نام: _____ تاریخ: _____ نمره: _____

WireGuard در برابر OpenVPN کاربرگ

مقایسهٔ پروتکل‌های WireGuard و OpenVPN، اندازهٔ کد، سرعت و استانداردهای رمزنگاری

مرور یادگیری VPN

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.

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 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

- پیچیدگی کد و سرعت ممیزی پروتکل‌ها را مقایسه کنید.
- مزایای عملکردی اجرا در فضای هسته را تحلیل کنید.
- رمزهای OpenSSL را با رمزنگاری مدرن WireGuard مقایسه کنید.
- جفت‌کلیدهای عمومی و خصوصی را برای دست‌دهی همتایان راه‌اندازی کنید.
- ترافیک VPN را از طریق پورت‌های دیوار آتش TCP و UDP هدایت کنید.

دستورالعمل‌های کاربرگ مقایسهٔ پروتکل‌ها

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 ممیزی پروتکل‌های مدرن به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

WIREGUARD در برابر OPENVPN (مقدمه)

انتخاب پروتکل VPN مستلزم ایجاد توازن بین سرعت و گزینه‌های پیکربندی است. OpenVPN دهه‌هاست استاندارد بوده و انعطاف‌پذیری پیکربندی TCP/UDP را ارائه می‌دهد. WireGuard جایگزینی مدرن است که مستقیماً در فضای هسته اجرا می‌شود و تنها 4,000 خط کد دارد. درک تفاوت پروتکل‌ها برای بهینه‌سازی شبکه‌های ایمن شما کلیدی است.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. اندازهٔ تقریبی کدبیس پروتکل WireGuard چقدر است؟

- A. تقریباً 70,000 خط
- B. بیش از 100,000 خط
- C. کمتر از 1,000 خط
- D. حدود 4,000 خط

2 2. WireGuard در کدام فضای سیستم‌عامل اجرا می‌شود؟

- A. فضای کاربر
- B. فضای هسته
- C. فضای برنامه
- D. فضای مجازی

3 3. OpenVPN عمدتاً به کدام کتابخانهٔ رمزنگاری متکی است؟

- A. ChaCha20-Poly1305
- B. کتابخانهٔ رمزنگاری OpenSSL
- C. چارچوب پروتکل Noise
- D. کدگذاری متنی ساده DES

4 4. مزیت کلیدی WireGuard نسبت به OpenVPN از نظر عملکرد چیست؟

- A. دست‌دهی‌های اتصال سریع‌تر و تأخیر کمتر
- B. دور زدن نیاز به نشانی‌های IP عمومی
- C. پشتیبانی بومی داخلی از دایال‌آپ قدیمی
- D. سربار باتری صفر در دستگاه‌های موبایل

5 5. WireGuard اتصال‌های همتا را چگونه احراز هویت می‌کند؟

- A. با تبادل گذرواژه‌های استاندارد کاربران
- B. با تأیید گواهی‌های ثبت دامنه
- C. با استفاده از جفت‌کلیدهای عمومی و خصوصی ایستا
- D. با بررسی شماره‌های سریال سخت‌افزار

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. کدبیس فشردهٔ WireGuard ممیزی آن را به‌طور چشمگیری آسان‌تر می‌کند.

درست نادرست

7 پرسش 7

7. OpenVPN عموماً از WireGuard سریع‌تر است، زیرا در فضای هسته اجرا می‌شود.

درست نادرست

8 پرسش 8

8. OpenVPN بسیار قابل پیکربندی است و از هر دو پروتکل UDP و TCP پشتیبانی می‌کند.

درست نادرست

9 پرسش 9

9. WireGuard از رمزنگاری مدرنی مانند ChaCha20 برای رمزگذاری سریع بسته‌ها استفاده می‌کند.

درست نادرست

10 پرسش 10

10. WireGuard برای احراز هویت به راه‌اندازی‌های پیچیدهٔ مرجع صدور گواهی نیاز دارد.

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 _____ مستقیماً درون هستهٔ سیستم‌عامل اجرا می‌شود.
2. پروتکل قدیمی _____ به کتابخانهٔ رمزنگاری OpenSSL متکی است.
3. اجرای کد در _____ سربار تعویض زمینه را کاهش می‌دهد.
4. OpenVPN در _____ اجرا می‌شود و بسته‌ها را از طریق رابط‌های مجازی مسیریابی می‌کند.
5. WireGuard برای شناسایی همتاهای اتصال از چند _____ عمومی و خصوصی استفاده می‌کند.
6. اندازهٔ کوچک کدبیس، _____ امنیتی نرم‌افزار را بهبود می‌بخشد.

