نام: _____ تاریخ: _____ نمره: _____

چگونه یک VPN انتخاب کنیم
کاربرگ

ارزیابی ارائه‌دهندگان VPN، استانداردهای امنیتی، حسابرسی‌ها و سیاست‌های ثبت گزارش

مرور یادگیری VPN

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 آشنایی با اصول بنیادین شبکه‌های خصوصی مجازی (VPN) راهنمایی می‌کند. می‌آموزید تونل‌های رمزگذاری‌شده چگونه از داده‌های شما محافظت می‌کنند، پروتکل‌های شبکه چگونه کار می‌کنند و چگونه می‌توان نشت‌های حریم خصوصی را شناسایی و کاهش داد.

ایستگاه‌های بررسی کاربرگ

- [ ] **بخش 1-4: بر مفاهیم و پروتکل‌های VPN 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 VPN در VPN.com

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

نقشهٔ راه یادگیری VPN شما

- قلمرو قضایی ارائه‌دهنده و سیاست‌های بدون ثبت گزارش را برای حریم خصوصی ارزیابی کنید.
- پروتکل‌های تونل‌زنی مانند WireGuard و OpenVPN را از نظر سرعت مقایسه کنید.
- ویژگی‌های امنیتی مانند Kill Switch و گره‌های سرور فقط-RAM را تحلیل کنید.
- هنگام انتخاب، ممیزی‌های امنیتی مستقل و طرح‌های قیمت‌گذاری را شناسایی کنید.
- موقعیت‌های سرور را بر اساس نیاز خود به سرعت و رفع مسدودیت جغرافیایی انتخاب کنید.

دستورالعمل کاربرگ انتخاب

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 انتخاب زیرساخت امن VPN به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

انتخاب VPN (مقدمه)

انتخاب VPN مناسب مستلزم نگاه کردن فراتر از تبلیغات است. یک ارائه‌دهندهٔ قابل اعتماد باید سیاست صفر لاگ اثبات‌شده، پروتکل‌های رمزگذاری امن و کلاینت‌های متن‌باز داشته باشد. با ارزیابی ویژگی‌های امنیتی، صلاحیت‌های قضایی و عملکرد سرعت می‌توانید VPN ای را انتخاب کنید که با نیازهای حفاظت دیجیتال شما سازگار است.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. عامل کلیدی هنگام انتخاب ارائه‌دهندهٔ VPN امن چیست؟

- A. تعداد کشورهای سرور
- B. سیاست بدون ثبت لاگ که به‌طور مستقل ممیزی شده است
- C. پایین‌ترین سطح قیمت ماهانه
- D. حمایت‌های مالی تبلیغاتی پرزرق‌وبرق

2 2. کدام پروتکل VPN بهترین توازن بین سرعت و قابلیت ممیزی را ارائه می‌دهد؟

- A. PPTP (قدیمی)
- B. L2TP/IPSec
- C. فقط OpenVPN روی TCP
- D. WireGuard

3 3. چرا کاربران باید برای فعالیت‌های حساس از VPNهای رایگان اجتناب کنند؟

- A. در ایالات متحده ممنوع‌اند
- B. اغلب تاریخچهٔ مرور وب شما را می‌فروشند
- C. از مرور پایهٔ وب پشتیبانی نمی‌کنند
- D. برای اتصال به سخت‌افزار ویژه نیاز دارند

4 4. صلاحیت قضایی کشور مبدأ یک ارائه‌دهنده چه چیزی را تعیین می‌کند؟

- A. سرعت اتصال سرور
- B. انواع دستگاه‌های پشتیبانی‌شده
- C. قوانین محلی حاکم بر نگهداری داده‌ها و حکم‌های بازرسی
- D. طرح بصری برنامهٔ کلاینت

5 5. هدف اصلی قابلیت «کیل سوئیچ» کلاینت VPN چیست؟

- A. برای مسدود کردن دسترسی به اینترنت در صورت قطع اتصال VPN
- B. حذف همهٔ برنامه‌های نصب‌شده روی دستگاه
- C. برای دو برابر کردن سرعت اتصال سرور
- D. برای راه‌اندازی مجدد سیستم‌عامل هنگام بیکاری

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. VPN از دستگاه شما در برابر دانلود بدافزار و فایل‌های ویروسی محافظت می‌کند.

درست نادرست

7 پرسش 7

7. ممیزی‌های مستقل شرکت‌هایی مانند Deloitte ادعاهای بدون ثبت را تأیید می‌کنند.

درست نادرست

8 پرسش 8

8. قوانین کشور مبدأ ارائه‌دهنده بر حریم خصوصی داده‌های کاربر تأثیری ندارد.

درست نادرست

9 پرسش 9

9. کدبیس فشردهٔ WireGuard نسبت به OpenVPN آسان‌تر ممیزی می‌شود.

