نام: _____ تاریخ: _____ نمره: _____

VPN دسترسی راه‌دور

ایمن‌سازی نقاط پایانی کارکنان دورکار، احراز هویت چندعاملی و پیکربندی تونل‌های IPsec.

مروری بر یادگیری VPN دسترسی از راه دور

یادگیرنده
وضعیت دانشجویی
مسیر مدافع شبکه

امن
وضعیت اتصال
محافظت از بسته‌های داده

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

خوش آمدید! این بستهٔ فعالیت شما را در بررسی شبکه‌های VPN دسترسی از راه دور راهنمایی می‌کند. با تونل‌های کلاینت‌به‌سایت، ورود چندعاملی، بررسی وضعیت نقاط پایانی، سقف پهنای باند و ممیزی امنیتی syslog آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

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

باز کردن راهنمای بهترین VPNهای VPN.com

URL: https://www.vpn.com/vpn/best-vpn-for-business/remote-access/

نقشهٔ راه یادگیری VPN دسترسی از راه دور شما

- نقاط پایانی ایمن کارکنان دورکار که به گره‌های شبکهٔ محلی دسترسی دارند.
- سیاست‌های احراز هویت چندعاملی را برای ورودهای از راه دور پیکربندی کنید.
- پیکربندی‌های IPsec و OpenVPN کلاینت‌به‌سایت را راه‌اندازی کنید.
- لاگ‌های اتصال از راه دور را برای یافتن نقض کنترل دسترسی ممیزی کنید.
- پیش از اعطای اتصال‌های شبکه، بررسی وضعیت دستگاه را پیاده‌سازی کنید.
- توان عملیاتی سرور را بهینه کنید تا پهنای باند دورکاری دچار گلوگاه نشود.

دستورالعمل‌های VPN دسترسی از راه دور

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 بررسی‌های وضعیت امنیتی (posture check) و ورودهای چندعاملی به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

تونل‌های کلاینت-به-سایت و انطباق نقطهٔ پایانی (مقدمه)

VPNهای دسترسی راه‌دور تونل‌های امن کلاینت به سایت را برای کارکنان بیرون از محل برقرار می‌کنند. امن‌سازی این اتصال‌ها مستلزم اعمال ورود با احراز هویت چندعاملی (MFA)، انجام بررسی‌های انطباق وضعیت نقطهٔ انتهایی و ممیزی گزارش‌ها از طریق گردآورنده‌های syslog مرکزی است.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. پورتال‌های VPN دسترسی از راه دور باید کدام استاندارد احراز هویت را الزامی کنند؟

- A) چندعاملی
- B) تک‌عاملی
- C) رمزگذاری‌نشده
- D) مهمان محلی

2. کدام پروتکل استاندارد ایمن‌سازی اتصال‌های کلاینت‌به‌سایت دورکاری است؟

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. کدام بررسی تعیین می‌کند لپ‌تاپ راه دور پیش از اتصال سالم است؟

- A) بررسی وضعیت امنیتی
- B) آزمون سرعت
- C) آزمون پینگ
- D) تعداد حافظه

4. گزارش‌های اتصال کارکنان دورکار برای ممیزی امنیتی کجا ذخیره می‌شود؟

- A) سرور Syslog
- B) کلید رجیستری
- C) حافظهٔ کلاینت
- D) مرورگر وب

5. وقتی تعداد کارکنان دورکار از ظرفیت پهنای باند دروازه فراتر می‌رود چه مشکلی پیش می‌آید؟

- A) گلوگاه پهنای باند
- B) نشت DNS
- C) عبور از دست‌دهی (handshake)
- D) افشای IP

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. احراز هویت چندعاملی یک توکن تأیید ثانویه برای ایمن‌سازی ورودهای راه‌دور اضافه می‌کند.

درست نادرست

7 پرسش 7

7. بررسی‌های وضعیت امنیتی به دستگاه‌های راه‌دور با دیوار آتش غیرفعال اجازه می‌دهند به سرورهای خصوصی دسترسی پیدا کنند.

