Nama: _____ Tanggal: _____ Nilai: _____

Ulasan IPVanish

Analisis teknis IPVanish VPN yang berkantor pusat di AS, infrastruktur server tier-1 milik sendiri, routing WireGuard berkinerja tinggi, fitur proksi SOCKS5, dan validasi kebijakan tanpa log.

GAMBARAN PEMBELAJARAN ULASAN IPVANISH

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 IPVanish. Anda akan mempelajari infrastruktur fisik milik sendiri, proksi SOCKS5 untuk torrent P2P, kinerja WireGuard, dan aturan data yurisdiksi AS.

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/ipvanish/

Peta Belajar IPVanish Anda

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

PETUNJUK ULASAN IPVANISH

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 proksi SOCKS5 dan infrastruktur server milik sendiri. Akhiri dengan aktivitas bonus Berpikir Cepat.

INFRASTRUKTUR MILIK SENDIRI & PROKSI P2P SOCKS5 (PENGANTAR)

IPVanish menonjol karena memiliki dan mengelola sebagian besar jaringan server fisiknya, yang meningkatkan kinerja dan keamanan. Layanan ini menawarkan protokol WireGuard yang cepat dan proksi SOCKS5 untuk torrent P2P, tetapi beroperasi di bawah yurisdiksi AS yang termasuk Five Eyes.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Protokol open source apa yang menjadi bawaan di aplikasi IPVanish?**
   - A) WireGuard
   - B) L2TP/IPSec
   - C) PPTP
   - D) Catapult Hydra

2. **2. Proksi apa yang disediakan IPVanish untuk torrent P2P?**
   - A) Proksi SOCKS5
   - B) Proksi HTTP
   - C) Relai Tor
   - D) Shadowsocks

3. **3. Firma mana yang melakukan audit tanpa log independen pertama IPVanish pada 2022?**
   - A) Leviathan Security Group
   - B) PwC
   - C) Deloitte
   - D) Cure53

4. **4. Di bawah yurisdiksi negara mana IPVanish beroperasi?**
   - A) Amerika Serikat
   - B) Swiss
   - C) Panama
   - D) Kepulauan Virgin Britania Raya

5. **5. Berapa koneksi perangkat bersamaan di paket premium IPVanish?**
   - A) Tanpa batas
   - B) Lima
   - C) Sepuluh
   - D) Tujuh

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. IPVanish mengelola dan memiliki sebagian besar infrastruktur server fisiknya.

○ Benar ○ Salah

7 Pertanyaan 7

7. Lalu lintas proksi SOCKS5 terenkripsi penuh seperti terowongan VPN standar.

○ Benar ○ Salah

8 Pertanyaan 8

8. Klien desktop IPVanish tidak punya fitur Kill Switch tingkat sistem.

○ Benar ○ Salah

9 Pertanyaan 9

9. IPVanish beroperasi dari Amerika Serikat, anggota aliansi intelijen Five Eyes.

○ Benar ○ Salah

10 Pertanyaan 10

10. Split tunneling di IPVanish memungkinkan lalu lintas aplikasi dirutekan di luar terowongan VPN.

○ 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. Protokol modern _____ diatur sebagai bawaan untuk kinerja perutean yang optimal.
2. Lalu lintas P2P dapat dirutekan lewat _____ yang cepat untuk menyamarkan lokasi asli klien.
3. Terhubung ke node yang dekat secara geografis memaksimalkan _____ yang nyata.
4. Untuk mencegah kebocoran data, pengguna perlu mengatur kontrol _____ bawaan.
5. Audit keamanan independen telah mengesahkan komitmen _____ penyedia.
6. Tidak seperti sebagian pesaing, IPVanish tidak menerapkan _____ aktif pada akun.

