نام: _____ تاریخ: _____ نمبر: _____

Surfshark کی سیکیورٹی

Surfshark کی سیکیورٹی خصوصیات کا جائزہ، جن میں CleanWeb اشتہار بلاکنگ، MultiHop متحرک روٹنگ، Nexus SDN آرکیٹیکچر، صرف RAM والا سرور فلیٹ، اور Camouflage موڈ شامل ہیں۔

SURFSHARK سیکیورٹی 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 Surfshark کے سیکیورٹی آرکیٹیکچر سے متعارف کراتا ہے۔ آپ صرف RAM پر چلنے والے سرور ہارڈ ویئر، Nexus SDN متحرک IP روٹیشن، CleanWeb ایڈ بلاکرز اور MultiHop روٹنگ 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/surfshark/security/

آپ کا Surfshark سیکیورٹی لرننگ روڈ میپ

- Surfshark سیکیورٹی کے تکنیکی فن تعمیر اور کنفیگریشن کے اصولوں کا تجزیہ کریں۔
- IP، DNS اور WebRTC ٹریفک لیکس کو روکنے کے لیے کلائنٹ کی سیٹنگز ترتیب دیں۔
- حسبِ ضرورت قیمتوں، ٹرائل اور کارکردگی کی خصوصیات کا معیاری ماڈلز سے موازنہ کریں۔

SURFSHARK سیکیورٹی گائیڈ 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 صرف RAM والے انفراسٹرکچر، Nexus SDN اور CleanWeb پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

صرف RAM سرور فلیٹ، Nexus SDN اور CleanWeb آرکیٹیکچر (تعارف)

Surfshark صارف کی رازداری کو صرف RAM پر چلنے والے سرور فلیٹ، IP Rotator کے ساتھ Nexus سافٹ ویئر ڈیفائنڈ نیٹ ورکنگ، CleanWeb ایڈ بلاکنگ، اور Dynamic MultiHop خفیہ کاری راستوں کے ذریعے محفوظ بناتا ہے۔

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

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. Surfshark کے مربوط اشتہار اور میل ویئر بلاکر کا نام کیا ہے؟
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. Surfshark اپنے تمام سرورز پر کون سا ہارڈ ویئر آرکیٹیکچر استعمال کرتا ہے؟
   - A) ہارڈ ڈسک ڈرائیوز
   - B) 100% RAM صرف
   - C) آپٹیکل اسٹوریج
   - D) مقناطیسی ٹیپ

3. کون سی خصوصیت ٹریفک کو دو الگ VPN سرورز سے گزارتی ہے؟
   - A) بائی پاسر
   - B) MultiHop (ڈبل VPN)
   - C) Nexus نیٹ ورک
   - D) جامد IP

4. کون سی ابفسکیشن خصوصیت VPN ٹریفک کو عام ویب ڈیٹا کے طور پر چھپاتی ہے؟
   - A) کل سوئچ
   - B) کیموفلاج موڈ
   - C) CleanWeb 2.0
   - D) اسپلٹ ٹنل

5. Surfshark Bypasser ٹول کا کام کیا ہے؟
   - A) اسپیڈ بوسٹر
   - B) اسپلٹ ٹنلنگ
   - C) پاس ورڈ مینیجر
   - D) DNS ریزولور

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. صرف RAM سرورز سرور ری بوٹ ہوتے ہی تمام آپریٹنگ ڈیٹا مٹا دیتے ہیں۔

