Nama: _____ Tanggal: _____ Nilai: _____

Ulasan TunnelBear

Analisis teknis TunnelBear yang berkantor pusat di Kanada, obfuskasi GhostBear, kill switch VigilantBear, audit keamanan independen tahunan, dan kebijakan tanpa log.

GAMBARAN PEMBELAJARAN ULASAN TUNNELBEAR

PELAJAR
STATUS SISWA
Jalur Pembela Jaringan

AMAN
STATUS KONEKSI
Melindungi paket data

AKTIF
PERLINDUNGAN KEBOCORAN
Perlindungan kebocoran DNS & IPv6

Selamat datang! Paket aktivitas ini memandu Anda mempelajari ulasan teknis TunnelBear. Anda akan mempelajari obfuskasi GhostBear, pengaturan kill switch VigilantBear, dan audit keamanan tahunan.

POS-POS LEMBAR KERJA

- [ ] **Bagian 1-4: Kuasai konfigurasi VPN dan keamanan jaringan.**
- [ ] **Bagian 5-7: Selesaikan teka-teki silang & pencarian kata.**
- [ ] **Bagian 8-9: Selesaikan studi kasus & tantangan sandi.**
- [ ] **Bagian 10: Pelajari halaman FAQ dasar & lanjutan.**
- [ ] **Bagian 11: Jelajahi 10 fakta menarik dari dunia nyata.**
- [ ] **Bonus: Tantangan Berpikir Cepat.**

Buka Panduan VPN Terbaik VPN.com

URL: https://www.vpn.com/id/vpn/tunnelbear/

Peta Belajar TunnelBear Anda

- Analisis arsitektur teknis dan standar enkripsi TunnelBear.
- Atur pengaturan aplikasi untuk mencegah kebocoran lalu lintas IP, DNS, dan WebRTC.
- Bandingkan protokol tunneling milik penyedia dengan implementasi standar.

PETUNJUK ULASAN TUNNELBEAR

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan kata dari bank kata, cocokkan definisi, lalu selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda pada obfuskasi GhostBear dan kill switch VigilantBear. Akhiri dengan aktivitas bonus Berpikir Cepat.

OBFUSKASI GHOSTBEAR & AUDIT INDEPENDEN TAHUNAN

TunnelBear dikenal karena audit keamanan independen tahunan oleh Cure53. Berkantor pusat di Kanada, TunnelBear menawarkan obfuskasi GhostBear untuk menembus sensor DPI, perlindungan kebocoran koneksi VigilantBear, dan koneksi perangkat tanpa batas.

(PENGANTAR)

TunnelBear dikenal karena audit keamanan independen tahunan oleh Cure53. Berkantor pusat di Kanada, TunnelBear menawarkan obfuskasi GhostBear untuk menembus sensor DPI, perlindungan kebocoran koneksi VigilantBear, dan koneksi perangkat tanpa batas.

BACA SETIAP POS DENGAN SAKSAMA DAN PILIH ATAU TULIS JAWABAN YANG BENAR.

Pos 1: Tantangan Pilihan Ganda

1. **1. Di negara mana badan usaha TunnelBear terdaftar?**
   - A) Kanada
   - B) Amerika Serikat
   - C) Swiss
   - D) Jerman

2. **2. Apa nama fitur obfuskasi TunnelBear untuk menembus sensor?**
   - A) GhostBear
   - B) Chameleon
   - C) Stealth
   - D) ShadowSocks

3. **3. Apa nama fitur kill switch bawaan TunnelBear?**
   - A) VigilantBear
   - B) Secure Core
   - C) NetShield
   - D) SafePath

4. **4. Perusahaan keamanan siber mana yang mengakuisisi TunnelBear pada 2018?**
   - A) McAfee
   - B) Avast
   - C) NortonLifeLock
   - D) Kape Technologies

5. **5. Protokol mana yang direkomendasikan TunnelBear untuk terowongan modern berkecepatan tinggi?**
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) PPTP

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. GhostBear mengacak metadata VPN untuk membantu menembus firewall yang memakai inspeksi paket mendalam.

