نام: _____ تاریخ: _____ نمره: _____

امنیت Surfshark

بررسی ویژگی‌های امنیتی Surfshark شامل مسدودسازی تبلیغات CleanWeb، مسیریابی پویای MultiHop، معماری SDN به نام Nexus، ناوگان سرور فقط RAM و حالت Camouflage.

مرور آموزشی امنیت SURFSHARK

خوش آمدید! این بستهٔ فعالیت شما را در بررسی معماری امنیتی Surfshark راهنمایی می‌کند. با سخت‌افزار سرور فقط-RAM، چرخش پویای IP با Nexus SDN، مسدودکننده‌های تبلیغات CleanWeb و مسیریابی MultiHop آشنا می‌شوید.

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

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/surfshark/security/

نقشهٔ راه یادگیری امنیت Surfshark شما

- معماری فنی و قواعد پیکربندی امنیت Surfshark را تحلیل کنید.
- تنظیمات کلاینت را برای جلوگیری از نشت ترافیک IP، DNS و WebRTC پیکربندی کنید.
- ویژگی‌های قیمت‌گذاری سفارشی، دورهٔ آزمایشی و عملکرد را با مدل‌های استاندارد مقایسه کنید.

دستورالعمل راهنمای امنیت SURFSHARK

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 زیرساخت فقط-RAM، Nexus SDN و CleanWeb به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

ناوگان سرور فقطRAM، Nexus SDN و معماری CleanWeb (مقدمه)

Surfshark با ناوگان سرور کاملاً فقط-RAM، شبکه‌سازی نرم‌افزارمحور Nexus با IP Rotator، مسدودسازی تبلیغات CleanWeb و مسیرهای رمزگذاری Dynamic MultiHop از حریم خصوصی کاربر محافظت می‌کند.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. نام مسدودکنندهٔ یکپارچهٔ تبلیغات و بدافزار **Surfshark** چیست؟

- A) AdGuard
- B) CleanWeb
- C) ThreatShield
- D) NetBlocker

2 2. **Surfshark** در همهٔ سرورهای خود از کدام معماری سخت‌افزاری استفاده می‌کند؟

- A) دیسک‌های سخت
- B) 100% فقط-RAM
- C) ذخیره‌سازی نوری
- D) نوار مغناطیسی

3 3. کدام ویژگی ترافیک را از دو سرور **VPN** متمایز عبور می‌دهد؟

- A) Bypasser
- B) MultiHop (Double VPN)
- C) شبکهٔ Nexus
- D) IP ایستا

4 4. کدام ویژگی مبهم‌سازی ترافیک **VPN** را به‌شکل داده‌های وب عادی درمی‌آورد؟

- A) Kill Switch
- B) حالت استتار
- C) CleanWeb 2.0
- D) تونل تفکیکی

5 5. کارکرد ابزار **Surfshark Bypasser** چیست؟

- A) Speed Booster
- B) تونل‌زنی تقسیم‌شده (Split Tunneling)
- C) مدیر گذرواژه
- D) تفکیک‌کنندهٔ DNS

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. سرورهای فقطRAM تمام داده‌های عملیاتی را بلافاصله پس از راه‌اندازی مجدد سرور پاک می‌کنند.

درست ○ نادرست ○

7 پرسش 7

7. حالت استتار از تشخیص استفادهٔ شما از VPN توسط ISPها جلوگیری می‌کند.

درست ○ نادرست ○

8 پرسش 8

8. CleanWeb 2.0 درون افزونه‌های مرورگر عمل می‌کند تا پنجره‌های بازشوی رضایت کوکی را مسدود کند.

درست ○ نادرست ○

9 پرسش 9

9. Surfshark مهر زمانی اتصال‌های موقت و گزارش‌های مصرف پهنای باند را نگه می‌دارد.

درست ○ نادرست ○

10 پرسش 10

10. شبکهٔ Nexus نشانی‌های IP کاربر را بدون قطع اتصال به‌صورت دوره‌ای تغییر می‌دهد.

