Ad Soyad: _____ Tarih: _____ Puan: _____

Proxy ve VPN Çalışma kâğıdı

Proxy sunucuları ile sanal özel ağların, şifreleme farklarının ve uygulama düzeyi ile sistem genelinde yönlendirmenin 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

- Uygulama proxy'lerini sistem genelindeki VPN şifrelemesiyle karşılaştır.
- SOCKS5'in temel HTTP proxy'lerine kıyasla yeteneklerini belirle.
- Tarayıcı tabanlı proxy'lerin arka plan uygulamalarını nasıl açıkta bıraktığını analiz et.
- ISS'lerin proxy tünellerinde şifrelenmemiş trafiği nasıl günlüğe kaydettiğini anla.
- Hız ve güvenlik ihtiyaçlarına göre doğru yönlendirme aracını seç.

PROXY 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: proxy'ler ile VPN'leri karşılaştırma. Hızlı Düşün bonus etkinliğiyle bitir.

PROXY VE VPN (GİRİŞ)

Proxy'ler ve VPN'ler farklı dijital gizlilik işlevleri sunar. Proxy sunucusu, uygulama katmanında bir yönlendirme görevi görür ve verileri şifrelemeden belirli programlar için IP adresini gizler. VPN ise ağ düzeyinde çalışır ve tüm sistem trafiğini şifrelemeyle korur. Doğru aracı seçmek güvenlik gereksinimlerine bağlıdır.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. **1. Standart bir HTTP proxy, OSI modelinin hangi katmanında çalışır?**
   - A. Fiziksel katman
   - B. Ağ katmanı
   - C. Uygulama katmanı
   - D. Veri Bağlantı katmanı

2. **2. SOCKS5'in standart HTTP proxy'lerine göre temel bir protokol avantajı nedir?**
   - A. Tam yük şifrelemesini zorunlu kılar
   - B. Her türlü TCP/UDP trafik yönlendirmesini destekler
   - C. DNS sızıntılarından etkilenmez
   - D. Doğrudan çekirdek alanında çalışır

3. **3. VPN, bir proxy sunucusundan neden genellikle daha güvenlidir?**
   - A. Daha hızlı uzak donanım üzerinde çalışır
   - B. Sistem genelindeki tüm ağ trafiğini şifreler
   - C. Yerel yönlendirme tablolarına ihtiyaç duymaz
   - D. Ağ gecikmesini tamamen ortadan kaldırır

4. **4. Hangi proxy türü trafiği varsayılan olarak hiç şifreleme olmadan yönlendirir?**
   - A. Basit bir HTTP proxy'si
   - B. Şifreli bir HTTPS proxy'si
   - C. Güvenli bir WireGuard istemcisi
   - D. Gizlemeli bir VPN sunucusu

5. **5. Tarayıcı proxy'si kullanılırken arka plandaki uygulama trafiğine ne olur?**
   - A. Otomatik olarak şifrelenir
   - B. Proxy sunucusu tarafından engellenir
   - C. Proxy tüneli üzerinden yönlendirilir
   - D. Proxy'yi atlar ve IP'ni açığa çıkarır

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Bir SOCKS5 proxy'si, sunucudan geçen tüm paket yüklerini şifreler.

○ Doğru ○ Yanlış

7 Soru 7

7. VPN, tüm sistem trafiğinin güvenliğini sağlamak için ağ katmanında çalışır.

○ Doğru ○ Yanlış

8 Soru 8

8. Proxy'ler, derin paket şifrelemesi yaptıkları için genellikle VPN'lerden daha hızlıdır.

○ Doğru ○ Yanlış

9 Soru 9

9. Bir proxy yapılandırmak, belirli uygulamalar içinde trafik yönlendirmeleri kurmayı gerektirir.

○ Doğru ○ Yanlış

10 Soru 10

10. Proxy kullanmak, veri trafiğini yerel ISS izlemesinden korumaz.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Uygulama katmanındaki bir _____ , diğer uygulamaları güvenceye almadan belirli tarayıcı trafiğini yönlendirir.