بانک واژگان

انتقال | اوپن‌اس‌اس‌ال | جفت کلید | فضای کاربر | فضای هسته | ممیزی‌پذیری | OpenVPN | WireGuard

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم شبکه

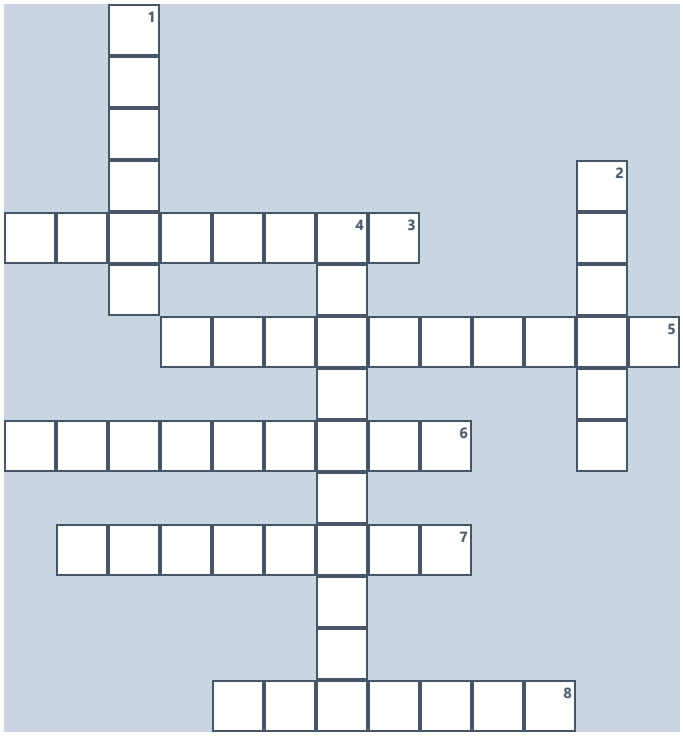
تطبیق تعاریف

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	ناحیهٔ اجرا که OpenVPN در آن اجرا می‌شود و سربار تعویض زمینه ایجاد می‌کند.
2. OpenVPN	B	اندازهٔ فشردهٔ پایگاه کد WireGuard که ممیزی آن را بسیار آسان‌تر می‌کند.
3. فضای هسته	C	کتابخانهٔ رمزنگاری که OpenVPN برای الگوریتم‌های رمز به آن متکی است.
4. فضای کاربر	D	پروتکل‌های انتقالی که OpenVPN پشتیبانی می‌کند؛ خود WireGuard فقط روی UDP اجرا می‌شود.
5. 4,000 خط	E	ناحیهٔ اجرای سطح سیستم‌عامل که WireGuard برای سرعت در آن اجرا می‌شود.
6. OpenSSL	F	توکن‌های نامتقارن که WireGuard برای تأیید اتصال همتاها از آن‌ها استفاده می‌کند.
7. جفت‌کلید	G	پروتکل VPN نوین که برای سرعت بالا و ممیزی ساده کد طراحی شده است.
8. TCP/UDP	H	پروتکل قدیمی و مقاوم با کدبیس پیکربندی بزرگ و پیچیده.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

3. پروتکل مدرن VPN که برای سرعت بالا و ممیزی ساده کد طراحی شده است (8)

5. پروتکل قدیمی و مقاوم با کدبیس پیکربندی بزرگ و پیچیده (10)

6. ناحیهٔ اجرایی که OpenVPN در آن اجرا می‌شود و سربار تعویض زمینه ایجاد می‌کند (9)