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. تبلیغات مزاحم وب، اسکریپت‌های ردیابی و پیوندهای فیشینگ با فیلترهای _____ مسدود می‌شوند.
2. فعالیت کاربر هیچ ردپای قضایی بر جای نمی‌گذارد، زیرا سرورها در حالت _____ کار می‌کنند.
3. مسیریابی داده از دو جهش سرور رمزگذاری‌شدهٔ جداگانه با تونل‌های _____ انجام می‌شود.
4. برای پنهان کردن استفاده از VPN از ارائه‌دهندگان خدمات اینترنت، کاربران حالت _____ را فعال می‌کنند.
5. اجازه دادن به برنامه‌های بانکی برای عبور از تونل VPN با تنظیمات _____ مدیریت می‌شود.
6. معماری نسل بعد SDN که ناوگان سرورها را به هم متصل می‌کند، سامانهٔ _____ است.

بانک واژگان

استتار | بایپسر | چندجهشی | فقط رم | قطع اضطراری | نکسوس | وایرگارد | CleanWeb

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم VPN و شبکه

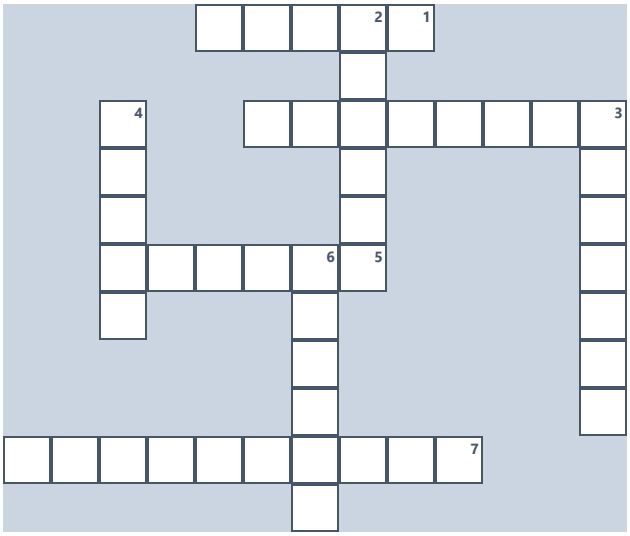
تطبیق تعاریف

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. کلین‌وب	A	قابلیت ایمنی خودکار که هنگام قطع VPN ترافیک شبکه را مسدود می‌کند.
2. فقط رم	B	قابلیت Split-tunneling که به برنامه‌های انتخاب‌شده اجازه می‌دهد VPN را دور بزنند.
3. چندجهشی	C	فیلتر پیشرفته‌ای که تبلیغات، بدافزار و بنرهای رضایت کوکی را مسدود می‌کند.
4. استتار	D	سخت‌افزار سرور با حافظهٔ فرار که در هر چرخهٔ روشن و خاموش شدن همهٔ داده‌ها را پاک می‌کند.
5. دورزن	E	قابلیتی که نشانی IP بیرونی شما را به‌طور منظم و بدون قطع تونل‌ها تغییر می‌دهد.
6. قطع اضطراری	F	فناوری مبهم‌سازی که امضاهای VPN را پنهان می‌کند تا شبیه ترافیک HTTPS معمولی شود.
7. نکسوس	G	قابلیت مسیریابی دو-VPN که ترافیک را در دو گرهٔ سرور متمایز رمزگذاری می‌کند.
8. چرخان	H	شبکهٔ نرم‌افزارمحور اختصاصی که همهٔ سرورها را در یک مش یکپارچه به هم متصل می‌کند.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

1. شبکهٔ نرم‌افزارمحور اختصاصی که همهٔ سرورها را در یک مش یکپارچه به هم متصل می‌کند (5)

3. ویژگی که نشانی IP بیرونی شما را بدون قطع تونل‌ها به‌طور منظم تغییر می‌دهد (8)

5. قابلیت تونل تفکیکی که به برنامه‌های انتخابی اجازه می‌دهد VPN را دور بزنند (6)

7. ویژگی ایمنی خودکار که با افتادن VPN ترافیک شبکه را مسدود می‌کند (10)

عمودی

2. فیلتر پیشرفته برای مسدودسازی تبلیغات، بدافزار و بنرهای رضایت کوکی (6)

3. قابلیت VPN دوگانه که ترافیک را از دو گرهٔ سرور جداگانه رمزگذاری می‌کند (7)

4. سخت‌افزار سرور با حافظهٔ فرار که با هر چرخهٔ روشن و خاموش همهٔ داده‌ها را پاک می‌کند (5)

