نام: _____ تاریخ: _____ نمره: _____

بررسی IPVanish

تحلیل فنی IPVanish VPN مستقر در آمریکا، سرور عمدتاً متعلق به خود شرکت

نمای کلی یادگیری بررسی IPVANISH

یادگیرنده
وضعیت دانشجویی
مسیر مدافع شبکه

امن
وضعیت اتصال
محافظت از بسته‌های داده

فعال
محافظت در برابر نشت
محافظت در برابر نشت DNS و IPv6

خوش آمدید! این بستهٔ فعالیت شما را در بررسی فنی IPVanish راهنمایی می‌کند. با زیرساخت فیزیکی متعلق به خود، پروکسی‌های SOCKS5 برای تورنت P2P، عملکرد WireGuard و مقررات داده تحت صلاحیت قضایی آمریکا آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: بر پیکربندی‌های VPN و امنیت شبکه مسلط شوید.**
- ☐ **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- ☐ **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- ☐ **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- ☐ **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- ☐ **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای بهترین VPNهای VPN.com

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

نقشهٔ راه یادگیری IPVanish شما

- معماری فنی و استانداردهای رمزگذاری در بررسی IPVanish را تحلیل کنید.
- تنظیمات کلاینت را برای جلوگیری از نشت ترافیک IP، DNS و WebRTC پیکربندی کنید.
- پروتکل‌های تونل‌زنی اختصاصی را با پیاده‌سازی‌های استاندارد مقایسه کنید.

راهنمای بررسی IPVANISH

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره پروکسی‌های SOCKS5 و زیرساخت سرور شخصی به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

زیرساخت متعلق به خود و پروکسی‌های P2P SOCKS5 (مقدمه)

IPVanish با مالکیت و مدیریت بخش بزرگی از شبکهٔ سرور فیزیکی خود متمایز است که عملکرد و امنیت را بهبود می‌دهد. این سرویس پروتکل پرسرعت WireGuard و پروکسی‌های SOCKS5 را برای تورنت P2P ارائه می‌دهد، اما تحت صلاحیت Five Eyes ایالات متحده فعالیت می‌کند.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. در برنامه‌های کلاینت **IPVanish** کدام پروتکل متن‌باز برای سرعت بالا پیش‌فرض است؟

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

2 2. **IPVanish** برای کمک به راه‌اندازی تورنت **P2P** چه نوع پراکسی سروری ارائه می‌دهد؟

- A) پراکسی SOCKS5
- B) پروکسی HTTP
- C) رلهٔ Tor
- D) Shadowsocks

3 3. کدام شرکت اولین ممیزی مستقل بدون‌ثبت گزارش **IPVanish** را در سال **2022** انجام داد؟

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

4 4. نهادهای شرکتی **IPVanish** تحت کدام صلاحیت ملی اصلی فعالیت می‌کنند؟

- A) ایالات متحده
- B) سوئیس
- C) پاناما
- D) جزایر ویرجین بریتانیا

5 5. در یک طرح ممتاز **IPVanish** چند اتصال هم‌زمان دستگاه مجاز است؟

- A) نامحدود
- B) پنج
- C) ده
- D) هفت

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. IPVanish بخش بزرگی از زیرساخت سرور فیزیکی خود را مدیریت می‌کند و مالک آن است.

درست ○ نادرست ○

7 پرسش 7

7. ترافیک پروکسی SOCKS5 در حین انتقال دقیقاً مانند تونل‌های استاندارد VPN کاملاً رمزگذاری می‌شود.

درست ○ نادرست ○

8 پرسش 8

8. کلاینت دسکتاپ IPVanish فاقد ویژگی Kill Switch در سطح سیستم است.

