نام: _____ تاریخ: _____ نمبر: _____

IPVanish کا جائزہ

امریکہ میں قائم IPVanish VPN کا تکنیکی تجزیہ، بڑی حد تک اپنی ملکیت کے سرور

IPVANISH جائزے کا تعلیمی جائزہ

سیکھنے والا
طالب علم کی حیثیت
نیٹ ورک ڈیفینڈر ٹریک

محفوظ
کنکشن کی صورتحال
ڈیٹا پیکٹس کی حفاظت

فعال
لیک سے تحفظ
DNS اور IPv6 لیک سے تحفظ

خوش آمدید! یہ سرگرمی پیکٹ آپ کو IPVanish کے تکنیکی جائزے سے متعارف کراتا ہے۔ آپ اپنی ملکیت کے فزیکل انفراسٹرکچر، P2P ٹورنٹنگ کے لیے SOCKS5 پراکسیز، WireGuard کی کارکردگی، اور امریکی دائرہ اختیار کے ڈیٹا ضوابط کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- ☐ **حصہ 1-4: VPN اور نیٹ ورک سیکیورٹی کنفیگریشنز میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

VPN.com بہترین VPNs گائیڈ کھولیں

URL: https://www.vpn.com/vpn/ipvanish/

آپ کا IPVanish لرننگ روڈ میپ

- IPVanish جائزے کے تکنیکی فن تعمیر اور خفیہ کاری کے معیارات کا تجزیہ کریں۔
- IP، DNS اور WebRTC ٹریفک لیکس کو روکنے کے لیے کلائنٹ کی سیٹنگز ترتیب دیں۔
- ملکیتی ٹنلنگ پروٹوکولز کا معیاری نفاذ سے موازنہ کریں۔

IPVANISH کے جائزے کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو SOCKS5 پراکسیز اور اپنی ملکیتی سرور انفراسٹرکچر پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

ذاتی ملکیتی انفراسٹرکچر اور SOCKS5 P2P پروکسیز (تعارف)

IPVanish اپنے فزیکل سرور نیٹ ورک کے ایک بڑے حصے کا مالک ہونے اور اس کا انتظام کرنے کی وجہ سے نمایاں ہے، جو کارکردگی اور سیکیورٹی بہتر بناتا ہے۔ یہ تیز رفتار WireGuard پروٹوکول اور P2P ٹورنٹنگ کے لیے SOCKS5 پراکسیز پیش کرتا ہے، لیکن امریکی Five Eyes دائرہ اختیار کے تحت کام کرتا ہے۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. IPVanish کلائنٹ ایپس میں تیز رفتار کے لیے کون سا اوپن سورس پروٹوکول ڈیفالٹ ہے؟

- A) WireGuard
- B) L2TP/IPSec
- C) PPTP
- D) Catapult Hydra

2. IPVanish P2P ٹورنٹنگ سیٹ اپ میں مدد کے لیے کس قسم کی سرور پراکسی فراہم کرتا ہے؟

- A) SOCKS5 پراکسی
- B) HTTP پراکسی
- C) Tor ریلے
- D) Shadowsocks

3. 2022 میں IPVanish کا پہلا آزاد نو لاگز آڈٹ کس فرم نے کیا؟

- A) Leviathan Security Group
- B) PwC
- C) Deloitte
- D) Cure53

4. IPVanish کے کارپوریٹ ادارے کس بنیادی قومی دائرہ اختیار کے تحت کام کرتے ہیں؟

- A) امریکہ
- B) سوئٹزرلینڈ
- C) پاناما
- D) برٹش ورجن آئی لینڈز

5. پریمیم IPVanish پلان کے تحت کتنے بیک وقت ڈیوائس کنکشنز کی اجازت ہے؟

- A) لامحدود
- B) پانچ
- C) دس
- D) سات

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. IPVanish اپنے فزیکل سرور انفراسٹرکچر کے ایک بڑے حصے کا انتظام کرتا ہے اور اس کا مالک ہے۔