BANK KATA KOSAKATA

ALAMAT IP | BATAS PERANGKAT | KEAMANAN | KECEPATAN SERVER | KILL SWITCH | LOG TERAUDIT | PROKSI SOCKS5 | WIREGUARD

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep VPN & Jaringan

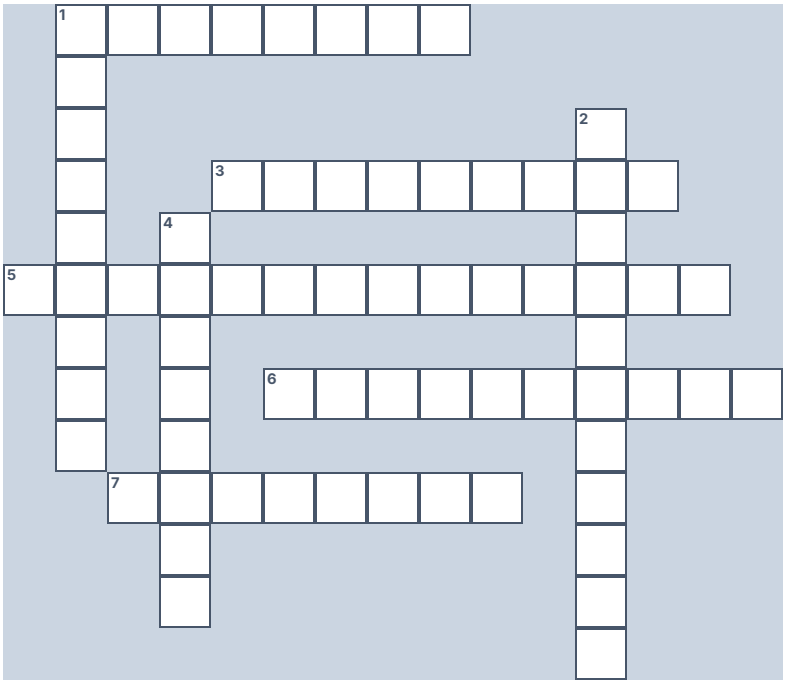
MENCOCOKKAN DEFINISI

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

☐	1. WireGuard	A	Mekanisme pengaman yang memblokir lalu lintas internet jika VPN gagal.
☐	2. Proksi SOCKS5	B	Protokol open source yang dikenal cepat dengan kriptografi modern.
☐	3. Kecepatan Server	C	Batasan jumlah sesi perangkat yang aktif.
☐	4. Kill Switch	D	Kapasitas throughput node server saat menangani lalu lintas aktif.
☐	5. Log Teraudit	E	Pengenal jaringan unik yang diberikan ke perangkat di internet.
☐	6. Batas Perangkat	F	Tingkat perlindungan keseluruhan sistem terowongan terenkripsi.
☐	7. Alamat IP	G	Catatan terverifikasi bahwa tidak ada aktivitas pengguna yang dilacak.
☐	8. Keamanan	H	Sistem perutean proksi tanpa enkripsi untuk menyamarkan lokasi klien P2P.

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

1. Tingkat perlindungan keseluruhan sistem terenkripsi (8)

3. Protokol open source modern yang cepat (9)

5. Jumlah perangkat bersamaan per akun (14)

6. Pengaman yang memutus lalu lintas saat koneksi gagal (10)

7. Alamat unik yang diberikan ke perangkat (8)

PETUNJUK MENURUN

1. Laju nyata server yang aktif (9)

2. Layanan SOCKS5 tanpa enkripsi yang menyembunyikan IP (11)

4. Kebijakan teraudit bahwa sesi tidak disimpan (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

1 mendatar: Tingkat perlindungan keseluruhan sistem terenkripsi (8 huruf):

3 mendatar: Protokol open source modern yang cepat (9 huruf):

5 mendatar: Jumlah perangkat bersamaan per akun (14 huruf):

6 mendatar: Pengaman yang memutus lalu lintas saat koneksi gagal (10 huruf):

7 mendatar: Alamat unik yang diberikan ke perangkat (8 huruf):

PETUNJUK MENURUN

1 menurun: Laju nyata server yang aktif (9 huruf):

2 menurun: Layanan SOCKS5 tanpa enkripsi yang menyembunyikan IP (11 huruf):

4 menurun: Kebijakan teraudit bahwa sesi tidak disimpan (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.

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

DAFTAR KOSAKATA

WIREGUARD PROKSISOCKS KECEPATAN KILLSWITCH TANPALOG
BATASPERANGKAT ALAMATIP KEAMANAN

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. WIREGUARD
B. PROKSISOCKS
C. KECEPATAN
D. KILLSWITCH
E. TANPALOG
F. BATASPERANGKAT
G. ALAMATIP
H. KEAMANAN

DEFINISI & KOLOM PENCOCOKAN

1. Layanan SOCKS5 tanpa enkripsi yang menyembunyikan IP.
2. Tingkat perlindungan keseluruhan sistem terenkripsi.
3. Jumlah perangkat bersamaan per akun.
4. Laju nyata server yang aktif.
5. Protokol open source modern yang cepat.
6. Alamat unik yang diberikan ke perangkat.
7. Pengaman yang memutus lalu lintas saat koneksi gagal.
8. Kebijakan teraudit bahwa sesi tidak disimpan.