درست ○ نادرست ○

9 پرسش 9

9. IPVanish از ایالات متحده، عضو اطلاعاتی Five Eyes، فعالیت می‌کند.

درست ○ نادرست ○

10 پرسش 10

10. Split tunneling در IPVanish اجازه می‌دهد ترافیک برنامه‌ها بیرون از تونل VPN مسیریابی شود.

درست ○ نادرست ○

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. پروتکل مدرن _____ به‌طور پیش‌فرض برای عملکرد مسیریابی بهینه پیکربندی شده است.
2. ترافیک P2P را می‌توان از طریق یک _____ سریع هدایت کرد تا مکان واقعی کلاینت پنهان شود.
3. اتصال به یک گرهٔ جغرافیایی نزدیک، نرخ‌های واقعی _____ را به حداکثر می‌رساند.
4. برای جلوگیری از نشت داده، کاربران باید کنترل‌های داخلی _____ را پیکربندی کنند.
5. حسابرسی‌های امنیتی مستقل، تعهد ارائه‌دهنده به سیاست _____ را تأیید کرده‌اند.
6. بر خلاف برخی رقبا، IPVanish هیچ _____ فعالی بر حساب‌ها اعمال نمی‌کند.

بانک واژگان

آی‌پی　امنیت　بدون لاگ ممیزی‌شده　پروکسی SOCKS5　سرعت سرور　قطع اضطراری
محدودیت تعداد دستگاه　WireGuard

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم VPN و شبکه

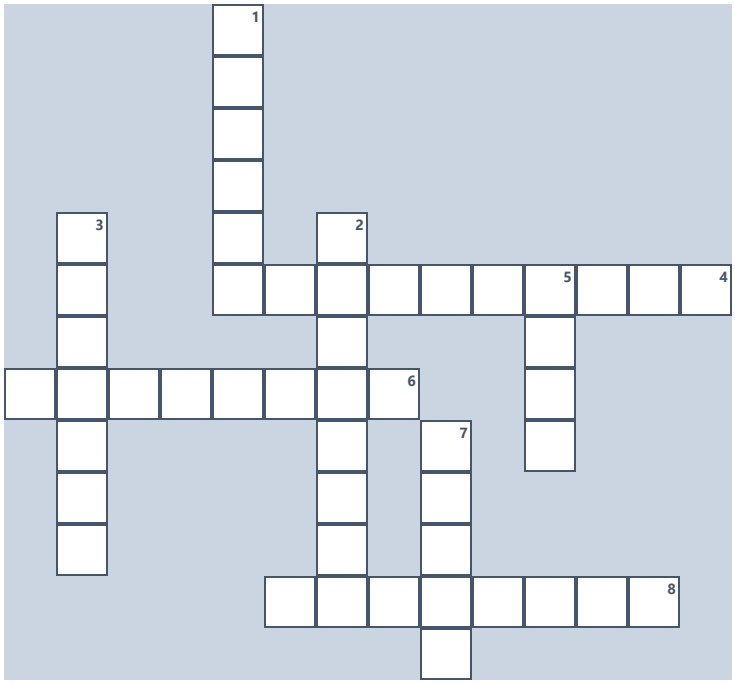
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. WireGuard	A	سازوکار ایمن‌شکست که اگر VPN از کار بیفتد، ترافیک اینترنت را مسدود می‌کند.
2. پروکسی SOCKS5	B	پروتکل متن‌باز شناخته‌شده برای سرعت و رمزنگاری مدرن.
3. سرعت سرور	C	محدودیتی که تعداد نشست‌های فعال دستگاه را محدود می‌کند.
4. Kill Switch	D	ظرفیت توان عملیاتی یک گره سرور تحت بار فعال ترافیک.
5. لاگ‌های ممیزی‌شده	E	شناسهٔ شبکهٔ یکتایی که به دستگاه‌های روی اینترنت اختصاص داده می‌شود.
6. محدودیت دستگاه	F	وضعیت کلی حفاظت از سامانهٔ تونل رمزگذاری‌شده.
7. آدرس IP	G	رکوردهای تأییدشده‌ای که تأیید می‌کنند هیچ فعالیت کاربری ردیابی نمی‌شود.
8. امنیت	H	سامانهٔ مسیریابی پراکسی رمزگذاری‌نشده که برای پنهان کردن مکان کلاینت‌های P2P به کار می‌رود.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