2. Sağlam bir _____ tüm cihaz veri paketlerini kapsüller ve şifreler.

3. Uygulama ve taşıma katmanları arasında yer alan protokol: _____ .

4. OSI modelinde uygulama katmanı olarak bilinen düzeyde, yani _____ düzeyinde, HTTP proxy'leri çalışır.

5. Standart proxy sunucuları yük _____ sunmaz ve verileri savunmasız bırakır.

6. Bir VPN, tüm ağ bağdaştırıcıları için _____ koruma sağlar.

KELİME BANKASI

GÖRÜNÜRLÜK PROXY SİSTEM GENELİ SOCKS5 ŞİFRELEME UDP DESTEĞİ VPN TÜNELİ YEDİNCİ KATMAN

Cevaplarını buraya yaz:

1. **2.**

3. **4.**

5. **6.**

Kontrol Noktası 4: Ağ kavramı eşleştirme

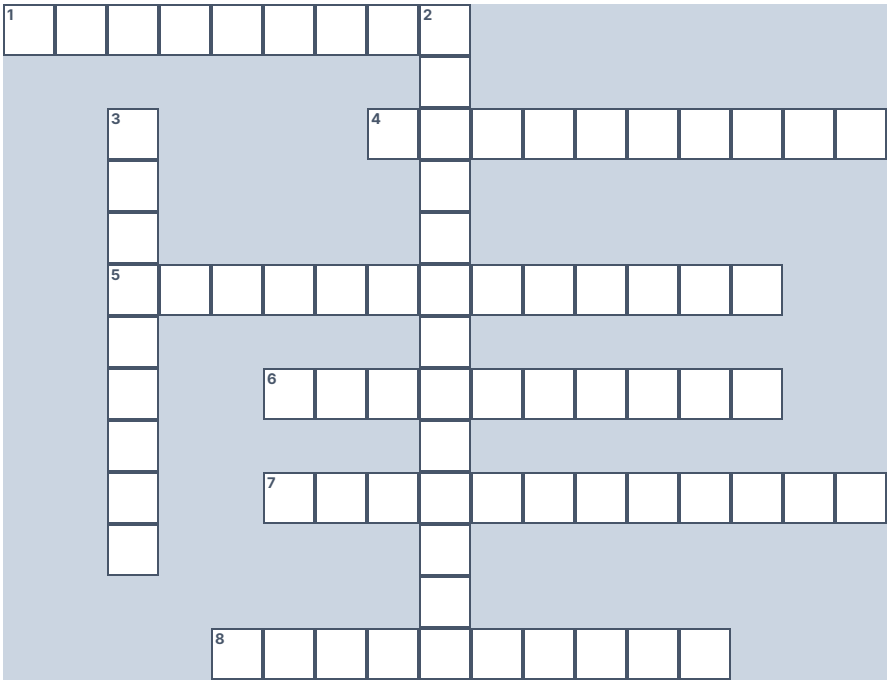
TANIM EŞLEŞTİRME

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

☐	1. HTTP Proxy	A	Tüm uygulama trafiğini şifreleyen işletim sistemi düzeyinde yönlendirme.
☐	2. SOCKS5 Proxy	B	Standart web proxy protokollerinin çalıştığı uygulama katmanı.
☐	3. VPN Tüneli	C	SOCKS5'in, düz HTTP proxy'lerinin aksine TCP'nin yanı sıra UDP'yi de iletebilme yeteneği.
☐	4. Sistem genelinde	D	Yalnızca tarayıcı kum havuzu içindeki trafiği gizleyen istemci uzantısı.
☐	5. OSI Katman 7	E	Tüm arka plan cihaz trafiğini saran şifreleme ve kapsülleme.
☐	6. UDP Desteği	F	Şifrelenmemiş proxy verilerinin ISS'ler tarafından görülebilir kaldığı trafik durumu.
☐	7. Tarayıcı Proxy'si	G	Belirli web tarayıcısı trafiğini yönlendiren uygulama katmanı proxy'si.
☐	8. İSS Görünürlüğü	H	Uygulama ve taşıma katmanları arasında çalışan, şifreleme içermeyen proxy protokolü.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

1. Belirli web tarayıcı trafiğini yönlendiren uygulama katmanı proxy'si (9)

4. Düz HTTP proxy'lerinin aksine SOCKS5'in TCP'nin yanı sıra UDP'yi de iletebilmesi (10)

5. Yalnızca tarayıcı kum havuzu içindeki trafiği gizleyen istemci eklentisi (13)

6. Uygulama ve taşıma katmanları arasında çalışan, şifreleme içermeyen proxy protokolü (10)

7. Tüm uygulama trafiğini şifreleyen işletim sistemi düzeyinde yönlendirme (12)

8. Şifrelenmemiş proxy verilerinin İSS'ler tarafından görülebilir kaldığı trafik durumu (10)