7. ناحیهٔ اجرای سیستم‌عامل که WireGuard برای سرعت در آن اجرا می‌شود (8)

8. توکن‌های نامتقارن که WireGuard برای تأیید اتصال همتاها به کار می‌برد (7)

عمودی

1. پروتکل‌های لایهٔ حمل که OpenVPN پشتیبانی می‌کند؛ خود WireGuard فقط روی UDP اجرا می‌شود (6)

2. اندازهٔ فشردهٔ کدبیس WireGuard که ممیزی آن را بسیار آسان‌تر می‌کند (6)

4. کتابخانهٔ رمزنگاری که OpenVPN برای الگوریتم‌های رمز به آن متکی است (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

3 افقی: پروتکل مدرن VPN که برای سرعت بالا و ممیزی ساده کد طراحی شده است (8 حرف):

5 افقی: پروتکل قدیمی و مقاوم با کدبیس پیکربندی بزرگ و پیچیده (10 حرف):

6 افقی: ناحیهٔ اجرایی که OpenVPN در آن اجرا می‌شود و سربار تعویض زمینه ایجاد می‌کند (9 حرف):

7 افقی: ناحیهٔ اجرای سیستم‌عامل که WireGuard برای سرعت در آن اجرا می‌شود (8 حرف):

8 افقی: توکن‌های نامتقارن که WireGuard برای تأیید اتصال همتاها به کار می‌برد (7 حرف):

عمودی

1 عمودی: پروتکل‌های لایهٔ حمل که OpenVPN پشتیبانی می‌کند؛ خود WireGuard فقط روی UDP اجرا می‌شود (6 حرف):

2 عمودی: اندازهٔ فشردهٔ کدبیس WireGuard که ممیزی آن را بسیار آسان‌تر می‌کند (6 حرف):

4 عمودی: کتابخانهٔ رمزنگاری که OpenVPN برای الگوریتم‌های رمز به آن متکی است (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.

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

فهرست واژگان

وایرگارد
اوپنوپیان
فضایهسته
فضایکاربر
کدکوچک
اوپناساسال
جفتکلید
انتقال

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. کتابخانهٔ رمزنگاری که OpenVPN برای الگوریتم‌های رمز به آن متکی است.
B. اوپنوپیان	2. ناحیهٔ اجرای سیستم‌عامل که WireGuard برای سرعت در آن اجرا می‌شود.
C. فضایهسته	3. پروتکل قدیمی و مقاوم با کدبیس پیکربندی بزرگ و پیچیده.
D. فضایکاربر	4. توکن‌های نامتقارن که WireGuard برای تأیید اتصال همتاها به کار می‌برد.
E. کدکوچک	5. پروتکل‌های لایهٔ حمل که OpenVPN پشتیبانی می‌کند؛ خود WireGuard فقط روی UDP اجرا می‌شود.
F. اوپناساسال	6. اندازهٔ فشردهٔ کدبیس WireGuard که ممیزی آن را بسیار آسان‌تر می‌کند.
G. جفتکلید	7. پروتکل مدرن VPN که برای سرعت بالا و ممیزی ساده کد طراحی شده است.
H. انتقال	8. ناحیهٔ اجرایی که OpenVPN در آن اجرا می‌شود و سربار تعویض زمینه ایجاد می‌کند.

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 ف ه ض ت س ه ا _____
3. ک ک و ک چ د _____
4. د ف ل ک ی ج ت _____
5. ی ی ن و ن پ و ا ا پ _____
6. ب ی ض ر ا ف ک ر ا _____
7. و ن ا ا س س ا ل ا پ _____
8. ت ل ا ا ق ن _____

فعالیت تکمیلی: سریع فکر کن

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

1	دلایل انتخاب WireGuard		
2	وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد		
3	دلایل انتخاب OpenVPN		
4	دلایل استفاده از VPN در سفر		
5	چیزهایی که ارائه‌دهندهٔ اینترنت شما می‌تواند ببیند		
6	روش‌های تشخیص شبکهٔ Wi-Fi جعلی		
7	افسانه‌ها دربارهٔ VPNها		
8	جاهایی که از VPN استفاده می‌کنید		
9	چیزهای سریع در زندگی روزمره		
10	چیزهایی که VPN نمی‌تواند از آن‌ها محافظتتان کند		
11	چیزهایی که بررسی کد را آسان‌تر می‌کنند		
12	چیزهایی که یک VPN می‌تواند پنهان کند		
13	تفاوت‌های WireGuard و OpenVPN		
14	واژه‌های مرتبط با حریم خصوصی		
15	نام‌های رمزگذاری که می‌شناسید		