○ Benar ○ Salah

7 Pertanyaan 7

7. Paket gratis TunnelBear mencakup data penjelajahan bulanan tanpa batas.

○ Benar ○ Salah

8 Pertanyaan 8

8. VigilantBear menjaga data tetap aman saat aplikasi sedang menyambung atau menyambung ulang.

○ Benar ○ Salah

9 Pertanyaan 9

9. TunnelBear adalah VPN konsumen pertama yang menerbitkan audit keamanan publik setiap tahun.

○ Benar ○ Salah

10 Pertanyaan 10

10. Penyedia ini beroperasi di bawah yurisdiksi hukum Panama yang ketat.

○ Benar ○ Salah

Pos 3: Mengisi Istilah Kunci

Baca setiap kalimat di bawah ini dan isi bagian yang kosong dengan istilah yang tepat dari Bank Kata.

1. TunnelBear berkantor pusat dan beroperasi dari _____ dengan hukum yang ketat.
2. Teknologi obfuskasi dijalankan oleh pengaturan sistem _____ .
3. Perlindungan kebocoran di tingkat sistem diatur oleh _____ .
4. Penyedia VPN ini diakuisisi oleh pengembang keamanan _____ pada 2018.
5. Kecepatan transmisi data yang tinggi dicapai melalui _____ protokol.
6. Koneksi klien desktop tradisional mengandalkan _____ protokol.

BANK KATA KOSAKATA

AUDIT GHOSTBEAR KANADA MCAFEE OPENVPN TANPALOG VIGILANTBEAR WIREGUARD

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep VPN & Jaringan

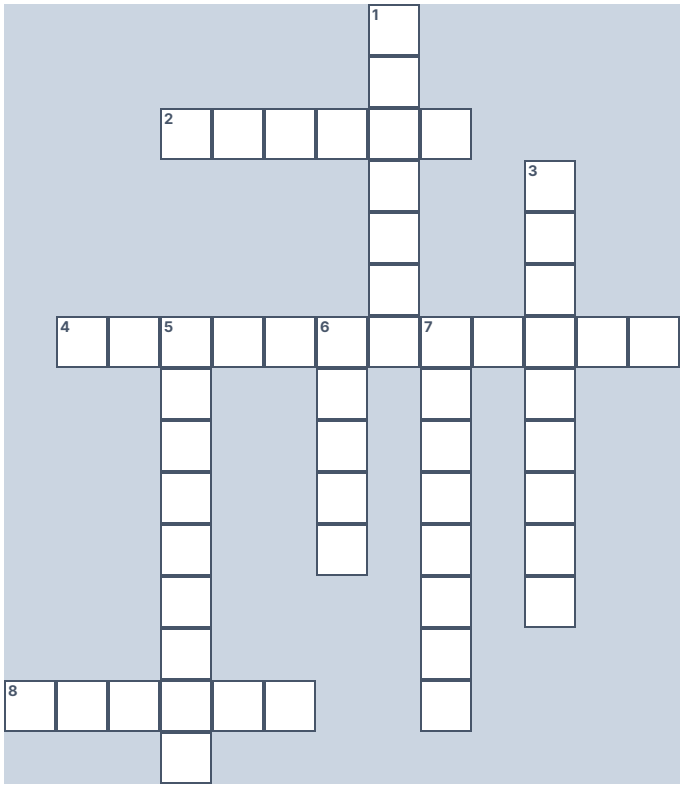
MENCOCOKKAN DEFINISI

Cocokkan setiap istilah di sebelah kiri dengan definisi yang benar di sebelah kanan dengan menulis huruf yang sesuai (A-H) di kotak isian.

