Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Bir VPN nasıl seçilir Çalışma kâğıdı

VPN sağlayıcılarını, güvenlik standartlarını, denetimleri ve kayıt tutma ilkelerini değerlendirme

VPN ÖĞRENME GENEL BAKIŞI

ÖĞRENCİ
ÖĞRENCİ DURUMU
Ağ Savunucusu Parkuru

GÜVENLİ
BAĞLANTI DURUMU
Veri paketlerini koruma

ETKİN
SIZINTI KORUMASI
DNS ve IPv6 sızıntı koruması

Hoş geldin! Bu etkinlik paketi sana Sanal Özel Ağların (VPN) temel ilkeleri konusunda rehberlik eder. Şifreli tünellerin verilerini nasıl güvence altına aldığını, ağ protokollerinin nasıl çalıştığını ve gizlilik sızıntılarının nasıl belirlenip azaltılacağını keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: VPN kavramlarında ve protokollerinde ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com VPN rehberini aç

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

VPN Öğrenme Yol Haritan

- Gizlilik için sağlayıcının yargı yetkisini ve sıfır kayıt ilkelerini değerlendir.
- WireGuard ve OpenVPN gibi tünelleme protokollerini hız açısından karşılaştır.
- Kill switch'ler ve yalnızca RAM'li sunucu düğümleri gibi güvenlik özelliklerini analiz et.
- Seçim yaparken bağımsız güvenlik denetimlerini ve fiyatlandırma planlarını belirle.
- Sunucu konumlarını hız ve coğrafi engel aşma ihtiyaçlarına göre seç.

SEÇİM ÇALIŞMA KÂĞIDI YÖNERGELERİ

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: güvenli VPN altyapısı seçimi. Hızlı Düşün bonus etkinliğiyle bitir.

VPN SEÇME (GİRİŞ)

Doğru VPN'i seçmek, pazarlama abartısının ötesine bakmayı gerektirir. Güvenilir bir sağlayıcının kanıtlanmış bir sıfır günlük politikası, güvenli şifreleme protokolleri ve açık kaynaklı istemcileri olmalıdır. Güvenlik özelliklerini, yetki alanlarını ve hız performansını değerlendirerek dijital koruma ihtiyaçlarına uyan bir VPN seçebilirsin.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ.

Kontrol Noktası 1: Çoktan seçmeli görev

1. Güvenli bir VPN sağlayıcısı seçerken temel etken nedir?

- A. Sunucu ülkelerinin sayısı
- B. Bağımsız olarak denetlenmiş bir kayıt tutmama politikası
- C. En düşük aylık fiyat kademesi
- D. Gösterişli reklam sponsorlukları

2. Hangi VPN protokolü hız ve denetlenebilirlik arasında en iyi dengeyi sunar?

- A. PPTP (Eski)
- B. L2TP/IPSec
- C. Yalnızca TCP üzerinden OpenVPN
- D. WireGuard

3. Kullanıcılar hassas etkinlikler için neden ücretsiz VPN'lerden kaçınmalıdır?

- A. Amerika Birleşik Devletleri'nde yasaklıdırlar
- B. Çoğunlukla web gezinme geçmişinizi satarlar
- C. Temel web gezintisini desteklemezler
- D. Bağlanmak için özel donanım gerektirirler

4. Bir sağlayıcının bulunduğu ülkenin yasal yargı yetkisi neyi belirler?

- A. Sunucu bağlantısının hızı
- B. Desteklenen cihaz türleri
- C. Veri saklama ve arama emirlerini düzenleyen yerel yasalar
- D. İstemci uygulamasının görsel teması

5. VPN istemcisindeki 'kill switch' özelliğinin temel amacı nedir?

- A. VPN bağlantısı koptuğunda internet erişimini engellemek için
- B. Cihazdaki tüm yüklü uygulamaları silmek
- C. Sunucu bağlantısının hızını ikiye katlamak için
- D. Boştayken işletim sistemini yeniden başlatmak için

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. VPN, cihazınızı kötü amaçlı yazılım indirmelerinden ve virüslü dosyalardan korur.

○ Doğru ○ Yanlış

7 Soru 7

7. Deloitte gibi firmaların bağımsız denetimleri, sıfır kayıt iddialarını doğrular.

○ Doğru ○ Yanlış

8 Soru 8

8. Bir sağlayıcının kendi ülkesinin yasaları, kullanıcı verilerinin gizliliğini etkilemez.

○ Doğru ○ Yanlış

9 Soru 9

9. WireGuard'ın kompakt kod tabanını denetlemek OpenVPN'inkinden daha kolaydır.

○ Doğru ○ Yanlış

10 Soru 10

10. Ücretsiz VPN'ler sunucu maliyetlerini karşılamak için sıklıkla reklam satar veya kullanıcıları izler.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Bağımsız olarak doğrulanmış bir _____ politikası, VPN sağlayıcısını çevrimiçi geçmişinizi kaydetmemeye taahhüt eder.