6. فناوری مبهم‌سازی که امضای VPN را پنهان می‌کند تا شبیه ترافیک HTTPS معمولی شود (6)

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

1 افقی: شبکهٔ نرم‌افزارمحور اختصاصی که همهٔ سرورها را در یک مش یکپارچه به هم متصل می‌کند (5 حرف):

3 افقی: ویژگی که نشانی IP بیرونی شما را بدون قطع تونل‌ها به‌طور منظم تغییر می‌دهد (8 حرف):

5 افقی: قابلیت تونل تفکیکی که به برنامه‌های انتخابی اجازه می‌دهد VPN را دور بزنند (6 حرف):

7 افقی: ویژگی ایمنی خودکار که با افتادن VPN ترافیک شبکه را مسدود می‌کند (10 حرف):

عمودی

2 عمودی: فیلتر پیشرفته برای مسدودسازی تبلیغات، بدافزار و بنرهای رضایت کوکی (6 حرف):

3 عمودی: قابلیت VPN دوگانه که ترافیک را از دو گرهٔ سرور جداگانه رمزگذاری می‌کند (7 حرف):

4 عمودی: سخت‌افزار سرور با حافظهٔ فرار که با هر چرخهٔ روشن و خاموش همهٔ داده‌ها را پاک می‌کند (5 حرف):

6 عمودی: فناوری مبهم‌سازی که امضای VPN را پنهان می‌کند تا شبیه ترافیک HTTPS معمولی شود (6 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.

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

فهرست واژگان

کلینوب فقطرم چندجهشی استتار بایپسر قطعاضطراری نکسوس چرخشایپی

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. کلینوب
B. فقطرم
C. چندجهشی
D. استتار
E. بایپسر
F. قطعاضطراری
G. نکسوس
H. چرخشاپی

	تعاریف و فیلدهای تطبیق
	1. فناوری مبهم‌سازی که امضای VPN را پنهان می‌کند تا شبیه ترافیک HTTPS معمولی شود.
	2. ویژگی ایمنی خودکار که با افتادن VPN ترافیک شبکه را مسدود می‌کند.
	3. فیلتر پیشرفته برای مسدودسازی تبلیغات، بدافزار و بنرهای رضایت کوکی.
	4. قابلیت تونل تفکیکی که به برنامه‌های انتخابی اجازه می‌دهد VPN را دور بزنند.
	5. سخت‌افزار سرور با حافظهٔ فرار که با هر چرخهٔ روشن و خاموش همهٔ داده‌ها را پاک می‌کند.
	6. ویژگی که نشانی IP بیرونی شما را بدون قطع تونل‌ها به‌طور منظم تغییر می‌دهد.
	7. قابلیت VPN دوگانه که ترافیک را از دو گرهٔ سرور جداگانه رمزگذاری می‌کند.
	8. شبکهٔ نرم‌افزارمحور اختصاصی که همهٔ سرورها را در یک مش یکپارچه به هم متصل می‌کند.

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. ی ک ن و ب ل
2. چ د ی ش ه ج ن
3. ب ی پ ر س ا
4. س س و ن ک
5. ط م ف ر ق
6. ا ت ا ت ر س
7. ط ا ق ر ط ا ر ی ض ع
8. ش ر ا ی چ پ ی خ

فعالیت تکمیلی: سریع فکر کن

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

1	ویژگی‌های امنیتی در Surfshark		
2	نشانه‌های کند بودن اتصال VPN شما		
3	پروتکل‌های VPN که می‌شناسید		
4	چیزهایی که رمزگذاری از آن‌ها محافظت می‌کند		
5	تهدیدهای Wi-Fi عمومی		
6	کشورهای شناخته‌شده به قوانین قوی حریم خصوصی		
7	روش‌های ساختن گذرواژهٔ قوی		
8	دستگاه‌هایی که Surfshark را روی آن‌ها نصب می‌کنید		
9	پرسش‌هایی برای پشتیبانی مشتریان Surfshark		
10	تنظیماتی که برای امنیت بیشتر روشن می‌کنید		
11	چیزهایی که Surfshark می‌تواند از شبکهٔ شما پنهان کند		
12	انواع نشت در VPN		
13	داده‌هایی که VPN هرگز نباید ذخیره کند		
14	واژه‌هایی که یک برنامهٔ VPN خوب را توصیف می‌کنند		
15	چیزهایی که یک ممیزی می‌تواند بررسی کند		

ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

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

مطالعهٔ موردی 1: دور زدن فیلترهای دانشگاه و محل کار



سناریو: دانشجویی می‌یابد که Wi-Fi پردیس دانشگاهش همهٔ پورت‌های استاندارد OpenVPN و WireGuard را مسدود می‌کند.