☐	1. KANADA	A	Kebijakan privasi yang melarang penyimpanan riwayat lalu lintas.
☐	2. GHOSTBEAR	B	Negara tempat perusahaan terdaftar dan berkantor pusat.
☐	3. VIGILANTBEAR	C	Penilaian keamanan oleh pihak ketiga yang dilakukan setiap tahun.
☐	4. MCAFEE	D	Protokol tunneling sumber terbuka standar yang dipakai di desktop.
☐	5. WIREGUARD	E	Perusahaan keamanan induk yang mengakuisisi TunnelBear.
☐	6. OPENVPN	F	Protokol berperforma tinggi dengan kriptografi modern.
☐	7. BERSAMA	G	Teknologi pengacak metadata untuk menembus inspeksi paket mendalam.
☐	8. TANPA LOG	H	Kill switch bawaan yang melindungi koneksi saat terputus.

Pos 5: Teka-Teki Silang

Selesaikan teka-teki silang dengan mengetik huruf di kotak putih yang aktif. Nomor-nomornya sesuai dengan petunjuk di bawah.



PETUNJUK MENDATAR

2. Perusahaan keamanan yang membeli TunnelBear (6)

4. Kill switch bawaan yang melindungi saat koneksi putus (12)

8. Negara tempat perusahaan terdaftar dan berkantor pusat (6)

PETUNJUK MENURUN

1. Protokol open source umum di komputer (7)

3. Protokol cepat dengan kriptografi modern (9)

5. Penyamaran metadata untuk menembus inspeksi paket mendalam (9)

6. Penilaian keamanan independen setiap tahun (5)

7. Kebijakan privasi yang tidak menyimpan riwayat lalu lintas (8)

Alternatif Pos 5: Petunjuk Teka-Teki Silang yang Aksesibel

Pengguna pembaca layar dan keyboard dapat mengetik jawaban teka-teki silang langsung di kolom teks di bawah ini.

PETUNJUK MENDATAR

2 mendatar: Perusahaan keamanan yang membeli TunnelBear (6 huruf):

4 mendatar: Kill switch bawaan yang melindungi saat koneksi putus (12 huruf):

8 mendatar: Negara tempat perusahaan terdaftar dan berkantor pusat (6 huruf):

PETUNJUK MENURUN

1 menurun: Protokol open source umum di komputer (7 huruf):

3 menurun: Protokol cepat dengan kriptografi modern (9 huruf):

5 menurun: Penyamaran metadata untuk menembus inspeksi paket mendalam (9 huruf):

6 menurun: Penilaian keamanan independen setiap tahun (5 huruf):

7 menurun: Kebijakan privasi yang tidak menyimpan riwayat lalu lintas (8 huruf):

Pos 6: Mencari Kata Tersembunyi

Temukan 8 istilah kunci yang tersembunyi dalam kisi di bawah ini. Kata dapat tersusun mendatar, menurun, atau diagonal.

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

DAFTAR KOSAKATA

KANADA GHOSTBEAR VIGILANTBEAR MCAFEE WIREGUARD OPENVPN AUDIT TANPALOG

Alternatif Pos 6: Pencocokan Kosakata yang Aksesibel

Cocokkan kedelapan istilah dari Pencarian Kata dengan definisi yang benar dengan menulis hurufnya (A-H) di tempat kosong.

ISTILAH KOSAKATA
A. KANADA
B. GHOSTBEAR
C. VIGILANTBEAR
D. MCAFEE
E. WIREGUARD
F. OPENVPN
G. AUDIT
H. TANPALOG

DEFINISI & KOLOM PENCOCOKAN

1. Protokol open source umum di komputer.
2. Kebijakan privasi yang tidak menyimpan riwayat lalu lintas.
3. Protokol cepat dengan kriptografi modern.
4. Negara tempat perusahaan terdaftar dan berkantor pusat.
5. Penilaian keamanan independen setiap tahun.
6. Penyamaran metadata untuk menembus inspeksi paket mendalam.
7. Perusahaan keamanan yang membeli TunnelBear.
8. Kill switch bawaan yang melindungi saat koneksi putus.

Pos 7: Tantangan Kata Acak

Susun ulang huruf di bawah ini untuk menemukan konsep dan istilah kunci Virtual Private Network (VPN). Tulis jawaban Anda di kotak isian yang tersedia.