درست غلط

7 سوال 7

7. کیموفلاج موڈ ISPs کو یہ معلوم کرنے سے روکتا ہے کہ آپ VPN استعمال کر رہے ہیں۔

درست غلط

8 سوال 8

8. CleanWeb 2.0 براؤزر ایکسٹینشنز کے اندر کام کرتا ہے تاکہ کوکی رضامندی کے پاپ اپس کو بلاک کرے۔

درست غلط

9 سوال 9

9. Surfshark عارضی کنکشن ٹائم اسٹیمپس اور بینڈ وڈتھ استعمال کے لاگز رکھتا ہے۔

درست غلط

10 سوال 10

10. Nexus نیٹ ورک بغیر منقطع کیے وقتاً فوقتاً صارفین کے IP ایڈریس بدلتا رہتا 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. پریشان کن ویب اشتہارات، ٹریکنگ اسکرپٹس اور فشنگ لنکس _____ فلٹرز سے بلاک ہوتے ہیں۔
2. صارف کی سرگرمی کا کوئی فرانزک نشان نہیں رہتا کیونکہ سرور _____ نظام پر چلتے ہیں۔
3. ڈیٹا کو دو الگ انکرپٹڈ سرور ہاپس سے گزارنا _____ ٹنلز کے ذریعے ہوتا ہے۔
4. انٹرنیٹ سروس فراہم کنندگان سے وی پی این کا استعمال چھپانے کے لیے صارفین _____ موڈ فعال کرتے ہیں۔
5. بینکنگ ایپلی کیشنز کو وی پی این ٹنل بائی پاس کرنے دینا _____ سیٹنگز سے سنبھالا جاتا ہے۔
6. سرور بیڑے کو جوڑنے والا اگلی نسل کا SDN ڈھانچہ _____ سسٹم ہے۔

الفاظ کا بینک

بائی پاسر | روٹیٹنگ | صرف ریم | کل سوئچ | کلین ویب | کیموفلاج | ملٹی ہاپ | نیکسس

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: VPN اور نیٹ ورک تصورات کا ملان

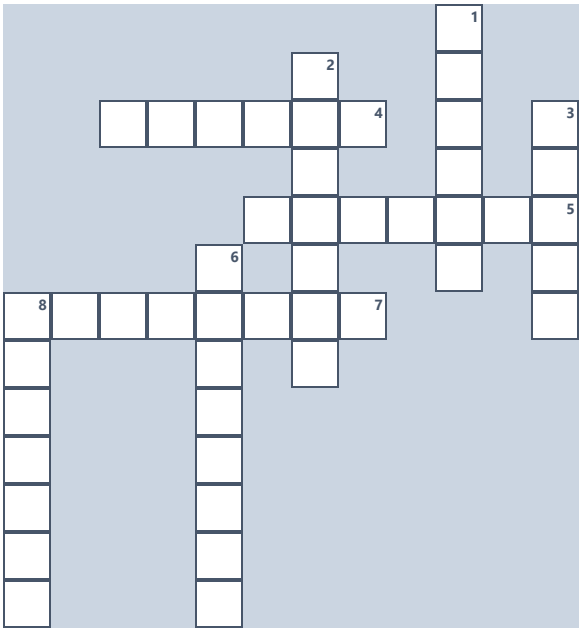
تعریفوں کا ملان

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. کلین ویب	A	خودکار حفاظتی فیچر جو VPN ٹوٹنے پر نیٹ ورک ٹریفک کو بلاک کرتا ہے۔
2. صرف ریم	B	اسپلٹ ٹنلنگ کی سہولت جو منتخب ایپلی کیشنز کو VPN بائی پاس کرنے دیتی ہے۔
3. ملٹی ہاپ	C	جدید فلٹر جو اشتہارات، میل ویئر اور کوکی رضامندی بینرز کو بلاک کرتا ہے۔
4. کیموفلاج	D	غیر مستقل میموری والا سرور ہارڈ ویئر جو ہر بار بجلی بند اور چالو ہونے پر تمام ڈیٹا مٹا دیتا ہے۔
5. بائی پاسر	E	ایسا فیچر جو ٹنلز کو روکے بغیر آپ کا بیرونی IP ایڈریس باقاعدگی سے تبدیل کرتا ہے۔
6. کل سوئچ	F	اوبفسکیشن ٹیکنالوجی جو VPN کی شناختی علامات چھپا کر عام HTTPS ٹریفک کی نقل کرتی ہے۔
7. Nexus نیٹ	G	ڈبل VPN روٹنگ فیچر جو ٹریفک کو دو الگ سرور نوڈز کے ذریعے خفیہ کرتا ہے۔
8. گردشی	H	ملکیتی سافٹ ویئر سے متعین نیٹ ورک جو تمام سرورز کو ایک متحد میش میں جوڑتا 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

4. خودکار حفاظتی فیچر جو وی پی این ڈراپ ہونے پر نیٹ ورک ٹریفک روک دیتا ہے (6)

5. اشتہارات، میل ویئر اور کوکی منظوری بینرز کو روکنے والا ایڈوانسڈ فلٹر (7)

7. اسپلٹ ٹنلنگ کی سہولت جو منتخب ایپلی کیشنز کو وی پی این بائی پاس کرنے دیتی ہے (8)