درست غلط

7 سوال 7

7. SOCKS5 پروکسی ٹریفک معیاری VPN ٹنلز کی طرح ٹرانزٹ میں مکمل طور پر خفیہ ہوتا ہے۔

درست غلط

8 سوال 8

8. IPVanish ڈیسک ٹاپ کلائنٹ میں سسٹم کی سطح کی Kill Switch خصوصیت موجود نہیں ہے۔

درست غلط

9 سوال 9

9. IPVanish ریاستہائے متحدہ سے کام کرتا ہے، جو Five Eyes انٹیلیجنس کا رکن ہے۔

درست غلط

10 سوال 10

10. IPVanish میں اسپلٹ ٹنلنگ ایپ ٹریفک کو VPN ٹنل سے باہر روٹ کرنے کی اجازت دیتی ہے۔

درست غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. جدید _____ پروٹوکول بہتر روٹنگ کارکردگی کے لیے بطور ڈیفالٹ ترتیب دیا گیا ہے۔
2. P2P ٹریفک کو تیز _____ کے ذریعے بھیجا جا سکتا ہے تاکہ کلائنٹ کے اصل مقامات چھپائے جا سکیں۔
3. قریبی جغرافیائی نوڈ سے جڑنے سے سرور کی حقیقی _____ کی شرحیں زیادہ سے زیادہ ہوتی ہیں۔
4. ڈیٹا لیکس سے بچنے کے لیے صارفین کو بلٹ اِن _____ کنٹرولز ترتیب دینے چاہییں۔
5. آزادانہ سیکیورٹی آڈٹس نے فراہم کنندہ کے _____ عہد کی تصدیق کی ہے۔
6. کچھ حریفوں کے برعکس IPVanish اکاؤنٹس پر کوئی فعال _____ نہیں لگاتا۔

الفاظ کا بینک

ایڈریس ڈیوائس حد رفتار ساکس پراکسی سیکیورٹی کل سوئچ نو لاگز وائر گارڈ

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: VPN اور نیٹ ورک تصورات کا ملان

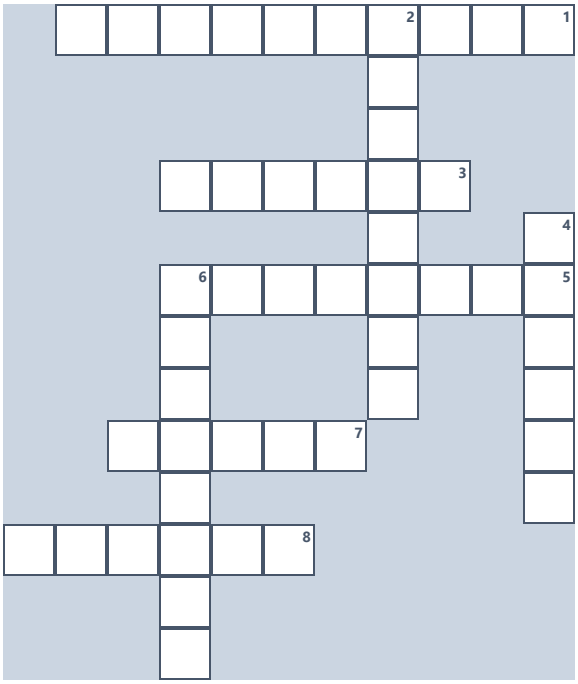
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. WireGuard		A — فیل سیف طریقہ کار جو VPN کے ناکام ہونے پر انٹرنیٹ ٹریفک بلاک کر دیتا ہے۔
2. SOCKS5 پروکسی		B — رفتار اور جدید کرپٹوگرافی کے لیے معروف اوپن سورس پروٹوکول۔
3. سرور اسپیڈ		C — فعال ڈیوائس سیشنز کی تعداد کو محدود کرنے والی پابندی۔
4. Kill Switch		D — فعال ٹریفک لوڈ کے تحت سرور نوڈ کی تھرو پٹ صلاحیت۔
5. آڈٹ شدہ لاگز		E — انٹرنیٹ پر ڈیوائسز کو تفویض کیا جانے والا منفرد نیٹ ورک شناخت کنندہ۔
6. ڈیوائس کی حد		F — انکرپٹڈ ٹنل سسٹم کا مجموعی تحفظی ڈھانچہ۔
7. IP ایڈریس		G — تصدیق شدہ ریکارڈز جو اس بات کی تصدیق کرتے ہیں کہ صارف کی کوئی سرگرمی ٹریک نہیں کی جاتی۔
8. سیکیورٹی		H — غیر خفیہ پراکسی روٹنگ سسٹم جو P2P کلائنٹ مقامات کو چھپانے کے لیے استعمال ہوتا ہے۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

1. غیر انکرپٹڈ پراکسی روٹنگ نظام جو P2P کلائنٹس کے مقامات چھپانے کے لیے استعمال ہوتا ہے (10)

