Nama: _____ Tanggal: _____ Nilai: _____

Ulasan Surfshark

Analisis teknis Surfshark VPN yang berkantor pusat di Belanda, rotasi IP dinamis SDN Nexus, filter DNS CleanWeb 2.0, konektivitas perangkat tanpa batas, dan mekanisme penembusan NoBorders.

GAMBARAN PEMBELAJARAN ULASAN SURFSHARK

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 Surfshark. Anda akan mempelajari rotasi IP Nexus berbasis SDN, filter CleanWeb 2.0, koneksi perangkat tanpa batas, dan penembusan sensor NoBorders.

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/surfshark/

Peta Belajar Surfshark Anda

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

PETUNJUK ULASAN SURFSHARK

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan bank kata, cocokkan definisi, serta selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda tentang jaringan SDN Nexus dan pemblokiran CleanWeb. Akhiri dengan aktivitas bonus Berpikir Cepat.

JARINGAN SDN NEXUS & PEMBLOKIR KONTEN CLEANWEB (PENGANTAR)

Surfshark punya jaringan Nexus berbasis SDN yang memungkinkan rotasi IP keluar secara dinamis. Surfshark mengizinkan perangkat tanpa batas, menjalankan node server hanya-RAM di bawah yurisdiksi Belanda, dan memadukan filter CleanWeb 2.0.

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

Pos 1: Tantangan Pilihan Ganda

1. Apa fungsi utama CleanWeb 2.0?

- A) Memblokir iklan, pelacak, pop-up cookie, dan malware
- B) Mengenkripsi email keluar dan drive cloud
- C) Merotasi IP server setiap sepuluh menit
- D) Meneruskan port router otomatis

2. Teknologi SDN Surfshark mana yang merotasi IP?

- A) Surfshark Nexus
- B) Secure Core
- C) WireGuard Core
- D) Mode Camouflage

3. Berapa batas perangkat bersamaan Surfshark?

- A) Tanpa batas
- B) Maks. lima perangkat
- C) Maks. sepuluh perangkat
- D) Hanya satu router

4. Mode Surfshark mana yang menembus firewall?

- A) Mode NoBorders
- B) Mode CleanWeb
- C) Mode Nexus
- D) Mode Bypass

5. Fitur server mana yang mencegah penyimpanan di disk?

- A) Server 100% hanya-RAM tanpa disk
- B) SSD terenkripsi
- C) Larik RAID berkapasitas tinggi
- D) Server virtual di AS

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. CleanWeb 2.0 berfungsi sebagai ekstensi browser dan filter klien yang mencegat iklan, pelacak, dan pop-up persetujuan cookie.

○ Benar ○ Salah

7 Pertanyaan 7

7. Arsitektur Nexus Surfshark menyatukan seluruh jaringan server menjadi satu SDN untuk mengoptimalkan perutean dan rotasi IP.

○ Benar ○ Salah

8 Pertanyaan 8

8. Surfshark membatasi pengguna maksimal lima koneksi perangkat sekaligus.

○ Benar ○ Salah

9 Pertanyaan 9

9. Mode NoBorders otomatis mendeteksi pembatasan internet setempat dan menyarankan node server yang dioptimalkan.

○ Benar ○ Salah

10 Pertanyaan 10

10. Surfshark beroperasi di bawah yurisdiksi Belanda.

○ 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. Agar bebas dari pop-up cookie dan iklan yang mengganggu, pengguna perlu mengaktifkan _____ di pengaturan klien.