پرسش برای بحث: کدام ویژگی Surfshark به دانشجو اجازه می‌دهد بدون شناسایی توسط مدیران شبکه وصل شود؟

مطالعهٔ موردی 2: تحقیق روزنامه‌نگاری پرخطر



سناریو: یک روزنامه‌نگار تحقیقی هنگام پژوهش در سوابق حساس شرکتی به محافظت بیشتر در برابر نظارت نیاز دارد.

پرسش برای بحث: Dynamic MultiHop چگونه حریم خصوصی برتری نسبت به مسیریابی تک‌سروره فراهم می‌کند؟

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

28	32	12	8		32	3	32	1		16	9	12	7		30		15	30	15	25	29

12	2	12	1	25

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: Surfshark CleanWeb چیست؟

CleanWeb یک ویژگی امنیتی یکپارچه است که تبلیغات، ردیاب‌ها، بدافزار و سایت‌های فیشینگ را مسدود می‌کند.

Q2: سرورهای فقط-RAM چیستند؟

سرورهای فقطRAM روی حافظهٔ فرار اجرا می‌شوند، یعنی داده‌های موجود در حافظه هر بار که سرورها راه‌اندازی مجدد شوند پاک می‌شوند.

Q3: Surfshark MultiHop چیست؟

MultiHop (Double VPN) اتصال اینترنت شما را از دو مکان سرور متفاوت مسیریابی و رمزگذاری می‌کند.

Q4: حالت Camouflage چگونه کار می‌کند؟

حالت استتار ترافیک VPN را مبهم می‌کند تا ISP شما نتواند تشخیص دهد از VPN استفاده می‌کنید.

Q5: ویژگی Bypasser چیست؟

Bypasser ابزار تونل‌زنی تقسیم‌شدهٔ Surfshark است که به برنامه‌ها یا وب‌سایت‌های مشخص اجازه می‌دهد VPN را دور بزنند.

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 Surfshark کیل‌سوییچ دارد؟

بله، Kill Switch اگر VPN به‌طور ناگهانی قطع شود، اتصال شما را به اینترنت قطع می‌کند.

Q7: Surfshark از چه استاندارد رمزگذاری استفاده می‌کند؟

Surfshark از AES-256-GCM و ChaCha20 و همچنین AEGIS-256X2 در پروتکل جدید Dausos خود استفاده می‌کند.

Q8: آیا سیاست بدون‌لاگ Surfshark ممیزی شده است؟

بله، Deloitte سیاست عدم ثبت گزارش Surfshark را در سال 2023 و دوباره در سال 2025 تأیید کرد.

Q9: Surfshark Nexus چیست؟

Nexus معماری پیشرفتهٔ SDN است که همهٔ سرورها را برای مسیریابی روان‌تر در یک شبکهٔ یکپارچه به هم وصل می‌کند.

Q10: ویژگی IP Rotator چیست؟

IP Rotator آدرس IP شما را هر چند دقیقه بدون قطع نشست VPN به‌طور خودکار تغییر می‌دهد.

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: Dynamic MultiHop چه تفاوتی با Double VPN سنتی دارد؟

Dynamic MultiHop به شما اجازه می‌دهد هر ترکیبی از سرورهای ورودی و خروجی را در سراسر جهان سفارشی کنید.

Q2: آیا CleanWeb 2.0 روی افزونه‌های مرورگر کار می‌کند؟

بله، CleanWeb 2.0 تبلیغات ویدیویی، پنجره‌های بازشوی رضایت کوکی و بنرهای هشدار را درون Chrome/Firefox مسدود می‌کند.

Q3: Alternative ID در مجموعهٔ امنیتی چیست؟

Alternative ID نام‌های مستعار شخصی یکتا، نشانی‌های ایمیل و پوشش‌های شمارهٔ تلفن می‌سازد.

Q4: Surfshark چگونه از نشت DNS جلوگیری می‌کند؟

Surfshark تمام درخواست‌های دامنه را از سرورهای DNS خصوصی خودش در هر گره عبور می‌دهد.