درست نادرست

10 پرسش 10

10. VPNهای رایگان اغلب برای پوشش هزینهٔ سرورها تبلیغات می‌فروشند یا کاربران را ردیابی می‌کنند.

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. سیاست _____ که مستقل راستی‌آزمایی شده باشد، ارائه‌دهندهٔ VPN را متعهد می‌کند تاریخچهٔ آنلاین شما را ثبت نکند.
2. پروتکل مدرن _____ سرعت بالایی دارد و از کدبیس بسیار کوچکی استفاده می‌کند.
3. ویژگی ایمنی به نام _____ اگر اتصال VPN ناگهان قطع شود، همهٔ ترافیک را متوقف می‌کند.
4. بررسی _____ ارائه‌دهنده تعیین می‌کند که آیا او مشمول معاهدات نظارتی است یا نه.
5. ایمن‌سازی سرورها با دیسک‌های _____ کمک می‌کند داده‌های کاربر پس از راه‌اندازی مجدد باقی نماند.
6. راستی‌آزمایی سیاست ادعای zero-knowledge نیازمند یک _____ امنیتی از شرکت‌های معتبر است.

بانک واژگان

بدون لاگ　پنج چشم　حوزهٔ قضایی　رایگان　فقط رم　قطع اضطراری　ممیزی　WireGuard

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم شبکه

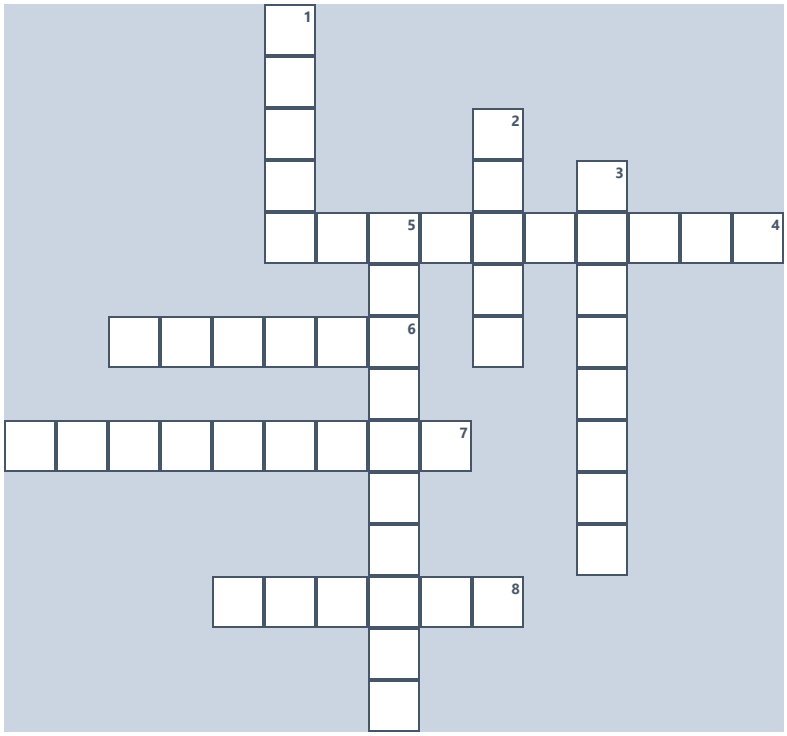
تطبیق تعاریف

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	سرویس اتصال پرخطر که اغلب با ثبت و فروش داده‌های مرور درآمدزایی می‌کند.
2. لاگ‌های ممیزی‌شده	B	سازوکار ایمنی که در صورت قطع تونل امن، مسیریابی اینترنت را مسدود می‌کند.
3. صلاحیت قضایی	C	ائتلاف بین‌المللی اشتراک اطلاعات بین ایالات متحده، بریتانیا، کانادا، استرالیا و نیوزیلند.
4. کلیدقطع‌کن	D	زیرساخت سخت‌افزاری که روی حافظهٔ فرار اجرا می‌شود، بنابراین داده‌ها روی دیسک ذخیره نمی‌شوند.
5. Five Eyes	E	منطقهٔ جغرافیایی که تعهدات قانونی ارائه‌دهندهٔ VPN را تعیین می‌کند.
6. VPN رایگان	F	پروتکل نوین و سریع که از حدود 4,000 خط کد بسیار قابل‌ممیزی استفاده می‌کند.
7. سرورهای فقط-RAM	G	پروتکل متن‌باز بالغ و به‌طور گسترده ممیزی‌شده با پایگاه کدی بسیار بزرگ‌تر از WireGuard.
8. OpenVPN	H	ادعای حریم خصوصی که شرکت‌های مستقل امنیت سایبری شخص ثالث آن را تأیید کرده‌اند.