YUKARIDAN AŞAĞI

2. Standart web proxy protokollerinin çalıştığı Uygulama katmanı (13)

3. Cihazın tüm arka plan trafiğini saran şifreleme ve kapsülleme (9)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

1 soldan sağa: Belirli web tarayıcı trafiğini yönlendiren uygulama katmanı proxy'si (9 harf):

4 soldan sağa: Düz HTTP proxy'lerinin aksine SOCKS5'in TCP'nin yanı sıra UDP'yi de iletebilmesi (10 harf):

5 soldan sağa: Yalnızca tarayıcı kum havuzu içindeki trafiği gizleyen istemci eklentisi (13 harf):

6 soldan sağa: Uygulama ve taşıma katmanları arasında çalışan, şifreleme içermeyen proxy protokolü (10 harf):

7 soldan sağa: Tüm uygulama trafiğini şifreleyen işletim sistemi düzeyinde yönlendirme (12 harf):

8 soldan sağa: Şifrelenmemiş proxy verilerinin İSS'ler tarafından görülebilir kaldığı trafik durumu (10 harf):

YUKARIDAN AŞAĞI

2 yukarıdan aşağı: Standart web proxy protokollerinin çalıştığı Uygulama katmanı (13 harf):

3 yukarıdan aşağı: Cihazın tüm arka plan trafiğini saran şifreleme ve kapsülleme (9 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

HTTPPROXY SOCKSPROXY VPNTÜNELİ SİSTEMGENELİ YEDİNCİKATMAN
UDPDESTEĞİ TARAYICIPROXY GÖRÜNÜRLÜK

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. HTTPPROXY

B. SOCKSPROXY

C. VPNTÜNELİ

D. SİSTEMGENELİ

E. YEDİNCİKATMAN

F. UDPDESTEĞİ

G. TARAYICIPROXY

H. GÖRÜNÜRLÜK

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Standart web proxy protokollerinin çalıştığı Uygulama katmanı.

2. Düz HTTP proxy'lerinin aksine SOCKS5'in TCP'nin yanı sıra UDP'yi de iletebilmesi.

3. Belirli web tarayıcı trafiğini yönlendiren uygulama katmanı proxy'si.

4. Yalnızca tarayıcı kum havuzu içindeki trafiği gizleyen istemci eklentisi.

5. Cihazın tüm arka plan trafiğini saran şifreleme ve kapsülleme.

6. Tüm uygulama trafiğini şifreleyen işletim sistemi düzeyinde yönlendirme.

7. Şifrelenmemiş proxy verilerinin İSS'ler tarafından görülebilir kaldığı trafik durumu.

8. Uygulama ve taşıma katmanları arasında çalışan, şifreleme içermeyen proxy protokolü.

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. RPPTHOXYT
2. İVLTPNEÜN
3. EYKTAANDİN CMİ
4. IXPRIYYCORT AA
5. OPYOKRSSXC
6. İENEMLESİGS T
7. DDUTSEĞİEP
8. ÜÜÜKGNÖRLR

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Proxy ile VPN arasındaki farklar			
2	VPN olmadan şifrelenmeden kalan şeyler			
3	Sahte Wi-Fi ağını fark etme yolları			
4	Günlük hayatta bir aracının yaptığı şeyler			
5	Proxy'nin yeterli olduğu durumlar			
6	VPN kullanabilen cihazlar			
7	Bildiğin proxy türleri			
8	Bir VPN'in gizleyebileceği şeyler			
9	VPN'lerle ilgili efsaneler			
10	İyi bir VPN sağlayıcısının verdiği sözler			
11	Bir VPN'in seni koruyamadığı şeyler			
12	Bu çalışma kâğıdından aklında tutmak istediğin sözcükler			
13	Seyahat ederken VPN kullanma nedenleri			
14	VPN istediğin durumlar			
15	VPN kullanacağın yerler			

Kontrol Noktası 8: VPN vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

SARAH (KAFEDEKİ ÖĞRENCİ)

👩‍💻 "Selam! Coffee & Bytes'tayım ve 'Free_Wi-Fi_No_Password' adlı açık bir ağdayım. Okul e-postama giriş yapmam gerekiyor; bir arkadaşım güvende kalmak için ücretsiz bir tarayıcı proxy'sinin yeterli olduğunu söylüyor. Proxy giriş bilgilerimi ve dosyalarımı korur mu, yoksa VPN'e mi ihtiyacım var?"

