Ad Soyad: _____ Tarih: _____ Puan: _____

WireGuard ve OpenVPN karşılaştırması Çalışma kâğıdı

WireGuard ve OpenVPN protokollerinin, kod tabanı boyutlarının, hızın ve şifreleme standartlarının karşılaştırılması

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

- Protokollerin kod tabanı karmaşıklığını ve denetim hızını karşılaştır.
- Çekirdek alanı içinde çalışmanın performans kazanımlarını analiz et.
- OpenSSL şifrelerini WireGuard'ın modern şifrelemesiyle karşılaştır.
- Eşler arası el sıkışmalar için açık ve özel anahtar çiftleri oluştur.
- VPN trafiğini TCP ve UDP güvenlik duvarı bağlantı noktalarından yönlendir.

PROTOKOL KARŞILAŞTIRMA 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: modern protokolleri denetleme. Hızlı Düşün bonus etkinliğiyle bitir.

WIREGUARD VE OPENVPN (GİRİŞ)

Bir VPN protokolü seçmek, hız ile yapılandırma seçenekleri arasında denge kurmayı gerektirir. OpenVPN onlarca yıldır standart olmuş ve TCP/UDP yapılandırma esnekliği sunar. WireGuard, yalnızca 4.000 satır kodla doğrudan çekirdek alanında çalışan modern bir alternatiftir. Protokol farklarını anlamak, güvenli ağlarını optimize etmenin anahtarıdır.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. WireGuard protokolünün yaklaşık kod tabanı boyutu nedir?

- A. Yaklaşık 70.000 satır
- B. 100.000'den fazla satır
- C. 1.000 satırdan az
- D. Yaklaşık 4.000 satır

2. WireGuard işletim sisteminin hangi alanında çalışır?

- A. Kullanıcı alanı
- B. Çekirdek alanı
- C. Uygulama alanı
- D. Sanal alan

3. OpenVPN öncelikli olarak hangi kriptografik kitaplığa dayanır?

- A. ChaCha20-Poly1305
- B. OpenSSL kriptografik kitaplığı
- C. Noise protokol çerçevesi
- D. Düz metin DES kodlaması

4. WireGuard'ın OpenVPN'e göre temel bir performans avantajı nedir?

- A. Daha hızlı bağlantı el sıkışmaları ve daha düşük gecikme
- B. Genel IP adreslerine olan ihtiyacı atlayarak
- C. Eski çevirmeli bağlantı için yerleşik yerel destek
- D. Mobil cihazlarda sıfır pil yükü

5. WireGuard eş bağlantılarının kimliğini nasıl doğrular?

- A. Standart kullanıcı parolalarını değiş tokuş ederek
- B. Alan adı kayıt sertifikalarını doğrulayarak
- C. Statik genel ve özel anahtar çiftleri kullanarak
- D. Donanım seri numaralarını kontrol ederek

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. WireGuard'ın kompakt kod tabanı, onu denetlemeyi belirgin şekilde kolaylaştırır.

○ Doğru ○ Yanlış

7 Soru 7

7. OpenVPN, çekirdek alanında çalıştığı için genellikle WireGuard'dan daha hızlıdır.

○ Doğru ○ Yanlış

8 Soru 8

8. OpenVPN son derece yapılandırılabilirdir ve hem UDP hem TCP protokollerini destekler.

○ Doğru ○ Yanlış

9 Soru 9

9. WireGuard, hızlı paket şifrelemesi için ChaCha20 gibi modern kriptografi kullanır.

○ Doğru ○ Yanlış

10 Soru 10

10. WireGuard, kimlik doğrulaması için karmaşık sertifika yetkilisi kurulumları gerektirir.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Modern _____ protokolü doğrudan işletim sistemi çekirdeğinin içinde çalışır.
2. Eski _____ protokolü OpenSSL kripto kitaplığına dayanır.
3. Kodu _____ içinde çalıştırmak bağlam değiştirme yükünü azaltır.
4. OpenVPN, paketleri sanal arayüzler üzerinden yönlendirerek _____ içinde çalışır.
5. WireGuard, bağlantı eşlerini tanımlamak için açık ve özel anahtardan oluşan _____ kullanır.
6. Küçük bir kod tabanı, yazılımın güvenlik açısından _____ düzeyini artırır.