2. Modern _____ protokolü yüksek hız sunar ve çok küçük bir kod tabanı kullanır.

3. VPN bağlantısı aniden kesilirse tüm trafiği durduran güvenlik özelliğinin adı: _____ .

4. Bir sağlayıcının hukuki durumunu belirleyen coğrafi bölge, yani _____ , gözetim anlaşmalarına tabi olup olmadığını gösterir.

5. Yalnızca bellek üzerinde çalışan bir _____ , yeniden başlatma sonrasında kullanıcı verilerinin kalıcı olmasını önlemeye yardımcı olur.

6. Sıfır bilgi iddiasını doğrulamak, saygın firmalardan alınmış üçüncü taraf güvenlik _____ raporu gerektirir.

KELİME BANKASI

DENETİM | KAYIT TUTMAMA | KILL SWITCH | RAM SUNUCUSU | ŞİFRELEME | ÜCRETSİZ VPN | WIREGUARD | YARGI YETKİSİ

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Ağ kavramı eşleştirme

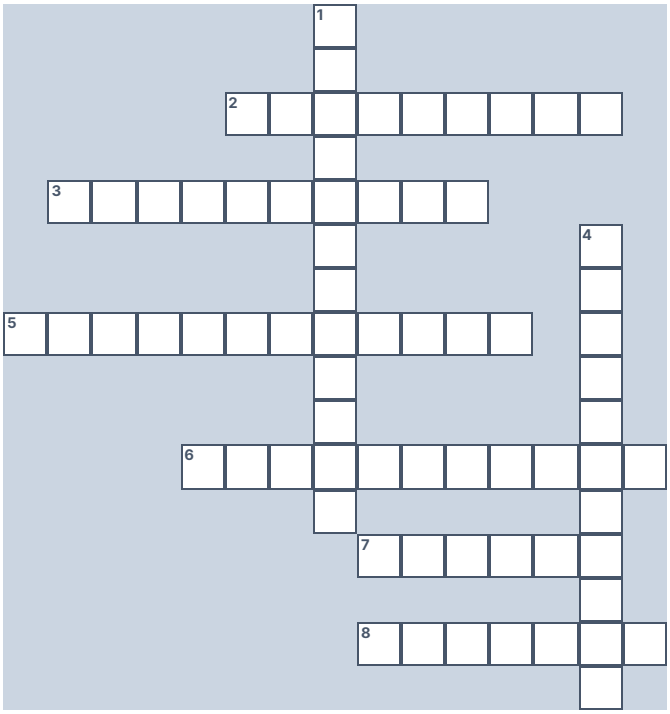
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

1. WireGuard	A	Çoğunlukla kayıt tutup tarayıcı verilerini satarak gelir elde eden yüksek riskli bağlantı hizmeti.
2. Denetlenmiş Kayıtlar	B	Güvenli tünel bağlantısı koparsa internet yönlendirmesini engelleyen güvenlik mekanizması.
3. Yargı Yetkisi	C	ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda arasındaki uluslararası istihbarat paylaşım ittifakı.
4. Kill Switch	D	Uçucu bellekte çalışan donanım altyapısı; bu nedenle veriler diske kaydedilmez.
5. Five Eyes	E	VPN sağlayıcısının yasal yükümlülüklerini belirleyen coğrafi bölge.
6. Ücretsiz VPN	F	Yaklaşık 4.000 satırlık, son derece denetlenebilir kod kullanan modern, hızlı protokol.
7. Yalnızca RAM'li Sunucular	G	WireGuard'dan çok daha büyük bir kod tabanına sahip, olgun ve yaygın olarak denetlenmiş açık kaynaklı protokol.
8. OpenVPN	H	Bağımsız üçüncü taraf siber güvenlik firmalarınca doğrulanmış gizlilik iddiası.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

2. Yaklaşık 4.000 satırlık, yüksek düzeyde denetlenebilir kod kullanan modern ve hızlı protokol (9)

3. Güvenli tünel bağlantısı kesilirse internet yönlendirmesini engelleyen güvenlik mekanizması (10)

5. Bağımsız üçüncü taraf siber güvenlik firmalarınca doğrulanmış gizlilik iddiası (12)

6. Tamamen geçici bellek üzerinde çalışan ve veri depolamayı önleyen donanım altyapısı (11)

7. ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda arasındaki uluslararası istihbarat paylaşım ittifakı (6)

8. WireGuard'dan çok daha büyük bir kod tabanına sahip, olgun ve yaygın biçimde denetlenmiş açık kaynaklı protokol (7)

YUKARIDAN AŞAĞI

1. VPN sağlayıcısının yasal yükümlülüklerini belirleyen coğrafi bölge (12)

4. Genellikle tarayıcı verilerini kaydedip satarak gelir elde eden yüksek riskli bağlantı hizmeti (11)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