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. UGEIWARDR
2. NKAEEATPC
3. PATALGON
4. MIPTAALA
5. CROSOSSIPKK
6. CSLITKIWHL
7. GANBAATTPKRAES
8. MEANKANA

Aktivitas Bonus: Berpikir Cepat

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

1	Kata yang menggambarkan aplikasi VPN yang baik			
2	Hal yang dapat disembunyikan IPVanish dari jaringan Anda			
3	Tempat Anda akan menyalakan IPVanish			
4	Protokol VPN yang Anda ketahui			
5	Pertanyaan untuk layanan pelanggan IPVanish			
6	Negara tempat Anda ingin server IPVanish			
7	Layanan VPN selain IPVanish			
8	Situasi saat kill switch membantu			
9	Alasan memilih IPVanish			
10	Tanda koneksi VPN Anda lambat			
11	Hal yang Anda lakukan online setiap hari			
12	Orang yang akan Anda sarankan memakai IPVanish			
13	Hal yang dicek sebelum membeli VPN			
14	Istilah keamanan yang Anda pelajari di lembar kerja ini			
15	Fitur yang Anda cari di IPVanish			

Pos 8: Studi Kasus VPN & Jaringan

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

STUDI KASUS 1: KONFIGURASI PUSAT MEDIA

👷

Skenario: Seorang klien ingin mengamankan pemutar media Android Fire TV dengan IPVanish agar streaming aman sambil tetap cepat.

Pertanyaan Diskusi: Mengapa WireGuard lebih dipilih daripada OpenVPN untuk perangkat streaming dengan sumber daya terbatas?

STUDI KASUS 2: PROKSI JARINGAN TORRENT

👷

Skenario: Seorang pengunggah P2P ingin menyembunyikan lokasinya tanpa beban enkripsi data penuh dengan konfigurasi SOCKS5.

Pertanyaan Diskusi: Bandingkan untung rugi keamanan dan kecepatan memakai proksi SOCKS5 dibanding terowongan VPN IPVanish penuh.

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

19	15	3	11	19		13	5	14	25	5	13	2	21	14	25	9	11	1	14

9	16		20	1	14	16	1		5	14	11	18	9	16	19	9

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: Protokol apa yang menjadi bawaan IPVanish?

Secara bawaan, lalu lintas dirutekan lewat WireGuard yang cepat.

Q2: Apakah IPVanish memiliki perangkat keras servernya?

Ya, IPVanish memiliki dan mengelola sebagian besar jaringan server fisiknya.

Q3: Di mana IPVanish berbasis?

IPVanish berbasis di Amerika Serikat dan tunduk pada hukum AS.

Q4: Berapa perangkat yang bisa terhubung bersamaan?

IPVanish menawarkan koneksi perangkat bersamaan tanpa batas per akun.

Q5: Apakah ada log koneksi yang disimpan?

Tidak, IPVanish menerapkan kebijakan tanpa log yang ketat dan divalidasi audit independen. [6]

Pos 10: FAQ Dasar VPN (Bagian B)

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

Q6: Apakah IPVanish menawarkan layanan proksi?

Ya, tersedia proksi SOCKS5 gratis untuk torrent.

Q7: Apakah ada kill switch?

Ada, kill switch tersedia di Windows, macOS, Android, dan iOS.

Q8: Bisakah menembus blokir wilayah dengan IPVanish?

Bisa, jaringan server globalnya memberi akses ke katalog yang dibatasi.

Q9: Apakah split tunneling didukung?

Ya, split tunneling tersedia, termasuk di Windows dan Android.

Q10: Sandi enkripsi apa yang dipakai?

Koneksi diamankan dengan enkripsi AES-256 dan ChaCha20.

Pos 10: FAQ Lanjutan VPN (Bagian C)

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

Q1: Bagaimana proksi SOCKS5 diatur?

Proksi diatur di klien torrent untuk menyembunyikan IP pengguna tanpa beban enkripsi.

Q2: Bagaimana kepemilikan server meningkatkan keamanan?

Hal ini mengurangi risiko menyewa server pihak ketiga dan memberi penyedia kendali langsung atas konfigurasi server.

Q3: Apa dampak yurisdiksi AS terhadap privasi?

Hukum AS tidak mewajibkan retensi data, tetapi memungkinkan surat keamanan nasional dan surat perintah.

Q4: Bagaimana kill switch mencegah kebocoran IP?