KELİME BANKASI

ANAHTAR ÇİFTİ | ÇEKİRDEK ALANI | DENETLENEBİLİRLİK | KULLANICI ALANI | OPENSSL | OPENVPN | TCP VE UDP | WIREGUARD

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Ağ kavramı eşleştirme

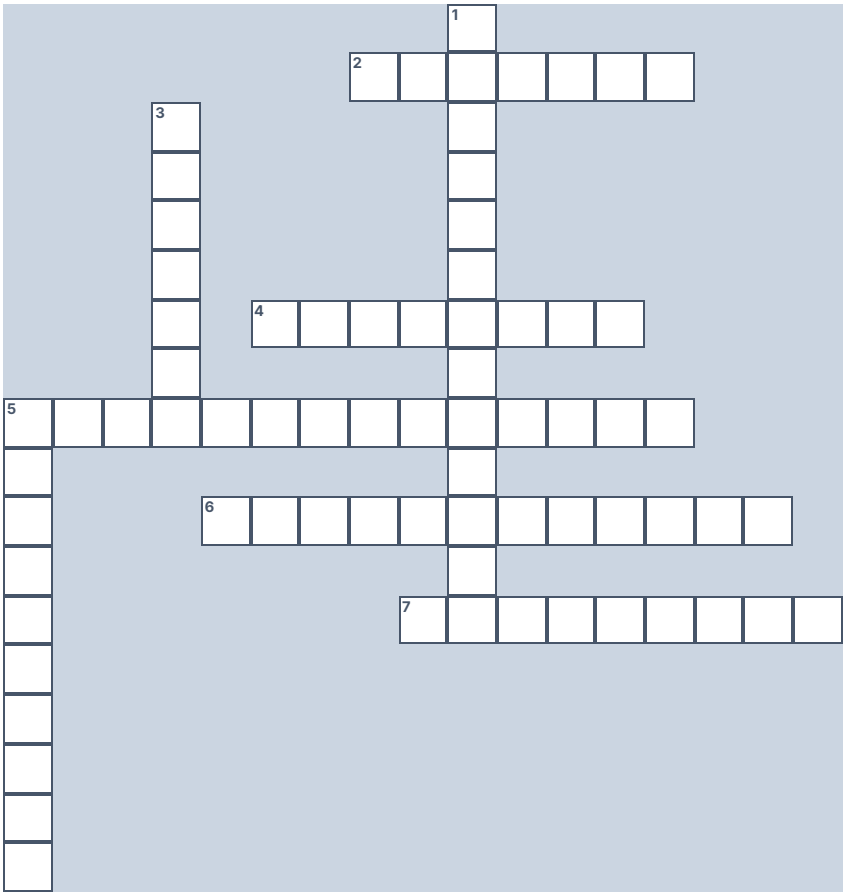
TANIM EŞLEŞTİRME

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

☐	1. WireGuard	A	OpenVPN'in çalıştığı, bağlam değiştirme yükü oluşturan yürütme alanı.
☐	2. OpenVPN	B	WireGuard kod tabanının, denetlemeyi çok daha kolay kılan küçük boyutu.
☐	3. Çekirdek Alanı	C	OpenVPN'in şifre algoritmaları için kullandığı şifreleme kütüphanesi.
☐	4. Kullanıcı Alanı	D	OpenVPN'in desteklediği taşıma protokolleri; WireGuard'ın kendisi yalnızca UDP üzerinden çalışır.
☐	5. 4.000 Satır	E	WireGuard'ın hız için çalıştığı işletim sistemi yürütme alanı.
☐	6. OpenSSL	F	WireGuard'ın eş bağlantılarını doğrulamak için kullandığı asimetrik belirteçler.
☐	7. Anahtar Çifti	G	Yüksek hız ve basit kod denetimi için tasarlanmış modern VPN protokolü.
☐	8. TCP/UDP	H	Büyük ve karmaşık bir yapılandırma kod tabanı kullanan sağlam eski protokol.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

