Nama: _____ Tanggal: _____ Nilai: _____

Keamanan Surfshark

Menelaah fitur keamanan Surfshark, termasuk pemblokiran iklan CleanWeb, routing dinamis MultiHop, arsitektur SDN Nexus, armada server yang hanya memakai RAM, dan mode Camouflage.

GAMBARAN PEMBELAJARAN KEAMANAN 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 arsitektur keamanan Surfshark. Anda akan mempelajari server hanya-RAM, rotasi IP dinamis SDN Nexus, pemblokir iklan CleanWeb, dan perutean MultiHop.

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/vpn/surfshark/security/

Peta Belajar Keamanan Surfshark Anda

- Analisis arsitektur teknis dan aturan konfigurasi keamanan Surfshark.
- Atur pengaturan aplikasi untuk mencegah kebocoran lalu lintas IP, DNS, dan WebRTC.
- Bandingkan harga khusus, masa uji coba, dan fitur kinerja dengan model standar.

PETUNJUK PANDUAN KEAMANAN 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 infrastruktur hanya-RAM, SDN Nexus, dan CleanWeb. Akhiri dengan aktivitas bonus Berpikir Cepat.

ARMADA SERVER HANYA-RAM, SDN NEXUS & ARSITEKTUR CLEANWEB (PENGANTAR)

Surfshark melindungi privasi pengguna dengan armada server yang seluruhnya berbasis RAM, jaringan terdefinisi perangkat lunak Nexus dengan IP Rotator, pemblokiran iklan CleanWeb, dan jalur enkripsi Dynamic MultiHop.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa nama pemblokir iklan & malware Surfshark?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Arsitektur perangkat keras apa yang dipakai semua server?**
   - A) Hard disk
   - B) 100% hanya-RAM
   - C) Penyimpanan optik
   - D) Pita magnetik

3. **3. Fitur apa yang merutekan lewat dua server VPN?**
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Jaringan Nexus
   - D) IP statis

4. **4. Fitur obfuskasi mana yang menyamarkan VPN sebagai data web biasa?**
   - A) Kill Switch
   - B) Mode Camouflage
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. **5. Apa fungsi alat Bypasser?**
   - A) Penambah kecepatan
   - B) Split Tunneling
   - C) Pengelola kata sandi
   - D) Resolver DNS

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Server hanya-RAM langsung menghapus semua data saat dinyalakan ulang.

Benar Salah

7 Pertanyaan 7

7. Mode Camouflage mencegah ISP mendeteksi pemakaian VPN.

Benar Salah

8 Pertanyaan 8

8. CleanWeb 2.0 bekerja di ekstensi browser untuk memblokir pop-up persetujuan cookie.

Benar Salah

9 Pertanyaan 9

9. Surfshark menyimpan stempel waktu koneksi dan log pemakaian bandwidth sementara.

Benar Salah

10 Pertanyaan 10

10. Jaringan Nexus berkala merotasi IP pengguna tanpa memutus koneksi.

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. Iklan, skrip pelacak, dan tautan phishing diblokir oleh filter _____ .
2. Aktivitas pengguna tak meninggalkan jejak forensik karena server berjalan di memori _____ .
3. Merutekan data lewat dua server terenkripsi dilakukan dengan terowongan _____ .
4. Untuk menyembunyikan pemakaian VPN dari ISP, pengguna mengaktifkan mode _____ .
5. Membiarkan aplikasi perbankan melewati terowongan VPN diatur lewat pengaturan _____ .
6. Arsitektur SDN generasi baru yang menghubungkan armada server adalah sistem _____ .

