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

VPN nedir? Çalışma kâğıdı

Ağ protokolleri, tünelleme ve güvenlik denetimleri üzerine pratik alıştırmalar.

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

- Veri tünelleme ve kapsülleme kavramını açıkla.
- Standart protokol yapılandırmalarını ve şifreleme yöntemlerini belirle.
- Sanal özel ağlarda sunucuların ve IP maskelemenin rollerini analiz et.
- ISS'lerin gezinmeyi nasıl izlediğini ve VPN'in bunu nasıl önlediğini anla.
- Sanal ağ topolojisinin işlevsel sınırlarını ayırt et.

VPN NEDİR REHBERİ TALİMATLARI

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: vaka çalışması bölümündeki gerçek dünya senaryoları. Hızlı Düşün bonus etkinliğiyle bitir.

VPN NEDİR? (GİRİŞ)

Sanal Özel Ağ, yalnızca bir gizlilik anahtarından ibaret değildir. İnternet trafiğinizi uzak bir sunucu üzerinden yönlendiren şifreli bir tüneldir. Bu, IP adresinizi gizler, İSS'nizin çevrimiçi eylemlerinizin kayıtlarını derlemesini önler ve verilerinizi herkese açık ağlarda güvenceye alır. Terminolojiyi anlamak, dijital güvenliği korumak için çok önemlidir.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. Sanal Özel Ağın (VPN) temel işlevi nedir?

- A. İnternet tarayıcısının görüntüleme hızını artırmak için
- B. Veri paketlerini şifrelemek ve genel IP'ni gizlemek
- C. Web sitesi çerez veritabanlarını yerel olarak depolamak için
- D. Fiziksel bilgisayar donanımını değiştirmek için

2. VPN bağlamında ağ tünelleme nedir?

- A. Yinelenen ağ günlük dosyalarını silmek
- B. Yerel veritabanı depolama dosyalarını kurmak
- C. Dosyaları yerel ağdaki diğer bilgisayarlarla paylaşmak
- D. Bir ağ paketini başka bir güvenli paketin içine yerleştirmek

3. VPN trafiğini korumak için yaygın olarak hangi şifreleme standardı kullanılır?

- A. Eski DES şifrelemesi
- B. Modern AES-256 standardı
- C. Düz metin base64 kodlaması
- D. Standart rot13 şifrelemesi

4. Ağ trafiğinin hangi bileşeni VPN tarafından şifrelenir?

- A. Yalnızca yerel cihaz ağ yazdırma işleri
- B. Fiziksel ethernet kablosu yönlendirme yolu
- C. Ağ paketinin veri yükü bölümünün tamamı
- D. Yalnızca web tarayıcısı arama geçmişin

5. Ağ iletişiminde 'şifreleme' terimi ne anlama gelir?

- A. Düz metin verisini okunamaz şifreli metne dönüştürmek
- B. Eski iletişim kayıtlarını silmek
- C. Yerel bant genişliği hız sınırlarını artırmak
- D. Veritabanı erişim anahtarlarını herkese açık paylaşmak

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. VPN, herkese açık Wi-Fi'de yerel dinlemeyi önlemek için trafiğinizi şifreler.

- ○ Doğru
- ○ Yanlış

7 Soru 7

7. VPN, yönlendirici cihazınızın donanım yapılandırmasını fiziksel olarak değiştirir.

- ○ Doğru
- ○ Yanlış

8 Soru 8

8. Tünelleme protokolleri, veri paketlerini şifreli bir aktarım katmanına sarar.

- ○ Doğru
- ○ Yanlış

9 Soru 9

9. Simetrik şifreleme, trafiği şifrelemek ve çözmek için aynı anahtarı kullanır.

- ○ Doğru
- ○ Yanlış

10 Soru 10

10. VPN kullanmak, internet bağlantını çevrimdışı elektrik kesintilerine karşı fiziksel olarak bağışık kılar.

- ○ Doğru
- ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Trafiğinizi güvence altına almak için VPN, veri paketlerinizi başka bir protokolün içine sarar; bu işleme _____ denir.

2. Yayın akışı sırasında indirme hızlarınız yavaşsa bunun nedeni sınırlı ağ _____ olabilir.

3. Yalnızca belirli bir ülkede kullanılabilen bir yayın hizmeti, küresel kullanıcıları kısıtlamak için bir _____ kullanır.

4. Şifreleme ve bağlantı parametrelerini tanımlayan bağlantı kurallarına VPN _____ denir.