3. انٹرنیٹ پر ڈیوائسز کو تفویض کیا جانے والا منفرد نیٹ ورک شناختی نمبر (6)

5. رفتار اور جدید کرپٹوگرافی کے لیے مشہور اوپن سورس پروٹوکول (8)

7. فعال ٹریفک لوڈ کے تحت سرور نوڈ کی تھرو پٹ کی صلاحیت (5)

8. ناکامی کی صورت میں وی پی این بند ہونے پر انٹرنیٹ ٹریفک روکنے کا حفاظتی میکانزم (6)

عمودی

2. انکرپٹڈ ٹنل سسٹم کی مجموعی حفاظتی کیفیت (8)

4. تصدیق شدہ ریکارڈ جو تصدیق کرتے ہیں کہ صارف کی کوئی سرگرمی ٹریک نہیں کی جاتی (6)

6. فعال سیشنز کی تعداد محدود کرنے والی پابندی (8)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

1 افقی: غیر انکرپٹڈ پراکسی روٹنگ نظام جو P2P کلائنٹس کے مقامات چھپانے کے لیے استعمال ہوتا ہے (10 حروف):

3 افقی: انٹرنیٹ پر ڈیوائسز کو تفویض کیا جانے والا منفرد نیٹ ورک شناختی نمبر (6 حروف):

5 افقی: رفتار اور جدید کرپٹوگرافی کے لیے مشہور اوپن سورس پروٹوکول (8 حروف):

7 افقی: فعال ٹریفک لوڈ کے تحت سرور نوڈ کی تھرو پٹ کی صلاحیت (5 حروف):

8 افقی: ناکامی کی صورت میں وی پی این بند ہونے پر انٹرنیٹ ٹریفک روکنے کا حفاظتی میکانزم (6 حروف):

عمودی

2 عمودی: انکرپٹڈ ٹنل سسٹم کی مجموعی حفاظتی کیفیت (8 حروف):

4 عمودی: تصدیق شدہ ریکارڈ جو تصدیق کرتے ہیں کہ صارف کی کوئی سرگرمی ٹریک نہیں کی جاتی (6 حروف):

6 عمودی: فعال سیشنز کی تعداد محدود کرنے والی پابندی (8 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ز	س	ش	ف	م	پ	ب	ا	ب	س	ش	ٹ	ی	ہ	ے
ن	ش	گ	گ	ک	ر	ت	س	گ	و	ت	ش	ے	ف	ش
ل	ن	ہ	پ	ل	چ	ی	ے	ہ	و	ن	گ	گ	چ	م
ی	ت	ڈ	ب	س	ہ	س	ی	ک	ی	و	ر	ٹ	ی	د
گ	ت	ح	د	و	ش	ج	ڈ	ح	س	پ	ئ	ح	ر	د
ل	ح	ا	ب	ئ	ے	پ	و	م	ا	ف	و	ت	ا	ح
ت	ر	چ	ج	چ	ت	ا	ل	ت	ک	ا	ش	ت	ت	س
ئ	و	ج	ی	ح	ئ	ہ	ر	ٹ	س	گ	ن	و	ف	ئ
ن	ف	ز	ے	ر	ن	گ	م	و	پ	ا	ا	ٹ	ر	ا
ف	ہ	ج	گ	ب	ز	گ	پ	ا	ر	ہ	ے	ہ	س	و
ر	چ	ا	ش	ا	ز	ز	ح	ی	ا	و	ا	ر	ڈ	ی
و	ر	ن	چ	م	ل	ی	ک	ڈ	ک	ک	س	و	گ	ڈ
ڈ	ز	ہ	ز	ب	ئ	و	ج	ر	س	ئ	ل	ا	ح	چ
ک	پ	ڈ	ل	ن	ل	س	ن	ی	ی	چ	ح	ک	چ	ب
ی	ئ	ل	ب	م	ئ	ش	ے	س	ڈ	م	ز	ج	ز	ح

الفاظ کی فہرست

وائرگارڈ
ساکسپراکسی
رفتار
کلسوئچ
نولاگز
ڈیوائسحد
ایڈریس
سیکیورٹی

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. وائرگارڈ
B. ساکسپراکسی
C. رفتار
D. کلسوئچ
E. نولاگز
F. ڈیوائسحد
G. ایڈریس
H. سیکیورٹی