2 soldan sağa: Yaklaşık 4.000 satırlık, yüksek düzeyde denetlenebilir kod kullanan modern ve hızlı protokol (9 harf):

3 soldan sağa: Güvenli tünel bağlantısı kesilirse internet yönlendirmesini engelleyen güvenlik mekanizması (10 harf):

5 soldan sağa: Bağımsız üçüncü taraf siber güvenlik firmalarınca doğrulanmış gizlilik iddiası (12 harf):

6 soldan sağa: Tamamen geçici bellek üzerinde çalışan ve veri depolamayı önleyen donanım altyapısı (11 harf):

7 soldan sağa: ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda arasındaki uluslararası istihbarat paylaşım ittifakı (6 harf):

8 soldan sağa: WireGuard'dan çok daha büyük bir kod tabanına sahip, olgun ve yaygın biçimde denetlenmiş açık kaynaklı protokol (7 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: VPN sağlayıcısının yasal yükümlülüklerini belirleyen coğrafi bölge (12 harf):

4 yukarıdan aşağı: Genellikle tarayıcı verilerini kaydedip satarak gelir elde eden yüksek riskli bağlantı hizmeti (11 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

İ	İ	D	J	Ö	L	I	R	A	F	N	İ	M	Ç	L
S	C	Ç	Ğ	H	B	B	A	N	P	K	O	U	Ş	H
İ	Y	F	Y	R	G	V	M	Ü	Ğ	E	P	Ş	M	Ş
K	İ	P	D	S	R	K	S	O	J	L	R	Ğ	İ	O
T	Ğ	Y	N	K	Ü	T	U	M	Y	Ö	Ö	B	Ü	A
E	J	O	L	B	J	H	N	F	H	M	Y	C	C	B
Y	Z	Z	Y	B	L	U	U	V	K	Ç	E	N	R	E
I	Ü	O	Ö	V	Ğ	D	C	Y	C	Ü	K	E	E	Ş
G	G	Ğ	Z	Ü	Ç	N	U	P	İ	Ü	V	P	T	G
R	J	Z	A	L	P	Z	S	P	K	G	R	U	S	Ö
A	K	A	Y	I	T	T	U	T	M	A	M	A	İ	Z
Y	F	J	W	I	R	E	G	U	A	R	D	Ü	Z	I
C	Y	K	I	L	L	S	W	I	T	C	H	Ç	V	C
Y	N	T	Z	N	Z	T	Ş	B	Ğ	U	O	V	P	Ç
L	K	N	P	V	N	E	P	O	Ğ	O	Ü	Y	N	Z

KELİME LİSTESİ

WIREGUARD · KAYITTUTMAMA · YARGIYETKİSİ · KILLSWITCH · BEŞGÖZ · ÜCRETSİZVPN · RAMSUNUCUSU · OPENVPN

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. WIREGUARD**
- **B. KAYITTUTMAMA**
- **C. YARGIYETKİSİ**
- **D. KILLSWITCH**
- **E. BEŞGÖZ**
- **F. ÜCRETSİZVPN**
- **G. RAMSUNUCUSU**
- **H. OPENVPN**

TANIMLAR VE EŞLEŞTİRME ALANLARI

_____ 1. ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda arasındaki uluslararası istihbarat paylaşım ittifakı.

_____ 2. Yaklaşık 4.000 satırlık, yüksek düzeyde denetlenebilir kod kullanan modern ve hızlı protokol.

_____ 3. WireGuard'dan çok daha büyük bir kod tabanına sahip, olgun ve yaygın biçimde denetlenmiş açık kaynaklı protokol.

_____ 4. Genellikle tarayıcı verilerini kaydedip satarak gelir elde eden yüksek riskli bağlantı hizmeti.

_____ 5. Güvenli tünel bağlantısı kesilirse internet yönlendirmesini engelleyen güvenlik mekanizması.

_____ 6. Tamamen geçici bellek üzerinde çalışan ve veri depolamayı önleyen donanım altyapısı.

_____ 7. VPN sağlayıcısının yasal yükümlülüklerini belirleyen coğrafi bölge.

_____ 8. Bağımsız üçüncü taraf siber güvenlik firmalarınca doğrulanmış gizlilik iddiası.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel VPN kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını doldurulabilir giriş kutularına yaz.