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 تونل امن قطع شود، مسیریابی اینترنت را مسدود می‌کند (10)

6. ائتلاف بین‌المللی تبادل اطلاعات اطلاعاتی میان آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند (6)

7. قلمرو جغرافیایی که تعهدات قانونی ارائه‌دهندهٔ VPN را تعیین می‌کند (9)

8. سرویس اتصال پرخطری که اغلب با ثبت و فروش داده‌های مرور کسب درآمد می‌کند (6)

عمودی

1. ادعای حریم خصوصی که شرکت‌های مستقل امنیت سایبری راستی‌آزمایی کرده‌اند (5)

2. زیرساخت سخت‌افزاری که کاملاً روی حافظهٔ فرار اجرا می‌شود و از ذخیرهٔ داده جلوگیری می‌کند (5)

3. پروتکل مدرن و سریع با حدود 4,000 خط کد که بازبینی آن بسیار آسان است (8)

5. پروتکل متن‌باز بالغ و بارها ممیزی‌شده با کدبیسی بسیار بزرگ‌تر از WireGuard (10)

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 تونل امن قطع شود، مسیریابی اینترنت را مسدود می‌کند (10 حرف):

6 افقی: ائتلاف بین‌المللی تبادل اطلاعات اطلاعاتی میان آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند (6 حرف):

7 افقی: قلمرو جغرافیایی که تعهدات قانونی ارائه‌دهندهٔ VPN را تعیین می‌کند (9 حرف):

8 افقی: سرویس اتصال پرخطری که اغلب با ثبت و فروش داده‌های مرور کسب درآمد می‌کند (6 حرف):

عمودی

1 عمودی: ادعای حریم خصوصی که شرکت‌های مستقل امنیت سایبری راستی‌آزمایی کرده‌اند (5 حرف):

2 عمودی: زیرساخت سخت‌افزاری که کاملاً روی حافظهٔ فرار اجرا می‌شود و از ذخیرهٔ داده جلوگیری می‌کند (5 حرف):

3 عمودی: پروتکل مدرن و سریع با حدود 4,000 خط کد که بازبینی آن بسیار آسان است (8 حرف):

5 عمودی: پروتکل متن‌باز بالغ و بارها ممیزی‌شده با کدبیسی بسیار بزرگ‌تر از WireGuard (10 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.

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

فهرست واژگان

وایرگارد ممیزی حوزهقضایی قطعاضطراری پنجچشم رایگان فقطرم اوپنوپیپان

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	تعاریف و فیلدهای تطبیق
A. وایرگارد	1. ائتلاف بین‌المللی تبادل اطلاعات اطلاعاتی میان آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند.
B. ممیزی	2. پروتکل مدرن و سریع با حدود 4,000 خط کد که بازبینی آن بسیار آسان است.
C. حوزهقضایی	3. پروتکل متن‌باز بالغ و بارها ممیزی‌شده با کدبیسی بسیار بزرگ‌تر از WireGuard.
D. قطعاضطراری	4. سرویس اتصال پرخطری که اغلب با ثبت و فروش داده‌های مرور کسب درآمد می‌کند.
E. پنجچشم	5. سازوکار ایمنی که اگر تونل امن قطع شود، مسیریابی اینترنت را مسدود می‌کند.
F. رایگان	6. زیرساخت سخت‌افزاری که کاملاً روی حافظهٔ فرار اجرا می‌شود و از ذخیرهٔ داده جلوگیری می‌کند.
G. فقطرم	7. قلمرو جغرافیایی که تعهدات قانونی ارائه‌دهندهٔ VPN را تعیین می‌کند.
H. اوپنوپیان	8. ادعای حریم خصوصی که شرکت‌های مستقل امنیت سایبری راستی‌آزمایی کرده‌اند.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی VPN آشکار شوند. پاسخ‌هایتان را در کادرهای پرشدنی بنویسید.

1. ر ر گ و ا ا د ی _____
2. ی ح ی ه و ض ا ق ز _____
3. پ ج چ م ش ن _____
4. ط م ر ف ق _____
5. ی ی م ز م _____
6. ر ض ا ر ا ق ط ط ی ع _____
7. ا ر گ ن ی ا _____
8. ا ن ی ن ا و و پ ی پ _____

