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

En Güvenli VPN Rehberi

Yüksek güvenlikli VPN tasarımı, yalnızca RAM kullanan geçici bellek sunucuları, Zero Trust erişim güvenliği, özel şifreli DNS sızıntı savunmaları ve denetlenmiş WireGuard yapılandırmalarının teknik analizi.

EN GÜVENLİ VPN REHBERİ 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 son derece güvenli VPN'lerin teknik standartları konusunda rehberlik eder. Yalnızca RAM kullanan sunucu donanımını, Sıfır Güven erişim güvenliğini, özel şifreli DNS çözümleyicilerini ve denetlenmiş WireGuard yapılandırmalarını keşfedeceksin.

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/en-guvenli-vpn/

En Güvenli VPN Öğrenme Yol Haritan

- Most Secure VPN Guide'ın teknik mimarisini ve şifreleme standartlarını analiz et.
- IP, DNS ve WebRTC trafiği sızıntılarını önlemek için istemci ayarlarını yapılandır.
- Kendi geliştirilen tünelleme protokollerini standart uygulamalarla karşılaştır.

EN GÜVENLİ VPN 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: yalnızca RAM kullanan sunucu donanımı ve Sıfır Güven sistemleri. Hızlı Düşün bonus etkinliğiyle bitir.

YALNIZCA RAM ALTYAPILARI VE SIFIR GÜVEN AĞLARI (GİRİŞ)

Gerçekten güvenli bir VPN; zero trust çerçevesine, günlüklerin disk el koymalarıyla açığa çıkmasını önleyen yalnızca RAM'li sunuculara, özel şifreli DNS çözümleyicilerine ve WireGuard gibi denetlenmiş protokollere dayanır. Bu birleşik denetimler, yüksek değerli dijital varlıkları araya girme tehditlerine karşı korur.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. 1. Modern VPN sunucularında en yüksek güvenliği sağlamak için hangi mimari temeldir?
   - A) Yalnızca RAM'li Sunucu Altyapısı
   - B) Disk Tabanlı Depolama
   - C) Dinamik DNS Yönlendirmesi
   - D) Port Yönlendirmeyi Etkinleştirme

2. 2. En güvenli ve modern VPN yapılandırmaları için yaygın olarak hangi protokol önerilir?
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. 3. Hangi güvenlik çerçevesi her bağlantının istisnasız sürekli doğrulanmasını gerektirir?
   - A) Zero Trust Mimarisi
   - B) Çevre Güvenlik Duvarları
   - C) Dinamik Yönlendirme
   - D) Paylaşılan Gizli Anahtarlar

4. 4. VPN istemcisinin DNS Sızıntı Koruması'nın temel rolü nedir?
   - A) Tüm DNS isteklerini özel şifreli çözümleyiciler üzerinden yönlendirir
   - B) IP paketlerini gizle
   - C) DNS sorgularını yerelde önbelleğe almak
   - D) Ad Sunucularını Devre Dışı Bırak

5. 5. Çok atlamalı (Multi-Hop) yönlendirme, bir VPN tünelinin genel güvenliğini nasıl artırır?
   - A) Veriyi art arda iki ayrı sunucu üzerinden yönlendirir
   - B) Sıkıştırma hızını artırır
   - C) Verileri düşük güvenlikli şifrelerle şifreler
   - D) Güvenlik Duvarlarını Aşar

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Yalnızca RAM kullanan sunucular günlük dosyalarını geçici bellekte saklar ve bu bellek yeniden başlatmada silinir.

○ Doğru ○ Yanlış

7 Soru 7

7. WireGuard, hız darboğazlarına karşı daha az savunmasız olan modern kriptografik algoritmalar kullanır.

○ Doğru ○ Yanlış

8 Soru 8

8. VPN kill switch, tünel koptuğunda tüm ağ trafiğini engelleyerek çalışır.

○ Doğru ○ Yanlış

9 Soru 9

9. Bağımsız üçüncü taraf denetimleri, güvenlik taahhütlerini doğrulamakla ilgisizdir.

○ Doğru ○ Yanlış

10 Soru 10

10. Sıfır Güven modelleri, tüm dahili ağ bağlantılarının varsayılan olarak güvenli olduğunu varsayar.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Yöneticiler katı bir _____ çerçevesi uygulayarak güvenliği sağlar.

