muistiin käynnistyksessä, joten levylle ei jää mitään uudelleenkäynnistyksen jälkeen.

2. VPN-OIVALLUS

WireGuard käyttää Noise-kehystä sekä Curve25519:ää, ChaCha20:tä, Poly1305:tä, BLAKE2s:ää ja HKDF:ää. [3]

3. VPN-OIVALLUS

Zero Trust myöntää pääsyn resurssikohtaisesti eikä anna implisiittistä luottamusta verkon sijainnin perusteella (NIST SP 800-207). [1]

4. VPN-OIVALLUS

Five Eyes -tiedusteluliittoumaan kuuluvat Yhdysvallat, Britannia, Kanada, Australia ja Uusi-Seelanti.

5. VPN-OIVALLUS

WebRTC-vuotoja syntyy, kun selaimet paljastavat asiakkaan oikean julkisen IP-osoitteen STUN-kyselyjen kautta.

6. VPN-OIVALLUS

Täydellinen eteenpäin salaisuus (PFS) varmistaa, ettei pitkäaikaisen avaimen vaarantuminen paljasta aiempia istuntoavaimia. [3]

7. VPN-TIETOA

Cure53, berliiniläinen tietoturvayritys, on julkaissut useiden VPN-palveluntarjoajien auditointeja.

8. VPN-TIETOA

DNS-vuodot syntyvät, kun DNS-kyselyt ohittavat VPN-tunnelin ja päätyvät paikallisen internetpalveluntarjoajan nimipalvelimille.

9. VPN-TIETOA

Haihtuvat RAM-piirit tarvitsevat jatkuvaa sähkövirtaa tietojen säilyttämiseen ja menettävät sisältönsä virran katketessa.

10. VPN-OIVALLUS

Yritysten Zero Trust -järjestelmät valvovat laitteen tilatarkistuksia ennen yhteyden sallimista suojattuihin resursseihin. [1]

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Vain RAM -palvelin** VAIN RAM — **Oikea vastaus: A**

OPETTAJALLE

Pelkkää RAM-muistia käyttävät palvelimet eivät tallenna lokeja levylle, ja tiedot tyhjenevät uudelleenkäynnistyksessä. Lähde: Most Secure VPN.

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

OPETTAJALLE

WireGuard yhdistää pienen, tarkastettavan koodikannan ja modernit salausalgoritmit.

3 **Zero Trust -malli** NOLLALUOTTAMUS — **Oikea vastaus: A**

OPETTAJALLE

Zero Trust -mallit varmentavat laitteen vaatimustenmukaisuuden jatkuvasti ennen pääsyä. Lähde: Most Secure VPN.

4 **DNS-suojaus** DNS-SUOJAUS — **Oikea vastaus: A**

OPETTAJALLE

DNS-vuodonesto reitittää hakukyselyt yksityisten nimipalvelimien kautta. Lähde: Most Secure VPN.

5 **Multi-Hop-tunnelit** MULTI-HOP — **Oikea vastaus: A**

OPETTAJALLE

Multi-Hop-reititys ketjuttaa kaksi erillistä palvelinsolmua peräkkäin. Lähde: Most Secure VPN.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Vain RAM -palvelin** VAIN RAM — **Oikea vastaus: Tosi**

OPETTAJALLE

Pelkkää RAM-muistia käyttävä palvelinlaitteisto ei kirjoita dataa levylle, ja kaikki tyhjenee uudelleenkäynnistyksessä. Lähde: Most Secure VPN.

7 **WireGuardin nopeus** WIREGUARD — **Oikea vastaus: Tosi**

OPETTAJALLE

WireGuard käyttää nykyaikaista kryptografiaa, joka välttää prosessoinnin pullonkaulat. Lähde: Most Secure VPN.

8 **Kill switch** VIKATURVAKYTKIN — **Oikea vastaus: Tosi**

OPETTAJALLE

Kill switch estää kaiken liikenteen, jos VPN-yhteys katkeaa. Lähde: Most Secure VPN.

9 **Kolmannen osapuolen auditoinnit** AUDITOINNIT OVAT OLENNAISIA — **Oikea vastaus: Epätosi**

OPETTAJALLE

Kolmannen osapuolen auditoinnit ovat välttämättömiä yritysten yksityisyysväitteiden todentamiseksi. Lähde: Most Secure VPN.