عمودی

1. عارضی میموری والا سرور ہارڈ ویئر جو ہر پاور سائیکل پر پورا ڈیٹا مٹا دیتا ہے (6)

2. ڈبل وی پی این روٹنگ فیچر جو ٹریفک کو دو الگ سرور نوڈز میں انکرپٹ کرتا ہے (7)

3. ملکیتی سافٹ ویئر ڈیفائنڈ نیٹ ورک جو تمام سرورز کو ایک متحد میش میں جوڑتا ہے (5)

6. اوبفسکیشن ٹیکنالوجی جو وی پی این دستخط چھپا کر عام HTTPS ٹریفک کی نقل کرتی ہے (8)

8. ایسا فیچر جو ٹنلز میں خلل ڈالے بغیر آپ کا بیرونی IP ایڈریس باقاعدگی سے بدلتا ہے (7)

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

4 افقی: خودکار حفاظتی فیچر جو وی پی این ڈراپ ہونے پر نیٹ ورک ٹریفک روک دیتا ہے (6 حروف):

5 افقی: اشتہارات، میل ویئر اور کوکی منظوری بینرز کو روکنے والا ایڈوانسڈ فلٹر (7 حروف):

7 افقی: اسپلٹ ٹنلنگ کی سہولت جو منتخب ایپلی کیشنز کو وی پی این بائی پاس کرنے دیتی ہے (8 حروف):

عمودی

1 عمودی: عارضی میموری والا سرور ہارڈ ویئر جو ہر پاور سائیکل پر پورا ڈیٹا مٹا دیتا ہے (6 حروف):

2 عمودی: ڈبل وی پی این روٹنگ فیچر جو ٹریفک کو دو الگ سرور نوڈز میں انکرپٹ کرتا ہے (7 حروف):

3 عمودی: ملکیتی سافٹ ویئر ڈیفائنڈ نیٹ ورک جو تمام سرورز کو ایک متحد میش میں جوڑتا ہے (5 حروف):

6 عمودی: اوبفسکیشن ٹیکنالوجی جو وی پی این دستخط چھپا کر عام HTTPS ٹریفک کی نقل کرتی ہے (8 حروف):

8 عمودی: ایسا فیچر جو ٹنلز میں خلل ڈالے بغیر آپ کا بیرونی IP ایڈریس باقاعدگی سے بدلتا ہے (7 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۔

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

الفاظ کی فہرست

کلینویب
صرفریم
ملٹیہاپ
کیموفلاج
بائیپاسر
کلسوئچ
نیکسس
روٹیٹنگ

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. کلینویب
B. صرفریم
C. ملٹیہاپ
D. کیموفلاج
E. بائیپاسر
F. کلسوئچ
G. نیکسس
H. روٹیٹنگ

	تعریفیں اور ملان کے خانے
	1. اوبفسکیشن ٹیکنالوجی جو وی پی این دستخط چھپا کر عام HTTPS ٹریفک کی نقل کرتی ہے۔
	2. خودکار حفاظتی فیچر جو وی پی این ڈراپ ہونے پر نیٹ ورک ٹریفک روک دیتا ہے۔
	3. اشتہارات، میل ویئر اور کوکی منظوری بینرز کو روکنے والا ایڈوانسڈ فلٹر۔
	4. اسپلٹ ٹنلنگ کی سہولت جو منتخب ایپلی کیشنز کو وی پی این بائی پاس کرنے دیتی ہے۔
	5. عارضی میموری والا سرور ہارڈ ویئر جو ہر پاور سائیکل پر پورا ڈیٹا مٹا دیتا ہے۔
	6. ایسا فیچر جو ٹنلز میں خلل ڈالے بغیر آپ کا بیرونی IP ایڈریس باقاعدگی سے بدلتا ہے۔
	7. ڈبل وی پی این روٹنگ فیچر جو ٹریفک کو دو الگ سرور نوڈز میں انکرپٹ کرتا ہے۔
	8. ملکیتی سافٹ ویئر ڈیفائنڈ نیٹ ورک جو تمام سرورز کو ایک متحد میش میں جوڑتا ہے۔

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. ن ی ک و ب ی ل
2. م ٹ پ ا ہ ی ل
3. ی ا ب پ ا ر س ئ
4. ک س س ن ی
5. ر ف م ص ی ر
6. ا ج و ل ک ف ی م
7. ئ ک و چ س ل
8. و ی گ ر ن ٹ ٹ