1. **N K A D A A** _____
2. **R I L A V E A G T B N I** _____
3. **W U G I A D E R R** _____
4. **D T I A U** _____
5. **E T H R B S G A O** _____
6. **E F M A E C** _____
7. **O P V N P N E** _____
8. **P A A G T O L N** _____

Aktivitas Bonus: Berpikir Cepat

3 JAWABAN UNTUK SETIAP KATEGORI. ORANG PERTAMA YANG MELENGKAPI DAFTAR MENANG.

1	Negara tempat Anda ingin server TunnelBear			
2	Hal yang dapat disembunyikan TunnelBear dari jaringan Anda			
3	Situasi saat kill switch membantu			
4	Istilah keamanan yang Anda pelajari di lembar kerja ini			
5	Protokol VPN yang Anda ketahui			
6	Perangkat tempat Anda memasang TunnelBear			
7	Tempat Anda akan menyalakan TunnelBear			
8	Aplikasi yang Anda pakai bersama TunnelBear			
9	Tanda koneksi VPN Anda lambat			
10	Hal yang dicek sebelum membeli VPN			
11	Kata yang menggambarkan aplikasi VPN yang baik			
12	Tombol atau menu di aplikasi VPN			
13	Layanan streaming yang Anda tonton			
14	Data yang tidak boleh disimpan VPN			
15	Fitur yang Anda cari di TunnelBear			

Pos 8: Studi Kasus VPN & Jaringan

Terapkan konsep yang telah Anda pelajari untuk menyelesaikan skenario nyata di bawah ini.

STUDI KASUS 1: MENEMBUS SENSOR



Skenario: Seorang peneliti yang bepergian ke negara yang memblokir protokol VPN perlu mengakses bahan penelitian.

Pertanyaan Diskusi: Pengaturan TunnelBear mana yang perlu diaktifkan untuk menembus inspeksi paket mendalam?

STUDI KASUS 2: HOTSPOT PUBLIK YANG TIDAK AMAN



Skenario: Seorang insinyur terhubung ke hotspot Wi-Fi terbuka di bandara dan koneksinya sering terputus.

Pertanyaan Diskusi: Bagaimana VigilantBear melindungi perangkat insinyur itu saat koneksi terputus?

Pos 9: Memecahkan Sandi

Seorang insinyur jaringan mengamankan jalur routing dan terowongan klien. Gunakan kunci Huruf-ke-Angka di bawah untuk memecahkan pesan dengan menulis huruf yang sesuai di tempat kosong.

KUNCI ENKRIPSI HURUF-KE-ANGKA

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

7	8	15	19	20	2	5	1	18

13	5	14	25	5	13	2	21	14	25	9	11	1	14	22	16	14

1	14	4	1

Pesan yang dipecahkan:

TIPS: SETIAP ANGKA MEWAKILI POSISI HURUF TERSEBUT DALAM ALFABET (MISALNYA 1 = A, 2 = B, 26 = Z).

Pos 10: FAQ Dasar VPN (Bagian A)

Pelajari pertanyaan dan jawaban paling umum tentang Virtual Private Network (VPN) dan tunneling.

Q1: Apakah TunnelBear aman?

Ya, TunnelBear memakai enkripsi AES-256 dan aplikasinya diaudit secara independen setiap tahun. [1]

Q2: Apa itu GhostBear?

GhostBear adalah fitur obfuskasi yang menyamarkan lalu lintas VPN untuk menembus pemblokiran sensor.

Q3: Apakah ada paket gratis?

Ya, TunnelBear menawarkan paket gratis terbatas dengan kuota data 2 GB per bulan. [1]

Q4: Di mana TunnelBear berkantor?

TunnelBear berkantor pusat di Toronto, Kanada, di bawah yurisdiksi Kanada.

Q5: Apa itu VigilantBear?

VigilantBear adalah kill switch bawaan TunnelBear yang mencegah kebocoran saat koneksi terputus.

Pos 10: FAQ Dasar VPN (Bagian B)

Pelajari pertanyaan dan jawaban paling umum tentang Virtual Private Network (VPN) dan tunneling.

Q6: Bisakah saya menghubungkan banyak perangkat?