ایستگاه بررسی 8: مطالعات موردی VPN

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

سارا (دانشجوی کافه)

👩‍💻 «سلام! من در Wi-Fi کافه‌ام و برنامهٔ VPN من اجازه می‌دهد WireGuard یا OpenVPN را انتخاب کنم. وقتی بین شبکهٔ کافه و هات‌اسپات گوشی‌ام جابه‌جا می‌شوم، تماس‌های تصویری‌ام مدام قطع می‌شود. کدام پروتکل را انتخاب کنم و چرا این جابه‌جایی را بهتر مدیریت می‌کند؟»

Alex (دانشجوی مسافر)

👨‍💻 «من خارج از کشورم و در شبکهٔ هتلی هستم که به نظر می‌رسد بیشتر ترافیک VPN را مسدود می‌کند. WireGuard اصلاً وصل نمی‌شود، اما باید به منابع مدرسه‌ام در کشورم دسترسی داشته باشم. احتمالاً چه چیزی مسدود می‌شود و OpenVPN چگونه می‌تواند به عبور من کمک کند؟»

ایستگاه بررسی 9: رمزگشایی

برای تکمیل آموزش ممیزی پروتکل، این پیام پنهان دربارهٔ اجرا در فضای هسته 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

1	2	29	1	32	3	32	30	29	3	30	1	32	1	24	4	12	1

21	32	12	15	27	29	30	4

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 پروتکل‌ها اهمیت دارند؟

پروتکل تعیین می‌کند VPN شما چگونه تونل خود را می‌سازد، کدام رمزنگاری از داده‌هایتان محافظت می‌کند، و اتصال و اتصال مجدد با چه سرعتی انجام می‌شود. WireGuard و OpenVPN دو پروتکل متن‌باز هستند که بیشتر برنامه‌های VPN ارائه می‌دهند و میان سادگی، سرعت و قابلیت پیکربندی مصالحه‌های متفاوتی دارند.

Q3: آیا یکی از آن‌ها خصوصی‌تر از دیگری است؟

هیچ‌کدام از این دو پروتکل شما را ناشناس نمی‌کنند. هر دو ترافیک تونل را با رمزهای قوی رمزگذاری می‌کنند؛ حریم خصوصی شما بیشتر به این بستگی دارد که ارائه‌دهندهٔ VPN چه چیزی را ثبت می‌کند و کلیدها، حساب‌ها و سرورها را چگونه مدیریت می‌کند.

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: آیا هر دو متن‌باز هستند؟

بله. WireGuard و نسخهٔ community از OpenVPN هر دو کد منبع خود را منتشر می‌کنند، بنابراین پژوهشگران مستقل می‌توانند آن‌ها را بررسی کنند. کد کوچک WireGuard بررسی کامل را بسیار سریع‌تر می‌کند.

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: کدام یک سریع‌تر است؟

WireGuard معمولاً سریع‌تر است: در هسته اجرا می‌شود، از رمزگذاری سبک ChaCha20-Poly1305 استفاده می‌کند و دست‌دهی را سریع تکمیل می‌کند. OpenVPN سربار بیشتری دارد، اما سرعت واقعی به بار سرور و فاصله هم بستگی دارد.