Kill switch memblokir semua adaptor internet jika koneksi VPN tiba-tiba terputus.

Q5: Enkripsi apa yang dipakai dengan WireGuard?

WireGuard memakai enkripsi kunci simetris ChaCha20 dan autentikasi Poly1305. [7]

Pos 10: FAQ Lanjutan VPN (Bagian D)

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

Q6: Bagaimana kebijakan tanpa log diverifikasi?

Leviathan Security Group mengauditnya pada 2022 dan Schellman pada 2025; tak ada log pengguna. [3]

Q7: Bagaimana kueri DNS IPv6 ditangani?

Semua kueri DNS dan IPv6 otomatis dirutekan lewat nameserver pribadinya.

Q8: Apakah IPVanish menawarkan fitur obfuskasi?

Ya, fitur Scramble menyamarkan lalu lintas OpenVPN untuk menembus firewall.

Q9: Bagaimana split tunneling bekerja di perangkat seluler?

Aplikasi pilihan dapat melewati terowongan VPN dan terhubung langsung.

Q10: Apakah konfigurasi router didukung?

Ya, konfigurasi OpenVPN dan WireGuard dapat dimuat manual ke router DD-WRT. [1]

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

IPVanish memiliki sebagian besar infrastruktur servernya alih-alih menyewa dari pihak ketiga. [3]

2. WAWASAN VPN

IPVanish beroperasi sejak 2012 dan dimiliki Ziff Davis, yang dulu bernama J2 Global. [2]

3. WAWASAN VPN

Proksi SOCKS5 menyembunyikan alamat IP publik klien tetapi tidak mengenkripsi paket data.

4. WAWASAN VPN

WireGuard adalah protokol bawaan, dengan OpenVPN dan IKEv2/IPSec juga tersedia di aplikasinya. [2]

5. WAWASAN VPN

OpenVPN Scramble standar menambahkan lapisan obfuskasi XOR pada header paket untuk menembus firewall.

6. WAWASAN VPN

Kebijakan koneksi bersamaan tanpa batas memungkinkan semua perangkat rumah tangga diamankan sekaligus. [2]

7. WAWASAN VPN

Audit oleh Leviathan Security Group (2022) dan Schellman (2025) memverifikasi klaim tanpa log. [3]

8. WAWASAN VPN

Aplikasi Android mendukung pengaturan VPN selalu aktif yang mencegah akses internet jika terowongan terputus.

9. WAWASAN VPN

Koneksi OpenVPN dapat memakai UDP demi kecepatan atau TCP demi perutean stabil melewati firewall.

10. WAWASAN VPN

Tersedia dukungan live chat 24/7, ditambah dukungan telepon pada jam kerja hari kerja. [5]

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[1] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 **WireGuard Bawaan** WIREGUARD Jawaban Benar: A

CATATAN PENGAJAR

WireGuard diatur sebagai bawaan untuk kecepatan perutean yang optimal.

2 **Proksi SOCKS5** PROKSI SOCKS5 Jawaban Benar: A

CATATAN PENGAJAR

Proksi SOCKS5 menyamarkan lokasi klien tanpa beban enkripsi.

3 **Soal 3** Jawaban Benar: A

CATATAN PENGAJAR

Leviathan Security Group melakukan audit tanpa log pertama IPVanish pada 2022; Schellman menyusul pada 2025. [3]

4 **Yurisdiksi AS** AMERIKA SERIKAT Jawaban Benar: A

CATATAN PENGAJAR

IPVanish berbasis di Amerika Serikat, di bawah aturan aliansi Five Eyes.

5 **Perangkat Tanpa Batas** TANPABATAS Jawaban Benar: A

CATATAN PENGAJAR

IPVanish mengizinkan koneksi perangkat bersamaan tanpa batas. [2]

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Perangkat Keras Server** JARINGAN SENDIRI — Jawaban Benar: Benar

CATATAN PENGAJAR

IPVanish memiliki dan mengelola sebagian besar jaringan server fisiknya.

7 **Soal 7** — Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: Proxy SOCKS5 menyamarkan alamat IP, tetapi tidak mengenkripsi data.

8 **Soal 8** — Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: IPVanish menyertakan kill switch di aplikasi desktop dan selulernya.

9 **Yurisdiksi AS** FIVE EYES AS — Jawaban Benar: Benar

CATATAN PENGAJAR

IPVanish berbasis di AS dan tunduk pada aturan pengawasan Five Eyes.