درست نادرست

8 پرسش 8

8. گزارش‌های VPN دسترسی راه‌دور برای ردیابی ورود غیرمجاز به شبکهٔ سازمانی ضروری هستند.

درست نادرست

9 پرسش 9

9. OpenVPN و IPsec پروتکل‌های قدیمی هستند که نمی‌توانند داده‌های کلاینت راه‌دور را رمزگذاری کنند.

درست نادرست

10 پرسش 10

10. گلوگاه پهنای باند دروازه زمانی رخ می‌دهد که ترافیک از راه دور از ظرفیت کارت اتصال بیشتر شود.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

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

1. برای محافظت از پورتال‌های سازمانی، ورود از راه دور باید احراز هویت _____ را الزامی کند.
2. کلاینت‌های راه دور بار داده‌های تونل را با پروتکل‌های استاندارد _____ رمزگذاری می‌کنند.
3. دستگاه‌ها باید پیش از دریافت پیوندهای شبکه، بررسی _____ امنیتی را بگذرانند.
4. گزارش‌های ورود قابل‌ممیزی به‌طور مداوم به سرور _____ مرکزی ارسال می‌شوند.
5. ترافیک سنگین در ساعات کاری می‌تواند به ازدحام _____ دروازه منجر شود.
6. درایورهای آداپتور مجازی، _____ کلاینت‌به‌سایت را در ویندوز و macOS مدیریت می‌کنند.

بانک واژگان

پهنای باند | تونل‌زنی | چندعاملی | دیوار آتش | رمزگذاری | سلامت | سیسلاگ | OpenVPN

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم کلیدی

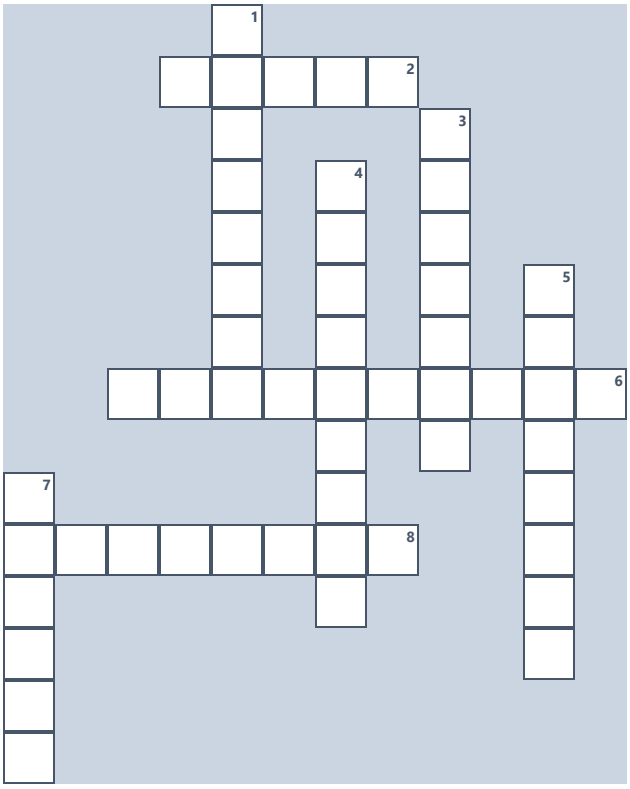
تطبیق تعاریف

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. چندعاملی	A	کپسوله کردن داده در مسیری امن.
2. OPENVPN	B	جمع‌آوری‌کنندهٔ مرکزی گزارش‌های امنیتی.
3. وضعیت امنیتی	C	حد ظرفیت داده شبکه.
4. SYSLOG	D	پروتکل استاندارد کلاینت‌به‌سایت.
5. پهنای باند	E	اعتبارسنجی سلامت دستگاه راه‌دور.
6. رمزگذاری	F	قواعد سامانهٔ فیلتر ترافیک.
7. تونل‌زنی	G	درهم‌سازی رمزنگاری بسته‌ها.
8. دیوار آتش	H	امنیت ورود که به توکن‌های اضافی نیاز دارد.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