2. Paketleri birden çok giriş noktası üzerinden yönlendirmek güvenli bir _____ yapılandırması gerektirir.

3. Çalınan disklerden veri sızıntısını önlemek için bir _____ tasarımı kullanırız.

4. İSS ele geçirmesi, yerel _____ özellikleri yapılandırılarak azaltılır.

5. Bağlantı hataları sırasında trafiği engellemek için _____ mekanizmasını etkinleştirin.

6. Saklanan veritabanı kayıtlarını en aza indirmek için tamamen _____ bir sağlayıcı seçin.

KELİME BANKASI

ÇOKLU ATLAMA | DENETLENMİŞ RAM SUNUCUSU | DNS KORUMASI | SIFIR GÜVEN | KILL SWITCH | ŞİFRELEME | PROTOKOL

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: VPN ve ağ kavramı eşleştirme

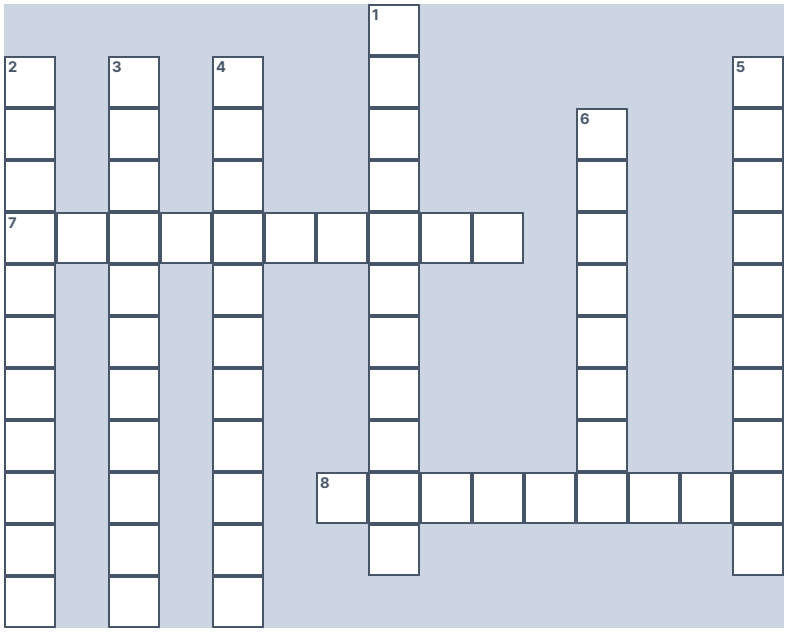
TANIM EŞLEŞTİRME

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

☐	1. Sıfır Güven	A	Hiçbir kaydın saklanmadığını doğrulayan, bağımsız olarak incelenmiş kurulum.
☐	2. Çoklu Atlama	B	Aktarımı güvenceye almak için veri yüklerinin şifreleme yoluyla karıştırılması.
☐	3. Yalnızca RAM sunucu	C	Tüm kullanıcıların sürekli kimlik doğrulamasını gerektiren güvenlik çerçevesi.
☐	4. DNS Koruması	D	Verilerin nasıl paketlenip gönderileceğini belirleyen teknik kurallar kümesi.
☐	5. Kill Switch	E	İki sunucu düğümünü birbirine zincirleyen kademeli VPN yönlendirmesi.
☐	6. Denetlenmiş Sistem	F	Veri yüklerini depolamak için geçici bellek kullanan sunucu mimarisi.
☐	7. Şifreleme	G	Ad sunucusu aramalarını korumak için özel DNS sorgularını zorunlu kılma.
☐	8. Protokol	H	VPN başarısız olursa trafiği engelleyen arıza durumunda güvenli mekanizma.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

7. VPN çökerse trafiği engelleyen güvenlik mekanizması (10)

8. İletimi güvence altına almak için veri yüklerinin kriptografik olarak karıştırılması (9)

YUKARIDAN AŞAĞI

1. Sıfır kaydın saklandığını doğrulayan, bağımsız olarak incelenmiş kurulum (11)

2. Ad sunucusu aramalarını korumak için özel DNS sorgularını zorunlu kılma (11)

3. İki sunucu düğümünü birbirine zincirleyen kademeli VPN yönlendirmesi (11)