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

OPETTAJALLE

Zero Trust ei anna implisiittistä luottamusta verkon sijainnin perusteella. [1]

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

C 1. Zero Trust	E 2. Multi-Hop	F 3. Vain RAM -palvelin	G 4. DNS-suojaus
H 5. Kill switch	A 6. Auditoitu järjestelmä	B 7. Salaus	D 8. Protokolla

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 NOLLALUOTTAMUS	2 MULTIHOP	3 RAM-PALVELIN	4 DNS-SUOJAUS
5 KILL SWITCH	6 TARKASTETTU		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 E – KILLSWITCH	2 D – DNSSUOJAUS	3 B – MULTIHOP	4 H – PROTOKOLLA
5 G – SALAUS	6 C – RAMPALVELIN	7 F – TARKASTETTU	8 A – NOLLALUOTTAMUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Zero Trust, Multi-Hop ja Vain RAM -palvelin omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

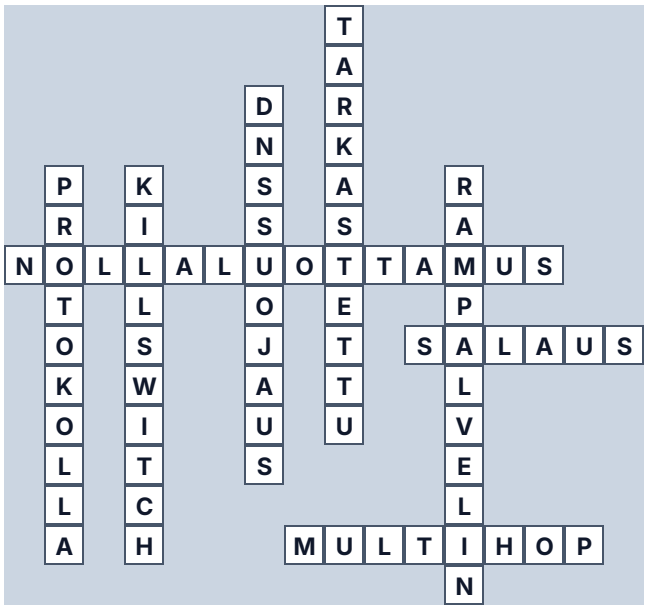
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

6 vaakasuoraan: NOLLALUOTTAMUS Tietoturvakehys, joka edellyttää kaikkien käyttäjien jatkuvaa todennusta (14 kirjainta)

7 vaakasuoraan: SALAUS Datasisältöjen kryptografinen sekoittaminen siirron turvaamiseksi (6 kirjainta)

8 vaakasuoraan: MULTIHOP Porrastettu VPN-reititys, joka ketjuttaa kaksi palvelinsolmua yhteen (8 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: TARKASTETTU Riippumattomasti tarkastettu järjestelmä, joka vahvistaa, ettei lokeja tallenneta (11 kirjainta)

2 pystysuoraan: DNSSUOJAUS Yksityisten DNS-kyselyjen valvominen nimipalvelinhakujen suojaamiseksi (10 kirjainta)

3 pystysuoraan: PROTOKOLLA Tekniset säännöt, jotka määrittävät, miten data paketoidaan ja lähetetään (10 kirjainta)

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

5 pystysuoraan: RAMPALVELIN Palvelinarkkitehtuuri, joka käyttää haihtuvaa muistia datasisältöjen tallentamiseen (11 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. ALOTULOTMNUSAL — **NOLLALUOTTAMUS**
2. ANARILMLEVP — **RAMPALVELIN**
3. KWCIISHLTL — **KILLSWITCH**
4. SALUSA — **SALAUS**
5. IHUPTMOL — **MULTIHOP**
6. UUSJADNOSS — **DNSSUOJAUS**
7. EATATUTTRSK — **TARKASTETTU**
8. LTKAPOROLO — **PROTOKOLLA**

SALAKIRJOITUSHAASTEEN AVAIN

"VPN SUOJAA ARVOKKAAT DIGIOMAISUUDET"

Tapaustutkimusten vastausavain

A TAPAUSTUTKIMUS 1: YRITYSINFRASTRUKTUURIN KOVENTAMINEN

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys-pankki uudistaa etäkäyttötopologiaansa. Se vaatii nollaluottamusarkkitehtuurin (zero trust), joka yhdistää kaikki asiakaslaitteet suojattuihin palvelimiin.
- Suositeltu strategia ja ratkaisu: Arviointiohje: Selitä, että mikrosegmentointi rajoittaa pääsyn tiettyihin resursseihin ja estää uhan sivuttaisliikkeen, jos laite vaarantuu.

B TAPAUSTUTKIMUS 2: RAM-VAIN-PALVELINTEN SUOJAUKSET

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Tietoturvaan keskittynyt VPN-palveluntarjoaja päivittää palvelimiaan estääkseen palvelimen fyysisen takavarikon paljastamasta käyttäjälokihistorioita.
- Suositeltu strategia ja ratkaisu: Arviointiohje: Kuvaa, että RAM-only-palvelimissa ei ole fyysistä levytilaa. Virran katkeaminen tyhjentää automaattisesti kaikki haihtuvassa muistissa olevat tilapäiset tiedot.