2. اعتبارسنجی وضعیت دستگاه راه دور (5)

6. پروتکل استاندارد کلاینت‌به‌سایت (10)

8. امنیت ورود که توکن‌های اضافی می‌خواهد (8)

عمودی

1. درهم‌سازی رمزنگاشتی بسته‌ها (8)

3. کپسوله کردن داده در یک مسیر امن (7)

4. سقف ظرفیت داده در شبکه (9)

5. قواعد سامانهٔ پالایش ترافیک (8)

7. گردآورندهٔ مرکزی گزارش‌های امنیتی (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

2 افقی: اعتبارسنجی وضعیت دستگاه راه دور (5 حرف):

6 افقی: پروتکل استاندارد کلاینت‌به‌سایت (10 حرف):

8 افقی: امنیت ورود که توکن‌های اضافی می‌خواهد (8 حرف):

عمودی

1 عمودی: درهم‌سازی رمزنگاشتی بسته‌ها (8 حرف):

3 عمودی: کپسوله کردن داده در یک مسیر امن (7 حرف):

4 عمودی: سقف ظرفیت داده در شبکه (9 حرف):

5 عمودی: قواعد سامانهٔ پالایش ترافیک (8 حرف):

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

فهرست واژگان

چندعاملی
اوپنوپیپان
سلامت
سیسلاگ
پهناییاند
رمزگذاری
تونلزنی
دیواراتش

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. چندعاملی
B. اوپنوپیپان
C. سلامت
D. سیسلاگ
E. پهنایباند
F. رمزگذاری
G. تونلزنی
H. دیواراتش

تعاریف و فیلدهای تطبیق
1. گردآورندهٔ مرکزی گزارش‌های امنیتی.
2. قواعد سامانهٔ پالایش ترافیک.
3. کپسوله کردن داده در یک مسیر امن.
4. درهم‌سازی رمزنگاشتی بسته‌ها.
5. پروتکل استاندارد کلاینت‌به‌سایت.
6. سقف ظرفیت داده در شبکه.
7. اعتبارسنجی وضعیت دستگاه راه دور.
8. امنیت ورود که توکن‌های اضافی می‌خواهد.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم کلیدی این کاربرگ آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ل ع ا چ م ن ی د
2. س ت م ا ل
3. پ ب ی ه ا د ا ن ن
4. ی و ز ل ن ت ن
5. ی ی ن و ن پ و ا ا پ
6. ا ل س س گ ی
7. ر ی ذ ا ر م گ ز
8. ا ی ر ش د ت ا و

فعالیت تکمیلی: سریع فکر کن

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

1	افسانه‌ها دربارهٔ VPNها		
2	واژه‌هایی که Zero Trust را توصیف می‌کنند		
3	برنامه‌های اداری که می‌شناسید		
4	قوانین کار از راه دور ایمن		
5	چیزهایی که ارائه‌دهندهٔ اینترنت شما می‌تواند ببیند		
6	سرویس‌های VPN که می‌شناسید		
7	جاهایی که کارمندان از آن‌ها کار می‌کنند		
8	ابزارهایی که یک شرکت هر روز استفاده می‌کند		
9	نقش‌ها در بخش فناوری اطلاعات		
10	دستگاه‌هایی که یک کارمند ممکن است داشته باشد		
11	داده‌هایی که یک شرکت باید محافظت کند		
12	کارهایی که پس از نقض امنیتی باید انجام داد		
13	چیزهایی که می‌توانند جلسهٔ ویدیویی را مختل کنند		
14	روش‌های ورود امن		
15	دلایل دادن VPN به کارمندان		

ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

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

مطالعهٔ موردی 1: اِعمال MFA



سناریو: یک تحلیلگر کسب‌وکار هنگام کار از راه دور تلاش می‌کند وارد پایگاه دادهٔ شرکت شود. او نام کاربری و گذرواژهٔ درست را وارد می‌کند، اما پورتال VPN دسترسی را مسدود می‌کند و کد توکن فیزیکی می‌خواهد.