Q7: آیا هر دو می‌توانند روی TCP و UDP اجرا شوند؟

خیر. OpenVPN می‌تواند روی UDP یا TCP اجرا شود و حالت TCP در شبکه‌هایی که UDP را مسدود می‌کنند کمک می‌کند. WireGuard بسته‌های خود را فقط روی UDP می‌فرستد، بنابراین در شبکه‌هایی که فقط TCP را اجازه می‌دهند ممکن است کار نکند. [4]

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 WireGuard و OpenVPN را روی گوشی خود استفاده کنم؟

بله. WireGuard چندسکویی است و برنامه‌هایی برای iOS، Linux، macOS، Windows و Android دارد و کلاینت‌های OpenVPN نیز برای همین سیستم‌ها وجود دارند. بیشتر برنامه‌های VPN اجازه می‌دهند یکی از این دو را انتخاب کنید. [1]

Q10: چرا WireGuard این‌قدر کوچک است؟

WireGuard به‌جای گزینه‌های متعدد، از یک مجموعهٔ ثابت از رمزهای مدرن پشتیبانی می‌کند. پیاده‌سازی لینوکسی آن به کمتر از 4,000 خط کد نیاز دارد و همین ممیزی آن را از کدبیس‌های بزرگ‌تر VPN آسان‌تر می‌کند. [3]

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 WireGuard، OpenVPN 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: WireGuard از کدام رمزها استفاده می‌کند؟

WireGuard برای رمزگذاری از ChaCha20 با Poly1305، برای تبادل کلید از Curve25519، برای درهم‌سازی از BLAKE2s و برای دست‌دهی از چارچوب Noise استفاده می‌کند. مذاکرهٔ رمز وجود ندارد، بنابراین کاربران نمی‌توانند گزینهٔ ضعیفی انتخاب کنند. [2]

Q3: OpenVPN از کدام رمزها و کتابخانه‌ها می‌تواند استفاده کند؟

OpenVPN با کتابخانهٔ OpenSSL یکپارچگی عمیقی دارد و برای تبادل کلید از TLS استفاده می‌کند. مدیران می‌توانند رمزهای کانال داده مانند AES-256-GCM را انتخاب کنند که انعطاف‌پذیری را بیشتر می‌کند، اما جا برای تنظیمات ضعیف را هم افزایش می‌دهد. [4]

Q4: هر پروتکل چگونه همتایان را احراز هویت می‌کند؟

همتاهای WireGuard یکدیگر را با کلیدهای عمومی ایستا شناسایی می‌کنند، مانند تبادل کلیدهای SSH، و هر کلید به IPهای مجاز تونل نگاشت می‌شود. OpenVPN معمولاً به یک مرجع صدور گواهی با گواهی‌های X.509 متکی است که اغلب با نام کاربری و گذرواژه ترکیب می‌شود.

Q5: مبهم‌سازی چگونه مسدودسازی VPN را دور می‌زند؟

مبهم‌سازی (یا «Stealth VPN») ترافیک VPN را طوری پنهان می‌کند که شبیه ترافیک HTTPS معمولی (پورت 443) به نظر برسد. این کار می‌تواند به عبور از بازرسی عمیق بسته (DPI) کمک کند 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: وقتی از Wi-Fi به موبایل تغییر می‌دهم چه اتفاقی می‌افتد؟

WireGuard بدون اتصال (connectionless) است: بسته‌ها را از نشانی جدید می‌فرستد و تونل پس از یک دست‌دهی سریع ادامه می‌یابد. OpenVPN وضعیت نشست را نگه می‌دارد، بنابراین تغییر شبکه ممکن است به اتصال مجدد نیاز داشته باشد که کمی بیشتر طول می‌کشد.

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: اگر WireGuard سریع‌تر است، آیا OpenVPN هنوز انتخاب خوبی است؟

بله. OpenVPN پخته و پرکاربرد است، وقتی UDP مسدود باشد روی TCP اجرا می‌شود و از راه‌اندازی‌های سازمانی مبتنی بر گواهی پشتیبانی می‌کند. بسیاری از ارائه‌دهندگان هر دو پروتکل را ارائه می‌دهند تا اگر یکی مسدود یا کند بود کاربران بتوانند تغییر دهند.

Q9: از کدام درگاه‌ها استفاده می‌کنند؟

پورت استاندارد OpenVPN برابر 1194 است، اما می‌توان آن را به هر پورت UDP یا TCP، از جمله 443، منتقل کرد. WireGuard روی یک پورت UDP گوش می‌دهد که در پیکربندی آن تعیین می‌شود؛ 51820 پورتی است که در نمونه‌های رسمی آن استفاده شده است.