فعالیت تکمیلی: سریع فکر کن

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

1	چیزهایی که یک VPN می‌تواند پنهان کند		
2	چیزهایی که مهم‌تر از قیمت هستند		
3	جاهایی که می‌توان نقد و بررسی VPN را خواند		
4	چیزهایی که VPN نمی‌تواند از آن‌ها محافظتتان کند		
5	پرسش‌هایی برای تیم فروش VPN		
6	چیزهایی که ارائه‌دهندهٔ اینترنت شما می‌تواند ببیند		
7	موارد فهرست بررسی شما هنگام انتخاب VPN		
8	جاهایی که از VPN استفاده می‌کنید		
9	نشانه‌های هشدار در یک ارائه‌دهندهٔ VPN		
10	واژه‌های مرتبط با حریم خصوصی		
11	چیزهایی که ابتدا آزمایش می‌کنید		
12	وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد		
13	دلایل استفاده از VPN در سفر		
14	دستگاه‌هایی که می‌توانند از VPN استفاده کنند		
15	افسانه‌ها دربارهٔ VPNها		

ایستگاه بررسی 8: مطالعات موردی VPN

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

سارا (دانشجوی کافه)

👩‍💻 «سلام! من در Coffee & Bytes نشسته‌ام. یک شبکهٔ عمومی ناامن به نام 'Free_Wi-Fi_No_Password' وجود دارد. می‌خواهم وارد ایمیل مدرسه‌ام شوم و تکلیفم را آپلود کنم، اما نگران هکرها هستم. استفاده از این شبکه بدون VPN چه خطرهایی دارد و VPN چگونه از داده‌های من محافظت می‌کند؟»

Alex (دانشجوی مسافر)

👨‍💻 «وای نه! برای یک پروژه به خارج از کشور سفر کرده‌ام و می‌خواهم یک مستند زیست‌شناسی را که روی سروری در کشور خودم میزبانی می‌شود تماشا کنم. اما سایت پیام 'This video is not available in your current location.' را نشان می‌دهد. چرا مسدود شده‌ام و VPN چگونه می‌تواند به تماشای آن کمک کند؟»

ایستگاه بررسی 9: رمزگشایی

برای تکمیل آموزش راهنمای انتخاب، این پیام پنهان دربارهٔ انتخاب زیرساخت امن 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	28	1	31	29	1	28	1	15	1	2	1	12	16	12	1	13	26		

10	32	6	29	15	2

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 پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q1: VPN چیست و چگونه کار می‌کند؟

شبکهٔ خصوصی مجازی (VPN) اتصال اینترنت شما را رمزگذاری می‌کند و ترافیک شما را از طریق یک سرور راه‌دور امن عبور می‌دهد. این کار IP عمومی شما را پنهان می‌کند و آنچه ناظران شبکهٔ محلی و ISP شما دربارهٔ ترافیک عبوری از تونل VPN می‌بینند را محدود می‌کند.

Q2: چرا باید از VPN استفاده کنم؟

VPN از حریم خصوصی دیجیتال شما محافظت می‌کند، اتصال شما را در شبکه‌های Wi-Fi عمومی (مانند کافه‌ها یا فرودگاه‌ها) ایمن می‌کند، ممکن است وقتی ISP نوع ترافیک رمزگذاری‌شده را شناسایی نکند، کاهش سرعت مبتنی بر فعالیت را کم کند، محدودیت‌های جغرافیایی را دور می‌زند تا به محتوای جهانی دسترسی پیدا کنید، و به ایمن‌سازی منابع کار از راه دور کمک می‌کند.

Q3: آیا VPN مرا در فضای آنلاین کاملاً ناشناس می‌کند؟

خیر. هرچند VPN نشانی IP شما را پنهان و ترافیک را رمزگذاری می‌کند، همچنان می‌توانید از طریق کوکی‌های مرورگر، حساب‌های فعال (مانند Google یا Facebook)، انگشت‌نگاری مرورگر، یا اگر ارائه‌دهندهٔ VPN شما داده‌هایتان را ثبت کند، ردیابی شوید.

Q4: آیا VPN سرعت اینترنت من را کاهش می‌دهد؟

بله، اندکی. فرایند رمزگذاری و فاصلهٔ فیزیکی تا سرور VPN تأخیر و سربار اضافه می‌کنند. این تأثیر بسته به ارائه‌دهنده، پروتکل، فاصلهٔ سرور، دستگاه و شرایط شبکه متفاوت است.

Q5: چگونه کسب درآمد می‌کند؟

مدل کسب‌وکار را بررسی کنید. اشتراک‌ها، سطوح فریمیوم و فروش داده همگی بر میزان اعتماد به یک VPN اثر می‌گذارند و سرویسی که هرگز داده‌های شما را جمع‌آوری نمی‌کند نمی‌تواند آن را بفروشد. ابتدا سیاست حریم خصوصی را بخوانید. [1]

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

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q6: آیا می‌توانم از VPN رایگان استفاده کنم؟

VPNهای رایگان ممکن است به تبلیغات، ویژگی‌های محدود، تحلیل‌های استفاده، سقف داده یا مدل‌های درآمدزایی دیگر متکی باشند. کاربران باید پیش از استفاده سیاست حریم خصوصی، مالکیت، ممیزی‌ها و مدل کسب‌وکار ارائه‌دهنده را بررسی کنند.