تعریفیں اور ملان کے خانے	
1. غیر انکرپٹڈ پراکسی روٹنگ نظام جو P2P کلائنٹس کے مقامات چھپانے کے لیے استعمال ہوتا ہے۔	
2. انکرپٹڈ ٹنل سسٹم کی مجموعی حفاظتی کیفیت۔	
3. فعال سیشنز کی تعداد محدود کرنے والی پابندی۔	
4. فعال ٹریفک لوڈ کے تحت سرور نوڈ کی تھرو پٹ کی صلاحیت۔	
5. رفتار اور جدید کرپٹوگرافی کے لیے مشہور اوپن سورس پروٹوکول۔	
6. انٹرنیٹ پر ڈیوائسز کو تفویض کیا جانے والا منفرد نیٹ ورک شناختی نمبر۔	
7. ناکامی کی صورت میں وی پی این بند ہونے پر انٹرنیٹ ٹریفک روکنے کا حفاظتی میکانزم۔	
8. تصدیق شدہ ریکارڈ جو تصدیق کرتے ہیں کہ صارف کی کوئی سرگرمی ٹریک نہیں کی جاتی۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

ورچوئل پرائیویٹ نیٹ ورک (VPN) کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ررگ واا ڈئ
2. ررا ت ف
3. ن ل ا ز گ و
4. س ر ڈ ی ا ی
5. ک ر ی ا س ا پ س س ک
6. ئ و ک س چ ل
7. ڈ د ئ س ح ی ا و
8. ی ی و ی س ٹ ر ک

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	اچھی VPN ایپ کو بیان کرنے والے الفاظ			
2	وہ چیزیں جو IPVanish آپ کے نیٹ ورک سے چھپا سکتا ہے			
3	وہ مقامات جہاں آپ IPVanish آن کریں گے			
4	آپ کے جانے پہچانے VPN پروٹوکولز کے نام			
5	IPVanish کی کسٹمر سپورٹ سے پوچھنے کے سوالات			
6	وہ ممالک جہاں آپ IPVanish کے سرورز چاہیں گے			
7	IPVanish کے علاوہ دیگر VPN سروسز کے نام			
8	وہ حالات جن میں کل سوئچ مددگار ہوتا ہے			
9	IPVanish کو منتخب کرنے کی وجوہات			
10	VPN کنکشن کے سست ہونے کی علامات			
11	وہ کام جو آپ روزانہ آن لائن کرتے ہیں			
12	وہ لوگ جنہیں آپ IPVanish تجویز کریں گے			
13	VPN خریدنے سے پہلے جانچنے کی چیزیں			
14	اس ورک شیٹ میں سیکھے گئے سیکیورٹی کے الفاظ			
15	IPVanish میں وہ خصوصیات جن کی آپ تلاش کرتے ہیں			

چیک پوائنٹ 8: VPN اور نیٹ ورک کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: میڈیا سینٹر کی ترتیب

منظرنامہ: ایک کلائنٹ تیز تھروپٹ برقرار رکھتے ہوئے محفوظ اسٹریمنگ کے لیے IPVanish کے ذریعے اپنا Android Fire TV میڈیا پلیئر محفوظ بنانا چاہتا ہے۔

بحث کا سوال: محدود وسائل والے اسٹریمنگ ہارڈ ویئر کے لیے OpenVPN کے مقابلے میں WireGuard پروٹوکول کو ترجیح کیوں دی جاتی ہے؟

کیس اسٹڈی 2: ٹورینٹ نیٹ ورک پراکسیز

منظرنامہ: ایک P2P اپ لوڈر SOCKS5 کنفیگریشن کے ذریعے مکمل ڈیٹا خفیہ کاری کے اوور ہیڈ کے بغیر اپنی لوکیشن چھپانا چاہتا ہے۔

بحث کا سوال: SOCKS5 پراکسی اور مکمل IPVanish VPN ٹنل کے استعمال کے سیکیورٹی اور رفتار کے سمجھوتوں کا موازنہ کریں۔

چیک پوائنٹ 9: سائفر حل کریں

نیٹ ورک انجینئر روٹنگ چینلز اور کلائنٹ ٹنلز کو محفوظ بناتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

16	29	1	30		34	32		4	10	18		33	37	31		19	32	37	34

31	1	23	32

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: VPN عمومی سوالات – بنیادی (حصہ A)