4. سازوکار ایمنی که اگر VPN از کار بیفتد، ترافیک اینترنت را مسدود می‌کند (10)

6. ظرفیت گذردهی یک گرهٔ سرور تحت بار ترافیک فعال (8)

8. سوابق راستی‌آزمایی‌شده که تأیید می‌کنند هیچ فعالیت کاربری ردیابی نمی‌شود (8)

عمودی

1. سامانهٔ مسیریابی بدون رمزگذاری که برای پنهان کردن مکان کلاینت‌های P2P به کار می‌رود (6)

2. پروتکل متن‌باز مشهور به سرعت و رمزنگاری مدرن (8)

3. قیدی برای تعداد نشست‌های فعال دستگاه (7)

5. شناسهٔ شبکه‌ای یکتا که به دستگاه‌ها در اینترنت اختصاص می‌یابد (4)

7. وضعیت کلی حفاظت از سامانهٔ تونل رمزگذاری‌شده (5)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

4 افقی: سازوکار ایمنی که اگر VPN از کار بیفتد، ترافیک اینترنت را مسدود می‌کند (10 حرف):

6 افقی: ظرفیت گذردهی یک گرهٔ سرور تحت بار ترافیک فعال (8 حرف):

8 افقی: سوابق راستی‌آزمایی‌شده که تأیید می‌کنند هیچ فعالیت کاربری ردیابی نمی‌شود (8 حرف):

عمودی

1 عمودی: سامانهٔ مسیریابی بدون رمزگذاری که برای پنهان کردن مکان کلاینت‌های P2P به کار می‌رود (6 حرف):

2 عمودی: پروتکل متن‌باز مشهور به سرعت و رمزنگاری مدرن (8 حرف):

3 عمودی: قیدی برای تعداد نشست‌های فعال دستگاه (7 حرف):

5 عمودی: شناسهٔ شبکه‌ای یکتا که به دستگاه‌ها در اینترنت اختصاص می‌یابد (4 حرف):

7 عمودی: وضعیت کلی حفاظت از سامانهٔ تونل رمزگذاری‌شده (5 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ک	ن	ژ	و	ز	ژ	و	ط	پ	ب	ا	پ	ر	ژ	چ
ش	خ	ظ	ع	م	ژ	ص	ص	ذ	ث	ر	ش	ع	ث	ز
پ	ف	د	ض	ح	ظ	ف	پ	خ	ک	ک	ف	غ	ع	ش
ت	گ	ه	ق	د	ث	م	م	ی	ز	ی	ش	د	ه	م
ن	ع	ث	ص	و	ث	ی	خ	ز	ق	ح	م	ی	ت	ر
ا	ژ	ث	ض	د	ی	ا	و	ب	ط	گ	پ	ظ	ی	و
ش	ع	غ	ث	ی	ذ	ا	خ	چ	ع	ث	ض	ث	ن	ر
ا	چ	ل	ع	ت	ی	چ	ق	ی	ا	ف	ذ	چ	م	س
ک	غ	ز	ع	ر	و	ک	ظ	ص	ض	ط	ع	ا	ا	ت
ا	ر	م	گ	ن	ف	ح	پ	پ	ط	ه	ص	ت	ف	ع
ز	غ	ا	ا	ش	ذ	ح	ژ	ر	ر	ه	ه	ی	غ	ر
ا	ر	ی	خ	ی	ع	ظ	خ	و	ا	ط	ق	س	س	س
د	س	خ	ب	ه	پ	ف	ه	ک	ر	پ	گ	ح	ل	ض
ح	ه	ی	س	پ	ن	ی	ص	س	ی	ظ	ض	ز	خ	ی
ل	خ	س	ک	ل	ض	ب	ظ	ی	گ	ژ	گ	م	ط	و