2. Büyük ve karmaşık bir yapılandırma kod tabanı kullanan sağlam eski protokol (7)

4. OpenVPN'in desteklediği taşıma protokolleri; WireGuard'ın kendisi yalnızca UDP üzerinde çalışır (8)

5. OpenVPN'in çalıştığı ve bağlam değiştirme yükü yaratan yürütme alanı (14)

6. WireGuard'ın eş bağlantılarını doğrulamak için kullandığı asimetrik jetonlar (12)

7. Yüksek hız ve basit kod denetimi için tasarlanmış modern VPN protokolü (9)

YUKARIDAN AŞAĞI

1. WireGuard'ın hız için çalıştığı işletim sistemi yürütme alanı (13)

3. OpenVPN'in şifre algoritmaları için dayandığı kriptografik kitaplık (7)

5. WireGuard kod tabanının kompakt boyutu; denetlemeyi çok daha kolay hâle getirir (10)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

2 soldan sağa: Büyük ve karmaşık bir yapılandırma kod tabanı kullanan sağlam eski protokol (7 harf):

4 soldan sağa: OpenVPN'in desteklediği taşıma protokolleri; WireGuard'ın kendisi yalnızca UDP üzerinde çalışır (8 harf):

5 soldan sağa: OpenVPN'in çalıştığı ve bağlam değiştirme yükü yaratan yürütme alanı (14 harf):

6 soldan sağa: WireGuard'ın eş bağlantılarını doğrulamak için kullandığı asimetrik jetonlar (12 harf):

7 soldan sağa: Yüksek hız ve basit kod denetimi için tasarlanmış modern VPN protokolü (9 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: WireGuard'ın hız için çalıştığı işletim sistemi yürütme alanı (13 harf):

3 yukarıdan aşağı: OpenVPN'in şifre algoritmaları için dayandığı kriptografik kitaplık (7 harf):

5 yukarıdan aşağı: WireGuard kod tabanının kompakt boyutu; denetlemeyi çok daha kolay hâle getirir (10 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

WIREGUARD OPENVPN ÇEKİRDEKALANI KULLANICIALANI KOMPAKTKOD
OPENSSL ANAHTARÇİFTİ TCPVEUDP

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. OPENVPN**
- **C. ÇEKİRDEKALANI**
- **D. KULLANICIALANI**
- **E. KOMPAKTKOD**
- **F. OPENSSL**
- **G. ANAHTARÇİFTİ**
- **H. TCPVEUDP**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. OpenVPN'in şifre algoritmaları için dayandığı kriptografik kitaplık.
2. WireGuard'ın hız için çalıştığı işletim sistemi yürütme alanı.
3. Büyük ve karmaşık bir yapılandırma kod tabanı kullanan sağlam eski protokol.
4. WireGuard'ın eş bağlantılarını doğrulamak için kullandığı asimetrik jetonlar.
5. OpenVPN'in desteklediği taşıma protokolleri; WireGuard'ın kendisi yalnızca UDP üzerinde çalışır.
6. WireGuard kod tabanının kompakt boyutu; denetlemeyi çok daha kolay hâle getirir.
7. Yüksek hız ve basit kod denetimi için tasarlanmış modern VPN protokolü.
8. OpenVPN'in çalıştığı ve bağlam değiştirme yükü yaratan yürütme alanı.

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. NREDKÇAEIALKİ
3. KKOTOADPKM
4. TÇTARİAFİANH
5. VNNEOPP
6. NILALACNAKUIIL
7. OSSLPNE
8. VCEPTDUP

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	WireGuard'ı seçme nedenleri			
2	İyi bir VPN sağlayıcısının verdiği sözler			
3	OpenVPN'i seçme nedenleri			
4	Seyahat ederken VPN kullanma nedenleri			
5	İnternet sağlayıcının görebildiği şeyler			
6	Sahte Wi-Fi ağını fark etme yolları			
7	VPN'lerle ilgili efsaneler			
8	VPN kullanacağın yerler			
9	Günlük hayattaki hızlı şeyler			
10	Bir VPN'in seni koruyamadığı şeyler			
11	Kodun denetlenmesini kolaylaştıran şeyler			
12	Bir VPN'in gizleyebileceği şeyler			
13	WireGuard ile OpenVPN arasındaki farklar			
14	Gizlilikle ilgili sözcükler			
15	Bildiğin şifreleme adları			

Kontrol Noktası 8: VPN vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

SARAH (KAFEDEKİ ÖĞRENCİ)

👩‍💻 "Selam! Kafenin Wi-Fi'sindeyim ve VPN uygulamam WireGuard veya OpenVPN seçmeme izin veriyor. Kafe ağı ile telefonumun hotspot'u arasında yürürken görüntülü görüşmelerim kopuyor. Hangi protokolü seçmeliyim ve bu geçişi neden daha iyi yönetir?"