4. Veri yüklerini saklamak için geçici bellek kullanan sunucu mimarisi (11)

5. Tüm kullanıcıların sürekli kimlik doğrulamasını gerektiren güvenlik çerçevesi (10)

6. Verinin nasıl paketlenip gönderileceğini belirleyen teknik kurallar bütünü (8)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

7 soldan sağa: VPN çökerse trafiği engelleyen güvenlik mekanizması (10 harf):

8 soldan sağa: İletimi güvence altına almak için veri yüklerinin kriptografik olarak karıştırılması (9 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Sıfır kaydın saklandığını doğrulayan, bağımsız olarak incelenmiş kurulum (11 harf):

2 yukarıdan aşağı: Ad sunucusu aramalarını korumak için özel DNS sorgularını zorunlu kılma (11 harf):

3 yukarıdan aşağı: İki sunucu düğümünü birbirine zincirleyen kademeli VPN yönlendirmesi (11 harf):

4 yukarıdan aşağı: Veri yüklerini saklamak için geçici bellek kullanan sunucu mimarisi (11 harf):

5 yukarıdan aşağı: Tüm kullanıcıların sürekli kimlik doğrulamasını gerektiren güvenlik çerçevesi (10 harf):

6 yukarıdan aşağı: Verinin nasıl paketlenip gönderileceğini belirleyen teknik kurallar bütünü (8 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

SIFIRGÜVEN ÇOKLUATLAMA RAMSUNUCUSU DNSKORUMASI KILLSWITCH
DENETLENMİŞ ŞİFRELEME PROTOKOL

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. SIFIRGÜVEN**
- **B. ÇOKLUATLAMA**
- **C. RAMSUNUCUSU**
- **D. DNSKORUMASI**
- **E. KILLSWITCH**
- **F. DENETLENMİŞ**
- **G. ŞİFRELEME**
- **H. PROTOKOL**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. VPN çökerse trafiği engelleyen güvenlik mekanizması.
2. Ad sunucusu aramalarını korumak için özel DNS sorgularını zorunlu kılma.
3. İki sunucu düğümünü birbirine zincirleyen kademeli VPN yönlendirmesi.
4. Verinin nasıl paketlenip gönderileceğini belirleyen teknik kurallar bütünü.
5. İletimi güvence altına almak için veri yüklerinin kriptografik olarak karıştırılması.
6. Veri yüklerini saklamak için geçici bellek kullanan sunucu mimarisi.
7. Sıfır kaydın saklandığını doğrulayan, bağımsız olarak incelenmiş kurulum.
8. Tüm kullanıcıların sürekli kimlik doğrulamasını gerektiren güvenlik çerçevesi.

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. **EÜGRISVNIF** _____
2. **UUARSNMUCUS** _____
3. **KWCIISHLTL** _____
4. **EEMRELŞİF** _____
5. **AOLTKAUAÇML** _____
6. **OIRMSADNUSK** _____
7. **NTDEEŞMİNLE** _____
8. **TROLPOKO** _____

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Her gün kullandığın kilitler veya anahtarlar			
2	Bir VPN'in gizleyebileceği şeyler			
3	Bir VPN'i güvenli yapan şeyler			
4	VPN'lerle ilgili efsaneler			
5	Seyahat ederken VPN kullanma nedenleri			
6	Gerçek dünyadaki güvenli yerler			
7	'Korumalı' anlamına gelen sözcükler			
8	İyi bir VPN sağlayıcısının verdiği sözler			
9	Gizlilikle ilgili sözcükler			
10	Denetim veya inceleme türleri			
11	Bu çalışma kâğıdından aklında tutmak istediğin sözcükler			
12	Bir hackerın çalmak istediği şeyler			
13	Sahte Wi-Fi ağını fark etme yolları			
14	VPN kullanacağın yerler			
15	İnternet sağlayıcının görebildiği şeyler			

Kontrol Noktası 8: VPN ve ağ vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KURUMSAL ALTYAPIYI SERTLEŞTİRME



Senaryo: Kurumsal bir banka, uzaktan erişim topolojisini yeniden tasarlıyor. Tüm istemci cihazlarını güvenli sunuculara bağlayan bir sıfır güven (zero trust) mimarisi istiyorlar.