BANK KATA KOSAKATA

BYPASSER CAMOUFLAGE CLEANWEB HANYARAM KILL SWITCH MULTI-HOP NEXUS NETWORK ROTASIIP

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep VPN & Jaringan

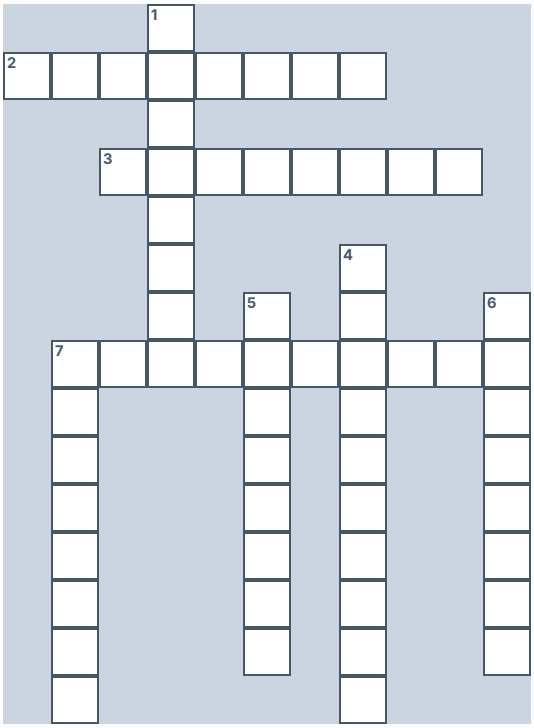
MENCOCOKKAN DEFINISI

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	Fitur pengaman otomatis yang memblokir lalu lintas saat VPN putus.
☐	2. HANYARAM	B	Fungsi split tunneling agar aplikasi tertentu melewati VPN.
☐	3. MULTI-HOP	C	Filter canggih yang memblokir iklan, malware, dan spanduk persetujuan cookie.
☐	4. CAMOUFLAGE	D	Server bermemori volatil yang menghapus semua data setiap kali dimatikan.
☐	5. BYPASSER	E	Fitur yang rutin mengganti IP eksternal tanpa memutus terowongan.
☐	6. KILL SWITCH	F	Teknologi obfuskasi yang menyembunyikan jejak VPN agar menyerupai HTTPS biasa.
☐	7. NEXUS NETWORK	G	Fitur VPN ganda yang mengenkripsi lalu lintas lewat dua node server.
☐	8. ROTASIIP	H	Jaringan berbasis perangkat lunak yang menyatukan semua server.

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. Mengganti IP tanpa memutus koneksi (8)

3. Membiarkan aplikasi melewati VPN (8)

7. Penyamaran yang menyerupai HTTPS (10)

PETUNJUK MENURUN

1. Server yang menghapus semuanya saat dinyalakan ulang (8)

4. Memblokir lalu lintas saat koneksi gagal (10)

5. VPN ganda lewat dua negara (8)

6. Jaringan server berbasis perangkat lunak (8)

7. Filter untuk iklan dan malware (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: Mengganti IP tanpa memutus koneksi (8 huruf):

3 mendatar: Membiarkan aplikasi melewati VPN (8 huruf):

7 mendatar: Penyamaran yang menyerupai HTTPS (10 huruf):

PETUNJUK MENURUN

1 menurun: Server yang menghapus semuanya saat dinyalakan ulang (8 huruf):

4 menurun: Memblokir lalu lintas saat koneksi gagal (10 huruf):

5 menurun: VPN ganda lewat dua negara (8 huruf):

6 menurun: Jaringan server berbasis perangkat lunak (8 huruf):

7 menurun: Filter untuk iklan dan malware (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.