Q5: آیا Surfshark در موبایل از رمزگذاری ChaCha20 پشتیبانی می‌کند؟

بله، WireGuard در اندروید و iOS برای کارایی برتر موبایل از ChaCha20-Poly1305 استفاده می‌کند.

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: حالت NoBorders در Surfshark چیست؟

NoBorders به‌طور خودکار محیط‌های شبکهٔ محدودکننده را شناسایی می‌کند و سرورهای تخصصی ارائه می‌دهد.

Q7: چه کسی ممیزی‌های امنیتی افزونه‌های مرورگر Surfshark را انجام داد؟

شرکت مستقل امنیت سایبری Cure53 ممیزی‌هایی روی افزونه‌های مرورگر و سامانه‌های سرور انجام داد.

Q8: Surfshark چگونه در برابر نشت IPv6 محافظت می‌کند؟

Surfshark ترافیک IPv6 را به‌صورت ایمن مسیریابی می‌کند یا آن را با ایمنی محدود می‌کند تا از هرگونه نشت رمزگذاری‌نشده جلوگیری شود.

Q9: حوزهٔ قضایی قانونی Surfshark در کجاست؟

Surfshark تحت قانون هلند فعالیت می‌کند و به استانداردهای سخت‌گیرانهٔ حریم خصوصی اروپایی GDPR پایبند است.

Q10: آیا Surfshark از احراز هویت دومرحله‌ای (2FA) پشتیبانی می‌کند؟

بله، و Surfshark One یک قفل 2FA اضافه می‌کند تا فقط شما بتوانید تنظیمات ویژگی‌ها را تغییر دهید.

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

1. Surfshark می‌گوید کل شبکهٔ بیش از 4,500 سرور آن روی سخت‌افزار فقطRAM بدون دیسک و فژار اجرا می‌شود.

2. بینش VPN

2. شرکت Deloitte از «چهار بزرگ» سیاست بدون لاگ Surfshark را در 2023 و دوباره در نوامبر 2025 راستی‌آزمایی کرد.

3. بینش VPN

3. معماری اختصاصی Nexus همهٔ سرورهای جهانی را در یک شبکهٔ نرم‌افزارمحور پویا به هم وصل می‌کند.

4. بینش VPN

4. IP چرخان نشانی IP شما را تقریباً هر پنج دقیقه بدون قطع اتصال VPN تغییر می‌دهد.

5. بینش VPN

5. CleanWeb 2.0 پنجره‌های مزاحم رضایت کوکی و تبلیغات ویدیویی را مستقیماً در مرورگرها مسدود می‌کند.

6. بینش VPN

6. MultiHop پویا به کاربران اجازه می‌دهد مسیرهای رمزگذاری دوسروری سفارشی را در 100 کشور بسازند.

7. بینش VPN

7. حالت استتار امضای سرایند VPN را حذف می‌کند و ترافیک را از HTTPS معمولی غیرقابل‌تشخیص می‌سازد.

8. بینش VPN

8. Alternative ID نام‌های مستعار یک‌بارمصرف و ایمیل‌های پوششی می‌سازد تا کاربران را از نشت پایگاه داده محافظت کند.

9. بینش VPN

9. Surfshark رمزگذاری متقارن AES-256-GCM را در کنار ChaCha20 روی پروتکل‌های WireGuard اعمال می‌کند.

10. بینش VPN

10. حالت NoBorders در شبکه‌های محدودشده به‌طور خودکار فعال می‌شود تا دسترسی تونل‌زنی پایدار فراهم کند.

منابع و مراجع فنی

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

منابع علمی و صنعتی

[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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 مسدودکنندهٔ محتوای یکپارچه
دفاع در برابر تبلیغات و بدافزار
پاسخ درست: B

نکتهٔ آموزشی

CleanWeb فیلتر امنیتی یکپارچهٔ Surfshark است که تبلیغات، دامنه‌های ردیاب، وب‌سایت‌های فیشینگ و اسکریپت‌های URL مخرب را در سطح شبکه مسدود می‌کند. منبع: CleanWeb Security Specs.