ALEX (GEZGİN ÖĞRENCİ)

👩‍💻 "Yurt dışındayım ve ülkemde barındırılan bir biyoloji belgeseli 'Bu video şu anki konumunuzda mevcut değil.' diyor. Bir sınıf arkadaşım proxy kullanıyor, bende ise VPN var. Neden engelleniyorum ve hangi araç daha iyi çalışır?"

Kontrol Noktası 9: Şifreyi Çöz

Proxy karşılaştırma eğitimini tamamlamak için güvenli tünellemeyle 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

24 21 1 7 12 9 12 17 12 2 12 21 27 6 14 12 15

22 25 17 25 3 25 28 15 1 28 6 17 12 5 6 17

28 19 17 15 6 17 5 12 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: Proxy sunucusu nedir?

Proxy sunucusu, uygulamanız ile hedef sunucu arasında istekleri ileten bir aracıdır. Web sitesi sizin IP adresiniz yerine proxy'nin IP adresini görür, ancak yalnızca proxy kullanacak şekilde yapılandırılmış uygulamaların trafiği yönlendirilir ve basit bir proxy bu trafiği şifrelemez.

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: Proxy bir VPN midir?

Hayır. Vekil sunucu (proxy), belirli uygulamalar için trafiği genellikle şifrelemeden aktarır. VPN ise ağ katmanında, arka plan uygulamaları dahil cihazın tüm trafiğini taşıyan şifreli bir tünel kurar.

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 proxy kullanabilir miyim?

Kullanabilirsin ama ücretsiz proxy'ler çoğunlukla bilinmeyen işletmenler tarafından yönetilir. Temel bir proxy trafiği şifrelemediği için işletmeni şifrelenmemiş sayfaları görebilir ve hatta değiştirebilir. Kullanmadan önce hizmeti kimin işlettiğini kontrol et.

Q7: Bir proxy kayıt tutar mı?

Olabilir. Bir proxy ilettiği her isteği işler; bu yüzden operatörü IP adresini, ziyaret ettiğin siteleri ve zamanlarını kaydedebilir. Kimin işlettiğini ve gizlilik politikasının ne dediğini kontrol et.

Q8: Proxy ne zaman yeterlidir?

Proxy, tek bir tarayıcının görünen konumunu değiştirmek gibi düşük riskli görevler için yeterli olabilir. Bankacılık, herkese açık Wi-Fi veya bir cihazdaki her uygulamayı korumak için tüm trafiği şifrelediğinden VPN daha güvenli bir seçimdir.

Q9: Bir proxy telefonumdaki tüm uygulamaları koruyabilir mi?

Hayır. Yalnızca vekil sunucu ayarına uyan uygulamalar onu kullanır; diğerleri doğrudan bağlanır. Bir VPN uygulaması ise telefonun tüm uygulamalarını şifreli tüneli üzerinden yönlendirir.

Q10: SOCKS5 proxy nedir?

RFC 1928'de tanımlanan SOCKS5, uygulama ve taşıma katmanları arasında yer alan bir proxy protokolüdür. TCP bağlantılarını ve UDP veri birimlerini aktarabilir ve kimlik doğrulamayı destekler, ancak yerleşik şifrelemesi yoktur. [1]

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: Proxy'ler ve VPN'ler hangi ağ katmanlarında çalışır?

HTTP proxy'si uygulama katmanında (Katman 7) çalışır ve web isteklerini anlar. SOCKS5, uygulama ile taşıma katmanları arasında yer alır. IPsec veya WireGuard gibi VPN protokolleri ağ katmanında çalışır, bu yüzden cihazdaki tüm IP trafiğini taşıyabilir.

Q2: HTTPS kullanan bir site proxy üzerinden de şifreli kalır mı?