Q7: سیاست «بدون‌لاگ» چیست؟

سیاست بدون ثبت گزارش مشخص می‌کند ارائه‌دهنده می‌گوید کدام داده‌های فعالیت و اتصال را نگه نمی‌دارد. دامنهٔ دقیق آن متفاوت است، بنابراین خوانندگان باید سیاست و یافته‌های ممیزی مستقل را بررسی کنند.

Q8: چگونه بهترین VPN را انتخاب کنم؟

به دنبال سیاست‌های عدم ثبت لاگِ ممیزی‌شده، پروتکل‌های قوی (WireGuard، OpenVPN)، مکان‌های امن سرور، سرعت بالا، سرورهای فقطRAM، قابلیت kill switch و صلاحیت قضایی خارج از اتحادهای تبادل اطلاعات اطلاعاتی (مانند 5/9/14 چشم) باشید.

Q9: آیا می‌توانم VPN را روی گوشی و تلویزیون هوشمند خود استفاده کنم؟

بله. ارائه‌دهندگان مدرن VPN برنامه‌های اختصاصی برای Linux، Windows، macOS، Android، iOS و تلویزیون‌های هوشمند و همچنین راه‌اندازی روی روتر برای محافظت از همهٔ دستگاه‌های شبکهٔ خانگی شما ارائه می‌دهند.

Q10: کلید قطع (Kill Switch) چیست؟

Kill Switch قابلیتی امنیتی است که اگر اتصال VPN قطع شود، دستگاه شما را به‌طور خودکار از اینترنت جدا می‌کند. این کار از نشت داده‌های رمزگذاری‌نشده یا IP واقعی شما جلوگیری می‌کند.

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

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q1: تفاوت OpenVPN، WireGuard و IKEv2 چیست؟

WireGuard یک پروتکل مدرن و سبک است (فقط حدود 4,000 خط کد) که سرعت بالا و زمان اتصال کوتاه ارائه می‌دهد. OpenVPN یک پروتکل متن‌باز بسیار امن و محک‌خورده است. IKEv2 به‌دلیل توانایی اتصال مجدد سریع هنگام تغییر شبکه برای دستگاه‌های موبایل عالی است.

Q2: مسیریابی دو VPN یا Multi-Hop چیست؟

روش چندجهشی ترافیک شما را به‌صورت متوالی از دو یا چند سرور VPN عبور می‌دهد. این کار لایهٔ رمزگذاری دوم اضافه می‌کند و اگر یک سرور آسیب ببیند، کمک می‌کند نشانی IP واقعی شما از جهش دوم پنهان بماند.

Q3: نشت WebRTC چیست و VPN چگونه از آن جلوگیری می‌کند؟

WebRTC یک پروتکل مرورگر است که حتی هنگام فعال بودن VPN می‌تواند نشانی‌های IP محلی و عمومی واقعی شما را فاش کند. VPNهای ممتاز درخواست‌های WebRTC را در برنامه‌های دسکتاپ/موبایل و افزونه‌های مرورگر خود مسدود یا جعل می‌کنند.

Q4: سرورهای فقطRAM چیستند و چرا اهمیت دارند؟

سرورهای سنتی داده را روی هارددیسک می‌نویسند که می‌تواند توقیف یا آسیب‌دیده شود. سرورهای فقط-RAM (بدون دیسک) کاملاً در حافظهٔ فرار (RAM) اجرا می‌شوند. وقتی سرور مجدداً راه‌اندازی یا خاموش شود، داده‌های موجود در حافظه پاک می‌شوند.

Q5: مبهم‌سازی چگونه مسدودسازی VPN را دور می‌زند؟

مبهم‌سازی (یا «Stealth VPN») بسته‌های ترافیک VPN را طوری پنهان می‌کند که شبیه ترافیک وب HTTPS معمولی (پورت 443) به نظر برسند. این کار به عبور از بازرسی عمیق بسته (DPI) کمک می‌کند که دولت‌ها یا شبکه‌های مدرسه و دفتر برای مسدود کردن VPN به کار می‌برند.

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

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q6: Split Tunneling چیست و چه زمانی باید از آن استفاده کنم؟

Split Tunneling به شما اجازه می‌دهد انتخاب کنید کدام برنامه‌ها از تونل رمزگذاری‌شدهٔ VPN عبور کنند و کدام مستقیماً به اینترنت وصل شوند. از آن استفاده کنید تا برنامه‌های بانکی حساس از VPN عبور کنند و بازی‌های محلی مستقیماً وصل شوند و تأخیر ناشی از VPN را نداشته باشند.