U S T E L J B M A B C P X L K

Y P K X T K D U Q M B J D I N

H I N K Q P G L M M Y Q R S T

C I T G C S Q T O H P S B W D

T S S Z V C C I Z W A F K C H

I A Z D N A D H Q X S P C L U

W T B A Z M N O H D S K A E D

S O O D F O H P A N E I D A R

L R Q M E U I R N E R Z S N F

L Q V F A F A Q Y X O N P W T

I X Q K R L U S A U D N Y E B

K F S X W A J A R S R Z Y B Y

L G I M R G J M A N L T O H Q

Q H Z A O E V G M E U B Y R Y

B H L Z G J O P N T W C M Z Y

DAFTAR KOSAKATA

CLEANWEB HANYARAM MULTIHOP CAMOUFLAGE BYPASSER KILLSWITCH NEXUSNET ROTASIIP

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. HANYARAM
C. MULTIHOP
D. CAMOUFLAGE
E. BYPASSER
F. KILLSWITCH
G. NEXUSNET
H. ROTASIIP

DEFINISI & KOLOM PENCOCOKAN

1. Penyamaran yang menyerupai HTTPS.
2. Memblokir lalu lintas saat koneksi gagal.
3. Filter untuk iklan dan malware.
4. Membiarkan aplikasi melewati VPN.
5. Server yang menghapus semuanya saat dinyalakan ulang.
6. Mengganti IP tanpa memutus koneksi.
7. VPN ganda lewat dua negara.
8. Jaringan server berbasis perangkat lunak.

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. **TMPUOHIL** _____

3. **AYBSSREP** _____

4. **UETNSNEX** _____

5. **ARAMYHAN** _____

6. **GUOLACAFEM** _____

7. **ILKIWTCHSL** _____

8. **AOSPRIIT** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Fitur keamanan di Surfshark			
2	Tanda koneksi VPN Anda lambat			
3	Protokol VPN yang Anda ketahui			
4	Hal yang dilindungi enkripsi			
5	Ancaman di Wi-Fi publik			
6	Negara dengan hukum privasi yang kuat			
7	Cara membuat kata sandi yang kuat			
8	Perangkat tempat Anda memasang Surfshark			
9	Pertanyaan untuk layanan pelanggan Surfshark			
10	Hal yang diaktifkan untuk keamanan lebih			
11	Hal yang dapat disembunyikan Surfshark dari jaringan Anda			
12	Jenis kebocoran dari VPN			
13	Data yang tidak boleh disimpan VPN			
14	Kata yang menggambarkan aplikasi VPN yang baik			
15	Hal yang diperiksa dalam audit			

Pos 8: Studi Kasus VPN & Jaringan

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

STUDI KASUS 1: MENEMBUS FILTER KAMPUS DAN KANTOR

👷

Skenario: Seorang mahasiswa mendapati Wi-Fi kampus memblokir semua port OpenVPN dan WireGuard standar.

Pertanyaan Diskusi: Fitur Surfshark mana yang memungkinkan mahasiswa terhubung tanpa terdeteksi administrator jaringan?

STUDI KASUS 2: INVESTIGASI JURNALISTIK BERISIKO TINGGI

👷

Skenario: Seorang jurnalis investigasi butuh perlindungan ekstra dari pengawasan saat meneliti dokumen perusahaan yang sensitif.

Pertanyaan Diskusi: Bagaimana Dynamic MultiHop memberi privasi lebih baik dibanding perutean satu server?

Pos 9: Memecahkan Sandi

Seorang insinyur jaringan mengamankan jalur perutean 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

3 1 13 15 21 6 12 1 7 5

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

4 1 18 9 9 19 16

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?

CleanWeb adalah fitur keamanan terpadu yang memblokir iklan, pelacak, malware, dan situs phishing.

Q2: Apa itu server hanya-RAM?

Server khusus RAM berjalan di memori volatil, artinya data yang tersimpan di memori terhapus setiap kali server reboot.

Q3: Apa itu Surfshark MultiHop?

MultiHop (Double VPN) merutekan dan mengenkripsi koneksi lewat dua lokasi server berbeda.

Q4: Bagaimana Mode Camouflage bekerja?

Mode Camouflage menyamarkan lalu lintas VPN sehingga ISP tidak tahu Anda memakai VPN.

Q5: Apa itu fitur Bypasser?

Bypasser adalah alat split tunneling Surfshark agar aplikasi atau situs tertentu melewati VPN.