فهرست واژگان

وایرگارد
پروکسی
سرعتسرور
قطعاضطراری
ممیزیشده
محدودیت
اپیی
امنیت

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان
A. وایرگارد
B. پروکسی
C. سرعتسرور
D. قطعاضطراری
E. ممیزیشده
F. محدودیت
G. ایپی
H. امنیت

	تعاریف و فیلدهای تطبیق
	1. سامانهٔ مسیریابی بدون رمزگذاری که برای پنهان کردن مکان کلاینت‌های P2P به کار می‌رود.
	2. وضعیت کلی حفاظت از سامانهٔ تونل رمزگذاری‌شده.
	3. قیدی برای تعداد نشست‌های فعال دستگاه.
	4. ظرفیت گذردهی یک گرهٔ سرور تحت بار ترافیک فعال.
	5. پروتکل متن‌باز مشهور به سرعت و رمزنگاری مدرن.
	6. شناسهٔ شبکه‌ای یکتا که به دستگاه‌ها در اینترنت اختصاص می‌یابد.
	7. سازوکار ایمنی که اگر VPN از کار بیفتد، ترافیک اینترنت را مسدود می‌کند.
	8. سوابق راستی‌آزمایی‌شده که تأیید می‌کنند هیچ فعالیت کاربری ردیابی نمی‌شود.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی شبکه خصوصی مجازی (VPN) آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ر ر گ و ا ا د ی
2. ت س ر ر و ر س ع
3. ز م م ی ش ه د ی
4. ی پ ا ی
5. ک و ی پ س ر
6. ر ض ا ر ا ق ط ط ی ع
7. م ی د ت ح و د
8. ت ا ن ی م

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	واژه‌هایی که یک برنامهٔ VPN خوب را توصیف می‌کنند		
2	چیزهایی که IPVanish می‌تواند از شبکهٔ شما پنهان کند		
3	جاهایی که IPVanish را روشن می‌کنید		
4	پروتکل‌های VPN که می‌شناسید		
5	پرسش‌هایی برای پشتیبانی مشتریان IPVanish		
6	کشورهایی که سرورهای IPVanish را در آن‌ها می‌خواهید		
7	سرویس‌های VPN غیر از IPVanish		
8	موقعیت‌هایی که Kill Switch کمک می‌کند		
9	دلایل انتخاب IPVanish		
10	نشانه‌های کند بودن اتصال VPN شما		
11	کارهایی که هر روز آنلاین انجام می‌دهید		
12	افرادی که IPVanish را به آن‌ها پیشنهاد می‌دهید		
13	چیزهایی که پیش از خرید VPN باید بررسی کنید		
14	واژه‌های امنیتی که در این کاربرگ یاد گرفتید		
15	ویژگی‌هایی که در IPVanish دنبال می‌کنید		

ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: پیکربندی مرکز رسانه

👷

سناریو: مشتری می‌خواهد پخش‌کنندهٔ رسانهٔ Android Fire TV خود را با IPVanish ایمن کند تا ضمن حفظ توان عملیاتی سریع، به‌طور ایمن استریم کند.

پرسش برای بحث: چرا پروتکل WireGuard برای سخت‌افزار استریم با منابع محدود به OpenVPN ترجیح داده می‌شود؟

مطالعهٔ موردی 2: پراکسی‌های شبکهٔ تورنت

👷

سناریو: یک آپلودکنندهٔ P2P می‌خواهد با پیکربندی SOCKS5 موقعیت خود را بدون سربار رمزگذاری کامل داده پنهان کند.

پرسش برای بحث: مصالحه‌های امنیت و سرعت استفاده از پراکسی SOCKS5 را در برابر یک تونل کامل IPVanish VPN مقایسه کنید.