ورچوئل پرائیویٹ نیٹ ورکس (VPNs) اور ٹنلنگ کے بارے میں سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q1: IPVanish میں ڈیفالٹ پروٹوکول کون سا ہے؟

یہ بطور ڈیفالٹ تیز رفتار WireGuard کے ذریعے روٹ کرتا ہے۔

Q2: کیا IPVanish اپنے سرور ہارڈ ویئر کا مالک ہے؟

ہاں، یہ اپنے فزیکل سرور نیٹ ورک کے ایک بڑے حصے کا مالک ہے اور اسے خود چلاتا ہے۔

Q3: IPVanish کہاں قائم ہے؟

اس کا مرکز ریاستہائے متحدہ میں ہے، جو امریکی قوانین کے تابع ہے۔

Q4: بیک وقت کتنے آلات جڑ سکتے ہیں؟

IPVanish فی اکاؤنٹ لامحدود بیک وقت ڈیوائس کنکشنز پیش کرتا ہے۔

Q5: کیا یہ کوئی کنکشن لاگز رکھتا ہے؟

نہیں، یہ سخت زیرو لاگز پالیسی نافذ کرتا ہے جس کی آزاد آڈٹس نے توثیق کی ہے۔ [6]

چیک پوائنٹ 10: VPN عمومی سوالات – بنیادی (حصہ B)

ورچوئل پرائیویٹ نیٹ ورکس (VPNs) اور ٹنلنگ کے بارے میں سب سے عام سوالات اور جوابات کا جائزہ لیں۔

Q6: کیا IPVanish پراکسی سروس پیش کرتا ہے؟

ہاں، یہ ٹورنٹنگ کے لیے مفت SOCKS5 پراکسی فراہم کرتا ہے۔

Q7: کیا اس میں کل سوئچ شامل ہے؟

جی ہاں، کِل سوئچ Windows، macOS، Android اور iOS پر دستیاب ہے۔

Q8: کیا میں IPVanish کے ساتھ جغرافیائی پابندیاں بائی پاس کر سکتا ہوں؟

ہاں، اس کے سرورز کا عالمی نیٹ ورک پابندی والی لائبریریوں تک رسائی دیتا ہے۔

Q9: کیا یہ اسپلٹ ٹنلنگ کو سپورٹ کرتا ہے؟

ہاں، اسپلٹ ٹنلنگ دستیاب ہے، بشمول Windows اور Android پر۔

Q10: یہ کون سے انکرپشن سائفرز استعمال کرتا ہے؟

یہ AES-256 اور ChaCha20 خفیہ کاری کے ذریعے کنکشنز کو محفوظ بناتا ہے۔

چیک پوائنٹ 10: VPN عمومی سوالات – اعلیٰ (حصہ C)

VPN ٹنلنگ پروٹوکولز، موبائل کلائنٹ انضمام اور انٹرپرائز تعیناتی کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: SOCKS5 پراکسی کیسے ترتیب دی جاتی ہے؟

اسے ٹورنٹ کلائنٹس میں صارف کا IP خفیہ کاری کے اوور ہیڈ کے بغیر چھپانے کے لیے ترتیب دیا جاتا ہے۔

Q2: سرور ہارڈ ویئر کا مالک ہونا سیکیورٹی کو کیسے بہتر بناتا ہے؟

یہ تیسرے فریق کے سرور کرائے پر لینے کے خطرات کم کرتا ہے اور فراہم کنندہ کو سرور کنفیگریشنز پر براہ راست کنٹرول دیتا ہے۔

Q3: امریکی دائرہ اختیار کے رازداری پر کیا اثرات ہیں؟

اگرچہ امریکی قوانین ڈیٹا برقرار رکھنے کا تقاضا نہیں کرتے، لیکن وہ قومی سلامتی کے خطوط اور وارنٹس کی اجازت دیتے ہیں۔

Q4: کل سوئچ IP لیکس کو کیسے روکتا ہے؟

اگر VPN کنکشن اچانک منقطع ہو جائے تو یہ تمام انٹرنیٹ اڈاپٹرز کو بلاک کر دیتا ہے۔

Q5: WireGuard کے ساتھ کون سی خفیہ کاری استعمال ہوتی ہے؟

WireGuard ChaCha20 سڈمیٹرک کی خفیہ کاری اور Poly1305 تصدیق استعمال کرتا ہے۔ [7]

چیک پوائنٹ 10: VPN عمومی سوالات – اعلیٰ (حصہ D)