Ya, paket berbayar mendukung koneksi bersamaan tanpa batas dalam satu akun.

Q7: Apakah TunnelBear mendukung WireGuard?

Ya, WireGuard didukung untuk koneksi berperforma tinggi dan hemat baterai.

Q8: Bagaimana kebijakan tanpa log mereka?

TunnelBear tidak mencatat alamat IP, kueri DNS, atau aktivitas penjelajahan pengguna.

Q9: Siapa pemilik TunnelBear?

TunnelBear diakuisisi oleh perusahaan keamanan siber besar McAfee pada 2018. [8]

Q10: Apakah iklan diblokir?

TunnelBear berfokus pada enkripsi; pemblokir iklan tidak tersedia di klien VPN utamanya. [4]

Pos 10: FAQ Lanjutan VPN (Bagian C)

Jelajahi aspek teknis lanjutan dari protokol tunneling VPN, integrasi aplikasi seluler, dan penerapan di perusahaan.

Q1: Bagaimana GhostBear menembus DPI?

Fitur ini membuat lalu lintas VPN terenkripsi tampak seperti HTTPS biasa, sehingga filter DPI sulit mendeteksinya.

Q2: Apakah Kanada termasuk negara 5-Eyes?

Ya, Kanada adalah anggota aliansi Five Eyes, sehingga yurisdiksinya perlu dipertimbangkan.

Q3: Bagaimana VigilantBear mencegah kebocoran data?

Fitur ini memblokir semua lalu lintas masuk dan keluar sampai koneksi VPN pulih.

Q4: Apa yang diperiksa dalam audit mereka?

Cure53 mengaudit kode aplikasi, konfigurasi server, infrastruktur, dan kontrol pencatatan log.

Q5: Apakah WireGuard berjalan secara bawaan?

Ya, aplikasi TunnelBear menyediakan WireGuard untuk koneksi yang cepat dan stabil.

Pos 10: FAQ Lanjutan VPN (Bagian D)

Jelajahi aspek teknis lanjutan dari protokol tunneling VPN, integrasi aplikasi seluler, dan penerapan di perusahaan.

Q6: Apakah ada server khusus P2P?

Tidak, lalu lintas P2P didukung di semua node server tanpa pembatasan.

Q7: Apakah TunnelBear mencegah kebocoran WebRTC?

Ya, klien mencegat dan merutekan permintaan WebRTC agar IP lokal tidak terungkap.

Q8: Bagaimana keamanan DNS dikelola?

Kueri DNS dirutekan melalui resolver DNS privat TunnelBear yang terenkripsi.

Q9: Bisakah saya memakainya di Linux?

TunnelBear tidak punya aplikasi Linux resmi; aplikasinya tersedia untuk Windows, macOS, iOS, dan Android. [5]

Q10: Bagaimana basis data penagihan dipisahkan?

Catatan penagihan disimpan terpisah dari log lalu lintas server untuk menjaga anonimitas.

Bagian 11: 10 Fakta & Wawasan VPN di Dunia Nyata

Pelajari fakta nyata tentang kecepatan enkripsi VPN, audit protokol, konektivitas seluler, dan kerja jarak jauh di perusahaan.

1. WAWASAN VPN
TunnelBear berkantor pusat di Toronto, Kanada, dan beroperasi di bawah yurisdiksi Kanada. [2]

2. WAWASAN VPN
Layanan ini diakuisisi McAfee pada 2018 untuk memperkuat portofolio keamanannya. [3]

3. WAWASAN VPN
GhostBear menyamarkan pola protokol VPN agar terlihat seperti paket HTTP/S biasa. [4]

4. WAWASAN VPN
VigilantBear berfungsi sebagai kill switch koneksi di tingkat firewall pada klien. [4]

5. WAWASAN VPN
Audit publik tahunan dilakukan Cure53 untuk memverifikasi keamanan aplikasi dan server. [6]

6. WAWASAN VPN
Langganan berbayar mendukung koneksi perangkat bersamaan tanpa batas. [1]

7. WAWASAN VPN
Jaringannya memakai enkripsi AES-256, standar keamanan global. [1]

8. WAWASAN VPN
TunnelBear mendukung terowongan dengan protokol OpenVPN, IKEv2, dan WireGuard. [5]

9. WAWASAN VPN
Tidak ada log yang disimpan tentang alamat IP tujuan atau riwayat penjelajahan pengguna.

10. WAWASAN VPN
Antarmukanya bertema beruang yang menyenangkan untuk mempermudah pengelolaan VPN.

Referensi & Sumber Teknis

Panduan belajar dan teka-teki interaktif ini disusun berdasarkan standar teknis, spesifikasi, dan kerangka regulasi global.