ALEX (GEZGİN ÖĞRENCİ)

👩‍💻 "Yurt dışında, çoğu VPN trafiğini engelliyor gibi görünen bir otel ağındayım. WireGuard hiç bağlanmıyor ama memleketimdeki okulumun kaynaklarına erişmem gerekiyor. Muhtemelen ne engelleniyor ve OpenVPN geçmeme nasıl yardımcı olabilir?"

Kontrol Noktası 9: Şifreyi Çöz

Protokol denetimi eğitimini tamamlamak için çekirdek alanında yürütmeyle 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

18	20	6	17	27	20	17	12		5	1	10	1		10	11	29	15	11
2	12	21		24	26	17	6	15	15	6		28	26	14	22	6	15	24

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: Protokoller neden önemlidir?

Protokol, VPN'inin tünelini nasıl kurduğunu, verilerini hangi şifrelemenin koruduğunu ve ne kadar hızlı bağlanıp yeniden bağlandığını belirler. WireGuard ve OpenVPN, çoğu VPN uygulamasının sunduğu iki açık kaynaklı protokoldür ve sadelik, hız ve yapılandırılabilirlik arasında farklı dengeler kurar.

Q3: Bunlardan biri diğerinden daha mı gizli?

Hiçbir protokol seni anonim yapmaz. İkisi de tünel trafiğini güçlü şifrelerle şifreler; gizliliğin çoğunlukla VPN sağlayıcısının neleri kaydettiğine ve anahtarları, hesapları ve sunucuları nasıl yönettiğine bağlıdır.

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: İkisi de açık kaynaklı mı?

Evet. WireGuard ve OpenVPN topluluk sürümü kaynak kodlarını yayımlar; böylece bağımsız araştırmacılar bunları inceleyebilir. WireGuard'ın küçük kod tabanı tam bir incelemeyi çok daha hızlı kılar.

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: Hangisi daha hızlı?

WireGuard genellikle daha hızlıdır: çekirdekte çalışır, hafif ChaCha20-Poly1305 şifrelemesi kullanır ve el sıkışmaları hızla tamamlar. OpenVPN'in yükü daha fazladır, ancak gerçek hızlar sunucu yüküne ve mesafeye de bağlıdır.

Q7: İkisi de hem TCP hem UDP üzerinden çalışabilir mi?

Hayır. OpenVPN, UDP veya TCP üzerinden çalışabilir ve TCP modu, UDP'yi engelleyen ağlarda yardımcı olur. WireGuard paketlerini yalnızca UDP üzerinden gönderir; bu yüzden yalnızca TCP'ye izin veren ağlarda başarısız olabilir. [4]

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 WireGuard ve OpenVPN'i kullanabilir miyim?

Evet. WireGuard çapraz platformdur; Windows, macOS, Linux, iOS ve Android için uygulamaları vardır ve OpenVPN istemcileri de aynı sistemler için mevcuttur. Çoğu VPN uygulaması ikisinden birini seçmene izin verir. [1]

Q10: WireGuard neden bu kadar küçüktür?

WireGuard, çok sayıda seçenek yerine tek bir sabit modern şifre kümesini destekler. Linux uygulaması 4.000 satırdan az kod gerektirir; bu da onu daha büyük VPN kod tabanlarından daha kolay denetlenebilir kılar. [3]

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: WireGuard hangi şifreleri kullanır?

WireGuard şifreleme için Poly1305 ile ChaCha20'yi, anahtar değişimi için Curve25519'u, özetleme için BLAKE2s'i ve el sıkışması için Noise çerçevesini kullanır. Şifre pazarlığı yoktur; bu nedenle kullanıcılar zayıf bir seçenek seçemez. [2]

Q3: OpenVPN hangi şifreleri ve kitaplıkları kullanabilir?

OpenVPN, OpenSSL kütüphanesiyle sıkı biçimde bütünleşiktir ve anahtar değişimi için TLS kullanır. Yöneticiler AES-256-GCM gibi veri kanalı şifrelerini seçebilir; bu esneklik sağlar ancak zayıf ayarlara da yer açar. [4]

Q4: Her protokol eşleri nasıl doğrular?

