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

Surfshark Güvenliği

Surfshark güvenlik özelliklerini; CleanWeb reklam engelleme, MultiHop dinamik yönlendirme, Nexus SDN mimarisi, yalnızca RAM kullanan sunucu filosu ve Camouflage modu dahil olmak üzere inceleme.

SURFSHARK GÜVENLİK ÖĞRENME ÖZETİ

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 Surfshark'ın güvenlik mimarisi konusunda rehberlik eder. Yalnızca RAM kullanan sunucu donanımını, Nexus SDN dinamik IP rotasyonunu, CleanWeb reklam engelleyicilerini ve MultiHop yönlendirmeyi inceleyeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: VPN ve ağ güvenliği yapılandırmalarında 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 en iyi VPN'ler rehberini aç

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

Surfshark Güvenlik Öğrenme Yol Haritan

- Surfshark Security'nin teknik mimarisini ve yapılandırma kurallarını analiz et.
- IP, DNS ve WebRTC trafiği sızıntılarını önlemek için istemci ayarlarını yapılandır.
- Özel fiyatlandırma, deneme ve performans özelliklerini standart modellerle karşılaştır.

SURFSHARK GÜVENLİK REHBERİ 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: yalnızca RAM kullanan altyapı, Nexus SDN ve CleanWeb. Hızlı Düşün bonus etkinliğiyle bitir.

YALNIZCA RAM SUNUCU FİLOSU, NEXUS SDN VE CLEANWEB MİMARİSİ (GİRİŞ)

Surfshark, yalnızca RAM kullanan sunucu filosu, IP Rotator'lı Nexus yazılım tanımlı ağı, CleanWeb reklam engelleme ve Dynamic MultiHop şifreleme yollarıyla kullanıcı gizliliğini korur.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. 1. Surfshark'ın entegre reklam ve kötü amaçlı yazılım engelleyicisinin adı nedir?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. 2. Surfshark tüm sunucularında hangi donanım mimarisini kullanır?
   - A) Sabit Disk Sürücüleri
   - B) %100 Yalnızca RAM
   - C) Optik Depolama
   - D) Manyetik Bant

3. 3. Hangi özellik trafiği iki farklı VPN sunucusu üzerinden yönlendirir?
   - A) Bypasser
   - B) MultiHop (Çift VPN)
   - C) Nexus Ağı
   - D) Statik IP

4. 4. Hangi gizleme özelliği VPN trafiğini normal web verisi gibi gösterir?
   - A) Kill Switch
   - B) Kamuflaj Modu
   - C) CleanWeb 2.0
   - D) Bölünmüş Tünel

5. 5. Surfshark Bypasser aracının işlevi nedir?
   - A) Speed Booster
   - B) Bölünmüş Tünelleme
   - C) Parola Yöneticisi
   - D) DNS Çözümleyici

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Yalnızca RAM kullanan sunucular, sunucu yeniden başlatıldığında tüm işletim verilerini hemen siler.

○ Doğru ○ Yanlış

7 Soru 7

7. Camouflage Modu, ISS'lerin VPN kullandığını tespit etmesini önler.

○ Doğru ○ Yanlış

8 Soru 8

8. CleanWeb 2.0, çerez onayı açılır pencerelerini engellemek için tarayıcı uzantıları içinde çalışır.

○ Doğru ○ Yanlış

9 Soru 9

9. Surfshark geçici bağlantı zaman damgalarını ve bant genişliği kullanım kayıtlarını tutar.

○ Doğru ○ Yanlış

10 Soru 10

10. Nexus ağı, bağlantıyı kesmeden kullanıcı IP adreslerini düzenli aralıklarla değiştirir.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Can sıkıcı web reklamları, izleme betikleri ve kimlik avı bağlantıları _____ filtreleriyle engellenir.

2. Kullanıcı etkinliği, tamamen geçici bellekte çalışan bir _____ üzerinde adli iz bırakmaz.

3. İki ayrı şifreli sunucu atlamasıyla veri yönlendirmek _____ tünelleriyle sağlanır.