Tartışma sorusu: Sıfır Güven VPN modelinde ağ mikro segmentasyonunun başlıca faydası nedir?

VAKA ÇALIŞMASI 2: YALNIZCA RAM'Lİ SUNUCU KORUMALARI



Senaryo: Güvenliğe odaklı bir VPN sağlayıcısı, fiziksel sunucuya el konulmasının kullanıcı kayıt geçmişlerini açığa çıkarmasını önlemek için sunucularını yükseltiyor.

Tartışma sorusu: Yalnızca RAM kullanan donanım yapılandırmalarının, fiziksel sunuculara el konulduğunda adli veri çıkarımını nasıl engellediğini açıkla.

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

8	26	27	6	17	15	12		27	20	17	15	6	21

5	6	9	6	21	15	12		5	12	13	12	24	1	15

27	1	21	15	11	14	15	1	21	11		14	18	21	25	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: Bir VPN'i 'en güvenli' yapan nedir?

Zero Trust, yalnızca RAM'li sunucular ve denetlenmiş protokollerin birleşimi.

Q2: Yalnızca RAM'li sunucular nedir?

Geçici bellekte çalışan, diske hiç kayıt yazmayacak şekilde tasarlanmış sunucular.

Q3: Sıfır Güven (Zero Trust) VPN nedir?

Her erişim isteğini ve bağlantıyı sürekli doğrulayan bir çerçeve.

Q4: WireGuard neden güvenli sayılır?

Küçük ve kolayca denetlenebilir bir kod tabanına sahiptir ve modern şifreler kullanır.

Q5: Güvenli VPN'ler DNS sızıntılarını nasıl önler?

Tüm sorguları özel, şifreli DNS çözümleyicileri üzerinden yönlendirerek.

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: Güvenli bir VPN denetim gerektirir mi?

Evet, bağımsız denetimler sıfır kayıt iddialarını ve kod güvenliğini doğrular.

Q7: Kill switch'in rolü nedir?

VPN bağlantısı kesilirse ağ trafiğini hemen durdurur.

Q8: Güvenli VPN'lerde hangi şifreleme kullanılır?

AES-256 ve ChaCha20 şifreleme için sektör standartlarıdır.

Q9: Multi-Hop yönlendirme güvenli mi?

Evet, trafik analizini önlemek için iki veya daha fazla sunucuyu zincirler.

Q10: Offshore yargı yetkisi nasıl yardımcı olur?

Hangi yasaların geçerli olduğunu sınırlayabilir, ancak mutlak bir dokunulmazlık sunmaz.

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: Yalnızca RAM'li sunucular veri el koyma risklerini nasıl önler?

RAM üzerinde çalıştıkları için fişi çekmek, bellekte tutulan verileri siler.

Q2: Sıfır Güven, standart çevre güvenliğinin yerini nasıl alır?

Her istemciye düşman gözüyle bakar ve sürekli kimlik doğrulaması gerektirir.

Q3: WireGuard kod tabanını denetlemeyi neyin kolaylaştırır?

Linux kodu 4.000 satırın altındadır; tipik VPN yığınlarından çok daha küçüktür. [4]

Q4: DNSSEC, DNS sorgularını nasıl korur?

DNS kayıtlarını imzalar; böylece çözümleyiciler sahte veya kurcalanmış yanıtları algılayabilir.

Q5: Multi-Hop trafik ilişkilendirmesini nasıl zorlaştırır?

Gelen ve giden IP'leri farklı barındırma sağlayıcılarına ayırarak.

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: Five Eyes yargı bölgeleri VPN'ler için neden risklidir?

Üye devletler istihbarat paylaşır ve kullanıcı verilerini talep etmek için hukuki emirler kullanabilir.

Q7: Kill switch çekirdek düzeyinde nasıl uygulanır?

Çıkışı engellemek için sistem güvenlik duvarı kurallarını (iptables veya WFP gibi) kullanır.

Q8: VPN el sıkışmalarında ileri gizlilik nedir?

Benzersiz oturum anahtarları üretir; böylece geçmiş oturumların şifresi çözülemez.