5. Bilgisayarınız, ağ trafiğini izlemek ve güvenli olmayan bağlantıları engellemek için yerel bir _____ kullanır.

6. Bir VPN'e bağlandığınızda, genel IP adresinizi gizlemek için verileriniz uzak bir _____ üzerinden yönlendirilir.

KELİME BANKASI

BANT GENİŞLİĞİ | COĞRAFİ ENGEL | GİZLİLİK | GÜVENLİK DUVARI | PROTOKOL | SAĞLAYICI | SUNUCU | TÜNELLEME

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Ağ kavramı eşleştirme

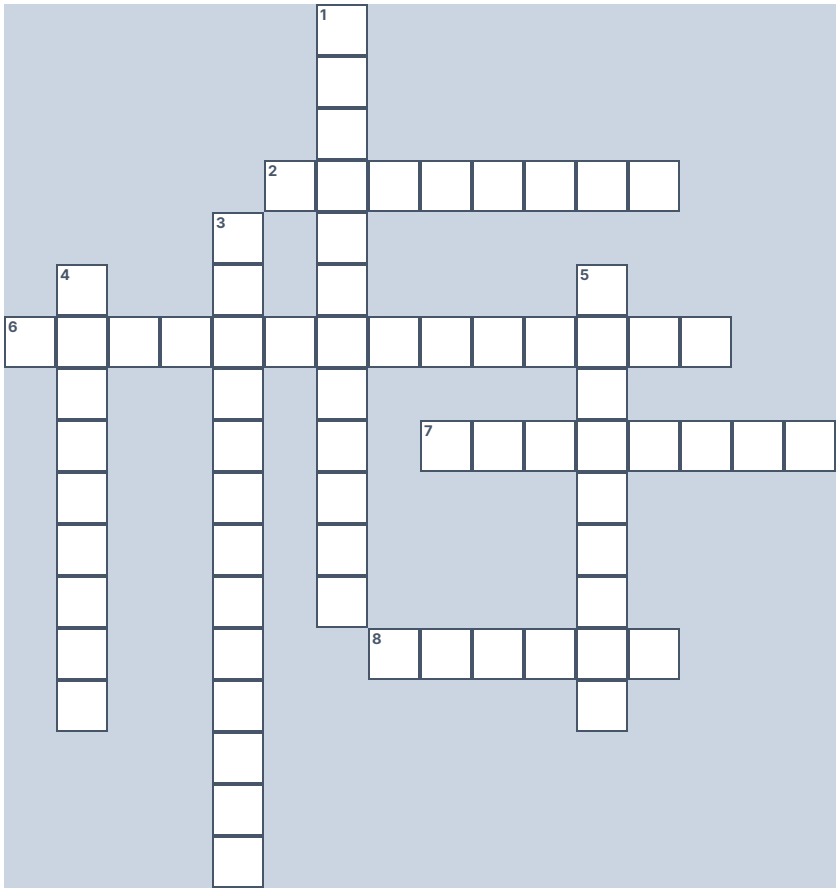
TANIM EŞLEŞTİRME

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

☐	1. Tünelleme	A	Trafiğinizi yönlendiren ve IP adresinizi maskeleyen uzak bilgisayar.
☐	2. Protokol	B	Trafiğini taşıyan ve şifrelenmemiş etkinliği görebilen İnternet Servis Sağlayıcısı.
☐	3. Bant genişliği	C	Fiziksel konuma göre web erişimini engelleyen kısıtlama.
☐	4. Sunucu	D	Yetkisiz trafiği izleyen ve engelleyen güvenlik sistemi.
☐	5. Coğrafi Engel	E	Verinin ağ üzerinden nasıl iletileceğini belirleyen kurallar kümesi.
☐	6. Güvenlik duvarı	F	İzlenmeden veya kamusal gözetimden uzak olma durumu.
☐	7. GİZLİLİK	G	Bir bağlantı üzerinden en yüksek veri aktarım hızı.
☐	8. İSS	H	Güvenli aktarım için veri paketlerini başka bir paketin içine sarmak.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

2. Verilerin ağ üzerinden nasıl iletileceğini belirleyen kurallar bütünü (8)

6. Yetkisiz trafiği izleyen ve engelleyen güvenlik sistemi (14)

7. İzlenmekten veya kamusal gözetimden uzak olma durumu (8)