اضافی سرگرمی: تیزی سے سوچیں

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

1	Surfshark میں سیکیورٹی کی خصوصیات		
2	VPN کنکشن کے سست ہونے کی علامات		
3	آپ کے جانے پہچانے VPN پروٹوکولز کے نام		
4	وہ چیزیں جنہیں خفیہ کاری محفوظ رکھتی ہے		
5	عوامی Wi-Fi پر موجود خطرات		
6	وہ ممالک جو رازداری کے مضبوط قوانین کے لیے مشہور ہیں		
7	مضبوط پاس ورڈ بنانے کے طریقے		
8	وہ ڈیوائسز جن پر آپ Surfshark انسٹال کریں گے		
9	Surfshark کی کسٹمر سپورٹ سے پوچھنے کے سوالات		
10	اضافی سیکیورٹی کے لیے آن کی جانے والی سیٹنگز		
11	وہ چیزیں جو Surfshark آپ کے نیٹ ورک سے چھپا سکتا ہے		
12	VPN لیکس کی اقسام		
13	وہ ڈیٹا جو VPN کو کبھی محفوظ نہیں کرنا چاہیے		
14	اچھی VPN ایپ کو بیان کرنے والے الفاظ		
15	وہ چیزیں جنہیں آڈٹ جانچ سکتا ہے		

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: کیمپس اور دفتر کے فلٹرز کو عبور کرنا



منظرنامہ: ایک طالب علم کو معلوم ہوتا ہے کہ اس کی یونیورسٹی کیمپس کا Wi-Fi تمام معیاری OpenVPN اور WireGuard پورٹس کو بلاک کرتا ہے۔

بحث کا سوال: Surfshark کی کون سی خصوصیت طالب علم کو نیٹ ورک ایڈمنسٹریٹرز کی نظر میں آئے بغیر کنیکٹ ہونے کی اجازت دیتی ہے؟

کیس اسٹڈی 2: اعلیٰ خطرے والی صحافتی تحقیق



منظرنامہ: ایک تحقیقاتی صحافی کو حساس کارپوریٹ ریکارڈز کی تحقیق کرتے ہوئے نگرانی کے خلاف اضافی تحفظ درکار ہے۔

بحث کا سوال: سنگل سرور روٹنگ کے مقابلے میں Dynamic MultiHop برتر رازداری کیسے فراہم کرتا ہے؟

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

37	3	37	39	1	29	32	5	37	5	34	14	18	18	28	37	32			
38	4	1	36	15	2	37	14	1	11	16	1	14							

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: Surfshark CleanWeb کیا ہے؟

CleanWeb ایک مربوط سیکیورٹی خصوصیت ہے جو اشتہارات، ٹریکرز، میل ویئر اور فشنگ سائٹس کو بلاک کرتی ہے۔

Q2: صرف RAM پر چلنے والے سرورز کیا ہیں؟

صرف RAM سرورز عارضی میموری پر چلتے ہیں، یعنی میموری میں موجود ڈیٹا جب بھی سرورز ری بوٹ ہوں مٹ جاتا ہے۔

Q3: Surfshark MultiHop کیا ہے؟

MultiHop (Double VPN) آپ کے انٹرنیٹ کنکشن کو دو مختلف سرور مقامات کے ذریعے روٹ اور خفیہ کرتا ہے۔

Q4: Camouflage Mode کیسے کام کرتا ہے؟

کیموفلاج موڈ VPN ٹریفک کو مبہم بناتا ہے تاکہ آپ کا ISP یہ نہ جان سکے کہ آپ VPN استعمال کر رہے ہیں۔

Q5: Bypasser فیچر کیا ہے؟

Bypasser، Surfshark کا اسپلٹ ٹنلنگ ٹول ہے جو مخصوص ایپس یا ویب سائٹس کو VPN کو بائی پاس کرنے دیتا ہے۔

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 Surfshark میں کل سوئچ موجود ہے؟

ہاں، VPN اچانک ٹوٹنے پر Kill Switch آپ کو انٹرنیٹ سے منقطع کر دیتا ہے۔

Q7: Surfshark کون سا خفیہ کاری کا معیار استعمال کرتا ہے؟

Surfshark AES-256-GCM اور ChaCha20 استعمال کرتا ہے، اور اپنے نئے Dausos پروٹوکول پر AEGIS-256X2 بھی استعمال کرتا ہے۔