VPN ٹنلنگ پروٹوکولز، موبائل کلائنٹ انضمام اور انٹرپرائز تعیناتی کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: زیرو لاگز پالیسی کی توثیق کیسے کی جاتی ہے؟

Leviathan Security Group نے 2022 میں اور Schellman نے 2025 میں اس کا آڈٹ کیا؛ کسی کو بھی صارفین کے لاگز نہیں ملے۔ [3]

Q7: یہ IPv6 DNS کوئریز کو کیسے سنبھالتا ہے؟

یہ تمام DNS اور IPv6 کوئریز کو خود بخود اپنے نجی نیم سرورز سے گزارتا ہے۔

Q8: کیا IPVanish اوبفسکیشن فیچرز پیش کرتا ہے؟

ہاں، اس کا Scramble فیچر فائر والز کو بائی پاس کرنے کے لیے OpenVPN ٹریفک کو obfuscate کرتا ہے۔

Q9: موبائل آلات پر اسپلٹ ٹنلنگ کیسے کام کرتی ہے؟

یہ منتخب ایپس کو VPN ٹنل بائی پاس کر کے براہ راست جڑنے کی اجازت دیتا ہے۔

Q10: کیا یہ راؤٹر کنفیگریشنز کو سپورٹ کرتا ہے؟

جی ہاں، OpenVPN اور WireGuard کنفیگریشنز کو DD-WRT راؤٹرز پر دستی طور پر لوڈ کیا جا سکتا ہے۔ [1]

حصہ 11: 10 حقیقی دنیا کے VPN حقائق اور بصیرتیں

VPN خفیہ کاری کی رفتار، پروٹوکول آڈٹس، موبائل کنیکٹیویٹی اور انٹرپرائز ریموٹ ورک کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. VPN بصیرت

IPVanish اپنے زیادہ تر سرور انفراسٹرکچر کا مالک ہے، اسے تیسرے فریقوں سے کرائے پر نہیں لیتا۔ [3]

2. VPN بصیرت

IPVanish 2012 سے کام کر رہا ہے اور اس کی مالک Ziff Davis ہے، جو پہلے J2 Global کے نام سے جانی جاتی تھی۔ [2]

3. VPN بصیرت

SOCKS5 پراکسی کلائنٹ کے عوامی IP ایڈریس کو چھپاتی ہے لیکن ڈیٹا پیکٹس کو خفیہ نہیں کرتی۔

4. VPN بصیرت

WireGuard ڈیفالٹ پروٹوکول ہے، جبکہ ایپس میں OpenVPN اور IKEv2/IPSec بھی دستیاب ہیں۔ [2]

5. VPN بصیرت

معیاری OpenVPN Scramble فائر والز کو بائی پاس کرنے کے لیے پیکٹ ہیڈرز میں XOR obfuscation کی ایک تہہ شامل کرتا ہے۔

6. VPN بصیرت

لامحدود بیک وقت کنکشنز کی پالیسی صارفین کو اپنے گھر کی تمام ڈیوائسز کو بیک وقت محفوظ بنانے کی اجازت دیتی ہے۔ [2]

7. VPN کی بصیرت

Leviathan Security Group (2022) اور Schellman (2025) کے آڈٹس نے اس کے نو لاگز دعووں کی تصدیق کی۔ [3]

8. VPN کی بصیرت

Android ایپ ہمیشہ آن VPN سیٹنگز کو سپورٹ کرتی ہے جو ٹنل منقطع ہونے پر انٹرنیٹ تک رسائی روک دیتی ہیں۔

9. VPN کی بصیرت

OpenVPN کنکشن رفتار کے لیے UDP یا فائر والز کے ذریعے مستحکم روٹنگ کے لیے TCP استعمال کر سکتے ہیں۔

10. VPN بصیرت

یہ 24/7 لائیو چیٹ سپورٹ پیش کرتا ہے، اور ہفتے کے مقررہ کاروباری اوقات میں فون سپورٹ بھی۔ [5]

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی تکنیکی معیارات، تصریحات اور ریگولیٹری فریم ورکس سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 **WireGuard ڈیفالٹ** WIREGUARD درست جواب: A

تدریسی نوٹ

WireGuard بطور ڈیفالٹ بہتر راؤٹنگ رفتار کے لیے ترتیب دیا گیا ہے۔ حوالہ: IPVanish Features۔