2. Surfshark menawarkan koneksi perangkat bersamaan _____ dalam satu paket langganan premium.

3. Arsitektur server eksklusif berbasis SDN bernama jaringan Surfshark _____ .

4. Untuk menembus sensor internet setempat secara otomatis, klien mengaktifkan mode _____ .

5. Agar riwayat sesi tidak tersimpan, penyedia merutekan lalu lintas lewat server _____ tanpa disk.

6. Lalu lintas OpenVPN dapat disamarkan sebagai lalu lintas web biasa dengan mode obfuskasi _____ milik Surfshark.

BANK KATA KOSAKATA

BYPASSER CAMOUFLAGE CLEANWEB HANYA-RAM NEXUS NOBORDERS TANPA BATAS WIREGUARD

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep VPN & Jaringan

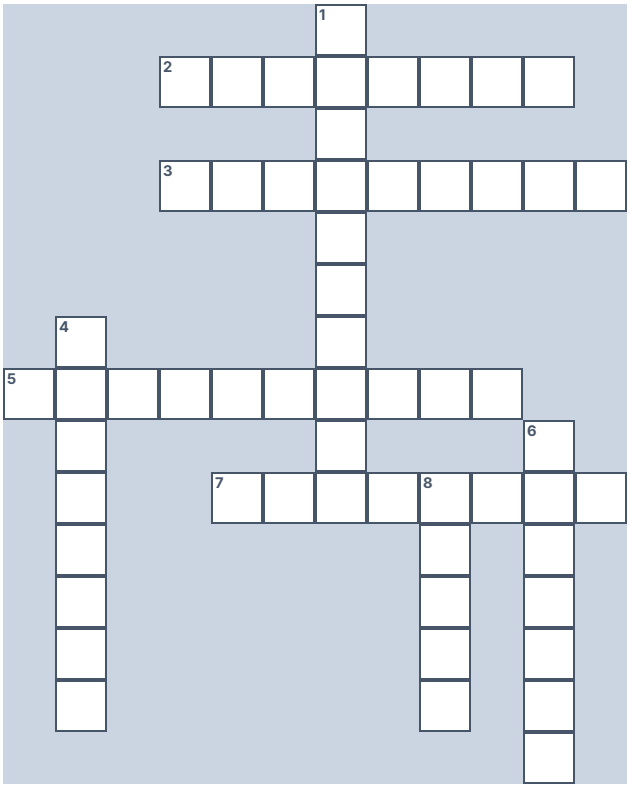
MENCOCOKKAN DEFINISI

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

☐	1. CleanWeb	A	Protokol koneksi open source modern yang cepat.
☐	2. Nexus	B	Mode penembus sensor dengan node yang dioptimalkan.
☐	3. Tanpa Batas	C	Teknologi obfuskasi yang menyamarkan lalu lintas VPN sebagai HTTPS.
☐	4. NoBorders	D	Pemblokir iklan, pelacak, pop-up, dan malware yang canggih.
☐	5. Hanya-RAM	E	Implementasi split tunneling untuk aplikasi tertentu.
☐	6. Camouflage	F	Jaringan server SDN untuk rotasi IP dan multi-hop.
☐	7. Bypasser	G	Server tanpa disk yang tidak menyimpan log.
☐	8. WireGuard	H	Kebijakan langganan dengan koneksi perangkat tanpa batas.

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. Split tunneling milik Surfshark (8)

3. Mode untuk menembus sensor (9)

5. Jumlah perangkat per akun (10)

7. Memblokir iklan dan pop-up cookie (8)

PETUNJUK MENURUN

1. Menyamarkan VPN sebagai HTTPS (10)

4. Server tanpa disk (8)

6. Negara asal Surfshark (7)

8. Jaringan SDN dengan rotasi IP (5)

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: Split tunneling milik Surfshark (8 huruf):

3 mendatar: Mode untuk menembus sensor (9 huruf):

5 mendatar: Jumlah perangkat per akun (10 huruf):

7 mendatar: Memblokir iklan dan pop-up cookie (8 huruf):

PETUNJUK MENURUN

1 menurun: Menyamarkan VPN sebagai HTTPS (10 huruf):

4 menurun: Server tanpa disk (8 huruf):

6 menurun: Negara asal Surfshark (7 huruf):

8 menurun: Jaringan SDN dengan rotasi IP (5 huruf):