Q10: راه‌اندازی دستی کدام پروتکل آسان‌تر است؟

WireGuard معمولاً ساده‌تر است: یک جفت کلید تولید کنید، کلیدهای عمومی را مبادله کنید و IPهای مجاز را فهرست کنید. OpenVPN به گواهی‌ها، یک CA و گزینه‌های بیشتری نیاز دارد، هرچند نمایه‌های .ovpn همه را در یک فایل جمع می‌کنند.

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) توسط گروهی از فروشندگان از جمله Microsoft توسعه یافت و در ژوئیهٔ 1999 برای پشتیبانی از VPNهای دسترسی راه‌دور به‌صورت RFC 2637 منتشر شد. [6]

2. دو انتقال

OpenVPN می‌تواند تونل خود را روی UDP یا TCP حمل کند و در حالت TLS کانال‌های کنترل و داده‌اش یک پورت واحد را به اشتراک می‌گذارند. [4]

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. رمزنگاری مدرن

WireGuard ChaCha20، Poly1305، Curve25519، BLAKE2s، SipHash24 و HKDF را درون چارچوب پروتکل Noise ترکیب می‌کند و هیچ انتخاب رمزی برای کاربران باقی نمی‌گذارد که بتوانند اشتباه انتخاب کنند. [2]

5. OPENSSL درون OPENVPN

OpenVPN با کتابخانهٔ OpenSSL یکپارچگی عمیقی دارد و بسیاری از قابلیت‌های رمزنگاری خود، از جمله TLS مورد استفاده برای تبادل کلید، را از آن می‌گیرد. [4]

6. بازرسی عمیق بسته

بازرسی عمیق بسته (DPI) محتوای بسته‌ها و الگوهای ترافیک را بررسی می‌کند، نه فقط سرآیندها را، و برخی دیوارهای آتش از آن برای شناسایی و مسدود کردن پروتکل‌های رایج VPN استفاده می‌کنند.

7. کلیدهای سبک SSH

اتصال‌های WireGuard با تبادل کلیدهای عمومی ساده راه‌اندازی می‌شوند، درست مانند تبادل کلیدهای SSH، و به مرجع صدور گواهی نیازی نیست. [1]

8. چندسکویی

WireGuard ابتدا برای هستهٔ لینوکس منتشر شد و اکنون برای ویندوز، macOS، BSD، iOS و اندروید در دسترس است، بنابراین همان پروتکل روی بیشتر دستگاه‌ها کار می‌کند. [1]

9. محرمانگی پیشرو

WireGuard دست‌دهی Noise_IK خود را هر چند دقیقه تکرار می‌کند تا کلیدهای نشست متقارن را بچرخاند و حتی اگر کلید بلندمدت بعداً نشت کند، محرمانگی پیشروی کامل را فراهم کند. [2]

10. رابط‌های TUN/TAP

OpenVPN برای کار با رابط شبکهٔ مجازی TUN/TAP طراحی شده است که در بیشتر پلتفرم‌ها موجود است و بسته‌های تونل را حمل می‌کند. [4]

منابع و مراجع فنی

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

منابع علمی و صنعتی

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

[2] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

کلید پاسخ: مقایسهٔ پروتکل‌های WireGuard و OpenVPN، اندازهٔ کدها، سرعت و استانداردهای رمزنگاری

1 **اندازهٔ کد WireGuard** — پروتکل‌ها — **پاسخ درست: D**

نکتهٔ آموزشی

WireGuard بسیار فشرده است و با حدود 4,000 خط کد اجرا می‌شود. این موضوع سطح حمله را کوچک نگه می‌دارد و ممیزی را آسان‌تر می‌کند. استناد: WireGuard Project.

2 **سرعت فضای هسته** — تأخیر — **پاسخ درست: B**

نکتهٔ آموزشی

WireGuard با اجرای مستقیم در فضای هسته از سربار تعویض زمینه (context switching) پرهیز می‌کند و توان عملیاتی بالا را ممکن می‌سازد. منبع: WireGuard Project.