Evet. Bir proxy üzerinden HTTPS sitesi açtığında TLS şifrelemesi tarayıcın ile site arasında uçtan uca çalışır; bu yüzden proxy alan adını görür ama sayfa içeriğini görmez. Düz HTTP sayfaları okunabilir kalır.

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: Şeffaf proxy nedir ve kimler kullanır?

Şeffaf proxy, kullanıcının cihazında hiçbir kurulum olmadan trafiği araya girerek yakalar. Okullar, şirketler ve İSS'ler bunları önbellekleme veya içerik filtreleme için kullanır. Kullanıcılar çoğu zaman bir tanesinin devrede olduğunu bilmez ve kullanıcılara hiçbir gizlilik sağlamaz.

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: Bir proxy neden VPN bağlantısından daha hızlı hissettirebilir?

Basit bir proxy şifrelemeyi atlar ve yalnızca tek bir uygulamanın trafiğini işler, bu yüzden daha az işlem yükü getirir. VPN ise cihazdan çıkan her paketi şifreler. Modern protokollerle fark çoğu zaman küçüktür ve proxy çok daha az koruma sunar.

Q8: Web siteleri proxy veya VPN kullandığımı anlayabilir mi?

Çoğu zaman evet. Birçok site IP adreslerini bilinen proxy ve VPN sunucuları listeleriyle karşılaştırır ve HTTP proxy'leri Via veya X-Forwarded-For gibi başlıklar ekleyebilir. Yayın hizmetleri genellikle ikisini de engeller.

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 proxy, İSS hız kısıtlamasını durdurabilir mi?

Nadiren. Temel bir proxy trafiği şifrelemez; bu nedenle ISS yine de ne tür bir etkinlik olduğunu görebilir. VPN trafik türlerini gizler, ancak hiçbir araç tıkanıklığı veya veri sınırlarını çözmez.

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. SOCKS STANDARDI

SOCKS Protocol Version 5, IETF tarafından Mart 1996'da RFC 1928 olarak yayımlandı ve bugün tarayıcıların ve uygulamaların kullandığı SOCKS5 proxy'leri için hâlâ referans belirtimdir. [1]

2. SHIM KATMANI

RFC 1928, SOCKS'u uygulama ve taşıma katmanları arasında bir ara katman olarak tanımlar; bu nedenle ICMP gibi ağ katmanı trafiğini iletemez. [1]

3. UDP RÖLESİ

SOCKS5, bir proxy'nin düz HTTP proxy'lerinin yapamadığı şekilde TCP bağlantılarının yanı sıra UDP veri birimlerini de aktarmasına olanak tanıyan UDP ASSOCIATE komutunu ekledi. [1]

4. VARSAYILAN SOCKS BAĞLANTI NOKTASI

SOCKS5 istemcileri, RFC 1928'de tanımlandığı üzere varsayılan olarak proxy sunucusuna TCP 1080 numaralı bağlantı noktasından bağlanır; birçok proxy hizmeti kullanıcıların başka bağlantı noktaları seçmesine izin verir. [1]

5. HTTP ARACILARI

HTTP standardı (RFC 9110), proxy'yi istemcinin seçtiği, istekleri kaynak sunucuya ileten bir mesaj iletme aracısı olarak tanımlar.

6. DERİN PAKET İNCELEMESİ

Derin Paket İncelemesi (DPI) paket içeriklerini ve trafik desenlerini inceler; şifrelenmemiş proxy trafiği DPI'a tamamen görünürken VPN trafiği çok daha azını ortaya çıkarır.

7. AĞ KATMANI VPN'LERİ

NIST SP 800-77'de açıklanan IPsec, trafiği ağ katmanında korur; böylece her uygulamanın IP paketleri, uygulama başına kurulum gerekmeden güvence altına alınabilir. [2]

8. YALNIZCA TARAYICI KAPSAMI

Tek bir tarayıcıda ayarlanan proxy yalnızca o tarayıcıyı etkiler; e-posta istemcileri, oyunlar ve sistem güncellemeleri cihazın normal bağlantısını kullanmaya devam eder.

9. TOR VE PROXY'LER

Tor trafiği üç gönüllü aktarıcı (koruyucu, orta ve çıkış) üzerinden gönderir ve genellikle yerel bir SOCKS proxy üzerinden erişilir; bu da tek bir proxy'nin sağlayamayacağı katmanlar ekler.