REFERENSI AKADEMIK & INDUSTRI

[1] TunnelBear, LLC. (2026). TunnelBear VPN - Apps on Google Play.

https://play.google.com/store/apps/details?id=com.tunnelbear.android&hl=en_US

[2] TunnelBear, LLC. (n.d.). TunnelBear: Safe and Fast VPN App - App Store.

https://apps.apple.com/us/app/tunnelbear-secure-vpn-wifi/id564842283

[3] TechCrunch. (2018). McAfee acquires VPN company TunnelBear.

https://techcrunch.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[4] PCWorld. (2024). TunnelBear VPN review: It's just right for beginners.

https://www.pcworld.com/article/406999/tunnelbear-vpn-review-2.html

[5] CyberInsider. (2026). TunnelBear Review & Test Results 2026 — Pros and Cons.

https://cyberinsider.com/vpn/reviews/tunnelbear/

[6] Cure53. (2024). Pentest-Report TunnelBear VPN Clients & Servers 10-11.2023.

https://cure53.de/pentest-report_tunnelbear_2023.pdf

[7] Cure53. (2020). TunnelBear Security Assessment Summary 11.2019.

https://cure53.de/summary-report_tunnelbear_2019.pdf

[8] VentureBeat. (2018). McAfee acquires VPN provider TunnelBear.

https://venturebeat.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

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

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

[10] Office of the Privacy Commissioner of Canada. (n.d.). The Personal Information Protection and Electronic Documents Act (PIPEDA).

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1 — **Jawaban Benar: A**

CATATAN PENGAJAR

Di negara mana badan usaha TunnelBear terdaftar? → Kanada

2 Soal 2 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa nama fitur obfuskasi TunnelBear untuk menembus sensor? → GhostBear

3 Soal 3 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa nama fitur kill switch bawaan TunnelBear? → VigilantBear

4 Soal 4 — **Jawaban Benar: A**

CATATAN PENGAJAR

Perusahaan keamanan siber mana yang mengakuisisi TunnelBear pada 2018? → McAfee [8]

5 Soal 5 — **Jawaban Benar: A**

CATATAN PENGAJAR

Protokol mana yang direkomendasikan TunnelBear untuk terowongan modern berkecepatan tinggi? → WireGuard

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Soal 6** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Benar: GhostBear menyamarkan lalu lintas VPN agar lolos dari deep packet inspection.

7 **Soal 7** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: paket gratis memberi 2GB data penjelajahan setiap bulan.

8 **Soal 8** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

VigilantBear menjaga data tetap aman saat aplikasi sedang menyambung atau menyambung ulang.

9 **Soal 9** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Benar: TunnelBear menyatakan sebagai VPN konsumen pertama yang menjalani audit pihak ketiga publik tahunan.

10 **Soal 10** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: TunnelBear berbasis di Toronto dan tunduk pada hukum Kanada.

Kunci Kosakata & Rubrik Penilaian

Rubrik Penilaian Pengajar: Berikan 1 poin untuk setiap pencocokan yang benar (total 8 poin) dan setiap istilah konteks yang benar (total 6 poin).