پرسش برای بحث: کدام سیاست امنیتی این گام تأیید دوگانه را اعمال می‌کند؟

مطالعهٔ موردی 2: انطباق وضعیت امنیتی



سناریو: یک پیمانکار لپ‌تاپ شخصی خود را به شبکهٔ راه دور شرکت وصل می‌کند. کلاینت VPN بلافاصله اتصال را قطع می‌کند و به کاربر اطلاع می‌دهد که تعاریف آنتی‌ویروس او قدیمی هستند.

پرسش برای بحث: کدام بررسی تخصصی دروازهٔ VPN جلوی این تلاش اتصال را گرفت؟

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

1	12	29	1	28	13	1	15	32	29	1	32	1	3	19	1	24	29

10	29	25	29	28	32	1

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: VPN دسترسی راه‌دور چیست؟

روش اتصال امن که به کارکنانی که بیرون از محل کار می‌کنند اجازه می‌دهد مستقیماً به سرورهای خصوصی شرکت وصل شوند.

Q2: چرا کلاینت به سایت با سایت به سایت فرق دارد؟

کلاینت-به-سایت دستگاه‌های کاربران را به‌صورت جداگانه وصل می‌کند، در حالی که سایت-به-سایت کل مکان‌های فیزیکی دفتر را به هم پیوند می‌دهد.

Q3: بررسی وضعیت دستگاه چیست؟

اسکنی که پیش از اعطای دسترسی، وضعیت امنیتی دستگاه راه‌دور (آنتی‌ویروس، سطح وصله‌های سیستم‌عامل) را بررسی می‌کند.

Q4: چرا OpenVPN برای دسترسی از راه دور استفاده می‌شود؟

به دلیل پروتکل امنیتی قوی، سازگاری چندسکویی و توانایی مدیریت اتصال‌های فردی.

Q5: MFA چگونه از دسترسی از راه دور محافظت می‌کند؟

یک توکن تأیید ثانویه اضافه می‌کند و حتی اگر گذرواژه‌های کارکنان لو برود یا دزدیده شود، از دسترسی جلوگیری می‌کند.

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

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

Q6: سرور syslog چیست؟

مخزن متمرکز گزارش‌ها که رویدادهای اتصال، ورودها و هشدارهای سیستم را برای ممیزی‌های انطباق ذخیره می‌کند.

Q7: چه چیزی باعث گلوگاه پهنای باند می‌شود؟

زمانی که مجموع نیاز پهنای باند کارکنان دورکار از سقف سرعت اینترنت دروازهٔ شرکت فراتر می‌رود.

Q8: آیا می‌توانم رایانهٔ خانگی خود را به VPN محل کار وصل کنم؟

فقط اگر دستگاه از ممیزی‌های بررسی وضعیت سازمانی عبور کند و مدیران IT آن را مجاز کرده باشند.

Q9: کپسوله‌سازی شبکه چیست؟

پیچیدن بسته‌های داده در حین انتقال درون سرایندهای پروتکل رمزگذاری‌شده برای امن‌سازی انتقال.

Q10: تونل‌زنی تفکیکی چگونه دسترسی راه‌دور را بهینه می‌کند؟

به کارکنان اجازه می‌دهد برای وب‌گردی استاندارد از ISP محلی خود استفاده کنند و فایل‌های مرتبط با کار را از طریق VPN مسیریابی کنند.

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: احراز هویت مبتنی بر گواهی چگونه دسترسی راه‌دور را تقویت می‌کند؟

مجوزهای اتصال را به گواهی‌های دیجیتال محلی از پیش نصب‌شده گره می‌زند و دستگاه‌های مدیریت‌نشده یا غیرمجاز را مسدود می‌کند.