2 زیرساخت 100% فقط‌RAM
معماری RAM
پاسخ درست: B

نکتهٔ آموزشی

Surfshark سرورهای فقط-RAM اجرا می‌کند، بنابراین داده‌های نگه‌داشته‌شده در حافظهٔ سرور با خاموش شدن یا راه‌اندازی مجدد سرور پاک می‌شوند. منبع: Cure53 Infrastructure Audit.

3 تونل‌زنی دوگانهٔ MultiHop
VPN چندجهشی
پاسخ درست: B

نکتهٔ آموزشی

MultiHop (Double VPN) ترافیک را از دو گرهٔ سرور متمایز در کشورهای جداگانه رمزگذاری می‌کند تا از حمله‌های همبستگی ترافیک جلوگیری شود. منبع: Surfshark MultiHop Guide.

4 مبهم‌سازی با حالت استتار
مبهم‌سازی
پاسخ درست: B

نکتهٔ آموزشی

حالت استتار سرایند بسته‌های OpenVPN را تغییر می‌دهد تا ترافیک VPN را به‌شکل ترافیک استاندارد HTTPS درآورد و مسدودسازی‌های دیوار آتش سخت‌گیر را دور بزند. منبع: Surfshark Stealth Whitepaper.

5 تونل‌زنی تقسیم‌شدهٔ Bypasser
تونل‌زنی تقسیمی
پاسخ درست: B

نکتهٔ آموزشی

Bypasser ابزار تونل‌زنی تقسیم‌شدهٔ Surfshark است که به کاربران اجازه می‌دهد برنامه‌ها یا وب‌سایت‌های مشخصی را انتخاب کنند تا مستقیماً از طریق اتصال معمولی ISP مسیریابی شوند. منبع: Surfshark Client Features.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **پاک‌سازی داده‌های حافظهٔ فرار** امنیت سرور

پاسخ درست: درست

نکتهٔ آموزشی

سرورهای فقطRAM هیچ داده‌ای روی هارددیسک‌های دائمی ذخیره نمی‌کنند؛ راه‌اندازی مجدد سخت‌افزار بلافاصله تمام حافظهٔ عملیاتی را پاک می‌کند. منبع: RAM Server Architecture.

7 **پنهان‌سازی از ISP با حالت استتار** پنهان‌سازی ترافیک

پاسخ درست: درست

نکتهٔ آموزشی

حالت استتار امضاهای پروتکل OpenVPN را حذف می‌کند و از تشخیص اتصال کاربر به تونل VPN توسط ISPها جلوگیری می‌کند. منبع: Deep Packet Inspection Guide.

8 **افزونه‌های مرورگر CleanWeb 2.0** افزونهٔ مرورگر

پاسخ درست: درست

نکتهٔ آموزشی

CleanWeb 2.0 درون افزونه‌های مرورگر عمل می‌کند تا پنجره‌های بازشوی رضایت کوکی، تبلیغات ویدیویی و اسکریپت‌های تغییر مسیر مخرب را در زمان واقعی مسدود کند. منبع: CleanWeb 2.0 Release Notes.

9 **عدم نگهداری لاگ اتصال** سیاست بدون لاگ

پاسخ درست: نادرست

نکتهٔ آموزشی

Surfshark سیاست سخت‌گیرانهٔ عدم ثبت گزارش را که به‌طور مستقل ممیزی شده حفظ می‌کند و هیچ نشانی IP، مهر زمانی اتصال یا گزارش پهنای باند ثبت نمی‌کند. منبع: Deloitte No-Logs Audit.

10 **چرخش پویای IP در Nexus** شبکهٔ NEXUS

پاسخ درست: درست

نکتهٔ آموزشی

شبکهٔ نرم‌افزارمحور Surfshark Nexus نشانی‌های IP کاربر را هر چند دقیقه به‌صورت پویا و بدون قطع اتصال فعال VPN تغییر می‌دهد. منبع: Surfshark Nexus Architecture.

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

C 1. کلین‌وب	D 2. فقط رم	G 3. چندجهشی	F 4. استتار
B 5. دورزن	A 6. قطع اضطراری	H 7. نکسوس	E 8. چرخان

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 CleanWeb	2 فقط رم	3 چندجهشی	4 استتار
5 بایپسر	6 نکسوس		

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

1 D – استتار	2 F – قطعاضطراری	3 A – کلینوب	4 E – بایپسر
5 B – فقطرم	6 H – چرخشایپی	7 C – چندجهشی	8 G – نکسوس

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند کلین‌وب، فقط رم و چندجهشی 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.