4. VPN kullanımını internet servis sağlayıcılarından gizlemek için kullanıcılar _____ modunu etkinleştirir.

5. Bankacılık uygulamalarının VPN tünelini atlamasına izin vermek _____ ayarlarıyla yönetilir.

6. Sunucu filosunu birbirine bağlayan yeni nesil SDN mimarisi, _____ sistemidir.

KELİME BANKASI

BYPASSER | CAMOUFLAGE | CLEANWEB | ÇOKLU ATLAMA | DEĞİŞEN IP | KILL SWITCH | NEXUS | RAM SUNUCUSU

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: VPN ve ağ kavramı eşleştirme

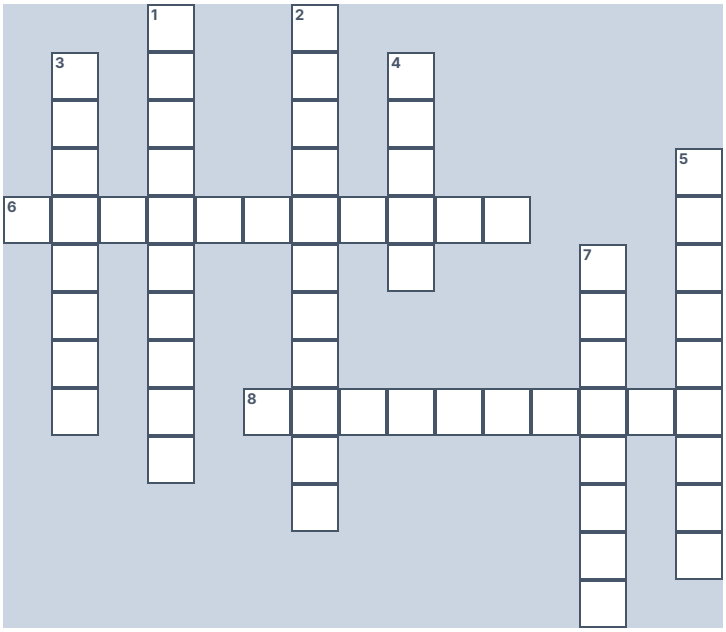
TANIM EŞLEŞTİRME

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

1. CLEANWEB	A	VPN koptuğunda ağ trafiğini engelleyen otomatik güvenlik özelliği.
2. RAM SUNUCUSU	B	Seçili uygulamaların VPN'i atlamasına olanak tanıyan bölünmüş tünelleme işlevi.
3. ÇOKLU ATLAMA	C	Reklamları, kötü amaçlı yazılımları ve çerez onay bannerlarını engelleyen gelişmiş filtre.
4. GİZLENME	D	Her güç döngüsünde tüm verileri silen geçici bellekli sunucu donanımı.
5. ATLAYICI	E	Tünelleri kesintiye uğratmadan dış IP adresinizi düzenli olarak değiştiren özellik.
6. KILL SWITCH	F	VPN imzalarını gizleyerek normal HTTPS trafiğini taklit eden gizleme teknolojisi.
7. NEXUS	G	Trafiği iki ayrı sunucu düğümü üzerinden şifreleyen çift VPN yönlendirme özelliği.
8. DÖNEN	H	Tüm sunucuları birleşik bir ağ örgüsüne bağlayan tescilli yazılım tanımlı ağ.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

6. Her güç döngüsünde tüm verileri silen geçici bellekli sunucu donanımı (11)

8. VPN imzalarını gizleyerek normal HTTPS trafiğini taklit eden gizleme teknolojisi (10)

YUKARIDAN AŞAĞI

1. VPN koptuğunda ağ trafiğini otomatik olarak engelleyen güvenlik özelliği (10)

2. Trafiği iki ayrı sunucu düğümü üzerinden şifreleyen çift VPN yönlendirme özelliği (11)

3. Seçili uygulamaların VPN'i atlamasına izin veren bölünmüş tünelleme işlevi (8)

4. Tüm sunucuları birleşik bir ağda birbirine bağlayan tescilli yazılım tanımlı ağ (5)

5. Tünelleri kesintiye uğratmadan harici IP adresinizi düzenli olarak değiştiren özellik (9)

7. Reklamları, kötü amaçlı yazılımları ve çerez onay bannerlarını engelleyen gelişmiş filtre (8)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