WireGuard eşleri, tıpkı SSH anahtarlarının değiş tokuşu gibi, statik genel anahtarlarla birbirini tanır ve her anahtar izin verilen tünel IP'leriyle eşlenir. OpenVPN ise genellikle X.509 sertifikalı bir sertifika yetkilisine dayanır ve çoğunlukla kullanıcı adı ve parolayla birleştirilir.

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: Wi-Fi'dan mobile geçtiğimde ne olur?

WireGuard bağlantısızdır: paketleri yeni adresten gönderir ve kısa bir el sıkışmadan sonra tünel devam eder. OpenVPN oturum durumunu tutar; bu nedenle bir ağ değişikliği, biraz daha uzun süren bir yeniden bağlantı gerektirebilir.

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: WireGuard daha hızlıysa OpenVPN hâlâ iyi bir seçim mi?

Evet. OpenVPN olgun ve yaygın biçimde kullanılır, UDP engellendiğinde TCP üzerinden çalışır ve sertifika tabanlı kurumsal kurulumları destekler. Çoğu sağlayıcı iki protokolü de sunar; böylece biri engellenirse veya yavaşsa kullanıcılar geçiş yapabilir.

Q9: Hangi bağlantı noktalarını kullanırlar?

OpenVPN'in standart portu 1194'tür, ancak 443 dahil herhangi bir UDP veya TCP portuna taşınabilir. WireGuard, yapılandırmasında belirlenen bir UDP portunu dinler; 51820 resmi örneklerinde kullanılan porttur.

Q10: Hangi protokolü elle kurmak daha kolaydır?

WireGuard genellikle daha basittir: bir anahtar çifti oluştur, genel anahtarları değiş tokuş et ve izin verilen IP'leri listele. OpenVPN sertifikalara, bir sertifika yetkilisine ve daha fazla seçeneğe ihtiyaç duyar; ancak .ovpn profilleri bunları tek bir dosyada toplar.

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. İKİ TAŞIMA YÖNTEMİ

OpenVPN tünelini UDP veya TCP üzerinden taşıyabilir ve TLS modunda kontrol ve veri kanalları tek bir portu paylaşır. [4]

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. MODERN KRİPTOGRAFİ

WireGuard, ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 ve HKDF'yi Noise protokol çerçevesi içinde birleştirir; kullanıcıların yanlış seçebileceği şifre seçenekleri yoktur. [2]

5. OPENVPN İÇİNDE OPENSSL

OpenVPN, OpenSSL kütüphanesiyle sıkı biçimde bütünleşiktir ve anahtar değişiminde kullanılan TLS dahil kriptografik yeteneklerinin çoğunu ondan alır. [4]

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. SSH TARZI ANAHTARLAR

WireGuard bağlantıları, tıpkı SSH anahtarlarının değiş tokuşu gibi, basit genel anahtarların değiş tokuşuyla kurulur; sertifika yetkilisi gerekmez. [1]

8. ÇAPRAZ PLATFORM

WireGuard ilk olarak Linux çekirdeği için yayımlandı ve artık Windows, macOS, BSD, iOS ve Android için de mevcuttur; bu nedenle aynı protokol çoğu cihazda çalışır. [1]

9. İLERİ GİZLİLİK

WireGuard, uzun vadeli bir anahtar sonradan sızsa bile kusursuz ileri gizlilik sağlamak için simetrik oturum anahtarlarını döndürmek üzere Noise_IK el sıkışmasını birkaç dakikada bir tekrarlar. [2]

10. TUN/TAP ARAYÜZLERİ

OpenVPN, çoğu platformda bulunan ve tünelin paketlerini taşıyan TUN/TAP sanal ağ arayüzüyle çalışmak üzere tasarlanmıştır. [4]

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[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

Cevap Anahtarı: WireGuard ve OpenVPN protokollerini, kod tabanı boyutlarını, hızı ve kriptografik standartları karşılaştırma

1 **WireGuard kod boyutu** PROTOKOLLER — **Doğru cevap: D**

ÖĞRETMEN NOTU

WireGuard son derece kompakttır ve yaklaşık 4.000 satır kodla çalışır. Bu, saldırı yüzeyini küçük tutar ve denetimi kolaylaştırır. Kaynak: WireGuard Project.