Pos 6: Mencari Kata Tersembunyi

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

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

DAFTAR KOSAKATA

CLEANWEB NEXUS TANPABATAS NOBORDERS HANYARAM CAMOUFLAGE BYPASSER BELANDA

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. CLEANWEB
B. NEXUS
C. TANPABATAS
D. NOBORDERS
E. HANYARAM
F. CAMOUFLAGE
G. BYPASSER
H. BELANDA

DEFINISI & KOLOM PENCOCOKAN

1. Server tanpa disk.
2. Memblokir iklan dan pop-up cookie.
3. Mode untuk menembus sensor.
4. Jumlah perangkat per akun.
5. Jaringan SDN dengan rotasi IP.
6. Split tunneling milik Surfshark.
7. Negara asal Surfshark.
8. Menyamarkan VPN sebagai HTTPS.

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. **EANCWLBE** _____
2. **APTAASATBN** _____
3. **YAHARMAN** _____
4. **AERSSBYP** _____
5. **XSNUE** _____
6. **ROOEDNRSB** _____
7. **AOCLFAGEUM** _____
8. **EAABDNL** _____

Aktivitas Bonus: Berpikir Cepat

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

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

Pos 8: Studi Kasus VPN & Jaringan

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

STUDI KASUS 1: KEAMANAN ROTASI IP NEXUS



Skenario: Seorang jurnalis lepas mengunggah wawancara sensitif. Agar tidak dilacak oleh pihak ketiga yang mungkin memantau IP tujuan, mereka mengaktifkan Rotasi IP Surfshark Nexus, yang mengganti IP keluar sekitar setiap lima menit tanpa memutus koneksi.

Pertanyaan Diskusi: Apa keunggulan teknis rotasi IP berbasis SDN dibanding koneksi VPN statis?

STUDI KASUS 2: UJI KONEKSI PERANGKAT TANPA BATAS



Skenario: Seorang administrator TI memakai satu langganan Surfshark untuk mengamankan semua perangkat uji di lab, menghubungkan 45 ponsel dan laptop uji sekaligus ke server lokal.

Pertanyaan Diskusi: Apa manfaat lisensi tanpa batas bagi pengembang yang menguji aplikasi multi-perangkat?

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

14	5	24	21	19		13	5	14	7	7	1	14	20	9		9	16

20	1	14	16	1		16	21	20	21	19

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: Apa itu Surfshark CleanWeb 2.0?

CleanWeb 2.0 adalah fitur canggih yang memblokir iklan, pelacak, malware, dan pop-up persetujuan cookie langsung di browser, sehingga lebih cepat dan aman.

Q2: Apa itu jaringan Surfshark Nexus?

Nexus adalah arsitektur server berbasis SDN yang merutekan lalu lintas lewat seluruh jaringan server, bukan satu terowongan, sehingga fitur seperti Rotasi IP dan MultiHop dimungkinkan.

Q3: Berapa perangkat yang bisa terhubung bersamaan?

Surfshark mengizinkan koneksi perangkat tanpa batas dalam satu akun langganan aktif.

Q4: Apa itu mode NoBorders?

NoBorders otomatis aktif saat klien mendeteksi pembatasan jaringan dan menampilkan daftar server yang dioptimalkan untuk menembus blokir setempat.

Q5: Apakah Surfshark memakai server hanya-RAM?

Ya, seluruh jaringan Surfshark berjalan di server khusus RAM tanpa disk, sehingga data yang tersimpan di memori terhapus saat server reboot.

Pos 10: FAQ Dasar VPN (Bagian B)

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

Q6: Apa itu Surfshark Bypasser?

Bypasser adalah fitur split tunneling Surfshark untuk memilih aplikasi atau situs yang melewati enkripsi VPN dan dirutekan lewat ISP lokal.

Q7: Apakah Surfshark bisa dipakai di smart TV dan konsol game?

Bisa, layanan Smart DNS Surfshark memungkinkan pengaturan DNS di smart TV dan konsol untuk membuka blokir streaming.

Q8: Apa itu mode Camouflage?