6 soldan sağa: Her güç döngüsünde tüm verileri silen geçici bellekli sunucu donanımı (11 harf):

8 soldan sağa: VPN imzalarını gizleyerek normal HTTPS trafiğini taklit eden gizleme teknolojisi (10 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: VPN koptuğunda ağ trafiğini otomatik olarak engelleyen güvenlik özelliği (10 harf):

2 yukarıdan aşağı: Trafiği iki ayrı sunucu düğümü üzerinden şifreleyen çift VPN yönlendirme özelliği (11 harf):

3 yukarıdan aşağı: Seçili uygulamaların VPN'i atlamasına izin veren bölünmüş tünelleme işlevi (8 harf):

4 yukarıdan aşağı: Tüm sunucuları birleşik bir ağda birbirine bağlayan tescilli yazılım tanımlı ağ (5 harf):

5 yukarıdan aşağı: Tünelleri kesintiye uğratmadan harici IP adresinizi düzenli olarak değiştiren özellik (9 harf):

7 yukarıdan aşağı: Reklamları, kötü amaçlı yazılımları ve çerez onay bannerlarını engelleyen gelişmiş filtre (8 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

CLEANWEB RAMSUNUCUSU ÇOKLUATLAMA CAMOUFLAGE BYPASSER
KILLSWITCH NEXUS DEĞİŞENIP

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. CLEANWEB**
- **B. RAMSUNUCUSU**
- **C. ÇOKLUATLAMA**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. DEĞİŞENIP**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. VPN imzalarını gizleyerek normal HTTPS trafiğini taklit eden gizleme teknolojisi.
2. VPN koptuğunda ağ trafiğini otomatik olarak engelleyen güvenlik özelliği.
3. Reklamları, kötü amaçlı yazılımları ve çerez onay bannerlarını engelleyen gelişmiş filtre.
4. Seçili uygulamaların VPN'i atlamasına izin veren bölünmüş tünelleme işlevi.
5. Her güç döngüsünde tüm verileri silen geçici bellekli sunucu donanımı.
6. Tünelleri kesintiye uğratmadan harici IP adresinizi düzenli olarak değiştiren özellik.
7. Trafiği iki ayrı sunucu düğümü üzerinden şifreleyen çift VPN yönlendirme özelliği.
8. Tüm sunucuları birleşik bir ağda birbirine bağlayan tescilli yazılım tanımlı ağ.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel Sanal Özel Ağ (VPN) kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. EANCWLBE
2. UAOÇMAKALTL
3. AYBSSREP
4. XSUNE
5. UACUMUUNRSS
6. GUOLACAFEM
7. ILKIWTCHSL
8. PŞIDİEENĞ

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Surfshark içindeki güvenlik özellikleri			
2	VPN bağlantının yavaş olduğunu gösteren işaretler			
3	Bildiğin VPN protokolleri			
4	Şifrelemenin korudukları			
5	Herkese açık Wi-Fi'daki tehditler			
6	Güçlü gizlilik yasalarıyla bilinen ülkeler			
7	Güçlü parola oluşturma yolları			
8	Surfshark uygulamasını yükleyeceğin cihazlar			
9	Surfshark müşteri desteğine sorulacak sorular			
10	Ekstra güvenlik için açtığın ayarlar			
11	Surfshark ile ağından gizleyebileceğin şeyler			
12	VPN sızıntısı türleri			
13	Bir VPN'in asla saklamaması gereken veriler			
14	İyi bir VPN uygulamasını anlatan sözcükler			
15	Bir denetimin kontrol edebileceği şeyler			

Kontrol Noktası 8: VPN ve ağ vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KAMPÜS VE İŞ YERİ FİLTRELERİNİ AŞMA



Senaryo: Bir öğrenci, üniversite kampüsünün Wi-Fi ağının tüm standart OpenVPN ve WireGuard portlarını engellediğini görüyor.

Tartışma sorusu: Hangi Surfshark özelliği öğrencinin ağ yöneticileri tarafından fark edilmeden bağlanmasına olanak tanır?

VAKA ÇALIŞMASI 2: YÜKSEK RİSKLİ GAZETECİLİK SORUŞTURMASI



Senaryo: Bir araştırmacı gazetecinin, hassas kurumsal kayıtları araştırırken gözetime karşı ekstra korumaya ihtiyacı var.