1. UGEIWARDR
2. İAIYYİSRTKEG
3. BŞGZÖE
4. USUNMUUCRAS
5. AATUAYTMTKMI
6. CSLITKIWHL
7. ZTÜCİNVPRSE
8. PNNOPVE

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Bir VPN'in gizleyebileceği şeyler			
2	Fiyattan daha önemli olan şeyler			
3	VPN incelemelerini okuyacağın yerler			
4	Bir VPN'in seni koruyamadığı şeyler			
5	Bir VPN satış ekibine sorulacak sorular			
6	İnternet sağlayıcının görebildiği şeyler			
7	VPN seçerken kontrol listendeki maddeler			
8	VPN kullanacağın yerler			
9	Bir VPN sağlayıcısındaki uyarı işaretleri			
10	Gizlilikle ilgili sözcükler			
11	İlk test edeceğin şeyler			
12	İyi bir VPN sağlayıcısının verdiği sözler			
13	Seyahat ederken VPN kullanma nedenleri			
14	VPN kullanabilen cihazlar			
15	VPN'lerle ilgili efsaneler			

Kontrol Noktası 8: VPN vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

SARAH (KAFEDEKİ ÖĞRENCİ)

👷 "Selam! Coffee & Bytes'ta oturuyorum. 'Free_Wi-Fi_No_Password' adlı güvenli olmayan bir genel ağ var. Okul e-postama giriş yapıp ödevimi yüklemek istiyorum ama bilgisayar korsanlarından endişeleniyorum. Bu ağı VPN olmadan kullanmanın riskleri neler ve VPN verilerimi nasıl korur?"

ALEX (GEZGİN ÖĞRENCİ)

👷 "Eyvah! Bir proje için yurt dışına seyahat ediyorum ve ülkemdeki bir sunucuda barındırılan bir biyoloji belgeseli izlemeye çalışıyorum. Ama site 'Bu video şu anki konumunuzda mevcut değil.' diyor. Neden engelleniyorum ve VPN izlememe nasıl yardımcı olabilir?"

Kontrol Noktası 9: Şifreyi Çöz

Seçim rehberi eğitimini tamamlamak için güvenli altyapı seçmeyle ilgili bu gizli mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10
I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20
R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

21	1	20	18	21	15	1	21	11	17	11		8	26	27	6	17	15	12
2	12	21		22	12	22	24	6	16	15	6							
14	1	21	23	11	15	1	23	24	11	21								

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: VPN hakkında sık sorulan sorular – temel düzey (Bölüm A)

Olası müşterilerin sanal özel ağları kullanmakla ilgili en sık sorduğu soruları ve cevapları incele.

Q1: VPN nedir ve nasıl çalışır?

Sanal Özel Ağ (VPN) internet bağlantınızı şifreler ve trafiğinizi güvenli bir uzak sunucu üzerinden yönlendirir. Bu, genel IP adresinizi maskeler ve yerel ağ gözlemcilerinin ile İSS'nizin VPN tüneli üzerinden yönlendirilen trafik hakkında görebileceklerini sınırlar.

Q2: Neden VPN kullanmalıyım?

VPN, dijital gizliliğinizi korur, kafeler veya havalimanları gibi herkese açık Wi-Fi ağlarında bağlantınızı güvenceye alır, İSS şifreli trafiğin türünü tanımlayamadığında etkinliğe dayalı kısıtlamayı azaltabilir, küresel içeriğe erişmek için coğrafi kısıtlamaları aşar ve uzaktan çalışma kaynaklarının güvenliğini sağlamaya yardımcı olur.

Q3: VPN beni çevrimiçi tamamen anonim yapar mı?

Hayır. Bir VPN IP adresini gizleyip trafiği şifrelese de tarayıcı çerezleri, açık hesaplar (Google veya Facebook gibi), tarayıcı parmak izi veya VPN sağlayıcının verilerini kaydetmesi yoluyla yine izlenebilirsin.

Q4: VPN internet hızımı yavaşlatır mı?

Evet, hafifçe. Şifreleme süreci ve VPN sunucusuna olan fiziksel mesafe gecikme ve ek yük getirir. Etki; sağlayıcıya, protokole, sunucu mesafesine, cihaza ve ağ koşullarına göre değişir.

Q5: Nasıl para kazanır?

İş modelini kontrol et. Abonelikler, freemium kademeleri ve veri satışı, bir VPN'e ne kadar güvenebileceğini etkiler; verilerini hiç toplamayan bir hizmet onları satamaz. Önce gizlilik politikasını oku. [1]

Kontrol Noktası 10: VPN hakkında sık sorulan sorular – temel düzey (Bölüm B)

Olası müşterilerin sanal özel ağları kullanmakla ilgili en sık sorduğu soruları ve cevapları incele.

Q6: Ücretsiz bir VPN kullanabilir miyim?

Ücretsiz VPN'ler reklamlara, sınırlı özelliklere, kullanım analizlerine, veri sınırlarına veya başka gelir modellerine dayanabilir. Kullanıcılar kullanmadan önce sağlayıcının gizlilik politikasını, sahipliğini, denetimlerini ve iş modelini incelemelidir.