10. HIZ TAVİZİ

Proxy'ler şifrelemeyi atladıkları için daha hızlı görünebilir, ancak WireGuard gibi modern VPN protokolleri çok az ek yük getirirken cihazın tüm trafiğini korur.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Cevap Anahtarı: Proxy sunucuları ile sanal özel ağları, şifreleme farklarını ve uygulama düzeyinde ile sistem genelinde yönlendirmeyi karşılaştırma

1 **Proxy OSI katmanı** PROTOKOLLER — **Doğru cevap: C**

ÖĞRETMEN NOTU

Standart HTTP/HTTPS proxy'leri Uygulama katmanında (Katman 7) çalışır ve belirli tarayıcı trafiğini yönlendirir. Sistem genelinde ağ yönlendirmesi yoktur. Kaynak: Tor Project Foundation.

2 **Soru 2** — **Doğru cevap: B**

ÖĞRETMEN NOTU

SOCKS5, uygulama ve taşıma katmanları arasında TCP ve UDP trafiğini iletir ancak varsayılan olarak şifrelemez; HTTP proxy'leri ise web isteklerini işler.

3 **VPN Sistem Şifrelemesi** WI-FI GÜVENLİĞİ — **Doğru cevap: B**

ÖĞRETMEN NOTU

VPN, tüm işletim sistemi trafiğini sistem genelinde kapsüller ve şifreler; proxy ise yalnızca yapılandırılmış belirli uygulamaların trafiğini yönlendirir. Kaynak: Deloitte Advisory.

4 **Proxy şifreleme eksikliği** YÖNLENDİRME DENETİMLERİ — **Doğru cevap: A**

ÖĞRETMEN NOTU

HTTP proxy'leri, tarayıcı trafiğini paket yüklerini şifrelemeden uygulama katmanında iletir; yani ağ operatörün veya İSS'n içerik trafiğini yine de izleyebilir. Kaynak: IETF Proxy Vulnerabilities.

5 **Atlama Açığı** GİZLİLİK — **Doğru cevap: D**

ÖĞRETMEN NOTU

Tarayıcı proxy'leri kuralları yalnızca web tarayıcısının kendisine uygular. Arka plan uygulamaları, işletim sistemi güncellemeleri ve e-posta istemcileri proxy'yi atlar ve yerel IP adresini açığa çıkarır. Kaynak: W3C Consortium.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** Doğru cevap: Yanlış

ÖĞRETMEN NOTU

SOCKS5 trafiği uygulama ve taşıma katmanları arasında iletir ancak varsayılan olarak şifreleme yapmaz, bu yüzden paket içerikleri aktarım sırasında okunabilir kalır.

7 **Ağ Katmanı Tünelleri** HIZLAR Doğru cevap: Doğru

ÖĞRETMEN NOTU

Ağ katmanında çalışan bir VPN, cihazından giden trafiği yönlendirir ve şifreler; bu da trafiğin sistem genelinde korunmasına yardımcı olur. Kaynak: Deloitte Advisory.

8 **Proxy şifreleme sınırı** PAKET DİNLEME RİSKİ Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Proxy'ler bazen daha hızlı olabilir, ancak bunun nedeni şifreleme YAPMAMALARIDIR. Bu şifreleme eksikliği verileri incelemeye karşı savunmasız bırakır. Kaynak: IETF Proxy Vulnerabilities.

9 **Uygulama Düzeyinde Yönlendirme** GÜVENLİK DUVARLARI Doğru cevap: Doğru

ÖĞRETMEN NOTU

Sistem genelindeki VPN'lerin aksine proxy sunucuları, tarayıcı ayarlarında veya uygulamaya özgü proxy alanlarında elle kurulum gerektirir. Kaynak: W3C Consortium.