ایستگاه بررسی 9: رمزگشایی

مهندس شبکه کانال‌های مسیریابی و تونل‌های کلاینت را ایمن می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

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

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

29	30	10	2		4	15	1	32	15		16	32	29	30	32	3	32	1	

10	12	1	10		26	1	27

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش A)

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q1: پروتکل پیش‌فرض در IPVanish کدام است؟

به‌طور پیش‌فرض از طریق WireGuard پرسرعت مسیریابی می‌کند.

Q2: آیا IPVanish مالک سخت‌افزار سرور خود است؟

بله، بخش بزرگی از شبکهٔ سرورهای فیزیکی خود را در مالکیت و مدیریت دارد.

Q3: IPVanish در کجا مستقر است؟

در ایالات متحده مستقر است و مشمول قوانین ایالات متحده است.

Q4: چند دستگاه می‌توانند هم‌زمان وصل شوند؟

IPVanish اتصال‌های هم‌زمان نامحدود دستگاه را برای هر حساب ارائه می‌دهد.

Q5: آیا هیچ لاگ اتصالی نگه می‌دارد؟

خیر، سیاست سخت‌گیرانهٔ عدم ثبت لاگ را اعمال می‌کند که ممیزی‌های مستقل تأیید کرده‌اند. [6]

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش B)

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q6: آیا IPVanish سرویس پراکسی ارائه می‌دهد؟

بله، یک پروکسی SOCKS5 رایگان برای تورنت فراهم می‌کند.

Q7: آیا کیل‌سوییچ دارد؟

بله، کیل سوئیچ در ویندوز، macOS، اندروید و iOS در دسترس است.

Q8: آیا می‌توانم با IPVanish محدودیت‌های جغرافیایی را دور بزنم؟

بله، شبکهٔ جهانی سرورهای آن امکان دسترسی به کتابخانه‌های محدودشده را فراهم می‌کند.

Q9: آیا از تونل‌بندی تفکیکی پشتیبانی می‌کند؟

بله، تونل تقسیمی در دسترس است، از جمله روی Windows و Android.

Q10: از چه رمزهای رمزگذاری استفاده می‌کند؟

اتصال‌ها را با رمزگذاری AES-256 و ChaCha20 ایمن می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q1: پروکسی SOCKS5 چگونه پیکربندی می‌شود؟

در کلاینت‌های تورنت تنظیم می‌شود تا IP کاربر را بدون سربار رمزگذاری پنهان کند.

Q2: مالکیت سخت‌افزار سرور چگونه امنیت را بهبود می‌دهد؟

خطرهای اجارهٔ سرور از شخص ثالث را کاهش می‌دهد و به ارائه‌دهنده کنترل مستقیم بر پیکربندی سرورها می‌دهد.

Q3: پیامدهای حریم خصوصی حوزهٔ قضایی ایالات متحده چیست؟

اگرچه قوانین آمریکا نگهداری داده را الزامی نمی‌کنند، اما اجازهٔ نامه‌های امنیت ملی و احکام قضایی را می‌دهند.

Q4: کیل‌سوییچ چگونه از نشت IP جلوگیری می‌کند؟

اگر اتصال VPN به‌طور ناگهانی قطع شود، همهٔ آداپتورهای اینترنت را مسدود می‌کند.

Q5: با WireGuard از چه رمزگذاری‌ای استفاده می‌شود؟

WireGuard از رمزگذاری کلید متقارن ChaCha20 و احراز هویت Poly1305 استفاده می‌کند. [7]

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q6: سیاست بدون‌لاگ چگونه راستی‌آزمایی می‌شود؟

Leviathan Security Group آن را در 2022 و Schellman در 2025 ممیزی کردند؛ هیچ‌کدام لاگ کاربران نیافتند. [3]

Q7: پرس‌وجوهای DNS مبتنی بر IPv6 را چگونه مدیریت می‌کند؟

به‌طور خودکار همهٔ درخواست‌های DNS و IPv6 را از طریق نام‌سرورهای خصوصی خود مسیریابی می‌کند.