Camouflage adalah fitur obfuskasi Surfshark yang menghapus jejak VPN dari koneksi, sehingga penyedia internet tidak tahu Anda memakai VPN.

Q9: Apakah Surfshark punya mesin pencari?

Ya, Surfshark Search adalah mesin pencari privat tanpa iklan yang tidak melacak kueri atau riwayat pencarian. [9]

Q10: Apa itu Surfshark Alert?

Surfshark Alert adalah alat pemantau dark web yang memindai basis data untuk email, kata sandi, dan data kartu kredit yang bocor, lalu memberi tahu Anda. [10]

Pos 10: FAQ Lanjutan VPN (Bagian C)

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

Q1: Bagaimana mode Camouflage menyamarkan lalu lintas VPN?

Camouflage memakai obfuskasi OpenVPN untuk menghapus jejak VPN dari header paket, sehingga alat DPI melihatnya sebagai penjelajahan HTTPS biasa.

Q2: Apa implikasi hukum dari beroperasinya Surfshark di bawah yurisdiksi Belanda?

Surfshark tunduk pada hukum Belanda. Belanda anggota 9-Eyes, tetapi hukumnya tidak mewajibkan VPN mencatat data pengguna, sehingga Surfshark dapat menjaga kebijakan tanpa log yang teraudit. [2]

Q3: Bagaimana fitur split tunneling Bypasser bekerja?

Bypasser mengubah tabel rute sistem agar aplikasi atau URL tertentu lewat gateway ISP lokal, bukan terowongan VPN terenkripsi.

Q4: Sandi apa yang dipakai koneksi WireGuard Surfshark?

Surfshark mengamankan lalu lintas WireGuard dengan sandi simetris ChaCha20 dan autentikator Poly1305 untuk enkripsi cepat.

Q5: Bagaimana Nexus IP Rotator bekerja tanpa memutus koneksi VPN?

Arsitektur SDN menghubungkan klien ke gateway lokal yang merotasi IP keluar di lapisan lain, sehingga enkripsi terowongan klien tidak diulang dan koneksi tetap terjaga.

Pos 10: FAQ Lanjutan VPN (Bagian D)

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

Q6: Bagaimana arsitektur SDN Nexus mengoptimalkan perutean?

Nexus menyatukan semua server dalam satu jaringan. Klien terhubung ke gateway masuk, lalu SDN merutekan paket secara dinamis ke gateway keluar terbaik untuk menekan latensi.

Q7: Apa keunggulan keamanan server 100% hanya-RAM?

Server khusus RAM menyimpan semua file operasional dan kunci enkripsi di memori volatil. Jika daya diputus atau server disita, data yang tersimpan di memori hilang, sehingga hanya sedikit yang dapat dipulihkan.

Q8: Bagaimana mode NoBorders mendeteksi jaringan yang dibatasi?

Aplikasi menguji koneksi ke titik penting. Jika terdeteksi paket hilang khas sensor atau pengalihan DNS, klien otomatis diarahkan ke server khusus.

Q9: Apa beda kriptografis IKEv2 dan WireGuard di Surfshark?

IKEv2 memakai IPSec dengan pertukaran kunci Diffie-Hellman dan enkripsi AES, sedangkan WireGuard memakai kriptografi modern seperti Noise Protocol Framework, Curve25519, dan ChaCha20-Poly1305.

Q10: Bagaimana MultiHop Surfshark mengamankan jalur koneksi?

MultiHop menyalurkan lalu lintas Anda melalui dua server VPN terpisah di negara berbeda. Server pertama mengenkripsi dan meneruskan paket, lalu server kedua mendekripsi dan mengirimkannya, sehingga lalu lintas jauh lebih sulit dilacak kembali ke Anda.

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

Surfshark berkantor pusat di Belanda dan tunduk pada hukum serta aturan privasi Belanda. [1]

2. WAWASAN VPN

Penyedia mengizinkan koneksi perangkat tanpa batas per akun.