Pos 10: FAQ Dasar VPN (Bagian B)

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

Q6: Apakah Surfshark punya Kill Switch?

Ya, Kill Switch memutus internet jika VPN tiba-tiba terputus. [9]

Q7: Standar enkripsi apa yang dipakai Surfshark?

Surfshark memakai AES-256-GCM dan ChaCha20, serta AEGIS-256X2 pada protokol barunya, Dausos.

Q8: Apakah kebijakan tanpa log Surfshark diaudit?

Ya, Deloitte memverifikasi kebijakan tanpa log Surfshark pada 2023 dan lagi pada 2025.

Q9: Apa itu Surfshark Nexus?

Nexus adalah arsitektur SDN canggih yang menyatukan semua server agar perutean lebih mulus.

Q10: Apa itu fitur IP Rotator?

IP Rotator otomatis mengganti alamat IP setiap beberapa menit tanpa memutus sesi VPN.

Pos 10: FAQ Lanjutan VPN (Bagian C)

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

Q1: Apa beda Dynamic MultiHop dengan Double VPN biasa?

Dynamic MultiHop memungkinkan Anda memilih kombinasi server masuk dan keluar mana pun di dunia.

Q2: Apakah CleanWeb 2.0 bekerja di ekstensi browser?

Ya, CleanWeb 2.0 memblokir iklan video, pop-up persetujuan cookie, dan spanduk peringatan di Chrome/Firefox.

Q3: Apa itu Alternative ID dalam paket keamanan?

Alternative ID membuat nama samaran, alamat email, dan nomor telepon penyamar yang unik. [11]

Q4: Bagaimana Surfshark mencegah kebocoran DNS?

Surfshark mengarahkan semua permintaan domain melalui server DNS privat miliknya di setiap node.

Q5: Apakah Surfshark mendukung ChaCha20 di ponsel?

Ya, WireGuard di Android dan iOS memakai ChaCha20-Poly1305 agar lebih efisien di ponsel.

Pos 10: FAQ Lanjutan VPN (Bagian D)

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

Q6: Apa itu mode NoBorders?

NoBorders otomatis mendeteksi jaringan yang membatasi dan menyediakan server khusus.

Q7: Siapa yang mengaudit ekstensi browser Surfshark?

Firma keamanan independen Cure53 mengaudit ekstensi browser dan sistem server. [10]

Q8: Bagaimana Surfshark melindungi dari kebocoran IPv6?

Surfshark merutekan IPv6 dengan aman atau membatasinya agar tidak ada kebocoran tanpa enkripsi.

Q9: Di mana yurisdiksi hukum Surfshark?

Surfshark tunduk pada hukum Belanda dan standar privasi Eropa GDPR yang ketat. [7]

Q10: Apakah Surfshark mendukung autentikasi dua faktor (2FA)?

Ya, dan Surfshark One menambahkan kunci 2FA agar hanya Anda yang bisa mengubah pengaturan fitur.

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

1. Surfshark menyatakan seluruh jaringannya yang berisi lebih dari 4.500 server berjalan di perangkat keras khusus RAM volatil tanpa disk. [8]

2. WAWASAN VPN

2. Firma Big Four Deloitte memverifikasi kebijakan tanpa log Surfshark pada 2023 dan lagi pada November 2025. [2]

3. WAWASAN VPN

3. Arsitektur Nexus menyatukan semua server global dalam jaringan berbasis perangkat lunak yang dinamis.

4. WAWASAN VPN

4. Rotating IP mengganti alamat IP Anda sekitar setiap lima menit tanpa memutus koneksi VPN. [6]

5. WAWASAN VPN

5. CleanWeb 2.0 memblokir pop-up persetujuan cookie dan iklan video langsung di browser. [4]

6. WAWASAN VPN

6. Dynamic MultiHop memungkinkan jalur enkripsi dua server pilihan di 100 negara. [5]

7. WAWASAN VPN

7. Mode Camouflage menghapus jejak header VPN sehingga lalu lintas tak bisa dibedakan dari HTTPS.

8. WAWASAN VPN

8. Alternative ID membuat nama samaran dan email sekali pakai untuk melindungi dari kebocoran basis data.

9. WAWASAN VPN

9. Surfshark memakai enkripsi simetris AES-256-GCM serta ChaCha20 pada protokol WireGuard. [3]

10. WAWASAN VPN

10. Mode NoBorders otomatis aktif di jaringan terbatas agar tunneling tetap bisa dipakai.

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.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