Q7: "Kayıt tutmama" politikası nedir?

Kayıt tutmama politikası, bir sağlayıcının hangi etkinlik ve bağlantı verilerini saklamadığını söylediğini açıklar. Kapsam değişiklik gösterir; bu yüzden okuyucular politikayı ve bağımsız denetim bulgularını incelemelidir.

Q8: En iyi VPN'i nasıl seçerim?

Denetlenmiş kayıt tutmama politikalarına, güçlü protokollere (WireGuard, OpenVPN), güvenli sunucu konumlarına, yüksek hızlara, yalnızca RAM kullanan sunuculara, kill switch özelliğine ve istihbarat paylaşım ittifaklarının (5/9/14 Eyes gibi) dışında bir hukuki yargı bölgesine bak.

Q9: Telefonumda ve akıllı TV'mde VPN kullanabilir miyim?

Evet. Modern VPN sağlayıcıları iOS, Android, macOS, Windows, Linux ve akıllı TV'ler için özel uygulamaların yanı sıra ev ağındaki tüm cihazları korumak için yönlendirici kurulumları sunar.

Q10: Kill Switch nedir?

Kill Switch, VPN bağlantısı koptuğunda cihazınızın internet bağlantısını otomatik olarak kesen bir güvenlik özelliğidir. Bu, şifrelenmemiş verilerinizin veya gerçek IP adresinizin sızmasını önler.

Kontrol Noktası 10: VPN hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Sanal özel ağların ve güvenli tünelleme protokollerinin teknik ve yapısal yönlerini keşfet.

Q1: WireGuard, OpenVPN ve IKEv2 arasındaki fark nedir?

WireGuard, hızlı hızlar ve kısa bağlantı süreleri sunan modern, hafif bir protokoldür (yalnızca yaklaşık 4.000 satır kod). OpenVPN, son derece güvenli ve sınanmış açık kaynaklı bir protokoldür. IKEv2, ağlar arasında geçiş yaparken hızla yeniden bağlanabildiği için mobil cihazlar için mükemmeldir.

Q2: Çift VPN veya Multi-Hop yönlendirme nedir?

Çoklu atlama, trafiğini art arda iki veya daha fazla VPN sunucusu üzerinden yönlendirir. Bu, ikinci bir şifreleme katmanı ekler ve bir sunucunun ele geçirilmesi durumunda gerçek IP adresinin ikinci atlamadan gizli kalmasına yardımcı olur.

Q3: WebRTC sızıntısı nedir ve VPN bunu nasıl önler?

WebRTC, VPN etkinken bile gerçek yerel ve genel IP adreslerini ortaya çıkarabilen bir tarayıcı protokolüdür. Premium VPN'ler masaüstü/mobil uygulamalarında ve tarayıcı uzantılarında WebRTC isteklerini engeller veya taklit eder.

Q4: Yalnızca RAM kullanan sunucular nedir ve neden önemlidir?

Geleneksel sunucular verileri ele geçirilebilen veya tehlikeye atılabilen sabit disklere yazar. Yalnızca RAM kullanan (disksiz) sunucular tamamen geçici bellekte (RAM) çalışır. Sunucu yeniden başlatıldığında veya kapatıldığında bellekteki veriler silinir.

Q5: Gizleme (obfuscation) VPN engellerini nasıl aşar?

Gizleme (veya "Stealth VPN"), VPN trafik paketlerini sıradan HTTPS web trafiği (443 numaralı port) gibi gösterir. Bu, hükümetlerin veya okul/ofis ağlarının VPN'leri engellemek için kullandığı Derin Paket İncelemesini (DPI) aşmaya yardımcı olur.

Kontrol Noktası 10: VPN hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Sanal özel ağların ve güvenli tünelleme protokollerinin teknik ve yapısal yönlerini keşfet.

Q6: Bölünmüş Tünel (Split Tunneling) nedir ve ne zaman kullanmalıyım?

Bölünmüş tünelleme, hangi uygulamaların şifreli VPN tüneli üzerinden yönlendirileceğini ve hangilerinin doğrudan internete bağlanacağını seçmeni sağlar. Hassas bankacılık uygulamalarını VPN üzerinden yönlendirip yerel oyunları doğrudan bağlayarak VPN'in eklediği gecikmeyi önlemek için kullan.

Q7: İleri Gizlilik (Mükemmel İleri Gizlilik) nasıl çalışır?

PFS, her oturum için benzersiz ve geçici bir şifreleme anahtarının üretilmesini sağlar. Özel anahtar gelecekte ele geçirilse bile, bağımsız anahtarlar kullanıldığı için geçmiş veya gelecek oturumların şifresini çözmekte kullanılamaz.

Q8: 5/9/14 Eyes ittifakları nedir ve neden önemsemeliyim?