3. WAWASAN VPN

CleanWeb 2.0 memblokir iklan, piksel pelacak, malware, dan pop-up cookie di tingkat browser dan klien. [3]

4. WAWASAN VPN

Arsitektur Nexus Surfshark menyatukan semua server dalam Software-Defined Network untuk rotasi IP keluar secara dinamis. [4]

5. WAWASAN VPN

Mode NoBorders otomatis aktif saat klien mendeteksi pembatasan jaringan dan menampilkan server yang dioptimalkan. [5]

6. WAWASAN VPN

Semua server Surfshark berjalan di perangkat keras 100% hanya-RAM tanpa disk, sehingga tidak ada berkas sesi yang ditulis ke disk.

7. WAWASAN VPN

Mode Camouflage menyamarkan lalu lintas OpenVPN dengan menghapus header VPN sehingga tampak seperti penjelajahan web aman biasa. [12]

8. WAWASAN VPN

Aplikasi klien punya Kill Switch yang memutus akses internet jika koneksi VPN terganggu. [11]

9. WAWASAN VPN

Bypasser adalah alat split tunneling milik Surfshark yang dapat mengecualikan aplikasi maupun situs. [7]

10. WAWASAN VPN

VPN ini memakai enkripsi ChaCha20 untuk WireGuard yang lebih cepat dan ringan daripada AES di prosesor seluler.

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[1] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[2] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[3] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[4] Surfshark. (n.d.). Surfshark Nexus technology – elevating VPNs to the next level.
https://surfshark.com/features/nexus

[5] Surfshark. (n.d.). Avoid network restrictions with NoBorders VPN.
https://surfshark.com/features/noborders

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). What is VPN split tunneling and how does it work?
https://surfshark.com/features/bypasser

[8] VPN.com. (n.d.). Surfshark Review: Unlimited Devices, Unbeatable Value.
https://www.vpn.com/vpn/surfshark/

[9] Surfshark. (n.d.). Hide your searches.
https://surfshark.com/search

[10] Surfshark. (n.d.). Surfshark Alert: protect your personal information.
https://surfshark.com/alert

[11] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

CleanWeb memblokir iklan, pelacak, malware, dan pop-up cookie, baik di aplikasi maupun di ekstensi browser Surfshark. [3]

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Nexus menghubungkan server Surfshark dalam satu jaringan berbasis perangkat lunak yang menjalankan fitur seperti Rotating IP.

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Setiap paket Surfshark mengizinkan koneksi perangkat bersamaan tanpa batas dalam satu akun.

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

NoBorders aktif otomatis saat aplikasi mendeteksi pembatasan jaringan dan menyarankan server yang berfungsi di sana.

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Semua server Surfshark hanya memakai RAM, jadi tidak ada yang ditulis ke disk dan data terhapus setiap kali dinyalakan ulang.

Kunci Jawaban: Pos 2 - Benar atau Salah

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

CATATAN PENGAJAR

Benar: CleanWeb bekerja di aplikasi dan ekstensi browser, memblokir iklan, pelacak, dan pop-up persetujuan cookie.

7 **Soal 7** **Jawaban Benar: Benar**

CATATAN PENGAJAR

Benar: Nexus menghubungkan semua server dalam satu SDN yang mengoptimalkan routing dan memungkinkan rotasi IP.

8 **Soal 8** **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: Surfshark tidak membatasi perangkat; setiap paket mengizinkan koneksi bersamaan tanpa batas.

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

CATATAN PENGAJAR

Benar: saat NoBorders mendeteksi pembatasan, fitur ini menawarkan daftar server yang paling andal dalam kondisi itu.

10 **Soal 10** **Jawaban Benar: Benar**

CATATAN PENGAJAR

Benar: Surfshark B.V. terdaftar di Amsterdam dan beroperasi di bawah hukum Belanda.