Tartışma sorusu: Dynamic MultiHop, tek sunuculu yönlendirmeye kıyasla nasıl üstün gizlilik sağlar?

Kontrol Noktası 9: Şifreyi Çöz

Bir ağ mühendisi, yönlendirme kanallarını ve istemci tünellerini güvenceye alır. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp 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

22	25	21	7	22	10	1	21	14		5	6	9	12	23	6	17		12	20

8	12	29	15	12	15	12	9	12	17	12		1	21	24	11	21	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)

Sanal Özel Ağlar (VPN'ler) ve tünelleme ile ilgili en sık sorulan soruları ve cevapları incele.

Q1: Surfshark CleanWeb nedir?

CleanWeb, reklamları, izleyicileri, kötü amaçlı yazılımları ve kimlik avı sitelerini engelleyen entegre bir güvenlik özelliğidir.

Q2: Yalnızca RAM'li sunucular nedir?

Yalnızca RAM kullanan sunucular geçici (volatile) bellekte çalışır; yani bellekte tutulan veriler sunucular her yeniden başladığında silinir.

Q3: Surfshark MultiHop nedir?

MultiHop (Double VPN), internet bağlantını iki farklı sunucu konumu üzerinden yönlendirir ve şifreler.

Q4: Kamuflaj Modu nasıl çalışır?

Camouflage Modu, VPN trafiğini gizler; böylece ISS'in VPN kullandığını anlayamaz.

Q5: Bypasser özelliği nedir?

Bypasser, Surfshark'ın belirli uygulamaların veya web sitelerinin VPN'i atlamasına olanak tanıyan bölünmüş tünelleme aracıdır.

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

Sanal Özel Ağlar (VPN'ler) ve tünelleme ile ilgili en sık sorulan soruları ve cevapları incele.

Q6: Surfshark'ın Kill Switch'i var mı?

Evet, Kill Switch, VPN beklenmedik şekilde kesilirse seni internetten ayırır.

Q7: Surfshark hangi şifreleme standardını kullanır?

Surfshark, AES-256-GCM ve ChaCha20 kullanır; yeni Dausos protokolünde ayrıca AEGIS-256X2 kullanır.

Q8: Surfshark'ın kayıt tutmama politikası denetlendi mi?

Evet, Deloitte, Surfshark'ın günlük tutmama politikasını 2023'te ve 2025'te yeniden doğruladı.

Q9: Surfshark Nexus nedir?

Nexus, daha akıcı yönlendirme için tüm sunucuları birleşik bir ağa bağlayan gelişmiş bir SDN mimarisidir.

Q10: IP Rotator özelliği nedir?

IP Rotator, VPN oturumunu kesmeden IP adresini birkaç dakikada bir otomatik olarak değiştirir.

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

VPN tünelleme protokollerinin, mobil istemci entegrasyonlarının ve kurumsal dağıtımın ileri düzey teknik yönlerini keşfet.

Q1: Dynamic MultiHop, geleneksel Double VPN'den nasıl farklıdır?

Dynamic MultiHop, dünya genelinde giriş ve çıkış sunucularının herhangi bir birleşimini özelleştirmene olanak tanır.

Q2: CleanWeb 2.0 tarayıcı uzantılarında çalışır mı?

Evet, CleanWeb 2.0 Chrome/Firefox içindeki video reklamlarını, çerez onayı açılır pencerelerini ve uyarı bantlarını engeller.

Q3: Güvenlik paketindeki Alternatif Kimlik nedir?

Alternative ID, benzersiz kişisel takma adlar, e-posta adresleri ve telefon maskeleri üretir.

Q4: Surfshark DNS sızıntılarını nasıl önler?

Surfshark, tüm alan adı isteklerini her düğümdeki kendi özel DNS sunucuları üzerinden yönlendirir.

Q5: Surfshark mobilde ChaCha20 şifrelemesini destekliyor mu?

Evet, Android ve iOS'ta WireGuard, üstün mobil verimlilik için ChaCha20-Poly1305 kullanır.