Q8: آیا IPVanish ویژگی‌های مبهم‌سازی ارائه می‌دهد؟

بله، قابلیت Scramble آن ترافیک OpenVPN را مبهم‌سازی می‌کند تا از دیوار آتش عبور کند.

Q9: تونل‌بندی تفکیکی در دستگاه‌های موبایل چگونه کار می‌کند؟

به برنامه‌های انتخاب‌شده اجازه می‌دهد تونل VPN را دور بزنند و مستقیماً متصل شوند.

Q10: آیا از پیکربندی روتر پشتیبانی می‌کند؟

بله، پیکربندی‌های OpenVPN و WireGuard را می‌توان به‌صورت دستی روی روترهای DD-WRT بارگذاری کرد. [1]

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ VPN

واقعیت‌های دنیای واقعی دربارهٔ سرعت رمزگذاری VPN، ممیزی پروتکل‌ها، اتصال موبایل و کار راه‌دور سازمانی را مرور کنید.

1. بینش VPN

IPVanish مالک بیشتر زیرساخت سرور خود است و آن را از اشخاص ثالث اجاره نمی‌کند. [3]

2. بینش VPN

IPVanish از سال 2012 فعالیت می‌کند و متعلق به Ziff Davis، با نام قبلی J2 Global، است. [2]

3. بینش VPN

پروکسی SOCKS5 نشانی IP عمومی کلاینت را پنهان می‌کند اما بسته‌های داده را رمزگذاری نمی‌کند.

4. بینش VPN

WireGuard پروتکل پیش‌فرض است و OpenVPN و IKEv2/IPSec نیز در برنامه‌ها در دسترس‌اند. [2]

5. بینش VPN

OpenVPN Scramble استاندارد یک لایهٔ مبهم‌سازی XOR به سرایند بسته‌ها اضافه می‌کند تا دیوارهای آتش را دور بزند.

6. بینش VPN

سیاست اتصال همزمان نامحدود به کاربران اجازه می‌دهد همهٔ دستگاه‌های خانه را همزمان ایمن کنند. [2]

7. بینش VPN

ممیزی‌های Leviathan Security Group (2022) و Schellman (2025) ادعاهای بدون ثبت لاگ آن را تأیید کرده‌اند. [3]

8. بینش VPN

برنامهٔ اندروید از تنظیمات VPN همیشه‌روشن پشتیبانی می‌کند که در صورت قطع تونل، دسترسی به اینترنت را مسدود می‌کند.

9. بینش VPN

اتصال‌های OpenVPN می‌توانند از UDP برای سرعت یا از TCP برای مسیریابی پایدار از میان دیوارهای آتش استفاده کنند.

10. بینش VPN

پشتیبانی چت زندهٔ 24/7 و همچنین پشتیبانی تلفنی در ساعات کاری مشخص روزهای هفته ارائه می‌دهد. [5]

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردها، مشخصات فنی و چارچوب‌های مقرراتی جهانی گردآوری شده‌اند.

منابع علمی و صنعتی

[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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پیش‌فرض WireGuard — WIREGUARD — پاسخ درست: A

نکتهٔ آموزشی

WireGuard به‌طور پیش‌فرض برای سرعت‌های بهینهٔ مسیریابی پیکربندی شده است. استناد: IPVanish Features.

2 پروکسی SOCKS5 — پروکسی SOCKS5 — پاسخ درست: A

نکتهٔ آموزشی

پروکسی‌های SOCKS5 موقعیت کلاینت‌ها را بدون بار رمزگذاری پنهان می‌کنند. منبع: IPVanish Support.