2 **Çekirdek alanı hızı** GECİKME — **Doğru cevap: B**

ÖĞRETMEN NOTU

WireGuard, doğrudan çekirdek alanında çalışarak bağlam değiştirme yükünden kaçınır ve yüksek verim sağlar. Kaynak: WireGuard Project.

3 **Soru 3** — **Doğru cevap: B**

ÖĞRETMEN NOTU

OpenVPN, AES-GCM gibi şifreleri sağlayan OpenSSL ile sıkı biçimde bütünleşiktir; bu da onu son derece yapılandırılabilir ama daha karmaşık kılar.

4 **Protokol performansı** YÖNLENDİRME DENETİMLERİ — **Doğru cevap: A**

ÖĞRETMEN NOTU

WireGuard el sıkışmalarını milisaniyeler içinde kurar ve ağ dolaşımına (ör. Wi-Fi'dan hücresele geçiş) anında yanıt verir. Kaynak: Microsoft Native Gateway, Apple Support.

5 **Asimetrik Kriptografi** GİZLİLİK — **Doğru cevap: C**

ÖĞRETMEN NOTU

WireGuard, SSH kurulum yapılandırmalarına benzer şekilde genel anahtarları izin verilen tünel IP adresleriyle ilişkilendiren Cryptokey Routing kullanır. Kaynak: WireGuard Project.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** Doğru cevap: Doğru

ÖĞRETMEN NOTU

WireGuard'ın Linux uygulaması 4.000 satırın altındadır, bu yüzden güvenlik ekipleri onu OpenVPN gibi çok daha büyük VPN kod tabanlarından çok daha hızlı inceleyebilir.

7 **Kullanıcı Alanı Gecikmesi** HIZLAR Doğru cevap: Yanlış

ÖĞRETMEN NOTU

OpenVPN kullanıcı alanında çalışır ve paketleri çekirdek sanal arayüzü ile arasında gidip getirir; bu da bağlam geçişi yükü ekler (OpenVPN DCO gibi çekirdek yük aktarımı kullanılmadıkça). Kaynak: DD-WRT custom firmware.

8 **OpenVPN yapılandırması** PAKET DİNLEME RİSKİ Doğru cevap: Doğru

ÖĞRETMEN NOTU

OpenVPN, TCP (güvenilirlik/güvenlik duvarı aşma için) veya UDP (hız için) üzerinden çalışmayı destekler; bu da onu karmaşık kurumsal güvenlik duvarlarıyla uyumlu kılar. Kaynak: IETF Cryptographic Protocols.

9 **Modern Kriptografi** GÜVENLİK DUVARLARI Doğru cevap: Doğru

ÖĞRETMEN NOTU

WireGuard, eski şifreleri bırakıp mobil işlemcilerde hızlı çalışan ChaCha20 ve Poly1305 gibi modern, güvenli yapı taşlarını tercih eder. Kaynak: WireGuard Project.

10 **Anahtar çifti basitleştirmesi** KAYIT TUTMAMA Doğru cevap: Yanlış

ÖĞRETMEN NOTU

WireGuard sertifika veya karmaşık sertifika yetkilisi hiyerarşileri kullanmaz; eşler arasında değiş tokuş edilen basit genel/özel anahtar çiftlerine dayanır. Kaynak: WireGuard Project.

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

G 1. WireGuard	H 2. OpenVPN	E 3. Çekirdek Alanı	A 4. Kullanıcı Alanı
B 5. 4.000 Satır	C 6. OpenSSL	F 7. Anahtar Çifti	D 8. TCP/UDP

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 WIREGUARD	2 OPENVPN	3 ÇEKİRDEK ALANI	4 KULLANICI ALANI
5 ANAHTAR ÇİFTİ	6 DENETLENEBİLİRLİK		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 F – OPENSSL	2 C – ÇEKİRDEKALANI	3 B – OPENVPN	4 G – ANAHTARÇİFTİ
5 H – TCPVEUDP	6 E – KOMPAKTKOD	7 A – WIREGUARD	8 D – KULLANICIALANI

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin WireGuard, OpenVPN ve Çekirdek Alanı terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