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

VPN tünelleme protokollerinin, mobil istemci entegrasyonlarının ve kurumsal dağıtımın ileri düzey teknik yönlerini keşfet.

Q6: Surfshark'ta NoBorders modu nedir?

NoBorders, kısıtlayıcı ağ ortamlarını otomatik olarak algılar ve özel sunucular sağlar.

Q7: Surfshark tarayıcı uzantılarının güvenlik denetimlerini kim yaptı?

Bağımsız siber güvenlik firması Cure53, tarayıcı uzantıları ve sunucu sistemleri üzerinde denetimler tamamladı.

Q8: Surfshark IPv6 sızıntılarına karşı nasıl koruma sağlar?

Surfshark, IPv6 trafiğini güvenli biçimde yönlendirir veya şifrelenmemiş sızıntıyı önlemek için güvenli biçimde kısıtlar.

Q9: Surfshark'ın yasal yargı yetkisi nerede?

Surfshark, Hollanda yasalarına tabidir ve sıkı GDPR Avrupa gizlilik standartlarına uyar.

Q10: Surfshark iki faktörlü kimlik doğrulamayı (2FA) destekliyor mu?

Evet, ve Surfshark One, özellik ayarlarını yalnızca senin değiştirebilmen için bir 2FA kilidi ekler.

Bölüm 11: VPN'lerle ilgili 10 gerçek dünya gerçeği ve içgörüsü

VPN şifreleme hızları, protokol denetimleri, mobil bağlantı ve kurumsal uzaktan çalışmayla ilgili gerçek dünya bilgilerini incele.

1. VPN İPUCU

1. Surfshark, 4.500'den fazla sunucudan oluşan ağının tamamının disksiz, geçici yalnızca RAM donanımında çalıştığını söylüyor.

2. VPN İPUCU

2. Dört Büyükler'den Deloitte, Surfshark'ın kayıt tutmama politikasını 2023'te ve yeniden Kasım 2025'te doğruladı.

3. VPN İPUCU

3. Tescilli Nexus mimarisi, tüm küresel sunucuları dinamik bir yazılım tanımlı ağa bağlar.

4. VPN İPUCU

4. Dönen IP, VPN bağlantısını kesmeden IP adresini yaklaşık her beş dakikada bir değiştirir.

5. VPN İPUCU

5. CleanWeb 2.0, müdahaleci çerez onay açılır pencerelerini ve video reklamlarını doğrudan tarayıcılarda engeller.

6. VPN İPUCU

6. Dinamik MultiHop, kullanıcıların 100 ülke genelinde özelleştirilmiş çift sunuculu şifreleme yolları oluşturmasına olanak verir.

7. VPN İÇGÖRÜSÜ

7. Camouflage Mode, VPN başlık imzalarını kaldırır ve trafiği normal HTTPS'ten ayırt edilemez hale getirir.

8. VPN İÇGÖRÜSÜ

8. Alternative ID, kullanıcıları veritabanı sızıntılarından korumak için tek kullanımlık takma adlar ve e-posta maskeleri üretir.

9. VPN İÇGÖRÜSÜ

9. Surfshark, WireGuard protokollerinde ChaCha20'nin yanı sıra AES-256-GCM simetrik şifrelemesini uygular.

10. VPN İPUCU

10. NoBorders modu, dayanıklı tünelleme erişimi sağlamak için kısıtlı ağlarda otomatik olarak etkinleşir.

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel teknik standartlardan, spesifikasyonlardan ve düzenleyici çerçevelerden derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Entegre içerik engelleyici** REKLAM VE KÖTÜ AMAÇLI YAZILIM SAVUNMASI — Doğru cevap: B

ÖĞRETMEN NOTU

CleanWeb, Surfshark'ın reklamları, izleyici alan adlarını, kimlik avı web sitelerini ve kötü amaçlı URL komut dosyalarını ağ düzeyinde engelleyen entegre güvenlik filtresidir. Kaynak: CleanWeb Güvenlik Belirtimleri.

2 **%100 Yalnızca RAM Altyapısı** RAM MİMARİSİ — Doğru cevap: B

ÖĞRETMEN NOTU

Surfshark yalnızca RAM kullanan sunucular çalıştırır; bu nedenle sunucu belleğindeki veriler sunucu kapatıldığında veya yeniden başlatıldığında silinir. Kaynak: Cure53 Infrastructure Audit.