Q8: کیا Surfshark کی نو لاگز پالیسی کا آڈٹ ہوا ہے؟

جی ہاں، Deloitte نے 2023 میں اور دوبارہ 2025 میں Surfshark کی نو لاگز پالیسی کی تصدیق کی۔

Q9: Surfshark Nexus کیا ہے؟

Nexus ایک جدید SDN آرکیٹیکچر ہے جو زیادہ ہموار روٹنگ کے لیے تمام سرورز کو ایک متحد نیٹ ورک میں جوڑتا ہے۔

Q10: IP Rotator فیچر کیا ہے؟

IP Rotator آپ کے VPN سیشن کو منقطع کیے بغیر ہر چند منٹ بعد آپ کا IP ایڈریس خود بخود تبدیل کرتا 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: Dynamic MultiHop روایتی Double VPN سے کیسے مختلف ہے؟

Dynamic MultiHop آپ کو دنیا بھر میں داخلی اور خارجی سرورز کا کوئی بھی امتزاج حسبِ ضرورت بنانے دیتا ہے۔

Q2: کیا CleanWeb 2.0 براؤزر ایکسٹینشنز پر کام کرتا ہے؟

جی ہاں، CleanWeb 2.0 Chrome/ Firefox کے اندر ویڈیو اشتہارات، کوکی رضامندی پاپ اپس اور الرٹ بینرز کو بلاک کرتا ہے۔

Q3: سیکیورٹی سوٹ میں Alternative ID کیا ہے؟

Alternative ID منفرد ذاتی فرضی نام، ای میل ایڈریس اور فون ماسک بناتا ہے۔

Q4: Surfshark DNS لیکس کو کیسے روکتا ہے؟

Surfshark ڈومین کی تمام درخواستوں کو ہر نوڈ پر اپنے نجی DNS سرورز کے ذریعے روٹ کرتا ہے۔

Q5: کیا Surfshark موبائل پر ChaCha20 خفیہ کاری کو سپورٹ کرتا ہے؟

جی ہاں، Android اور iOS پر WireGuard بہتر موبائل کارکردگی کے لیے ChaCha20-Poly1305 استعمال کرتا ہے۔

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: Surfshark میں NoBorders موڈ کیا ہے؟

NoBorders پابندی والے نیٹ ورک ماحول کا خودکار طور پر پتا لگاتا ہے اور خصوصی سرورز فراہم کرتا ہے۔

Q7: Surfshark براؤزر ایکسٹینشنز کے سیکیورٹی آڈٹس کس نے کیے؟

آزاد سائبر سیکیورٹی فرم Cure53 نے براؤزر ایکسٹینشنز اور سرور سسٹمز کے آڈٹس مکمل کیے۔

Q8: Surfshark IPv6 لیکس سے تحفظ کیسے دیتا ہے؟

Surfshark IPv6 ٹریفک کو محفوظ طریقے سے روٹ کرتا ہے یا کسی بھی غیر خفیہ لیکیج کو روکنے کے لیے اسے محفوظ طریقے سے محدود کر دیتا ہے۔

Q9: Surfshark کا قانونی دائرہ اختیار کہاں قائم ہے؟

Surfshark نیدرلینڈز کے قانون کے تحت کام کرتا ہے اور سخت GDPR یورپی رازداری معیارات کی پابندی کرتا ہے۔

Q10: کیا Surfshark ٹو فیکٹر تصدیق (2FA) کو سپورٹ کرتا ہے؟

جی ہاں، اور Surfshark One ایک 2FA لاک شامل کرتا ہے تاکہ صرف آپ ہی خصوصیات کی سیٹنگز تبدیل کر سکیں۔

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

1. Surfshark کا کہنا ہے کہ اس کا پورا 4,500+ سرور نیٹ ورک بغیر ڈسک کے، غیر مستقل صرف-RAM ہارڈ ویئر پر چلتا ہے۔

2. VPN بصیرت

2. بگ فور فرم Deloitte نے 2023 میں اور دوبارہ نومبر 2025 میں Surfshark کی نو لاگز پالیسی کی تصدیق کی۔

3. VPN بصیرت

3. ملکیتی Nexus آرکیٹیکچر تمام عالمی سرورز کو متحرک سافٹ ویئر ڈیفائنڈ نیٹ ورک میں جوڑتا ہے۔