Q2: خطر امنیتی تونل‌زنی تفکیکی برای دورکاری چیست؟

پلی بالقوه ایجاد می‌کند که از طریق آن یک دستگاه محلی در معرض خطر می‌تواند تهدیدهای خارجی را به شبکهٔ خصوصی هدایت کند.

Q3: بررسی‌های وضعیت چگونه تنظیمات رجیستری را بازرسی می‌کنند؟

کلاینت VPN اسکریپت‌های محلی را اجرا می‌کند که مسیرهای رجیستری را بررسی می‌کنند تا معلوم شود نرم‌افزار امنیتی سازمانی فعال است یا نه.

Q4: چرا syslog به‌طور پیش‌فرض از درگاه UDP 514 استفاده می‌کند؟

برای انتقال سریع گزارش‌ها با کمترین سربار، هرچند پیکربندی‌های امن اکنون کپسوله‌سازی TLS روی TCP را الزامی می‌کنند.

Q5: شرکت‌ها گلوگاه‌های پهنای باند دروازه را چگونه حل می‌کنند؟

با پیاده‌سازی متعادل‌کننده‌های بار و توزیع ترافیک راه دور بین گره‌های سرور منطقه‌ای.

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: کارکرد آداپتورهای مجازی TAP/TUN در کلاینت‌های راه دور چیست؟

آن‌ها مانند کارت شبکهٔ مجازی عمل می‌کنند و ترافیک TCP/IP سطح دستگاه را مستقیماً به تونل رمزگذاری‌شدهٔ VPN هدایت می‌کنند.

Q7: IKEv2 MOBIKE چگونه از تحرک نیروی کار دورکار پشتیبانی می‌کند؟

اتصال‌های آدرس IP را به‌صورت پویا به‌روزرسانی می‌کند و VPN را در حین جابه‌جایی کاربر بین Wi-Fi و داده‌های تلفن همراه فعال نگه می‌دارد.

Q8: تفاوت مسیریابی تونل تفکیکی و تونل کامل چیست؟

مسیریابی کامل همهٔ ترافیک اینترنت دستگاه را از VPN عبور می‌دهد، در حالی که مسیریابی تقسیم‌شده فقط IPهای مقصد سازمانی را ارسال می‌کند.

Q9: دستگاه‌های NAT اتصال‌های VPN راه دور را چگونه مدیریت می‌کنند؟

با نگاشت بازه‌های پورت محلی به نشانی‌های IP دروازهٔ عمومی برای مسیریابی بسته‌های داده رمزگذاری‌شدهٔ بازگشتی.

Q10: کدام استانداردهای انطباق، ممیزی دسترسی راه‌دور را الزامی می‌کنند؟

استانداردهایی مانند HIPAA، SOC 2 و PCI DSS ثبت گزارش و پایش تمام نشست‌های اتصال راه‌دور را الزامی می‌کنند.

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

VPNهای دسترسی راه‌دور تونل‌های امن کلاینت به سایت را برای کارکنان بیرون از محل برقرار می‌کنند.

2. بینش VPN

قوانین انطباق، احراز هویت چندعاملی را برای محافظت از پورتال‌های راه‌دور کسب‌وکار الزامی می‌کنند.

3. بینش VPN

بررسی‌های وضعیت امنیتی پیش از اعطای دسترسی به شبکهٔ خصوصی، تنظیمات امنیتی کلاینت محلی را راستی‌آزمایی می‌کنند.

4. بینش VPN

سرورهای Syslog گزارش‌های اتصال را گردآوری می‌کنند تا تلاش‌های دسترسی غیرمجاز ممیزی و شناسایی شوند.

5. بینش VPN

گلوگاه‌های پهنای باند دروازه زمانی رخ می‌دهند که تقاضای ترافیک تجمعی از راه دور از محدودیت‌های اینترنت سرور بیشتر شود.

6. بینش VPN

آداپتورهای شبکهٔ مجازی پرس‌وجوهای شبکهٔ سیستم‌عامل را درون پروتکل‌های امن کپسوله می‌کنند.