Q7: رازداری پیشرو (Perfect Forward Secrecy) چگونه کار می‌کند؟

PFS تضمین می‌کند که برای هر نشست یک کلید رمزگذاری منحصربه‌فرد و موقت تولید شود. حتی اگر کلید خصوصی در آینده فاش شود، نمی‌توان از آن برای رمزگشایی نشست‌های گذشته یا آینده استفاده کرد، زیرا آن‌ها از کلیدهای مستقل استفاده کرده‌اند.

Q8: ائتلاف‌های 5/9/14 Eyes چیستند و چرا باید برایم مهم باشند؟

صلاحیت قضایی می‌تواند بر فرایند حقوقی‌ای که یک ارائه‌دهنده ممکن است با آن روبه‌رو شود اثر بگذارد، اما خطر عملی برای حریم خصوصی به این هم بستگی دارد که ارائه‌دهنده چه داده‌هایی را نگه می‌دارد، معماری فنی، مالکیت، گزارش‌دهی شفافیت و سابقهٔ ممیزی آن چیست.

Q9: محافظت در برابر نشت DNS چیست؟

محافظت در برابر نشت DNS دستگاه شما را وادار می‌کند پرس‌وجوهای جست‌وجوی وب‌سایت (پرس‌وجوهای DNS) را به‌جای سرورهای ISP شما، از طریق سرورهای DNS خصوصی و رمزگذاری‌شدهٔ VPN ارسال کند. این کار مانع می‌شود ISP شما بتواند ردیابی کند از چه سایت‌هایی بازدید می‌کنید.

Q10: چرا باید بررسی کرد چه کسی VPN را اداره و تأیید می‌کند؟

شهرت مهم است. دربارهٔ مالکان و رهبران شرکت پژوهش کنید، به دنبال ممیزی‌های عمومی شخص ثالث باشید و پیش از اعتماد، نظر کارشناسان مستقل امنیت و رسانه‌ها را بررسی کنید. [1]

بخش 11: 10 واقعیت جالب و بینش‌های دنیای واقعی دربارهٔ VPN

این واقعیت‌ها و بینش‌های بسیار ارزشمند و دنیای واقعی دربارهٔ تاریخچه، بازار و فناوری VPNها را مرور کنید.

1. نخستین پروتکل VPN

PPTP (Point-to-Point Tunneling Protocol)، یک پروتکل VPN اولیه از گروهی به رهبری Microsoft در دههٔ 1990، اکنون ناامن به شمار می‌رود، بنابراین VPNهای مدرن از WireGuard یا OpenVPN استفاده می‌کنند. [1]

2. ارزش‌گذاری بازار

بازار جهانی VPN رشد سریعی داشته است که ناشی از افزایش نیاز به دورکاری و تقاضاهای امنیتی سازمانی است.

3. انقلاب WIREGUARD

WireGuard کدبیس بسیار ساده‌شده‌ای دارد که برای کارایی طراحی شده و بررسی آسیب‌پذیری‌های امنیتی آن را از پروتکل‌های سنتی آسان‌تر می‌کند. [3]

4. استانداردهای سخت‌گیرانهٔ ممیزی

ارائه‌دهندگان برتر VPN از شرکت‌هایی مانند Deloitte، KPMG یا PwC برای بررسی ادعاهای بدون ثبت گزارش و از شرکت‌های امنیتی مانند Cure53 برای آزمون برنامه‌ها و سرورهایشان استفاده می‌کنند. [4]

5. خاستگاه اتحاد EYES-5

مشارکت اطلاعاتی Five Eyes شامل آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند از همکاری اطلاعات سیگنالی دوران جنگ جهانی دوم میان متفقین پدید آمد.

6. بازرسی عمیق بسته

دیوارهای آتش پیشرفته از بازرسی عمیق بسته (DPI) برای تحلیل فراداده‌های بستهٔ شبکه و مسدود کردن ویژگی‌های استاندارد اتصال VPN استفاده می‌کنند.

7. استفادهٔ سازمانی

بسیاری از سازمان‌ها برای دسترسی کارکنان راه‌دور به سیستم‌های داخلی مانند پایگاه‌های داده، VPN در اختیارشان می‌گذارند و همین VPN را به ابزار امنیتی رایج محل کار تبدیل می‌کند.

8. VPNهای غیرمتمرکز

VPNهای غیرمتمرکز (dVPN) ترافیک را در شبکه‌ای از گره‌های مدیریت‌شده توسط همتایان توزیع می‌کنند و وابستگی به یک ارائه‌دهندهٔ متمرکز را کاهش می‌دهند.

9. گمنامی Tor در برابر VPN

VPN ترافیک را از یک ارائه‌دهندهٔ واحد عبور می‌دهد، در حالی که Tor (The Onion Router) ترافیک را از سه رله داوطلب (نگهبان، میانی، خروجی) می‌فرستد تا حریم خصوصی به بیشینه برسد. [5]

10. هزینهٔ نقض داده‌ها

ترکیب VPN با مدل دسترسی اعتماد صفر، که هر کاربر و دستگاه را بررسی می‌کند، به سازمان‌ها کمک می‌کند از داده‌ها محافظت کنند و آسیب نقض داده را محدود سازند.