Yargı yetkisi, bir sağlayıcının karşılaşabileceği yasal süreci etkileyebilir; ancak pratik gizlilik riski ayrıca sağlayıcının hangi verileri sakladığına, teknik mimarisine, sahipliğine, şeffaflık raporlamasına ve denetim geçmişine bağlıdır.

Q9: DNS Sızıntı Koruması nedir?

DNS sızıntı koruması, cihazının web sitesi arama sorgularını (DNS sorguları) İSS'nin sunucuları yerine VPN'in özel, şifreli DNS sunucuları üzerinden göndermesini sağlar. Bu, İSS'nin hangi siteleri ziyaret ettiğini izlemesini engeller.

Q10: Bir VPN'i kimin işlettiğini ve desteklediğini neden kontrol etmelisin?

İtibar önemlidir. Güvenmeden önce şirketin sahiplerini ve yöneticilerini araştır, herkese açık üçüncü taraf denetimlerine bak ve bağımsız güvenlik uzmanlarının ve basının ne dediğini kontrol et. [1]

Bölüm 11: 10 ilginç VPN gerçeği ve gerçek dünya içgörüsü

VPN'lerin tarihi, pazarı ve teknolojisiyle ilgili bu çok değerli, gerçek dünya bilgilerini incele.

1. İLK VPN PROTOKOLÜ

1990'larda Microsoft öncülüğündeki bir grubun geliştirdiği erken bir VPN protokolü olan PPTP (Point-to-Point Tunneling Protocol) artık güvensiz kabul edilir; bu yüzden modern VPN'ler WireGuard veya OpenVPN kullanır. [1]

2. PİYASA DEĞERLEMESİ

Küresel VPN pazarı, artan uzaktan çalışma ihtiyaçları ve kurumsal güvenlik talepleriyle hızla büyümüştür.

3. WIREGUARD DEVRİMİ

WireGuard, verimlilik için tasarlanmış son derece sadeleştirilmiş bir kod tabanına sahiptir; bu da güvenlik açıkları açısından geleneksel protokollerden daha kolay denetlenmesini sağlar. [3]

4. KATI DENETİM STANDARTLARI

Önde gelen VPN sağlayıcıları günlük tutmama iddialarını denetlemesi için Deloitte, KPMG veya PwC gibi firmalarla, uygulamalarını ve sunucularını test etmesi için Cure53 gibi güvenlik firmalarıyla çalışır. [4]

5. 5 GÖZ İTTİFAKININ KÖKENLERİ

ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda'dan oluşan Five Eyes istihbarat ortaklığı, Müttefiklerin II. Dünya Savaşı dönemindeki sinyal istihbaratı iş birliğinden doğmuştur.

6. DERİN PAKET İNCELEMESİ

Gelişmiş güvenlik duvarları, ağ paketi meta verilerini analiz etmek ve standart VPN bağlantı özelliklerini engellemek için Derin Paket Denetimi (DPI) kullanır.

7. KURUMSAL KULLANIM

Birçok kuruluş, uzaktan çalışan personeline veritabanları gibi iç sistemlere erişmesi için VPN verir; bu da VPN'leri yaygın bir iş yeri güvenlik aracı yapar.

8. MERKEZİ OLMAYAN VPN'LER

Merkezsiz VPN'ler (dVPN'ler), trafiği eşler tarafından işletilen düğümlerden oluşan bir ağa dağıtarak tek bir merkezi sağlayıcıya bağımlılığı azaltır.

9. TOR VE VPN ANONİMLİĞİ

VPN trafiği tek bir sağlayıcı üzerinden tüneller; Tor (The Onion Router) ise gizliliği en üst düzeye çıkarmak için trafiği üç gönüllü röle (giriş, orta, çıkış) üzerinden gönderir. [5]

10. VERİ İHLALLERİNİN MALİYETİ

VPN'i, her kullanıcıyı ve cihazı kontrol eden sıfır güven erişim modeliyle birleştirmek, kuruluşların verileri korumasına ve veri ihlallerinin zararını sınırlamasına yardımcı olur.

Teknik Referanslar ve Kaynaklar

Bu çalışma kâğıdında kullanılan atıf yapılan yayınlar, şifreleme belirtimleri ve resmî belge standartları.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Cevap Anahtarı: VPN Sağlayıcılarını, Güvenlik Standartlarını, Denetimleri ve Kayıt Politikalarını Değerlendirme

1 **Denetlenmiş Kayıt Politikası** PROTOKOLLER — **Doğru cevap: B**

ÖĞRETMEN NOTU

Bağımsız olarak denetlenmiş bir kayıt tutmama politikası, bir sağlayıcının sıfır bilgi gizliliği iddialarını kontrol etmenin en pratik yoludur. Gösterişli pazarlama veya kendi beyanları yeterli değildir. Kaynak: Deloitte Advisory, Cure53 Audit.