3 **MultiHop Çift Tünelleme** ÇOKLU ATLAMALI VPN — Doğru cevap: B

ÖĞRETMEN NOTU

MultiHop (Double VPN), trafik ilişkilendirme saldırılarını önlemek için trafiği ayrı ülkelerdeki iki farklı sunucu düğümü üzerinden şifreler. Kaynak: Surfshark MultiHop Rehberi.

4 **Camouflage Modu ile Gizleme** OBFUSKASYON — Doğru cevap: B

ÖĞRETMEN NOTU

Camouflage Modu, OpenVPN paket başlıklarını değiştirerek VPN trafiğini standart HTTPS trafiği gibi gösterir ve kısıtlayıcı güvenlik duvarı engellerini aşar. Kaynak: Surfshark Stealth Teknik Belgesi.

5 **Bypasser Bölünmüş Tünelleme** BÖLÜNMÜŞ TÜNELLEME — Doğru cevap: B

ÖĞRETMEN NOTU

Bypasser, Surfshark'ın kullanıcıların belirli uygulamaları veya web sitelerini doğrudan normal ISS bağlantıları üzerinden yönlendirmek üzere seçmesini sağlayan bölünmüş tünelleme aracıdır. Kaynak: Surfshark Client Features.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Geçici bellekteki verilerin silinmesi** SUNUCU GÜVENLİĞİ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Yalnızca RAM kullanan sunucular kalıcı sabit disklerde hiç veri saklamaz; donanımı yeniden başlatmak tüm işletim belleğini hemen temizler. Kaynak: RAM Server Architecture.

7 **Camouflage Modu ile ISS'den Gizlenme** TRAFİK GİZLEME — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Camouflage Modu, OpenVPN protokol imzalarını kaldırır; böylece ISS'ler kullanıcının bir VPN tüneline bağlı olduğunu tespit edemez. Kaynak: Derin Paket İnceleme Rehberi.

8 **CleanWeb 2.0 Tarayıcı Uzantıları** TARAYICI EKLENTİSİ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

CleanWeb 2.0, çerez onayı açılır pencerelerini, video reklamlarını ve kötü amaçlı yönlendirme komut dosyalarını gerçek zamanlı engellemek için tarayıcı uzantıları içinde çalışır. Kaynak: CleanWeb 2.0 Sürüm Notları.

9 **Sıfır Bağlantı Kaydı Tutma** KAYIT TUTMAMA POLİTİKASI — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Surfshark, bağımsız olarak denetlenen sıkı bir kayıt tutmama politikası uygular; IP adreslerini, bağlantı zaman damgalarını veya bant genişliği kayıtlarını tutmaz. Kaynak: Deloitte No-Logs Audit.

10 **Nexus IP Dinamik Döndürme** NEXUS AĞI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Surfshark Nexus yazılım tanımlı ağı, etkin VPN bağlantısını kesmeden kullanıcı IP adreslerini birkaç dakikada bir dinamik olarak değiştirir. Kaynak: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. RAM SUNUCUSU	G 3. ÇOKLU ATLAMA	F 4. GİZLENME
B 5. ATLAYICI	A 6. KILL SWITCH	H 7. NEXUS	E 8. DÖNEN

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 CLEANWEB	2 RAM SUNUCUSU	3 ÇOKLU ATLAMA	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMSUNUCUSU	6 H – DEĞİŞENIP	7 C – ÇOKLUATLAMA	8 G – NEXUS

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin CLEANWEB, RAM SUNUCUSU ve ÇOKLU ATLAMA terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