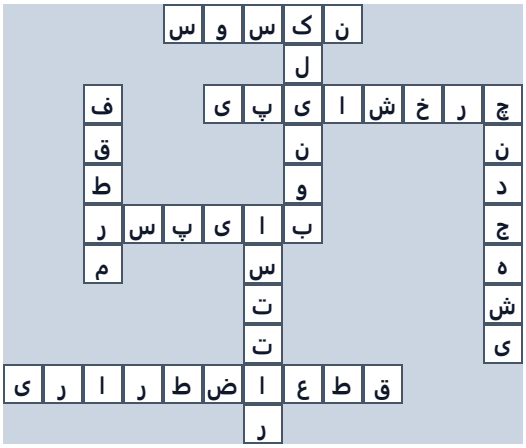
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

1 افقی: نکسوس شبکهٔ نرم‌افزارمحور اختصاصی که همهٔ سرورها را در یک مش یکپارچه به هم متصل می‌کند (5 حرف)

3 افقی: چرخشایپی ویژگی که نشانی IP بیرونی شما را بدون قطع تونل‌ها به‌طور منظم تغییر می‌دهد (8 حرف)

5 افقی: بایپسر قابلیت تونل تفکیکی که به برنامه‌های انتخابی اجازه می‌دهد VPN را دور بزنند (6 حرف)

7 افقی: قطعاضطراری ویژگی ایمنی خودکار که با افتادن VPN ترافیک شبکه را مسدود می‌کند (10 حرف)

عمودی

2 عمودی: کلینوب فیلتر پیشرفته برای مسدودسازی تبلیغات، بدافزار و بنرهای رضایت کوکی (6 حرف)

3 عمودی: چندجهشی قابلیت VPN دوگانه که ترافیک را از دو گرهٔ سرور جداگانه رمزگذاری می‌کند (7 حرف)

4 عمودی: فقطرم سخت‌افزار سرور با حافظهٔ فرار که با هر چرخهٔ روشن و خاموش همهٔ داده‌ها را پاک می‌کند (5 حرف)

6 عمودی: استتار فناوری مبهم‌سازی که امضای VPN را پنهان می‌کند تا شبیه ترافیک HTTPS معمولی شود (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. یکنویل — کلینوب
2. چدیشهجن — چندجهشی
3. بیپرسا — بایپسر
4. سسونک — نکسوس
5. طمفرق — فقطرم
6. اتاترس — استتار
7. طاقرطاریضع — قطعاضطراری
8. شرایچپیخ — چرخشایپی

کلید چالش رمز مخفی

"نکسوس و چرخش آیپی حریم کاربر"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: دور زدن فیلترهای دانشگاه و محل کار

پاسخ معلم

بارم‌بندی و راهنمای پاسخ‌ها

- تحلیل سناریو: یک دانشجو متوجه می‌شود Wi-Fi پردیس دانشگاهش همهٔ پورت‌های استاندارد OpenVPN و WireGuard را مسدود می‌کند.
- پرسش کانونی: کدام ویژگی Surfshark به دانشجو اجازه می‌دهد بدون شناسایی توسط مدیران شبکه متصل شود؟
- راهبرد و راه‌حل توصیه‌شده: حالت Camouflage (OpenVPN) را فعال کنید که فراداده VPN را پنهان می‌کند تا دیوارهای آتش مرور عادی HTTPS را ببینند.

B مطالعهٔ موردی 2: تحقیق روزنامه‌نگاری پرخطر

پاسخ معلم

بارم‌بندی و راهنمای پاسخ‌ها

- تحلیل سناریو: یک روزنامه‌نگار تحقیقی هنگام پژوهش دربارهٔ اسناد حساس شرکتی به محافظت بیشتری در برابر نظارت نیاز دارد.
- پرسش کانونی: Dynamic MultiHop چگونه حریم خصوصی برتری نسبت به مسیریابی تک‌سروری فراهم می‌کند؟
- راهبرد و راه‌حل توصیه‌شده: Dynamic MultiHop ترافیک را از طریق سرورهای ورودی و خروجی در دو کشور هدایت می‌کند، بنابراین هیچ سرور واحدی نمی‌تواند کاربر را افشا کند.