8. Trafiğinizi yönlendiren ve IP adresinizi gizleyen uzak bilgisayar (6)

YUKARIDAN AŞAĞI

1. Fiziksel konuma göre web erişimini engelleyen kısıtlama (12)

3. Bir bağlantı üzerindeki azami veri aktarım hızı (13)

4. Güvenli iletim için veri paketlerini başka bir paketin içine sarma (9)

5. İnternet servis sağlayıcısı; şifrelenmedikçe trafiğinizi kaydeder (9)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

2 soldan sağa: Verilerin ağ üzerinden nasıl iletileceğini belirleyen kurallar bütünü (8 harf):

6 soldan sağa: Yetkisiz trafiği izleyen ve engelleyen güvenlik sistemi (14 harf):

7 soldan sağa: İzlenmekten veya kamusal gözetimden uzak olma durumu (8 harf):

8 soldan sağa: Trafiğinizi yönlendiren ve IP adresinizi gizleyen uzak bilgisayar (6 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Fiziksel konuma göre web erişimini engelleyen kısıtlama (12 harf):

3 yukarıdan aşağı: Bir bağlantı üzerindeki azami veri aktarım hızı (13 harf):

4 yukarıdan aşağı: Güvenli iletim için veri paketlerini başka bir paketin içine sarma (9 harf):

5 yukarıdan aşağı: İnternet servis sağlayıcısı; şifrelenmedikçe trafiğinizi kaydeder (9 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

TÜNELLEME PROTOKOL BANTGENİŞLİĞİ SUNUCU COĞRAFİENGEL
GÜVENLİKDUVARI GİZLİLİK SAĞLAYICI

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. TÜNELLEME**
- **B. PROTOKOL**
- **C. BANTGENİŞLİĞİ**
- **D. SUNUCU**
- **E. COĞRAFİENGEL**
- **F. GÜVENLİKDUVARI**
- **G. GİZLİLİK**
- **H. SAĞLAYICI**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Verilerin ağ üzerinden nasıl iletileceğini belirleyen kurallar bütünü.
2. Fiziksel konuma göre web erişimini engelleyen kısıtlama.
3. Yetkisiz trafiği izleyen ve engelleyen güvenlik sistemi.
4. İzlenmekten veya kamusal gözetimden uzak olma durumu.
5. İnternet servis sağlayıcısı; şifrelenmedikçe trafiğinizi kaydeder.
6. Güvenli iletim için veri paketlerini başka bir paketin içine sarma.
7. Trafiğinizi yönlendiren ve IP adresinizi gizleyen uzak bilgisayar.
8. Bir bağlantı üzerindeki azami veri aktarım hızı.

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. LLEÜTEMEN
2. ĞGAENBİNİŞLİT
3. COEİENĞFLAGR
4. LİKLİGİZ
5. OKRLTPOO
6. CUSNUU
7. VRUGDÜVILAKEİN
8. IACSLAYIĞ

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Bir IP adresinin ele verebileceği şeyler			
2	VPN'lerle ilgili efsaneler			
3	İnternet üzerinde yol alan şeyler			
4	İyi bir VPN sağlayıcısının verdiği sözler			
5	Şifreleyeceğin sırlar			
6	Bir VPN'in seni koruyamadığı şeyler			
7	Sahte Wi-Fi ağını fark etme yolları			
8	Gizlilikle ilgili sözcükler			
9	VPN kullanabilen cihazlar			
10	'Bağlan'a bastığında olan şeyler			
11	VPN kullanacağın yerler			
12	Seyahat ederken VPN kullanma nedenleri			
13	Tünele benzeyen gerçek hayattaki şeyler			
14	Bu çalışma kâğıdından aklında tutmak istediğin sözcükler			
15	VPN'i bir çocuğa anlatmak için sözcükler			

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

VPN, güvenliğini sağlamak için trafiğinizi şifreler. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp siber güvenlik mesajının 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

8	12	29	15	12	15	12	9	12	17	12		8	26	27	6	17	15	12

2	12	21		24	26	17	6	15	15	6		14	18	21	25

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: VPN kullanmak yasal mı?

VPN kullanımı birçok ülkede yasaldır, ancak bazı yargı bölgeleri VPN hizmetlerini kısıtlar, düzenler veya engeller. Kullanıcılar kullanmadan önce güncel yerel yasaları doğrulamalıdır. Daha fazla bilgi için VPN.com'daki yasallık kılavuzlarına bak.

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. [4]

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 trafiğini sıradan HTTPS trafiği (443 numaralı port) gibi gösterir. Bu, hükümetlerin veya okul/ofis ağlarının VPN'leri engellemek için kullandığı Derin Paket İncelemesini (DPI) aşmasına yardımcı olabilir.