3 **پرسش 3** — **پاسخ درست: B**

نکتهٔ آموزشی

OpenVPN به‌طور تنگاتنگ با OpenSSL یکپارچه است که رمزهایی مانند AES-GCM را فراهم می‌کند و آن را بسیار قابل پیکربندی اما پیچیده‌تر می‌سازد.

4 **عملکرد پروتکل** — کنترل‌های مسیریابی — **پاسخ درست: A**

نکتهٔ آموزشی

WireGuard دست‌دهی را در چند میلی‌ثانیه برقرار می‌کند و بلافاصله به جابه‌جایی شبکه (مثلاً تغییر از وای‌فای به شبکهٔ تلفن همراه) پاسخ می‌دهد. استناد: [3] Microsoft Native Gateway, Apple Support.

5 **رمزنگاری نامتقارن** — حریم خصوصی — **پاسخ درست: C**

نکتهٔ آموزشی

WireGuard از Cryptokey Routing استفاده می‌کند که کلیدهای عمومی را با نشانی‌های IP مجاز تونل مرتبط می‌کند، مشابه پیکربندی‌های راه‌اندازی SSH. استناد: WireGuard Project.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: درست

نکتهٔ آموزشی

پیاده‌سازی WireGuard در لینوکس کمتر از 4,000 خط است، بنابراین تیم‌های امنیتی می‌توانند آن را بسیار سریع‌تر از پایگاه‌های کد بزرگ‌تر VPN مانند OpenVPN بررسی کنند.

7 تأخیر فضای کاربر

سرعت‌ها

پاسخ درست: نادرست

نکتهٔ آموزشی

OpenVPN در فضای کاربر اجرا می‌شود و بسته‌ها را میان رابط مجازی هسته و خودش رد و بدل می‌کند، که سربار تعویض زمینه ایجاد می‌کند (مگر اینکه از تخلیهٔ بار هسته مانند OpenVPN DCO استفاده شود). منبع: DD-WRT custom firmware.

8 پیکربندی OpenVPN

خطر شنود

پاسخ درست: درست

نکتهٔ آموزشی

OpenVPN از اجرا روی TCP (برای قابلیت اطمینان و عبور از دیوار آتش) یا UDP (برای سرعت) پشتیبانی می‌کند و همین آن را با دیوارهای آتش پیچیدهٔ سازمانی سازگار می‌کند. منبع: IETF Cryptographic Protocols.

9 رمزنگاری نوین

دیوارهای آتش

پاسخ درست: درست

نکتهٔ آموزشی

WireGuard رمزهای قدیمی را کنار می‌گذارد و به‌جای آن‌ها از مؤلفه‌های مدرن و امن مانند ChaCha20 و Poly1305 استفاده می‌کند که روی CPUهای موبایل سریع اجرا می‌شوند. استناد: WireGuard Project.

10 سادگی جفت کلید

بدون لاگ

پاسخ درست: نادرست

نکتهٔ آموزشی

WireGuard از گواهی یا سلسله‌مراتب پیچیدهٔ CA استفاده نمی‌کند؛ به جفت کلیدهای عمومی/خصوصی ساده‌ای متکی است که بین همتاها مبادله می‌شود. استناد: WireGuard Project.

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

G .1 WireGuard	H .2 OpenVPN	E .3 فضای هسته	A .4 فضای کاربر
B .5 4,000 خط	C .6 OpenSSL	F .7 جفت‌کلید	D .8 TCP/UDP

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 WireGuard	2 OpenVPN	3 فضای هسته	4 فضای کاربر
5 جفت کلید	6 ممیزی‌پذیری		

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

1 F – اوپناساسال	2 C – فضایهسته	3 B – اوپنوپیپان	4 G – جفتکلید
5 H – انتقال	6 E – کدکوچک	7 A – وایرگارد	8 D – فضایکاربر

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند WireGuard، OpenVPN و فضای هسته 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.