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

D 1. CleanWeb	F 2. Nexus	H 3. Tanpa Batas	B 4. NoBorders
G 5. Hanya-RAM	C 6. Camouflage	E 7. Bypasser	A 8. WireGuard

POS 3: KUNCI ISTILAH KUNCI

1 CLEANWEB	2 TANPA BATAS	3 NEXUS	4 NOBORDERS
5 HANYA-RAM	6 CAMOUFLAGE		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 E – HANYARAM	2 A – CLEANWEB	3 D – NOBORDERS	4 C – TANPABATAS
5 B – NEXUS	6 G – BYPASSER	7 H – BELANDA	8 F – CAMOUFLAGE

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan CleanWeb, Nexus, dan Tanpa Batas dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

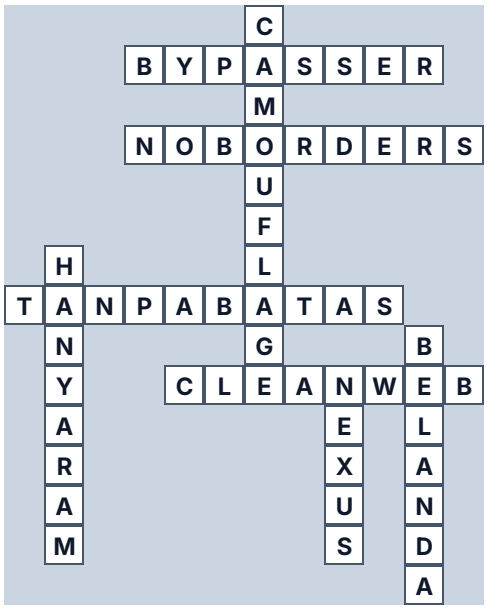
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

2 mendatar: BYPASSER Split tunneling milik Surfshark (8 huruf)

3 mendatar: NOBORDERS Mode untuk menembus sensor (9 huruf)

5 mendatar: TANPABATAS Jumlah perangkat per akun (10 huruf)

7 mendatar: CLEANWEB Memblokir iklan dan pop-up cookie (8 huruf)

PETUNJUK MENURUN

1 menurun: CAMOUFLAGE Menyamarkan VPN sebagai HTTPS (10 huruf)

4 menurun: HANYARAM Server tanpa disk (8 huruf)

6 menurun: BELANDA Negara asal Surfshark (7 huruf)

8 menurun: NEXUS Jaringan SDN dengan rotasi IP (5 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	E A N C W L B E	CLEANWEB	5.	X S N U E	NEXUS
2.	A P T A A S A T B N	TANPABATAS	6.	R O O E D N R S B	NOBORDERS
3.	Y A H A R M A N	HANYARAM	7.	A O C L F A G E U M	CAMOUFLAGE
4.	A E R S S B Y P	BYPASSER	8.	E A A B D N L	BELANDA

KUNCI TANTANGAN SANDI RAHASIA

"NEXUS MENGGANTI IP TANPA PUTUS"

Kunci Jawaban Studi Kasus

A STUDI KASUS 1: KEAMANAN ROTASI IP NEXUS

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang jurnalis lepas mengunggah wawancara sensitif. Untuk mencegah pelacakan oleh pihak ketiga yang mungkin memantau IP tujuan, ia mengaktifkan Rotasi IP Surfshark Nexus, yang mengganti IP keluar sekitar setiap lima menit tanpa memutus koneksi.
- Strategi & Solusi yang Disarankan: Rotasi IP mengganti alamat IP keluar secara dinamis, sehingga pelacak tidak bisa menyusun log lalu lintas berkelanjutan dari satu IP statis.

B STUDI KASUS 2: UJI KONEKSI PERANGKAT TANPA BATAS

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang administrator TI memakai satu langganan Surfshark untuk mengamankan semua perangkat uji di lab, menghubungkan 45 ponsel dan laptop uji sekaligus ke server lokal.
- Strategi & Solusi yang Disarankan: Batas koneksi dan bentrokan login hilang, sehingga pengembang dapat memperluas lingkungan uji tanpa mengelola banyak akun.