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, İSS'in internet hız kısıtlamasını aşabilir mi?

Bazen. Bir İSS belirli etkinliklerin hızını seçici olarak düşürdüğünde VPN yardımcı olabilir, ancak tıkanıklığı, veri kotalarını, hesap düzeyindeki hız sınırlarını veya zayıf ağ kalitesini aşamaz.

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

PPTP (Point-to-Point Tunneling Protocol), Microsoft'un da aralarında bulunduğu bir satıcı grubu tarafından geliştirildi ve uzaktan erişim VPN'lerini desteklemek için Temmuz 1999'da RFC 2637 olarak yayımlandı. [6]

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. [4]

4. KATI DENETİM STANDARTLARI

Önde gelen VPN sağlayıcıları, bağımsız kod incelemeleri yaptırmak ve kullanıcı etkinliğini kaydetmediklerini doğrulatmak için (Cure53 veya PwC gibi) harici denetçiler tutar.

5. 5 GÖZ İTTİFAKININ KÖKENLERİ

Five Eyes ittifakı, ABD ile Birleşik Krallık arasındaki 1946 tarihli UKUSA sinyal istihbaratı anlaşmasından doğmuş, sonradan Kanada, Avustralya ve Yeni Zelanda katılmıştır.

6. DERİN PAKET İNCELEMESİ

Derin Paket İncelemesi (DPI) yalnızca başlıkları değil, paket içeriklerini ve trafik desenlerini inceler; bazı güvenlik duvarları yaygın VPN protokollerini tespit edip engellemek için DPI kullanır.

7. KURUMSAL KULLANIM

Dünya genelinde kurumsal çalışanların büyük bir yüzdesi iç veritabanlarına giriş yapmak için güvenli VPN'ler kullanır; bu da onu önemli bir güvenlik standardı 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 hiçbir rölenin her iki ucu birden bilmemesi için trafiği üç gönüllü röle (giriş, orta ve çıkış) üzerinden gönderir.

10. VERİ İHLALLERİNİN MALİYETİ

VPN ile sıfır güven güvenli erişim modeli kullanmak, kuruluşların fikri mülkiyeti korumasına ve veri ihlallerinin mali etkisini azaltmasına yardımcı olur.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

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

[4] 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/

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

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

Cevap Anahtarı: VPN Nedir Çalışma Kâğıdı

1 **Birincil işlev** PROTOKOLLER **Doğru cevap: B**

ÖĞRETMEN NOTU

VPN'in ana görevi, paket yük verilerini koruyan ve kullanıcının genel IP adresini maskeleyen şifreli bir tünel kurmaktır. Kaynak: IETF Tunnel RFC.

2 **Ağ Tünelleme** GECİKME **Doğru cevap: D**

ÖĞRETMEN NOTU

Tünelleme protokolleri, herkese açık ağlardan güvenle geçmek için özgün veri paketlerini dıştaki taşıyıcı paketlerin içine kapsüller. Kaynak: IETF Tunnel RFC.

3 **Soru 3** **Doğru cevap: B**

ÖĞRETMEN NOTU

VPN trafiğini korumak için yaygın olarak hangi şifreleme standardı kullanılır? → Modern AES-256 standardı

4 **Şifreli Bileşenler** YÖNLENDİRME DENETİMLERİ **Doğru cevap: C**

ÖĞRETMEN NOTU

VPN, IP veri paketlerinin yük bölümünün tamamını şifreler ve iletimin içeriğini gizli tutar. Kaynak: IETF Tunnel RFC.

5 **Soru 5** **Doğru cevap: A**

ÖĞRETMEN NOTU

Şifreleme, düz metni okunamaz şifreli metne dönüştürmek için bir algoritma ve bir anahtar kullanır.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Dinlemeyi Engelleme** IP MASKELEME — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Şifreli tüneller, paket yüklerinin yerel Wi-Fi ağlarındaki verileri yakalayan kişiler tarafından okunamaz kalmasını sağlar. Kaynak: Deloitte Advisory.

7 **Donanım değişiklikleri** HIZLAR — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

VPN'ler yazılım tabanlı ağ tünelleridir ve ağ geçidi yönlendiricisinin donanımını fiziksel olarak değiştirmez. Kaynak: Cure53 Audit.

8 **Tünelleme Paketleri** PAKET DİNLEME RİSKİ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Tünelleme, özgün ağ paketlerini iletim için aktarım başlıklarının içine sararak çalışır. Kaynak: IETF Tunnel RFC.