7. بینش VPN

پشتیبانی از MOBIKE به کلاینت‌های راه‌دور اجازه می‌دهد بدون قطع تونل VPN، شبکه را عوض کنند.

8. بینش VPN

مسیریابی تونل کامل ترافیک اینترنت همهٔ کارکنان را ایمن می‌کند، اما بار دروازهٔ سازمانی را افزایش می‌دهد.

9. بینش VPN

احراز هویت با گواهی، مجوز اتصال VPN را مستقیماً به سخت‌افزار تحت مدیریت شرکت پیوند می‌دهد.

10. بینش VPN

چارچوب‌هایی مانند SOC 2 و PCI DSS ثبت و پایش نشست‌های دسترسی از راه دور را انتظار دارند.

منابع و مراجع فنی

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

منابع علمی و صنعتی

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 **توکن‌های ورود** امنیت MFA — پاسخ درست: **A**

نکتهٔ آموزشی

احراز هویت چندعاملی برای ورودها تأیید ثانویه را اجباری می‌کند. منبع: MFA Implementation.

2 **تونل OpenVPN** کلاینت-به-سایت — پاسخ درست: **A**

نکتهٔ آموزشی

OpenVPN پروتکل استانداردی برای ایمن‌سازی تونل‌های کلاینت به سایت است. منبع: OpenVPN Client.

3 **ممیزی‌های وضعیت امنیتی** بررسی دستگاه — پاسخ درست: **A**

نکتهٔ آموزشی

بررسی‌های وضعیت امنیتی نقاط پایانی را از نظر دیوار آتش و ابزارهای آنتی‌ویروس فعال پویش می‌کنند. منبع: Posture Compliance.

4 **گردآورندهٔ لاگ** سرور SYSLOG — پاسخ درست: **A**

نکتهٔ آموزشی

سرورهای Syslog گزارش‌های رویدادهای امنیتی را جمع‌آوری می‌کنند تا تخلف‌های دسترسی پایش شود. منبع: Syslog Standard.

5 **سرریز کارت** گلوگاه دروازه — پاسخ درست: **A**

نکتهٔ آموزشی

گلوگاه پهنای باند دروازه زمانی رخ می‌دهد که ترافیک کاربران از محدودیت‌های سرور بیشتر شود. منبع: Capacity Planning.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **توکن‌های ورود** — بررسی‌های MFA — پاسخ درست: درست

نکتهٔ آموزشی

احراز هویت چندعاملی برای ورودها تأیید ثانویه را اجباری می‌کند. منبع: MFA Implementation.

7 **پرسش 7** — پاسخ درست: نادرست

نکتهٔ آموزشی

بررسی‌های وضعیت (posture checks) دستگاه‌هایی را که دیوار آتش یا آنتی‌ویروس‌شان خاموش است مسدود می‌کنند، بنابراین چنین دستگاه‌هایی رد می‌شوند.

8 **گردآورندهٔ لاگ** — سرور SYSLOG — پاسخ درست: درست

نکتهٔ آموزشی

سرورهای Syslog گزارش‌های رویدادهای امنیتی را جمع‌آوری می‌کنند تا تخلف‌های دسترسی پایش شود. منبع: Syslog Standard.

9 **پرسش 9** — پاسخ درست: نادرست

نکتهٔ آموزشی

OpenVPN و IPsec پروتکل‌های رایجی هستند که ترافیک کلاینت راه‌دور را رمزگذاری می‌کنند.

10 **سرریز کارت** — گلوگاه دروازه — پاسخ درست: درست

نکتهٔ آموزشی

گلوگاه پهنای باند دروازه زمانی رخ می‌دهد که ترافیک کاربران از محدودیت‌های سرور بیشتر شود. منبع: Capacity Planning.