Q9: Güvenli VPN'ler WebRTC sızıntılarını nasıl azaltır?

WebRTC isteklerini engelleyerek veya tünel üzerinden yönlendirerek.

Q10: Bağımsız denetimler gizlilik uyumluluğunu nasıl güvence altına alır?

Denetçiler sızma testi yapar ve sunucu yapılandırmalarını inceler.

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

Yalnızca RAM kullanan sunucular işletim sistemini açılışta belleğe yükler; bu nedenle yeniden başlatmadan sonra diskte hiçbir şey kalmaz.

2. VPN İPUCU

WireGuard, Curve25519, ChaCha20, Poly1305, BLAKE2s ve HKDF ile Noise çerçevesini kullanır. [3]

3. VPN İPUCU

Sıfır Güven, erişimi kaynak başına verir ve ağ konumuna dayalı örtük güven tanımaz (NIST SP 800-207). [1]

4. VPN İPUCU

Five Eyes istihbarat ittifakı ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda'yı kapsar.

5. VPN İPUCU

WebRTC sızıntıları, tarayıcıların STUN sorguları aracılığıyla istemcinin gerçek genel IP adresini ortaya çıkarması durumunda oluşur.

6. VPN İPUCU

Mükemmel ileri gizlilik (PFS), uzun vadeli bir anahtarın ele geçirilmesinin geçmiş oturum anahtarlarını ifşa etmemesini sağlar. [3]

7. VPN İÇGÖRÜSÜ

Berlin merkezli bir güvenlik firması olan Cure53, birkaç VPN sağlayıcısının denetimlerini yayımladı.

8. VPN İÇGÖRÜSÜ

DNS sızıntıları, DNS sorgularının VPN tünelini atlayıp yerel İSS'nin ad sunucularına gitmesiyle oluşur.

9. VPN İÇGÖRÜSÜ

Geçici RAM çipleri verileri tutmak için sürekli elektrik gücü gerektirir; güç kesildiğinde içerikleri kaybolur.

10. VPN İPUCU

Kurumsal Sıfır Güven sistemleri, güvenli kaynaklara bağlantıya izin vermeden önce cihaz durumu denetimlerini zorunlu kılar. [1]

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Yalnızca RAM sunucu** YALNIZCA RAM — **Doğru cevap: A**

ÖĞRETMEN NOTU

Yalnızca RAM kullanan sunucular diske kayıt saklamaz; yeniden başlatmada veriler silinir. Kaynak: Most Secure VPN.

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

WireGuard, küçük ve denetlenebilir bir kod tabanını modern şifrelerle bir araya getirir.

3 **Sıfır Güven Modeli** SIFIR GÜVEN — **Doğru cevap: A**

ÖĞRETMEN NOTU

Sıfır Güven modelleri, erişimden önce cihaz uyumluluğunu sürekli doğrular. Kaynak: Most Secure VPN.

4 **DNS Koruması** DNS KORUMASI — **Doğru cevap: A**

ÖĞRETMEN NOTU

DNS Sızıntı Koruması, arama sorgularını özel çözümleyiciler üzerinden yönlendirir. Kaynak: Most Secure VPN.

5 **Çoklu Atlamalı Tüneller** ÇOKLU ATLAMA — **Doğru cevap: A**

ÖĞRETMEN NOTU

Çoklu atlama yönlendirmesi, iki ayrı sunucu düğümünü art arda zincirler. Kaynak: En Güvenli VPN.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Yalnızca RAM sunucu** YALNIZCA RAM — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Yalnızca RAM kullanan sunucu donanımı diske veri yazmaz; yeniden başlatmada silinir. Kaynak: Most Secure VPN.

7 **WireGuard hızı** WIREGUARD — Doğru cevap: Doğru

ÖĞRETMEN NOTU

WireGuard, işlem darboğazlarından kaçınan modern kriptografi kullanır. Kaynak: Most Secure VPN.

8 **Kill Switch** FAİL-SAFE ANAHTARI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Kill switch, VPN bağlantısı koptuğunda tüm trafiği engeller. Kaynak: Most Secure VPN.