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

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

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

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

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

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

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[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 **Pemblokir Konten Terpadu** PERTAHANAN IKLAN & MALWARE — **Jawaban Benar: B**

CATATAN PENGAJAR

CleanWeb adalah filter keamanan terpadu Surfshark yang memblokir iklan, domain pelacak, situs phishing, dan skrip URL jahat di tingkat jaringan.

2 **Infrastruktur 100% Hanya-RAM** ARSITEKTUR RAM — **Jawaban Benar: B**

CATATAN PENGAJAR

Surfshark menjalankan server yang hanya memakai RAM, sehingga data di memori server terhapus saat server dimatikan atau dinyalakan ulang.

3 **Terowongan Ganda MultiHop** VPN MULTIHOP — **Jawaban Benar: B**

CATATAN PENGAJAR

MultiHop (Double VPN) mengenkripsi lalu lintas lewat dua node server di negara berbeda untuk mencegah serangan korelasi.

4 **Obfuskasi Mode Camouflage** PENYAMARAN — **Jawaban Benar: B**

CATATAN PENGAJAR

Mode Camouflage mengubah header paket OpenVPN agar lalu lintas VPN tampak seperti HTTPS biasa dan menembus firewall ketat.

5 **Split Tunneling Bypasser** SPLIT TUNNELING — **Jawaban Benar: B**

CATATAN PENGAJAR

Bypasser adalah alat split tunneling Surfshark untuk memilih aplikasi atau situs yang dirutekan langsung lewat koneksi ISP biasa.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Penghapusan Data Memori Volatil** KEAMANAN SERVER — Jawaban Benar: Benar

CATATAN PENGAJAR

Server hanya-RAM tidak menyimpan data di hard drive permanen; menyalakan ulang langsung menghapus seluruh memori.

7 **Penyamaran dari ISP dengan Camouflage** PENYAMARAN LALU LINTAS — Jawaban Benar: Benar

CATATAN PENGAJAR

Mode Camouflage menghapus jejak protokol OpenVPN sehingga ISP tidak dapat mendeteksi pengguna tersambung ke VPN.

8 **Ekstensi Browser CleanWeb 2.0** EKSTENSI BROWSER — Jawaban Benar: Benar

CATATAN PENGAJAR

CleanWeb 2.0 bekerja di ekstensi browser untuk memblokir pop-up persetujuan cookie, iklan video, dan skrip pengalihan jahat secara real time. [4]

9 **Tanpa Penyimpanan Log Koneksi** KEBIJAKAN TANPA LOG — Jawaban Benar: Salah

CATATAN PENGAJAR

Surfshark menjaga kebijakan tanpa log yang diaudit independen, tanpa mencatat alamat IP, stempel waktu koneksi, atau bandwidth.

10 **Rotasi IP Dinamis Nexus** JARINGAN NEXUS — Jawaban Benar: Benar

CATATAN PENGAJAR

Jaringan Nexus Surfshark merotasi IP pengguna secara dinamis setiap beberapa menit tanpa memutus koneksi VPN.