2 **WireGuard üstünlüğü** GECİKME — **Doğru cevap: D**

ÖĞRETMEN NOTU

WireGuard, kompakt kod tabanıyla (~4.000 satır) çekirdek alanında modern ve hızlı bağlantı yönlendirmesi sunar; bu da denetimleri son derece verimli kılar. Kaynak: IETF Protocol RFC, WireGuard Project.

3 **Soru 3** — **Doğru cevap: B**

ÖĞRETMEN NOTU

Ücretsiz VPN'ler de sunucuları için ödeme yapar ve FTC, bazı VPN uygulamalarının kullanıcı verilerini örneğin reklam sunmak için üçüncü taraflarla paylaştığı konusunda uyarıyor.

4 **Hukuki Yargı Bölgeleri** YÖNLENDİRME DENETİMLERİ — **Doğru cevap: C**

ÖĞRETMEN NOTU

Yargı yetkisi, VPN'in gözetim yasalarına, yerel veri saklama zorunluluklarına ve gizli hükümet celp emirlerine tabi olup olmadığını belirler. Kaynak: Privacy Rights Clearinghouse.

5 **Kill Switch koruması** GİZLİLİK — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kill switch, tünel koparsa sistem ağ adaptörü yönlendirmesini hemen keser ve gerçek IP ile DNS ifşası sızıntılarını önler. Kaynak: IETF Tunnel RFC.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Kötü Amaçlı Yazılım Sınırlamaları** IP MASKELEME — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

VPN güvenli bir şifreli hat sağlar ancak yükleri veya dosyaları taramaz. Kötü amaçlı yazılımı engellemek için antivirüs yazılımı gerekir. Kaynak: Deloitte Advisory.

7 **Bağımsız denetim** HIZLAR — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Denetim raporları sunucu yazılımı yapılandırmalarını, yalnızca RAM kullanımı uyumluluğunu ve kayıt veritabanlarının bulunmadığını doğrular. Kaynak: Deloitte Advisory, Cure53 Audit.

8 **Soru 8** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Sağlayıcılar kendi ülkelerinin yasalarına uymak zorundadır; bu yasalar veri saklama kurallarını ve elindeki verileri teslim etme emirlerini içerebilir.

9 **Protokol kod tabanı boyutu** GÜVENLİK DUVARLARI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Daha küçük bir kod tabanı potansiyel saldırı yüzeyini azaltır ve güvenlik ekiplerinin protokol bütünlüğünü doğrulamasını kolaylaştırır. Kaynak: WireGuard Project.

10 **Reklam Gelirleştirme** KAYIT TUTMAMA — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Abonelik ücretleri olmadan ücretsiz VPN'ler gelir elde etmek için veri madenciliğine, trafik profillemeye ve tarayıcı reklam enjeksiyonlarına dayanır. Kaynak: EDRi Retention Guidelines.

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

F 1. WireGuard	H 2. Denetlenmiş Kayıtlar	E 3. Yargı Yetkisi	B 4. Kill Switch
C 5. Five Eyes	A 6. Ücretsiz VPN	D 7. Yalnızca RAM'li Sunucular	G 8. OpenVPN

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 KAYIT TUTMAMA	2 WIREGUARD	3 KILL SWITCH	4 YARGI YETKİSİ
5 RAM SUNUCUSU	6 DENETİM		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 E – BEŞGÖZ	2 A – WIREGUARD	3 H – OPENVPN	4 F – ÜCRETSİZVPN
5 D – KILLSWITCH	6 G – RAMSUNUCUSU	7 C – YARGIYETKİSİ	8 B – KAYITTUTMAMA

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin WireGuard, Denetlenmiş Kayıtlar ve Yargı Yetkisi terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

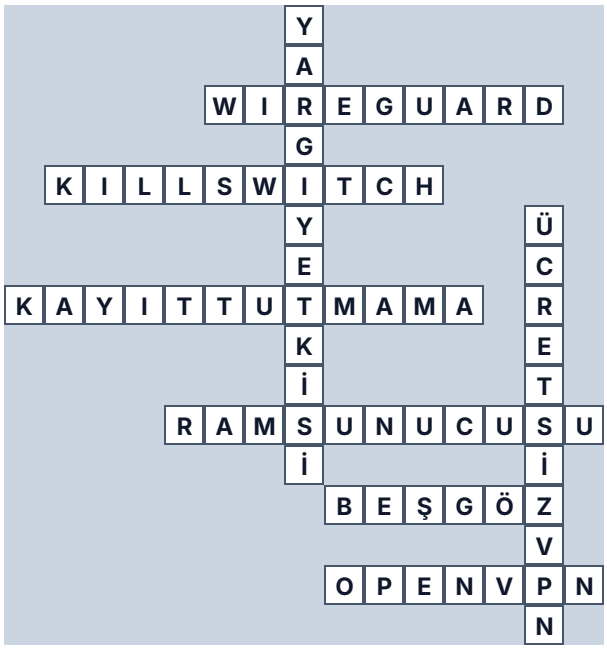
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