2 **SOCKS5 پروکسی** SOCKS5 پروکسی درست جواب: A

تدریسی نوٹ

SOCKS5 پروکسیز خفیہ کاری کے بوجھ کے بغیر کلائنٹ کے مقامات چھپاتی ہیں۔ حوالہ: IPVanish Support۔

3 **سوال 3** درست جواب: A

تدریسی نوٹ

Leviathan Security Group نے 2022 میں IPVanish کا پہلا نو لاگز آڈٹ کیا؛ 2025 میں Schellman نے اس کے بعد آڈٹ کیا۔ [3]

4 **امریکی دائرہ اختیار** ریاستہائے متحدہ درست جواب: A

تدریسی نوٹ

IPVanish کا مرکز ریاستہائے متحدہ میں ہے، جو Five Eyes اتحاد کے اصولوں کے تحت ہے۔ حوالہ: IPVanish Review۔

5 **لامحدود ڈیوائسز** لامحدود درست جواب: A

تدریسی نوٹ

IPVanish لامحدود بیک وقت ڈیوائس کنکشنز کی اجازت دیتا ہے۔ حوالہ: IPVanish Support۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سرور ہارڈ ویئر — نیٹ ورک کا مالک — درست جواب: درست

تدریسی نوٹ

IPVanish اپنے فزیکل سرور نیٹ ورک کے ایک بڑے حصے کا مالک ہے اور اس کا انتظام کرتا ہے۔ حوالہ: IPVanish Support۔

7 سوال 7 — درست جواب: غلط

تدریسی نوٹ

غلط: SOCKS5 پراکسی آپ کے IP ایڈریس کو چھپاتی ہے لیکن ڈیٹا کو خفیہ نہیں کرتی۔

8 سوال 8 — درست جواب: غلط

تدریسی نوٹ

غلط: IPVanish اپنی ڈیسک ٹاپ اور موبائل ایپس میں کل سوئچ شامل کرتا ہے۔

9 امریکی دائرہ اختیار — Five Eyes امریکہ — درست جواب: درست

تدریسی نوٹ

IPVanish کا مرکز امریکہ میں ہے، جو Five Eyes کی نگرانی کے اصولوں کے تابع ہے۔ حوالہ: IPVanish Review۔

10 اسپلٹ ٹنل — اسپلٹ روٹ — درست جواب: درست

تدریسی نوٹ

اسپلٹ ٹنلنگ مخصوص ایپ ٹریفک کو محفوظ ٹنل سے باہر روٹ کرتی ہے۔ حوالہ: IPVanish Support۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

B .1 WireGuard	H .2 SOCKS5 پروکسی	D .3 سرور اسپیڈ	A .4 Kill Switch
G .5 آڈٹ شدہ لاگز	C .6 ڈیوائس کی حد	E .7 IP ایڈریس	F .8 سیکیورٹی

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 وائر گارڈ	2 ساکس پراکسی	3 رفتار	4 کل سوئچ
5 نو لاگز	6 ڈیوائس حد		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 B – ساکسپراکسی	2 H – سیکیورٹی	3 F – ڈیوائسحد	4 C – رفتار
5 A – وائرگارڈ	6 G – ایڈریس	7 D – کلسوئچ	8 E – نولاگز

اساتذہ کے لیے بحث کے نوٹس

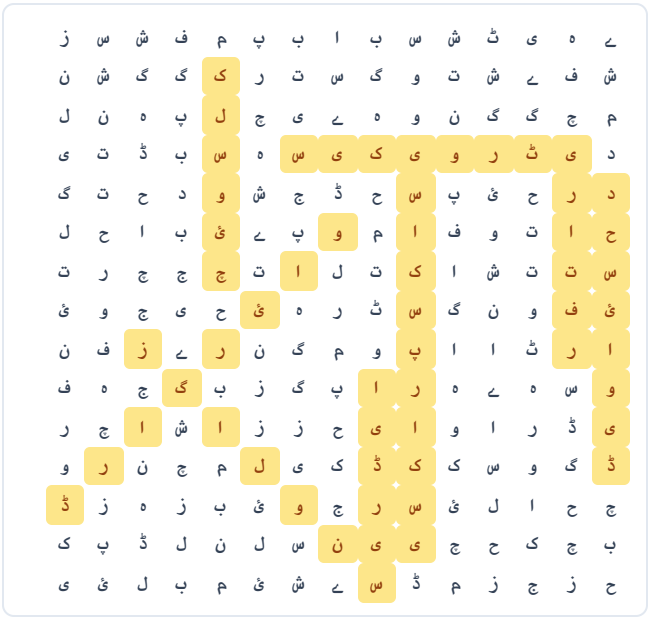
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ WireGuard، SOCKS5 پروکسی اور سرور اسپیڈ کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