POS 4: KUNCI PENCOCOKAN KONSEP

B 1. KANADA	G 2. GHOSTBEAR	H 3. VIGILANTBEAR	E 4. MCAFEE
F 5. WIREGUARD	D 6. OPENVPN	C 7. BERSAMA	A 8. TANPA LOG

POS 3: KUNCI ISTILAH KUNCI

1 KANADA	2 GHOSTBEAR	3 VIGILANTBEAR	4 MCAFEE
5 WIREGUARD	6 OPENVPN		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 F – OPENVPN	2 H – TANPALOG	3 E – WIREGUARD	4 A – KANADA
5 G – AUDIT	6 B – GHOSTBEAR	7 D – MCAFEE	8 C – VIGILANTBEAR

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan KANADA, GHOSTBEAR, dan VIGILANTBEAR dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

Studi Kasus:
Minta siswa mendukung rekomendasi mereka dengan fakta dari lembar kerja, bukan asumsi.

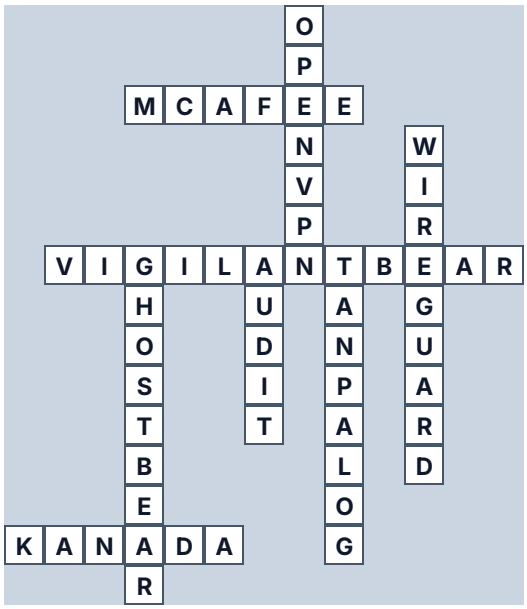
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

2 mendatar: MCAFEE Perusahaan keamanan yang membeli TunnelBear (6 huruf)

4 mendatar: VIGILANTBEAR Kill switch bawaan yang melindungi saat koneksi putus (12 huruf)

8 mendatar: KANADA Negara tempat perusahaan terdaftar dan berkantor pusat (6 huruf)

PETUNJUK MENURUN

1 menurun: OPENVPN Protokol open source umum di komputer (7 huruf)

3 menurun: WIREGUARD Protokol cepat dengan kriptografi modern (9 huruf)

5 menurun: GHOSTBEAR Penyamaran metadata untuk menembus inspeksi paket mendalam (9 huruf)

6 menurun: AUDIT Penilaian keamanan independen setiap tahun (5 huruf)

7 menurun: TANPALOG Kebijakan privasi yang tidak menyimpan riwayat lalu lintas (8 huruf)

Kunci Jawaban Kata Acak & Sandi

Kunci penilaian untuk aktivitas menyusun kata acak dan Tantangan Sandi Rahasia.

KUNCI KATA ACAK

1.	NKADAA	KANADA	5.	ETHRBSGAO	GHOSTBEAR
2.	RILAVEAGTBNI	VIGILANTBEAR	6.	EFMAEC	MCAFEE
3.	WUGIADERR	WIREGUARD	7.	OPVNPNE	OPENVPN
4.	DTIAU	AUDIT	8.	PAAGTOLN	TANPALOG

KUNCI TANTANGAN SANDI RAHASIA

"GHOSTBEAR MENYEMBUNYIKAN VPN ANDA"

Kunci Jawaban Studi Kasus

A STUDI KASUS 1: MENEMBUS SENSOR

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang peneliti yang bepergian ke negara yang memblokir protokol VPN perlu mengakses bahan penelitian.
- Strategi & Solusi yang Disarankan: GhostBear harus diaktifkan untuk mengacak metadata paket VPN agar terlihat seperti lalu lintas HTTPS biasa.

B STUDI KASUS 2: HOTSPOT PUBLIK YANG TIDAK AMAN

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang insinyur terhubung ke hotspot Wi-Fi terbuka di bandara dan koneksinya sering terputus.
- Strategi & Solusi yang Disarankan: VigilantBear membekukan semua antarmuka jaringan dan memblokir kebocoran lalu lintas tak terenkripsi sampai terowongan VPN pulih.