İ	İ	D	J	Ö	L	I	R	A	F	N	İ	M	Ç	L
S	C	Ç	Ğ	H	B	B	A	N	P	K	O	U	Ş	H
İ	Y	F	Y	R	G	V	M	Ü	Ğ	E	P	Ş	M	Ş
K	İ	P	D	S	R	K	S	O	J	L	R	Ğ	İ	O
T	Ğ	Y	N	K	Ü	T	U	M	Y	Ö	Ö	B	Ü	A
E	J	O	L	B	J	H	N	F	H	M	Y	C	C	B
Y	Z	Z	Y	B	L	U	U	V	K	Ç	E	N	R	E
I	Ü	O	Ö	V	Ğ	D	C	Y	C	Ü	K	E	E	Ş
G	G	Ğ	Z	Ü	Ç	N	U	P	İ	Ü	V	P	T	G
R	J	Z	A	L	P	Z	S	P	K	G	R	U	S	Ö
A	K	A	Y	I	T	T	U	T	M	A	M	A	İ	Z
Y	F	J	W	I	R	E	G	U	A	R	D	Ü	Z	I
C	Y	K	I	L	L	S	W	I	T	C	H	Ç	V	C
Y	N	T	Z	N	Z	T	Ş	B	Ğ	U	O	V	P	Ç
L	K	N	P	V	N	E	P	O	Ğ	O	Ü	Y	N	Z

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: WIREGUARD Yaklaşık 4.000 satırlık, yüksek düzeyde denetlenebilir kod kullanan modern ve hızlı protokol (9 harf)

3 soldan sağa: KILLSWITCH Güvenli tünel bağlantısı kesilirse internet yönlendirmesini engelleyen güvenlik mekanizması (10 harf)

5 soldan sağa: KAYITTUTMAMA Bağımsız üçüncü taraf siber güvenlik firmalarınca doğrulanmış gizlilik iddiası (12 harf)

6 soldan sağa: RAMSUNUCUSU Tamamen geçici bellek üzerinde çalışan ve veri depolamayı önleyen donanım altyapısı (11 harf)

7 soldan sağa: BEŞGÖZ ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda arasındaki uluslararası istihbarat paylaşım ittifakı (6 harf)

8 soldan sağa: OPENVPN WireGuard'dan çok daha büyük bir kod tabanına sahip, olgun ve yaygın biçimde denetlenmiş açık kaynaklı protokol (7 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: YARGIYETKİSİ VPN sağlayıcısının yasal yükümlülüklerini belirleyen coğrafi bölge (12 harf)

4 yukarıdan aşağı: ÜCRETSİZVPN Genellikle tarayıcı verilerini kaydedip satarak gelir elde eden yüksek riskli bağlantı hizmeti (11 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. U G E I W A R D R — **WIREGUARD**
2. İ A I Y Y İ S R T K E G — **YARGIYETKİSİ**
3. B Ş G Z Ö E — **BEŞGÖZ**
4. U S U N M U U C R A S — **RAMSUNUCUSU**
5. A A T U A Y T M T K M I — **KAYITTUTMAMA**
6. C S L I T K I W H L — **KILLSWITCH**
7. Z T Ü C İ N V P R S E — **ÜCRETSİZVPN**
8. P N N O P V E — **OPENVPN**

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"RAPORLARINI GÜVENLİ BİR SİSTEMLE KARŞILAŞTIR"

Vaka çalışmaları cevap anahtarı

A Senaryo A: Genel Ağ Güvenliği

PAKET DİNLEME VE ŞİFRELEME | Sarah'nın İkilemi

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Riskler: Paket dinleme, veri ele geçirme ve ortadaki adam saldırıları. Aynı kafe ağındaki biri giriş bilgilerini veya ödev dosyasını yakalayabilir.
- VPN Koruması: Ağ paketi yüklerini şifreler; VPN doğru yapılandırıldığında yakalanan tünel trafiğini pasif yerel ağ dinleyicileri için okunamaz kılar.

B Senaryo B: Engellenen Kaynaklara Erişim

COĞRAFİ ENGEL VE IP'LER | Alex'in İkilemi

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Engelleme nedeni: Yayın sunucusu coğrafi engelleme kullanır; bu, gezginin yerel IP adresini fiziksel ülkesiyle eşleştirir ve bölgesel lisanslamaya göre engeller.
- VPN nasıl yardımcı olur: Trafiği kendi ülkesindeki bir sunucudan geçirerek gerçek konumunu maskeler. Site ana ülkedeki IP'yi görür ve erişime izin verir.