9 **Üçüncü Taraf Denetimleri** DENETİMLER ŞART — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Kurumsal gizlilik iddialarını doğrulamak için üçüncü taraf denetimleri şarttır. Kaynak: Most Secure VPN.

10 **Soru 10** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Zero Trust, ağ konumuna dayalı hiçbir örtük güven tanımaz.

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. Sıfır Güven	E 2. Çoklu Atlama	F 3. Yalnızca RAM sunucu	G 4. DNS Koruması
H 5. Kill Switch	A 6. Denetlenmiş Sistem	B 7. Şifreleme	D 8. Protokol

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 SIFIR GÜVEN	2 ÇOKLU ATLAMA	3 RAM SUNUCUSU	4 DNS KORUMASI
5 KILL SWITCH	6 DENETLENMİŞ		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 E – KILLSWITCH	2 D – DNSKORUMASI	3 B – ÇOKLUATLAMA	4 H – PROTOKOL
5 G – ŞİFRELEME	6 C – RAMSUNUCUSU	7 F – DENETLENMİŞ	8 A – SIFIRGÜVEN

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin Sıfır Güven, Çoklu Atlama ve Yalnızca RAM sunucu 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

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

BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

7 soldan sağa: KILLSWITCH VPN çökerse trafiği engelleyen güvenlik mekanizması (10 harf)

8 soldan sağa: ŞİFRELEME İletimi güvence altına almak için veri yüklerinin kriptografik olarak karıştırılması (9 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: DENETLENMİŞ Sıfır kaydın saklandığını doğrulayan, bağımsız olarak incelenmiş kurulum (11 harf)

2 yukarıdan aşağı: DNSKORUMASI Ad sunucusu aramalarını korumak için özel DNS sorgularını zorunlu kılma (11 harf)

3 yukarıdan aşağı: ÇOKLUATLAMA İki sunucu düğümünü birbirine zincirleyen kademeli VPN yönlendirmesi (11 harf)

4 yukarıdan aşağı: RAMSUNUCUSU Veri yüklerini saklamak için geçici bellek kullanan sunucu mimarisi (11 harf)

5 yukarıdan aşağı: SIFIRGÜVEN Tüm kullanıcıların sürekli kimlik doğrulamasını gerektiren güvenlik çerçevesi (10 harf)

6 yukarıdan aşağı: PROTOKOL Verinin nasıl paketlenip gönderileceğini belirleyen teknik kurallar bütünü (8 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. EÜGRISVNIF — **SIFIRGÜVEN**
2. UUARSNMUCUS — **RAMSUNUCUSU**
3. KWCIISHLTL — **KILLSWITCH**
4. EEMRELŞİF — **ŞİFRELEME**
5. AOLTKAUAÇML — **ÇOKLUATLAMA**
6. OIRMSADNUSK — **DNSKORUMASI**
7. NTDEEŞMİNLE — **DENETLENMİŞ**
8. TROLPOKO — **PROTOKOL**

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"GÜVENLİ VPNLER DEĞERLİ DİJİTAL VARLIKLARI KORUR"

Vaka çalışmaları cevap anahtarı

A VAKA ÇALIŞMASI 1: KURUMSAL ALTYAPIYI SERTLEŞTİRME

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Kurumsal bir banka uzaktan erişim topolojisini yeniden tasarlıyor. Tüm istemci cihazları güvenli sunuculara bağlayan bir sıfır güven mimarisi gerekiyor.
- Önerilen Strateji ve Çözüm: Değerlendirme rehberi: Mikro bölümlendirmenin belirli kaynaklara erişimi sınırladığını ve bir cihaz ele geçirilirse tehdidin yanal hareketini önlediğini açıkla.

B VAKA ÇALIŞMASI 2: YALNIZCA RAM'Lİ SUNUCU KORUMALARI

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Güvenlik odaklı bir VPN sağlayıcısı, fiziksel sunucuya el konulmasının kullanıcı günlük geçmişlerini açığa çıkarmasını önlemek için sunucularını yükseltiyor.
- Önerilen Strateji ve Çözüm: Değerlendirme rehberi: RAM-Only sunucuların fiziksel disk depolaması olmadığını ayrıntılandır. Elektrik kesintisi, geçici bellekteki tüm geçici verileri otomatik olarak siler.