3 پرسش 3 — پاسخ درست: A

نکتهٔ آموزشی

Leviathan Security Group اولین ممیزی بدون‌ثبت گزارش IPVanish را در سال 2022 انجام داد؛ Schellman در سال 2025 دنبال کرد. [3]

4 صلاحیت قضایی آمریکا — ایالات متحده — پاسخ درست: A

نکتهٔ آموزشی

IPVanish در ایالات متحده و تحت قواعد ائتلاف Five Eyes مستقر است. منبع: IPVanish Review.

5 دستگاه‌های نامحدود — نامحدود — پاسخ درست: A

نکتهٔ آموزشی

IPVanish اتصال‌های هم‌زمان نامحدود دستگاه را مجاز می‌کند. منبع: IPVanish Support.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 سخت‌افزار سرور — OWNS NETWORK — پاسخ درست: درست

نکتهٔ آموزشی

IPVanish مالک و مدیر بخش بزرگی از شبکهٔ سرور فیزیکی خود است. منبع: IPVanish Support.

7 پرسش 7 — پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: پراکسی SOCKS5 نشانی IP شما را پنهان می‌کند اما داده‌ها را رمزگذاری نمی‌کند.

8 پرسش 8 — پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: IPVanish در برنامه‌های دسکتاپ و موبایل خود Kill Switch دارد.

9 صلاحیت قضایی آمریکا — پنج‌چشم آمریکا — پاسخ درست: درست

نکتهٔ آموزشی

IPVanish در ایالات متحده مستقر است و مشمول قواعد نظارتی Five Eyes است. منبع: IPVanish Review.

10 Split Tunnel — مسیر تقسیمی — پاسخ درست: درست

نکتهٔ آموزشی

Split tunneling ترافیک برنامه‌های مشخص را بیرون از تونل امن مسیریابی می‌کند. منبع: IPVanish Support.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

B .1 WireGuard	H .2 پروکسی SOCKS5	D .3 سرعت سرور	A .4 Kill Switch
G .5 لاگ‌های ممیزی‌شده	C .6 محدودیت دستگاه	E .7 آدرس IP	F .8 امنیت

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 WireGuard	2 پروکسی SOCKS5	3 سرعت سرور	4 قطع اضطراری
5 بدون لاگ ممیزی‌شده	6 محدودیت تعداد دستگاه		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 B – پروکسی	2 H – امنیت	3 F – محدودیت	4 C – سرعتسرور
5 A – وایرگارد	6 G – اپپی	7 D – قطعاضطراری	8 E – ممیزیشده

یادداشت‌های بحث برای مدرسان

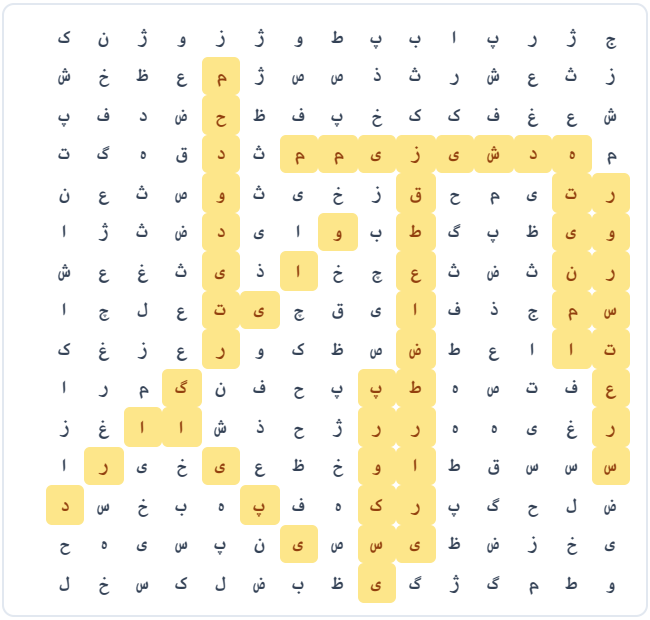
اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند WireGuard، پروکسی SOCKS5 و سرعت سرور را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