10 **Split Tunnel** RUTE TERPISAH — Jawaban Benar: Benar

CATATAN PENGAJAR

Split tunneling merutekan lalu lintas aplikasi tertentu di luar terowongan aman.

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. WireGuard	H 2. Proksi SOCKS5	D 3. Kecepatan Server	A 4. Kill Switch
G 5. Log Teraudit	C 6. Batas Perangkat	E 7. Alamat IP	F 8. Keamanan

POS 3: KUNCI ISTILAH KUNCI

1 WIREGUARD	2 PROKSI SOCKS5	3 KECEPATAN SERVER	4 KILL SWITCH
5 LOG TERAUDIT	6 BATAS PERANGKAT		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 B – PROKSISOCKS	2 H – KEAMANAN	3 F – BATASPERANGKAT	4 C – KECEPATAN
5 A – WIREGUARD	6 G – ALAMATIP	7 D – KILLSWITCH	8 E – TANPALOG

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan WireGuard, Proksi SOCKS5, dan Kecepatan Server dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

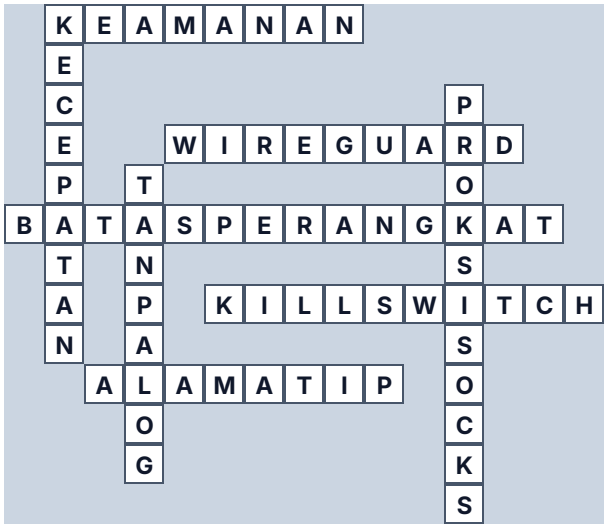
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: KEAMANAN Tingkat perlindungan keseluruhan sistem terenkripsi (8 huruf)

3 mendatar: WIREGUARD Protokol open source modern yang cepat (9 huruf)

5 mendatar: BATASPERANGKAT Jumlah perangkat bersamaan per akun (14 huruf)

6 mendatar: KILLSWITCH Pengaman yang memutus lalu lintas saat koneksi gagal (10 huruf)

7 mendatar: ALAMATIP Alamat unik yang diberikan ke perangkat (8 huruf)

PETUNJUK MENURUN

1 menurun: KECEPATAN Laju nyata server yang aktif (9 huruf)

2 menurun: PROKSISOCKS Layanan SOCKS5 tanpa enkripsi yang menyembunyikan IP (11 huruf)

4 menurun: TANPALOG Kebijakan teraudit bahwa sesi tidak disimpan (8 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. U G E I W A R D R — **WIREGUARD**
2. N K A E E A T P C — **KECEPATAN**
3. P A T A L G O N — **TANPALOG**
4. M I P T A A L A — **ALAMATIP**
5. C R O S O S S I P K K — **PROKSISOCKS**
6. C S L I T K I W H L — **KILLSWITCH**
7. G A N B A A T T P K R A E S — **BATASPERANGKAT**
8. M E A N K A N A — **KEAMANAN**

KUNCI TANTANGAN SANDI RAHASIA

"SOCKS MENYEMBUNYIKAN IP TANPA ENKRIPSI"

Kunci Jawaban Studi Kasus

A STUDI KASUS 1: KONFIGURASI PUSAT MEDIA

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang klien ingin mengamankan pemutar media Android Fire TV dengan IPVanish agar streaming aman sambil tetap cepat.
- Strategi & Solusi yang Disarankan: Panduan Penilaian: Jelaskan bahwa WireGuard berkode lebih ringkas, berjalan di ruang kernel, dan memakai lebih sedikit siklus CPU, sehingga kecepatan maksimal di perangkat ringan.

B STUDI KASUS 2: PROKSI JARINGAN TORRENT

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang pengunggah P2P ingin menyembunyikan lokasinya tanpa beban enkripsi data penuh dengan konfigurasi SOCKS5.
- Strategi & Solusi yang Disarankan: Panduan Penilaian: Catat bahwa SOCKS5 menyembunyikan alamat IP tanpa mengenkripsi lalu lintas, sehingga lebih cepat tetapi tanpa privasi terhadap inspeksi paket oleh ISP.