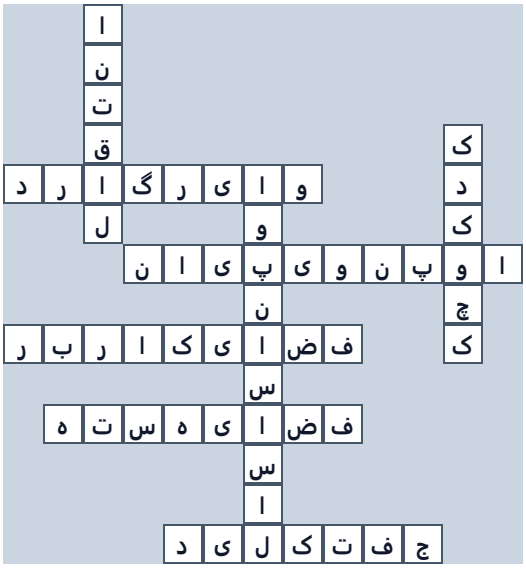
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

3 افقی: وایرگارد پروتکل مدرن VPN که برای سرعت بالا و ممیزی ساده کد طراحی شده است (8 حرف)

5 افقی: اوپنوپیان پروتکل قدیمی و مقاوم با کدبیس پیکربندی بزرگ و پیچیده (10 حرف)

6 افقی: فضایکاربر ناحیهٔ اجرایی که OpenVPN در آن اجرا می‌شود و سربار تعویض زمینه ایجاد می‌کند (9 حرف)

7 افقی: فضایهسته ناحیهٔ اجرای سیستم‌عامل که WireGuard برای سرعت در آن اجرا می‌شود (8 حرف)

8 افقی: جفتکلید توکن‌های نامتقارن که WireGuard برای تأیید اتصال همتاها به کار می‌برد (7 حرف)

عمودی

1 عمودی: انتقال پروتکل‌های لایهٔ حمل که OpenVPN پشتیبانی می‌کند؛ خود WireGuard فقط روی UDP اجرا می‌شود (6 حرف)

2 عمودی: کدکوچک اندازهٔ فشردهٔ کدبیس WireGuard که ممیزی آن را بسیار آسان‌تر می‌کند (6 حرف)

4 عمودی: اوپناسال کتابخانهٔ رمزنگاری که OpenVPN برای الگوریتم‌های رمز به آن متکی است (10 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. ررگواادی — وایرگارد
2. یفهضتسها — فضایهسته
3. ککوکچد — کدکوچک
4. دفلکیجت — جفتکلید
5. ییتونپوااپ — اوپنوپیپیان
6. بیضرافکرا — فضایکاربر
7. وناااسسالاپ — اوپناساسال
8. تلااقن — انتقال

کلید چالش رمز مخفی

"ارتقای اوپنوپیپیان با تونل سریع"

کلید پاسخ مطالعات موردی

A سناریو A: انتخاب پروتکل

شنود و رمزگذاری | معمای سارا

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- توصیه: WireGuard. طراحی سبک و بدون اتصال آن باعث می‌شود تونل هنگام تغییر شبکهٔ او سریع بازیابی شود و ChaCha20-Poly1305 رمزگذاری را سریع نگه می‌دارد.
- امنیت: هر دو پروتکل ترافیک او را در Wi-Fi کافه رمزگذاری می‌کنند، بنابراین در صورت پیکربندی درست هر کدام از ورودهای او محافظت می‌کند؛ انتخاب بیشتر بر سرعت و پایداری اثر می‌گذارد.

B سناریو B: عبور از مسدودسازی‌های VPN

مسدودسازی جغرافیایی و IPها | دوراهی Alex

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- دلیل مسدود شدن: WireGuard فقط از UDP استفاده می‌کند و دیوار آتش هتل احتمالاً UDP را مسدود می‌کند یا بسته‌های WireGuard را از طریق فیلتر کردن یا بازرسی عمیق بسته‌ها (Deep Packet Inspection) تشخیص می‌دهد.
- OpenVPN چگونه کمک می‌کند: می‌تواند روی TCP اجرا شود، از جمله درگاه 443 که HTTPS استفاده می‌کند و دیوارهای آتش هتل‌ها به‌ندرت آن را کاملاً مسدود می‌کنند، چون وب‌گردی به آن وابسته است.