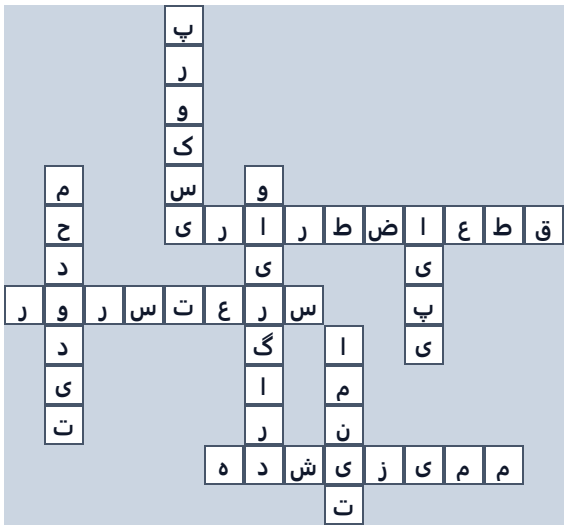
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات



پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

4 افقی: قطعاضطراری سازوکار ایمنی که اگر VPN از کار بیفتد، ترافیک اینترنت را مسدود می‌کند (10 حرف)

6 افقی: سرعتسرور ظرفیت گذردهی یک گرهٔ سرور تحت بار ترافیک فعال (8 حرف)

8 افقی: ممیزیشده سوابق راستی‌آزمایی‌شده که تأیید می‌کنند هیچ فعالیت کاربری ردیابی نمی‌شود (8 حرف)

عمودی

1 عمودی: پروکسی سامانهٔ مسیریابی بدون رمزگذاری که برای پنهان کردن مکان کلاینت‌های P2P به کار می‌رود (6 حرف)

2 عمودی: وایرگارد پروتکل متن‌باز مشهور به سرعت و رمزنگاری مدرن (8 حرف)

3 عمودی: محدودیت قیدی برای تعداد نشست‌های فعال دستگاه (7 حرف)

5 عمودی: اپپی شناسهٔ شبکه‌ای یکتا که به دستگاه‌ها در اینترنت اختصاص می‌یابد (4 حرف)

7 عمودی: امنیت وضعیت کلی حفاظت از سامانهٔ تونل رمزگذاری‌شده (5 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. رگواادی — وایرگارد
2. تسررورسع — سرعتسرور
3. زممیشهدی — ممیزیشده
4. پیای — اپیی
5. کوپسر — پروکسی
6. رضاراقطعطیع — قطعاضطراری
7. میدتحود — محدودیت
8. تانیم — امنیت

کلید چالش رمز مخفی

"آیپیونیش سیاست بدون لاگ دارد"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: پیکربندی مرکز رسانه

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک مشتری می‌خواهد پخش‌کنندهٔ رسانهٔ Android Fire TV خود را با IPVanish ایمن کند تا ضمن حفظ توان عملیاتی بالا با امنیت پخش کند.
- راهبرد و راه‌حل پیشنهادی: راهنمای نمره‌دهی: توضیح دهید که WireGuard کد کوچک‌تری دارد، در فضای هسته اجرا می‌شود و از چرخه‌های CPU کمتری استفاده می‌کند و سرعت را روی سخت‌افزار سبک به حداکثر می‌رساند.

B مطالعهٔ موردی 2: پراکسی‌های شبکهٔ تورنت

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک بارگذارندهٔ P2P می‌خواهد با پیکربندی SOCKS5، بدون بار رمزگذاری کامل داده، موقعیت خود را پنهان کند.
- راهبرد و راه‌حل پیشنهادی: راهنمای نمره‌دهی: توجه کنید که SOCKS5 نشانی IP را بدون رمزگذاری ترافیک پنهان می‌کند؛ سرعت بیشتری می‌دهد اما در برابر بازرسی بستهٔ ISP هیچ حریم خصوصی ندارد.