منابع و مراجع فنی

نشریات ارجاع‌شده، مشخصات رمزنگاری و استانداردهای رسمی اسنادی که در سراسر این کاربرگ استفاده شده‌اند.

منابع علمی و صنعتی

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

کلید پاسخ: ارزیابی ارائه‌دهندگان VPN، استانداردهای امنیتی، ممیزی‌ها و سیاست‌های ثبت لاگ

1 سیاست لاگ‌های ممیزی‌شده

پروتکل‌ها

پاسخ درست: B

نکتهٔ آموزشی

سیاست بدون ثبت گزارش با ممیزی مستقل عملی‌ترین راه برای بررسی ادعاهای حریم خصوصی بدون دانش ارائه‌دهنده است. بازاریابی پرزرق‌وبرق یا ادعاهای خودگزارشی کافی نیستند. منبع: Deloitte Advisory، Cure53 Audit.

2 برتری WireGuard

تأخیر

پاسخ درست: D

نکتهٔ آموزشی

WireGuard مسیریابی مدرن و سریع اتصال را در فضای هسته با کدبیسی فشرده (~4,000 خط) ارائه می‌دهد و ممیزی را بسیار کارآمد می‌کند. استناد: IETF Protocol RFC, WireGuard Project.

3 پرسش 3

پاسخ درست: B

نکتهٔ آموزشی

VPNهای رایگان هم برای سرورها هزینه می‌پردازند و FTC هشدار می‌دهد برخی برنامه‌های VPN داده‌های کاربران را با اشخاص ثالث به اشتراک می‌گذارند، مثلاً برای نمایش تبلیغات.

4 صلاحیت‌های قضایی

کنترل‌های مسیریابی

پاسخ درست: C

نکتهٔ آموزشی

صلاحیت قضایی تعیین می‌کند که آیا VPN مشمول قوانین نظارتی، الزامات محلی نگهداری داده و احکام احضار محرمانهٔ دولتی است. منبع: Privacy Rights Clearinghouse.

5 حفاظت Kill Switch

حریم خصوصی

پاسخ درست: A

نکتهٔ آموزشی

اگر تونل قطع شود، kill switch بلافاصله مسیریابی آداپتور شبکهٔ سیستم را قطع می‌کند و از نشت IP واقعی و DNS جلوگیری می‌کند. منبع: IETF Tunnel RFC.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 محدودیت‌های بدافزار — پنهان‌سازی IP — پاسخ درست: نادرست

نکتهٔ آموزشی

VPN یک مجرای رمزگذاری‌شدهٔ امن فراهم می‌کند، اما بارها یا فایل‌ها را اسکن نمی‌کند. برای مسدود کردن بدافزار به نرم‌افزار آنتی‌ویروس نیاز است. منبع: Deloitte Advisory.

7 ممیزی مستقل — سرعت‌ها — پاسخ درست: درست

نکتهٔ آموزشی

گزارش‌های ممیزی پیکربندی نرم‌افزار سرور، رعایت راه‌اندازی فقط-RAM و نبود پایگاه‌های داده لاگ را تأیید می‌کنند. منبع: Deloitte Advisory، Cure53 Audit.

8 پرسش 8 — پاسخ درست: نادرست

نکتهٔ آموزشی

ارائه‌دهندگان باید از قوانین کشور مبدأ خود پیروی کنند که می‌تواند شامل قواعد نگهداری داده و دستورهای تحویل داده‌های نگهداری‌شده باشد.

9 اندازهٔ کدبیس پروتکل — دیوارهای آتش — پاسخ درست: درست

نکتهٔ آموزشی

پایگاه کد کوچک‌تر سطح حملهٔ بالقوه را کاهش می‌دهد و بررسی یکپارچگی پروتکل را برای تیم‌های امنیتی آسان‌تر می‌کند. منبع: WireGuard Project.

10 کسب‌درآمد از تبلیغات — بدون لاگ — پاسخ درست: درست

نکتهٔ آموزشی

بدون هزینهٔ اشتراک، VPNهای رایگان برای کسب درآمد به داده‌کاوی، پروفایل‌سازی ترافیک و تزریق تبلیغات در مرورگر متکی هستند. استناد: EDRi Retention Guidelines.