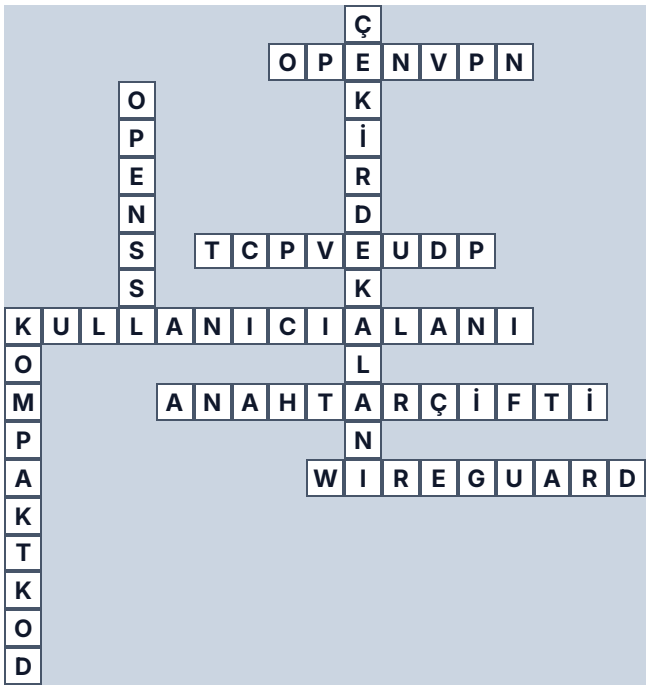
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: OPENVPN Büyük ve karmaşık bir yapılandırma kod tabanı kullanan sağlam eski protokol (7 harf)

4 soldan sağa: TCPVEUDP OpenVPN'in desteklediği taşıma protokolleri; WireGuard'ın kendisi yalnızca UDP üzerinde çalışır (8 harf)

5 soldan sağa: KULLANICIALANI OpenVPN'in çalıştığı ve bağlam değiştirme yükü yaratan yürütme alanı (14 harf)

6 soldan sağa: ANAHTARÇİFTİ WireGuard'ın eş bağlantılarını doğrulamak için kullandığı asimetrik jetonlar (12 harf)

7 soldan sağa: WIREGUARD Yüksek hız ve basit kod denetimi için tasarlanmış modern VPN protokolü (9 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: ÇEKİRDEKALANI WireGuard'ın hız için çalıştığı işletim sistemi yürütme alanı (13 harf)

3 yukarıdan aşağı: OPENSSL OpenVPN'in şifre algoritmaları için dayandığı kriptografik kitaplık (7 harf)

5 yukarıdan aşağı: KOMPAKTKOD WireGuard kod tabanının kompakt boyutu; denetlemeyi çok daha kolay hâle getirir (10 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. UGEIWARDR — **WIREGUARD**
2. NREDKÇAEIALKİ — **ÇEKİRDEKALANI**
3. KKOTOADPKM — **KOMPAKTKOD**
4. TÇTARİAFİANH — **ANAHTARÇİFTİ**
5. VNNEOPP — **OPENVPN**
6. NILALACNAKUIIL — **KULLANICIALANI**
7. OSSLPNE — **OPENSSL**
8. VCEPTDUP — **TCPVEUDP**

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"OPENVPNİ DAHA HIZLI BİR TÜNELLE YÜKSELT"

Vaka çalışmaları cevap anahtarı

A Senaryo A: Protokol Seçimi

PAKET DİNLEME VE ŞİFRELEME · Sarah'nın İkilemi

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Öneri: WireGuard. Hafif ve bağlantısız tasarımı, ağı değiştiğinde tünelin hızla toparlanmasını sağlar; ChaCha20-Poly1305 ise şifrelemeyi hızlı tutar.
- Güvenlik: Her iki protokol de kafedeki Wi-Fi'da trafiğini şifreler, bu yüzden doğru yapılandırıldığında ikisi de girişlerini korur; seçim esas olarak hızı ve kararlılığı etkiler.

B Senaryo B: VPN Engellerini Aşma

COĞRAFİ ENGEL VE IP'LER · Alex'in İkilemi

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Engelleme nedeni: WireGuard yalnızca UDP kullanır ve otel güvenlik duvarı büyük olasılıkla UDP'yi engeller veya WireGuard paketlerini filtreleme ya da Derin Paket İncelemesi (DPI) ile tanır.
- OpenVPN nasıl yardımcı olur: HTTPS tarafından kullanılan 443 numaralı bağlantı noktası dahil TCP üzerinden çalışabilir; otel güvenlik duvarları, web taraması buna bağlı olduğu için bu bağlantı noktasını nadiren tamamen engeller.