4. VPN بصیرت

4. Rotating IP آپ کا IP ایڈریس تقریباً ہر پانچ منٹ بعد VPN کنکشن ٹوٹے بغیر بدل دیتا ہے۔

5. VPN بصیرت

5. CleanWeb 2.0 براؤزرز میں مداخلت کرنے والے کوکی کنسنٹ پاپ اپس اور ویڈیو اشتہارات کو براہِ راست بلاک کرتا ہے۔

6. VPN بصیرت

6. Dynamic MultiHop صارفین کو 100 ممالک میں حسبِ ضرورت دوہرے سرور انکرپشن راستے بنانے کی اجازت دیتا ہے۔

7. VPN کی بصیرت

7. کیموفلاج موڈ VPN ہیڈر کے نشانات ہٹا دیتا ہے، جس سے ٹریفک عام HTTPS سے الگ پہچانی نہیں جاتی۔

8. VPN کی بصیرت

8. Alternative ID ڈیٹا بیس لیکس سے صارفین کو بچانے کے لیے عارضی فرضی نام اور ای میل ماسک بناتا ہے۔

9. VPN کی بصیرت

9. Surfshark، WireGuard پروٹوکولز پر ChaCha20 کے ساتھ AES-256-GCM سمیٹرک خفیہ کاری نافذ کرتا ہے۔

10. VPN بصیرت

10. NoBorders موڈ پابندی والے نیٹ ورکس پر خود بخود فعال ہو جاتا ہے تاکہ مضبوط ٹنلنگ رسائی فراہم کرے۔

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] 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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 **مربوط مواد بلاکر** اشتہارات اور میل ویئر سے دفاع — درست جواب: **B**

تدریسی نوٹ

Surfshark، CleanWeb کا مربوط سیکیورٹی فلٹر ہے جو نیٹ ورک کی سطح پر اشتہارات، ٹریکر ڈومینز، فشنگ ویب سائٹس اور نقصان دہ URL اسکرپٹس کو بلاک کرتا ہے۔ حوالہ: CleanWeb Security Specs۔

2 **100% صرف-RAM انفراسٹرکچر** RAM آرکیٹیکچر — درست جواب: **B**

تدریسی نوٹ

Surfshark صرف RAM پر چلنے والے سرورز استعمال کرتا ہے، اس لیے سرور میموری میں موجود ڈیٹا سرور بند یا ری بوٹ ہونے پر مٹ جاتا ہے۔ حوالہ: Cure53 Infrastructure Audit۔

3 **MultiHop ڈبل ٹنلنگ** ملٹی ہاپ VPN — درست جواب: **B**

تدریسی نوٹ

MultiHop (Double VPN) ٹریفک کی باہمی ربط والے حملوں سے بچنے کے لیے ٹریفک کو الگ الگ ممالک کے دو مختلف سرور نوڈز کے ذریعے خفیہ کرتا ہے۔ حوالہ: Surfshark MultiHop Guide۔

4 **کیموفلاج موڈ کی اوبفسکیشن** اوبفسکیشن — درست جواب: **B**

تدریسی نوٹ

کیموفلاج موڈ OpenVPN پیکٹ ہیڈرز میں ترمیم کرتا ہے تاکہ VPN ٹریفک معیاری HTTPS ٹریفک کی طرح نظر آئے اور سخت فائر وال کی پابندیاں عبور کی جا سکیں۔ حوالہ: Surfshark Stealth Whitepaper۔

5 **بائی پاسر اسپلٹ ٹنلنگ** اسپلٹ ٹنلنگ — درست جواب: **B**

تدریسی نوٹ

Surfshark، Bypasser کا اسپلٹ ٹنلنگ ٹول ہے جو صارفین کو مخصوص ایپس یا ویب سائٹس منتخب کرنے دیتا ہے تاکہ انہیں ان کے باقاعدہ ISP کنکشن سے براہ راست روٹ کیا جائے۔ حوالہ: Surfshark Client Features۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 غیر مستقل میموری ڈیٹا کا خاتمہ — سرور سیکیورٹی — درست جواب: درست

تدریسی نوٹ

صرف RAM سرورز مستقل ہارڈ ڈرائیوز پر کوئی ڈیٹا محفوظ نہیں کرتے؛ ہارڈ ویئر ری بوٹ کرنے سے تمام آپریشنل میموری فوراً صاف ہو جاتی ہے۔ حوالہ: RAM Server Architecture۔