10 **İSS izleme riski** KAYIT TUTMAMA Doğru cevap: Doğru

ÖĞRETMEN NOTU

Standart HTTP/SOCKS5 proxy'leri veri yükünü şifrelemediğinden, yerel ISS'n çevrimiçi eylemlerini tamamen görebilir. 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

G 1. HTTP Proxy	H 2. SOCKS5 Proxy	E 3. VPN Tüneli	A 4. Sistem genelinde
B 5. OSI Katman 7	C 6. UDP Desteği	D 7. Tarayıcı Proxy'si	F 8. İSS Görünürlüğü

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 PROXY	2 VPN TÜNELİ	3 SOCKS5	4 YEDİNCİ KATMAN
5 ŞİFRELEME	6 SİSTEM GENELİ		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 E – YEDİNCİKATMAN	2 F – UDPDESTEĞİ	3 A – HTTPPROXY	4 G – TARAYICIPROXY
5 C – VPNTÜNELİ	6 D – SİSTEMGENELİ	7 H – GÖRÜNÜRLÜK	8 B – SOCKSPROXY

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin HTTP Proxy, SOCKS5 Proxy ve VPN Tüneli terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

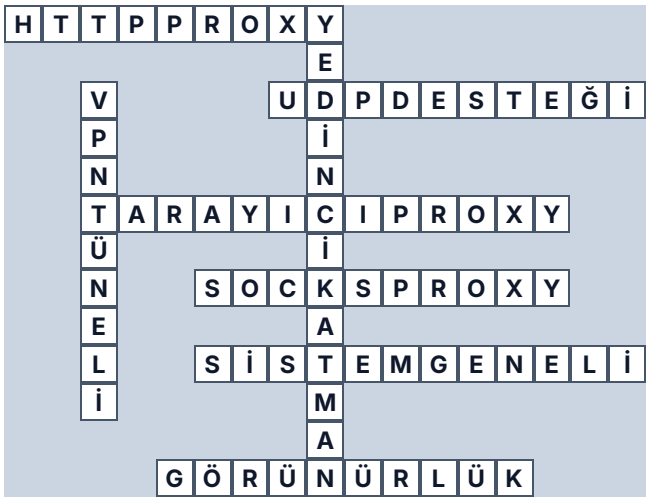
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

1 soldan sağa: HTTPPROXY Belirli web tarayıcı trafiğini yönlendiren uygulama katmanı proxy'si (9 harf)

4 soldan sağa: UDPDESTEĞİ Düz HTTP proxy'lerinin aksine SOCKS5'in TCP'nin yanı sıra UDP'yi de iletebilmesi (10 harf)

5 soldan sağa: TARAYICIPROXY Yalnızca tarayıcı kum havuzu içindeki trafiği gizleyen istemci eklentisi (13 harf)

6 soldan sağa: SOCKSPROXY Uygulama ve taşıma katmanları arasında çalışan, şifreleme içermeyen proxy protokolü (10 harf)

7 soldan sağa: SİSTEMGENELİ Tüm uygulama trafiğini şifreleyen işletim sistemi düzeyinde yönlendirme (12 harf)

8 soldan sağa: GÖRÜNÜRLÜK Şifrelenmemiş proxy verilerinin İSS'ler tarafından görülebilir kaldığı trafik durumu (10 harf)

YUKARIDAN AŞAĞI

2 yukarıdan aşağı: YEDİNCİKATMAN Standart web proxy protokollerinin çalıştığı Uygulama katmanı (13 harf)

3 yukarıdan aşağı: VPNTÜNELİ Cihazın tüm arka plan trafiğini saran şifreleme ve kapsülleme (9 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	RPPTHOXYT	HTTPPROXY	5.	OPYOKRSSXC	SOCKSPROXY
2.	İVLTPNEÜN	VPNTÜNELİ	6.	İENEMLESİGST	SİSTEMGENELİ
3.	EYKTAANDİNCMİ	YEDİNCİKATMAN	7.	DDUTSEĞİEP	UDPDESTEĞİ
4.	IXPRIYYCORTAA	TARAYICIPROXY	8.	ÜÜÜKGNÖRLR	GÖRÜNÜRLÜK

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"TRAFİĞİNİ BİR VEKİL SUNUCUYLA YENİDEN YÖNLENDİR"

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.
- Proxy ve VPN: Temel bir tarayıcı proxy'si onun trafiğini şifrelemez. VPN ise cihazdaki her şeyi şifreler ve ele geçirilen paketleri yerel gözetleyiciler için okunamaz hale getirir.

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.
- Hangisi daha iyi çalışır: İkisi de ona kendi ülkesinin IP'sini verir, ancak proxy yalnızca yapılandırılmış uygulamayı kapsar; VPN ise cihazının tüm trafiğini de şifreler.