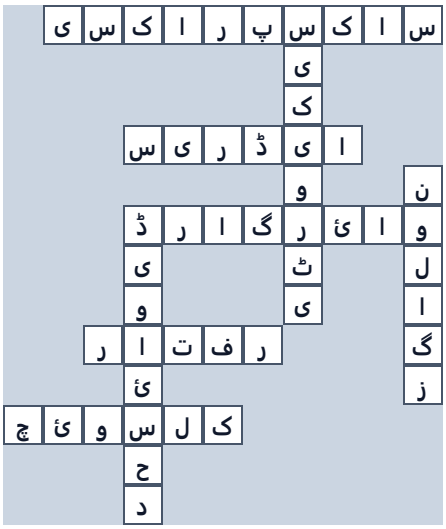
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل



کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

1 افقی: ساکسپراکسی غیر انکرپٹڈ پراکسی روٹنگ نظام جو P2P کلائنٹس کے مقامات چھپانے کے لیے استعمال ہوتا ہے (10 حروف)

3 افقی: ایڈریس انٹرنیٹ پر ڈیوائسز کو تفویض کیا جانے والا منفرد نیٹ ورک شناختی نمبر (6 حروف)

5 افقی: وائرگارڈ رفتار اور جدید کرپٹوگرافی کے لیے مشہور اوپن سورس پروٹوکول (8 حروف)

7 افقی: رفتار فعال ٹریفک لوڈ کے تحت سرور نوڈ کی تھرو پٹ کی صلاحیت (5 حروف)

8 افقی: کلسوئچ ناکامی کی صورت میں وی پی این بند ہونے پر انٹرنیٹ ٹریفک روکنے کا حفاظتی میکانزم (6 حروف)

عمودی

2 عمودی: سیکیورٹی انکرپٹڈ ٹنل سسٹم کی مجموعی حفاظتی کیفیت (8 حروف)

4 عمودی: نولاگز تصدیق شدہ ریکارڈ جو تصدیق کرتے ہیں کہ صارف کی کوئی سرگرمی ٹریک نہیں کی جاتی (6 حروف)

6 عمودی: ڈیوائسحد فعال سیشنز کی تعداد محدود کرنے والی پابندی (8 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. ررگوااڈئ — وائرگارڈ
2. رراتف — رفتار
3. نلازگو — نولاگز
4. سرڈیای — ایڈریس
5. کریاساپسسک — ساکسپراکسی
6. ئوکسچل — کلسوئچ
7. ڈدئسحیاو — ڈیوائسحد
8. ییویسٹرک — سیکیورٹی

خفیہ سائفر چیلنج کی کلید

"وینش میں سخت نو لاگز نظام"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: میڈیا سینٹر کی ترتیب

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک کلائنٹ تیز تھروپٹ برقرار رکھتے ہوئے محفوظ اسٹریمنگ کے لیے IPVanish کے ذریعے اپنے Android Fire TV میڈیا پلیئر کو محفوظ بنانا چاہتا ہے۔
- تجویز کردہ حکمت عملی اور حل: درجہ بندی کی ہدایت: وضاحت کریں کہ WireGuard کا کوڈ چھوٹا ہے، یہ کرنل اسپیس میں کام کرتا ہے اور کم CPU سائیکل استعمال کرتا ہے، جس سے ہلکے ہارڈ ویئر پر رفتار زیادہ سے زیادہ ہو جاتی ہے۔

B کیس اسٹڈی 2: ٹورینٹ نیٹ ورک پراکسیز

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک P2P اپ لوڈر SOCKS5 کنفیگریشن کے ذریعے ڈیٹا کی مکمل خفیہ کاری کے بوجھ کے بغیر اپنا مقام چھپانا چاہتا ہے۔
- تجویز کردہ حکمت عملی اور حل: درجہ بندی کی ہدایت: نوٹ کریں کہ SOCKS5 ٹریفک کو خفیہ کیے بغیر IP ایڈریس چھپاتا ہے، جس سے رفتار تیز ملتی ہے لیکن ISP کے پیکٹ معائنے کے خلاف رازداری بالکل نہیں ملتی۔