7 کیموفلاج موڈ سے ISP سے چھپاؤ — ٹریفک کو چھپانا — درست جواب: درست

تدریسی نوٹ

کیموفلاج موڈ OpenVPN پروٹوکول کے دستخط ہٹا دیتا ہے، جس سے ISPs یہ معلوم نہیں کر پاتے کہ صارف VPN ٹنل سے جڑا ہوا ہے۔ حوالہ: Deep Packet Inspection Guide۔

8 CleanWeb 2.0 براؤزر ایکسٹینشنز — براؤزر ایکسٹینشن — درست جواب: درست

تدریسی نوٹ

CleanWeb 2.0 براؤزر ایکسٹینشنز کے اندر کام کرتا ہے تاکہ کوکی رضامندی کے پاپ اپس، ویڈیو اشتہارات اور نقصان دہ ری ڈائریکٹ اسکرپٹس کو رینل ٹائم میں بلاک کرے۔ حوالہ: CleanWeb 2.0 Release Notes۔

9 کنکشن لاگز کی صفر برقراری — نو لاگز پالیسی — درست جواب: غلط

تدریسی نوٹ

Surfshark ایک سخت، آزادانہ طور پر آڈٹ شدہ زیرو لاگز پالیسی برقرار رکھتا ہے، اور کوئی IP ایڈریس، کنکشن ٹائم اسٹیمپ یا بینڈ وڈتھ لاگ ریکارڈ نہیں کرتا۔ حوالہ: Deloitte No-Logs Audit۔

10 Nexus IP ڈائنامک روٹیشن — Nexus نیٹ ورک — درست جواب: درست

تدریسی نوٹ

Surfshark Nexus سافٹ ویئر ڈیفائنڈ نیٹ ورک فعال VPN کنکشن منقطع کیے بغیر ہر چند منٹ بعد صارفین کے IP ایڈریس متحرک طور پر بدلتا ہے۔ حوالہ: Surfshark Nexus Architecture۔

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

C 1. کلین ویب	D 2. صرف ریم	G 3. ملٹی ہاپ	F 4. کیموفلاج
B 5. بائی پاسر	A 6. کل سوئچ	H 7. Nexus نیٹ	E 8. گردشی

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 کلین ویب	2 صرف ریم	3 ملٹی ہاپ	4 کیموفلاج
5 بائی پاسر	6 نیکسس		

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

1 D – کیموفلاج	2 F – کلسوئچ	3 A – کلینویب	4 E – بائیپاسر
5 B – صرفریم	6 H – روٹیٹنگ	7 C – ملٹیہاپ	8 G – نیکسس

اساتذہ کے لیے بحث کے نوٹس

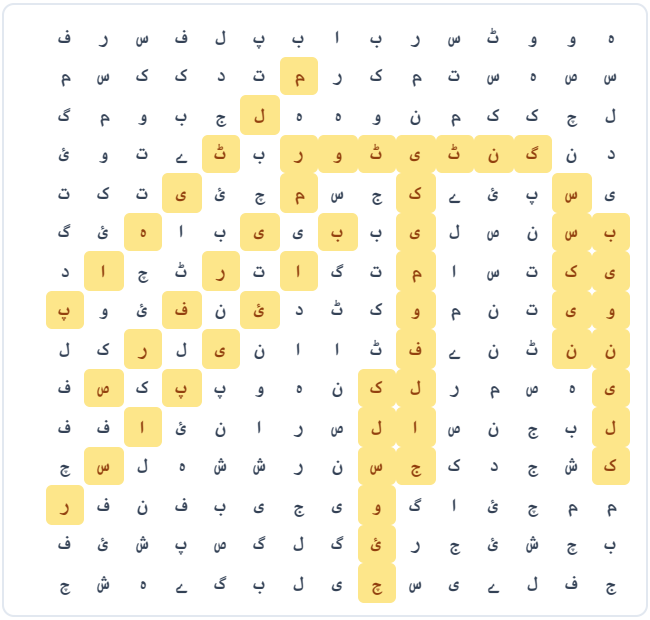
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ کلین ویب، صرف ریم اور ملٹی ہاپ کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