9 **Simetrik Anahtarlar** GÜVENLİK DUVARLARI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Simetrik kriptografi, ağ akışlarını hem şifrelemek hem de çözmek için ortak bir anahtardan yararlanır. Kaynak: WireGuard Project.

10 **Güç bağışıklığı** KAYIT TUTMAMA — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

VPN yalnızca etkin bağlantı sinyallerini şifreler; yerel elektrik kesintilerinden kaynaklanan hizmet kopmalarını önleyemez. 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

H 1. Tünelleme	E 2. Protokol	G 3. Bant genişliği	A 4. Sunucu
C 5. Coğrafi Engel	D 6. Güvenlik duvarı	F 7. GİZLİLİK	B 8. İSS

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 TÜNELLEME	2 BANT GENİŞLİĞİ	3 COĞRAFİ ENGEL	4 PROTOKOL
5 GÜVENLİK DUVARI	6 SUNUCU		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 B – PROTOKOL	2 E – COĞRAFİENGEL	3 F – GÜVENLİKDUVARI	4 G – GİZLİLİK
5 H – SAĞLAYICI	6 A – TÜNELLEME	7 D – SUNUCU	8 C – BANTGENİŞLİĞİ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin Tünelleme, Protokol ve Bant genişliği terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

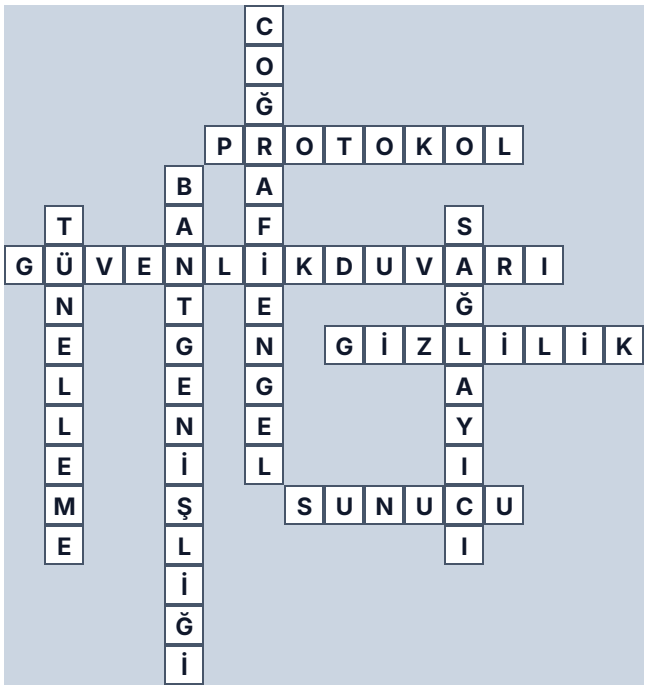
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: PROTOKOL Verilerin ağ üzerinden nasıl iletileceğini belirleyen kurallar bütünü (8 harf)

6 soldan sağa: GÜVENLİKDUVARI Yetkisiz trafiği izleyen ve engelleyen güvenlik sistemi (14 harf)

7 soldan sağa: GİZLİLİK İzlenmekten veya kamusal gözetimden uzak olma durumu (8 harf)

8 soldan sağa: SUNUCU Trafiğinizi yönlendiren ve IP adresinizi gizleyen uzak bilgisayar (6 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: COĞRAFİENGEL Fiziksel konuma göre web erişimini engelleyen kısıtlama (12 harf)

3 yukarıdan aşağı: BANTGENİŞLİĞİ Bir bağlantı üzerindeki azami veri aktarım hızı (13 harf)

4 yukarıdan aşağı: TÜNELLEME Güvenli iletim için veri paketlerini başka bir paketin içine sarma (9 harf)

5 yukarıdan aşağı: SAĞLAYICI İnternet servis sağlayıcısı; şifrelenmedikçe trafiğinizi kaydeder (9 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	LLEÜTEMEN	TÜNELLEME	5.	OKRLTPOO	PROTOKOL
2.	ĞGAENBİNİŞLİT	BANTGENİŞLİĞİ	6.	CUSNUU	SUNUCU
3.	COEİENĞFLAGR	COĞRAFİENGEL	7.	VRUGDÜVILAKEİN	GÜVENLİKDUVARI
4.	LİKLİGİZ	GİZLİLİK	8.	IACSLAYIĞ	SAĞLAYICI

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"GİZLİLİĞİNİ GÜVENLİ BİR TÜNELLE KORU"

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.