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

H 1. چندعاملی	D 2. OPENVPN	E 3. وضعیت امنیتی	B 4. SYSLOG
C 5. پهنای باند	G 6. رمزگذاری	A 7. تونل‌زنی	F 8. دیوار آتش

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 چندعاملی	2 OpenVPN	3 سلامت	4 سیسلاگ
5 پهنای باند	6 تونل‌زنی		

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

1 D – سیسلاگ	2 H – دیواراتش	3 G – تونلزنی	4 F – رمزگذاری
5 B – اوپنوپیان	6 E – پهناپیاند	7 C – سلامت	8 A – چندعاملی

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند چندعاملی، OPENVPN و وضعیت امنیتی 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.

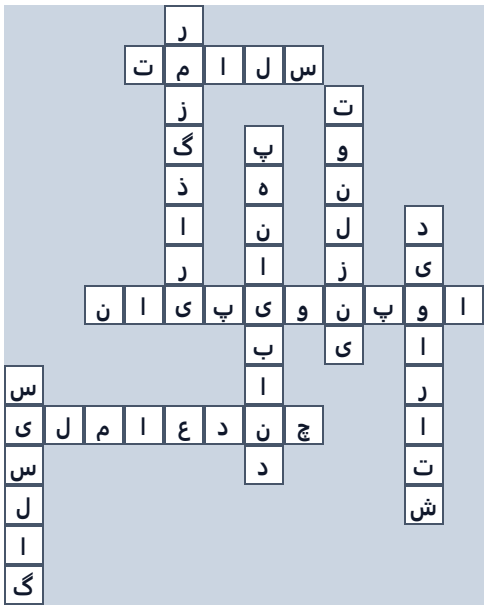
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: سلامت اعتبارسنجی وضعیت دستگاه راه دور (5 حرف)

6 افقی: اوپنوپیپان پروتکل استاندارد کلاینت‌به‌سایت (10 حرف)

8 افقی: چندعاملی امنیت ورود که توکن‌های اضافی می‌خواهد (8 حرف)

عمودی

1 عمودی: رمزگذاری درهم‌سازی رمزنگاشتی بسته‌ها (8 حرف)

3 عمودی: تونلزنی کپسوله کردن داده در یک مسیر امن (7 حرف)

4 عمودی: پهناییباند سقف ظرفیت داده در شبکه (9 حرف)

5 عمودی: دیواراتش قواعد سامانهٔ پالایش ترافیک (8 حرف)

7 عمودی: سیسلاگ گردآورندهٔ مرکزی گزارش‌های امنیتی (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. لعاچمنید — چندعاملی
2. ستمال — سلامت
3. پبیهادانن — پهناییباند
4. یوزلنتن — تونلزنی
5. یینونپوااپ — اوپنوپیپیان
6. السسگی — سیسلاگ
7. ریذارمگز — رمزگذاری
8. ایرشدتاو — دیواراتش

کلید چالش رمز مخفی

"نقاط پایانی سازمان را ایمن کند"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: اِعمال MFA

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک تحلیلگر کسب‌وکار هنگام کار از راه دور تلاش می‌کند وارد پایگاه داده سازمانی خود شود. او نام کاربری و گذرواژهٔ درست را وارد می‌کند، اما پورتال VPN دسترسی را مسدود می‌کند و کد توکن فیزیکی می‌خواهد.
- راهبرد و راه‌حل پیشنهادی: پورتال VPN سازمانی برای امن‌سازی ورودهای راه‌دور، سیاست سخت‌گیرانهٔ احراز هویت چندعاملی (MFA) را اعمال می‌کند.

B مطالعهٔ موردی 2: انطباق وضعیت امنیتی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک پیمانکار لپ‌تاپ شخصی خود را به شبکهٔ سازمانی راه‌دور وصل می‌کند. کلاینت VPN بلافاصله اتصال را قطع می‌کند و به کاربر اطلاع می‌دهد که تعریف‌های آنتی‌ویروسش منسوخ است.
- راهبرد و راه‌حل پیشنهادی: دروازهٔ دسترسی راه‌دور بررسی وضعیت نقطهٔ انتهایی را انجام داد و دستگاه را به‌دلیل پیکربندی‌های امنیتی منسوخ مسدود کرد.