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

C 1. CLEANWEB	D 2. HANYARAM	G 3. MULTI-HOP	F 4. CAMOUFLAGE
B 5. BYPASSER	A 6. KILL SWITCH	H 7. NEXUS NETWORK	E 8. ROTASIIP

POS 3: KUNCI ISTILAH KUNCI

1 CLEANWEB	2 HANYARAM	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS NETWORK		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – HANYARAM	6 H – ROTASIIP	7 C – MULTIHOP	8 G – NEXUSNET

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan CLEANWEB, HANYARAM, dan MULTI-HOP dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

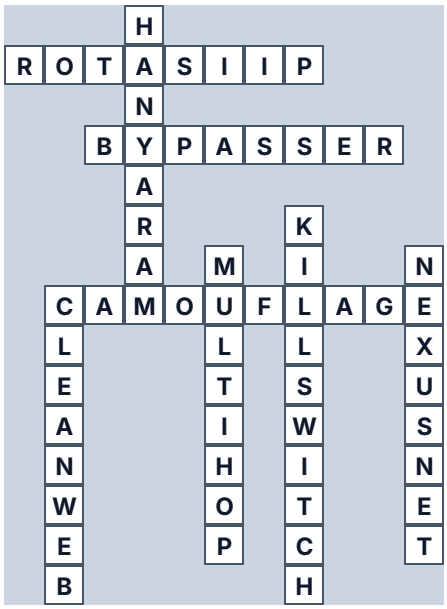
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

2 mendatar: ROTASIIP Mengganti IP tanpa memutus koneksi (8 huruf)

3 mendatar: BYPASSER Membiarkan aplikasi melewati VPN (8 huruf)

7 mendatar: CAMOUFLAGE Penyamaran yang menyerupai HTTPS (10 huruf)

PETUNJUK MENURUN

1 menurun: HANYARAM Server yang menghapus semuanya saat dinyalakan ulang (8 huruf)

4 menurun: KILLSWITCH Memblokir lalu lintas saat koneksi gagal (10 huruf)

5 menurun: MULTIHOP VPN ganda lewat dua negara (8 huruf)

6 menurun: NEXUSNET Jaringan server berbasis perangkat lunak (8 huruf)

7 menurun: CLEANWEB Filter untuk iklan dan malware (8 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. EANCWLBE	CLEANWEB	5. ARAMYHAN	HANYARAM
2. TMPUOHIL	MULTIHOP	6. GUOLACAFEM	CAMOUFLAGE
3. AYBSSREP	BYPASSER	7. ILKIWTCHSL	KILLSWITCH
4. UETNSNEX	NEXUSNET	8. AOSPRIIT	ROTASIIP

KUNCI TANTANGAN SANDI RAHASIA

"CAMOUFLAGE MENYEMBUNYIKAN VPN DARI ISP"

Kunci Jawaban Studi Kasus

A STUDI KASUS 1: MENEMBUS FILTER KAMPUS DAN KANTOR

Jawaban Pengajar

RUBRIK PENILAIAN & PEDOMAN JAWABAN

- Analisis Skenario: Seorang mahasiswa mendapati Wi-Fi kampus memblokir semua port OpenVPN dan WireGuard standar.
- Pertanyaan Fokus: Fitur mana yang memungkinkan mahasiswa terhubung tanpa terdeteksi administrator jaringan?
- Strategi & Solusi yang Disarankan: Aktifkan Mode Camouflage (dengan OpenVPN) yang menghapus header VPN sehingga firewall melihatnya sebagai penjelajahan HTTPS biasa.

B STUDI KASUS 2: INVESTIGASI JURNALISTIK BERISIKO TINGGI

Jawaban Pengajar

RUBRIK PENILAIAN & PEDOMAN JAWABAN

- Analisis Skenario: Seorang jurnalis investigasi butuh perlindungan ekstra dari pengawasan saat meneliti dokumen perusahaan yang sensitif.
- Pertanyaan Fokus: Bagaimana Dynamic MultiHop memberi privasi lebih baik dibanding satu server?
- Strategi & Solusi yang Disarankan: Dynamic MultiHop mengenkripsi data dua kali lewat server masuk dan keluar di negara berbeda, sehingga tak ada satu titik pembobolan.