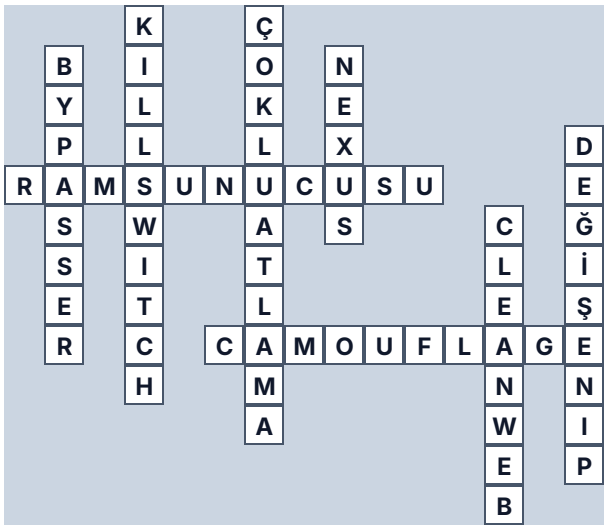
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

6 soldan sağa: RAMSUNUCUSU Her güç döngüsünde tüm verileri silen geçici bellekli sunucu donanımı (11 harf)

8 soldan sağa: CAMOUFLAGE VPN imzalarını gizleyerek normal HTTPS trafiğini taklit eden gizleme teknolojisi (10 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: KILLSWITCH VPN koptuğunda ağ trafiğini otomatik olarak engelleyen güvenlik özelliği (10 harf)

2 yukarıdan aşağı: ÇOKLUATLAMA Trafiği iki ayrı sunucu düğümü üzerinden şifreleyen çift VPN yönlendirme özelliği (11 harf)

3 yukarıdan aşağı: BYPASSER Seçili uygulamaların VPN'i atlamasına izin veren bölünmüş tünelleme işlevi (8 harf)

4 yukarıdan aşağı: NEXUS Tüm sunucuları birleşik bir ağda birbirine bağlayan tescilli yazılım tanımlı ağ (5 harf)

5 yukarıdan aşağı: DEĞİŞENIP Tünelleri kesintiye uğratmadan harici IP adresinizi düzenli olarak değiştiren özellik (9 harf)

7 yukarıdan aşağı: CLEANWEB Reklamları, kötü amaçlı yazılımları ve çerez onay bannerlarını engelleyen gelişmiş filtre (8 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	EANCWLBE	CLEANWEB	5.	UACUMUUNRSS	RAMSUNUCUSU
2.	UAOÇMAKALTL	ÇOKLUATLAMA	6.	GUOLACAFEM	CAMOUFLAGE
3.	AYBSSREP	BYPASSER	7.	ILKIWTCHSL	KILLSWITCH
4.	XSUNE	NEXUS	8.	PŞIDİEENĞ	DEĞİŞENIP

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SURFSHARK DEĞİŞEN İP GİZLİLİĞİNİ ARTIRIR"

Vaka çalışmaları cevap anahtarı

A VAKA ÇALIŞMASI 1: KAMPÜS VE İŞ YERİ FİLTRELERİNİ AŞMA

Öğretmen çözümü

NOTLANDIRMA ÖLÇEĞİ VE ÇÖZÜM YÖNERGELERİ

- Senaryo analizi: Bir öğrenci, üniversite kampüsü Wi-Fi'ının tüm standart OpenVPN ve WireGuard bağlantı noktalarını engellediğini görür.
- Odak sorusu: Hangi Surfshark özelliği öğrencinin ağ yöneticileri tarafından fark edilmeden bağlanmasını sağlar?
- Önerilen strateji ve çözüm: Güvenlik duvarlarının normal HTTPS gezintisi görmesi için VPN meta verilerini gizleyen Kamuflaj Modu'nu (OpenVPN) etkinleştir.

B VAKA ÇALIŞMASI 2: YÜKSEK RİSKLİ GAZETECİLİK SORUŞTURMASI

Öğretmen çözümü

NOTLANDIRMA ÖLÇEĞİ VE ÇÖZÜM YÖNERGELERİ

- Senaryo analizi: Bir araştırmacı gazeteci, hassas kurumsal kayıtları araştırırken gözetlemeye karşı ek korumaya ihtiyaç duyuyor.
- Odak sorusu: Dynamic MultiHop, tek sunuculu yönlendirmeye kıyasla nasıl daha üstün gizlilik sağlar?
- Önerilen strateji ve çözüm: Dinamik MultiHop trafiği iki ülkedeki giriş ve çıkış sunucularından geçirir; böylece hiçbir tek sunucu kullanıcıyı açığa çıkaramaz.