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

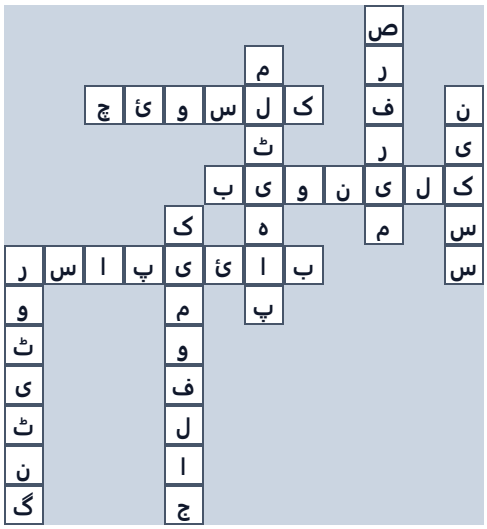
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

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

4 افقی: کلسوئچ خودکار حفاظتی فیچر جو وی پی این ڈراپ ہونے پر نیٹ ورک ٹریفک روک دیتا ہے (6 حروف)

5 افقی: کلینویب اشتہارات، میل ویئر اور کوکی منظوری بینرز کو روکنے والا ایڈوانسڈ فلٹر (7 حروف)

7 افقی: بائیپاسر اسپلٹ ٹنلنگ کی سہولت جو منتخب ایپلی کیشنز کو وی پی این بائی پاس کرنے دیتی ہے (8 حروف)

عمودی

1 عمودی: صرفریم عارضی میموری والا سرور ہارڈ ویئر جو ہر پاور سائیکل پر پورا ڈیٹا مٹا دیتا ہے (6 حروف)

2 عمودی: ملٹیہاپ ڈبل وی پی این روٹنگ فیچر جو ٹریفک کو دو الگ سرور نوڈز میں انکرپٹ کرتا ہے (7 حروف)

3 عمودی: نیکسس ملکیتی سافٹ ویئر ڈیفائنڈ نیٹ ورک جو تمام سرورز کو ایک متحد میش میں جوڑتا ہے (5 حروف)

6 عمودی: کیموفلاج اوبفسکیشن ٹیکنالوجی جو وی پی این دستخط چھپا کر عام HTTPS ٹریفک کی نقل کرتی ہے (8 حروف)

8 عمودی: روٹیٹنگ ایسا فیچر جو ٹنلز میں خلل ڈالے بغیر آپ کا بیرونی IP ایڈریس باقاعدگی سے بدلتا ہے (7 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. نیکوبیل — کلینویب
2. مٹپاہیل — ملٹیہاپ
3. یابپارسئ — بائیپاسر
4. کسسنی — نیکسس
5. رفمصیر — صرفریم
6. اجولکفیم — کیموفلاج
7. ئکوچسل — کلسوئچ
8. ویگرنٹٹ — روٹیٹنگ

خفیہ سائفر چیلنج کی کلید

"نیکسس روٹیٹنگ آئی پی رازداری بڑھاتے"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: کیمپس اور دفتر کے فلٹرز کو عبور کرنا

استاد کا حل

گریڈنگ روبرک اور حل کی ہدایات

- منظرنامے کا تجزیہ: ایک طالب علم کو معلوم ہوتا ہے کہ اس کی یونیورسٹی کیمپس کا Wi-Fi تمام معیاری OpenVPN اور WireGuard پورٹس کو بلاک کرتا ہے۔
- مرکزی سوال: Surfshark کی کون سی خصوصیت طالب علم کو نیٹ ورک ایڈمنسٹریٹرز کی نظر میں آئے بغیر جڑنے کی اجازت دیتی ہے؟
- تجویز کردہ حکمت عملی اور حل: Camouflage Mode (OpenVPN) فعال کریں، جو VPN میٹا ڈیٹا کو چھپاتا ہے تاکہ فائر والز کو عام HTTPS براؤزنگ نظر آئے۔

B کیس اسٹڈی 2: اعلیٰ خطرے والی صحافتی تحقیق

استاد کا حل

گریڈنگ روبرک اور حل کی ہدایات

- منظرنامے کا تجزیہ: ایک تحقیقاتی صحافی کو حساس کارپوریٹ ریکارڈز پر تحقیق کے دوران نگرانی کے خلاف اضافی تحفظ درکار ہے۔
- مرکزی سوال: Dynamic MultiHop واحد سرور روٹنگ کے مقابلے میں بہتر رازداری کیسے فراہم کرتا ہے؟
- تجویز کردہ حکمت عملی اور حل: Dynamic MultiHop ٹریفک کو دو ممالک میں انٹری اور ایگزٹ سرورز کے ذریعے روٹ کرتا ہے، اس لیے کوئی ایک سرور صارف کو بے نقاب نہیں کر سکتا۔