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

F 1. WireGuard	H 2. لاگ‌های ممیزی‌شده	E 3. صلاحیت قضایی	B 4. کلیدقطع‌کن
C 5. Five Eyes	A 6. VPN رایگان	D 7. سرورهای فقط-RAM	G 8. OpenVPN

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 بدون لاگ	2 WireGuard	3 قطع اضطراری	4 حوزهٔ قضایی
5 فقط رم	6 ممیزی		

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

1 E – پنجچشم	2 A – وایرگارد	3 H – اوپنوپیپان	4 F – رایگان
5 D – قطعاضطراری	6 G – فقطرم	7 C – حوزهقضایی	8 B – ممیزی

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند WireGuard، لاگ‌های ممیزی‌شده و صلاحیت قضایی 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.

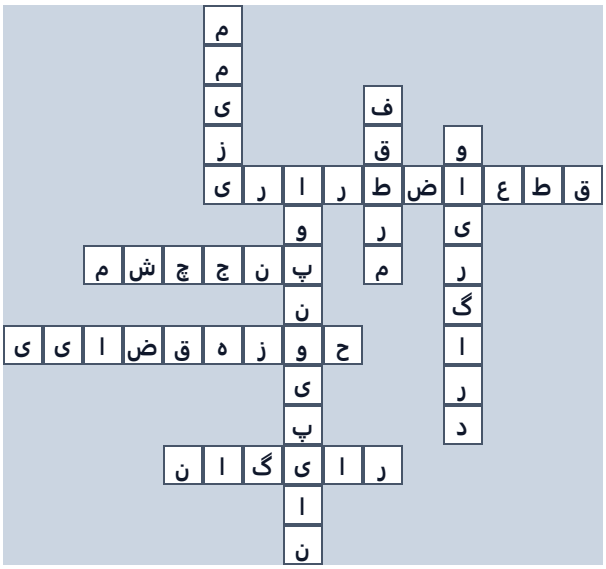
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

4 افقی: قطعاضطراری سازوکار ایمنی که اگر تونل امن قطع شود، مسیریابی اینترنت را مسدود می‌کند (10 حرف)

6 افقی: پنجچشم ائتلاف بین‌المللی تبادل اطلاعات اطلاعاتی میان آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند (6 حرف)

7 افقی: حوزهقضایی قلمرو جغرافیایی که تعهدات قانونی ارائه‌دهندهٔ VPN را تعیین می‌کند (9 حرف)

8 افقی: رایگان سرویس اتصال پرخطری که اغلب با ثبت و فروش داده‌های مرور کسب درآمد می‌کند (6 حرف)

عمودی

1 عمودی: ممیزی ادعای حریم خصوصی که شرکت‌های مستقل امنیت سایبری راستی‌آزمایی کرده‌اند (5 حرف)

2 عمودی: فقطرم زیرساخت سخت‌افزاری که کاملاً روی حافظهٔ فرار اجرا می‌شود و از ذخیرهٔ داده جلوگیری می‌کند (5 حرف)

3 عمودی: وایرگارد پروتکل مدرن و سریع با حدود 4,000 خط کد که بازبینی آن بسیار آسان است (8 حرف)

5 عمودی: اوپنوپیان پروتکل متن‌باز بالغ و بارها ممیزی‌شده با کدبیسی بسیار بزرگ‌تر از WireGuard (10 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. ررگوادی
2. یحیهوضاقز
3. پجچمشن
4. طمرفق
5. ییمزم
6. رضاراقططیع
7. ارگنیا
8. انیناوویپپ

وایرگارد
حوزههقضایی
پنجچشم
فقطرم
ممیزی
قطعاضطراری
رایگان
اوپنوپیپیان

کلید چالش رمز مخفی

"گزارش را با سامانه امن بسنجید"

کلید پاسخ مطالعات موردی

A سناریو A: امنیت شبکهٔ عمومی

شنود و رمزگذاری | معمای سارا

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- خطرها: شنود بسته، رهگیری داده و حمله‌های مرد میانی. فردی در همان شبکهٔ کافه می‌تواند جزئیات ورود یا فایل تکلیف او را ضبط کند.
- محافظت VPN: محتوای بسته‌های شبکه را رمزگذاری می‌کند و وقتی VPN درست پیکربندی شده باشد، ترافیک تونل رهگیری‌شده را برای شنودگران منفعل شبکهٔ محلی ناخوانا می‌کند.

B سناریو B: دسترسی به منابع مسدودشده

مسدودسازی جغرافیایی و IPها | دوراهی Alex

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- دلیل مسدود شدن: میزبان پخش از مسدودسازی جغرافیایی استفاده می‌کند که IP محلی مسافر را به کشور فیزیکی او نگاشت می‌کند و بر اساس مجوزهای قلمرویی آن را مسدود می‌کند.
- VPN چگونه کمک می‌کند: پنهان کردن مکان واقعی او با مسیریابی ترافیک از طریق سروری در کشور خودش. سایت IP کشور خود او را می‌بیند و دسترسی را مجاز می‌کند.