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

Uzaktan Erişim VPN'i

Uzaktan çalışan uç noktalarını güvenceye alma, çok faktörlü kimlik doğrulama ve IPsec tüneli yapılandırmaları.

UZAKTAN ERİŞİM VPN'LERİ 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 uzaktan erişim VPN ağları konusunda rehberlik eder. İstemciden siteye tünelleri, çok faktörlü girişleri, uç nokta duruş kontrollerini, bant genişliği sınırlarını ve syslog güvenlik denetimini 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/isletmeler-icin-en-iyi-vpn/uzaktan-erisim/

Uzaktan Erişim VPN'i Öğrenme Yol Haritan

- Yerel ağ düğümlerine erişen güvenli uzaktan çalışan uç noktaları.
- Uzaktan girişler için çok faktörlü kimlik doğrulama politikalarını yapılandır.
- İstemciden siteye IPsec ve OpenVPN yapılandırmaları kur.
- Erişim kontrolü ihlalleri için uzak bağlantı kayıtlarını denetle.
- Ağ bağlantıları vermeden önce cihaz durumu denetimleri uygula.
- Uzaktan çalışmada bant genişliği tıkanmasını önlemek için sunucu verimini optimize et.

UZAKTAN ERİŞİM VPN'LERİ 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: duruş (posture) denetimleri ve çok faktörlü girişler. Hızlı Düşün bonus etkinliğiyle bitir.

İSTEMCİDEN SİTEYE TÜNELLER VE UÇ NOKTA UYUMLULUĞU (GİRİŞ)

Uzaktan erişim VPN'leri, ofis dışındaki çalışanlar için güvenli istemciden siteye tüneller kurar. Bu bağlantıları güvenceye almak, çok faktörlü kimlik doğrulama (MFA) girişlerini zorunlu kılmayı, uç nokta durumu uyumluluk kontrolleri yapmayı ve günlükleri merkezi syslog toplayıcılarıyla denetlemeyi gerektirir.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1 **1. Uzaktan erişim VPN portalları hangi kimlik doğrulama standardını zorunlu kılmalıdır?**

- A) Çok faktörlü
- B) Tek faktör
- C) Şifrelenmemiş
- D) Yerel misafir

2 **2. Uzaktan çalışmada istemciden siteye bağlantıları güvenceye almak için standart olan protokol hangisidir?**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3 **3. Hangi kontrol, uzaktaki bir dizüstü bilgisayarın bağlanmadan önce temiz olup olmadığını doğrular?**

- A) Duruş denetimi
- B) Hız testi
- C) Ping testi
- D) Bellek sayısı

4 **4. Güvenlik denetimi için uzaktan çalışan bağlantı günlükleri nerede saklanır?**

- A) Syslog sunucusu
- B) Kayıt defteri anahtarı
- C) İstemci belleği
- D) Web tarayıcısı

5 **5. Uzaktan çalışan sayısı ağ geçidi bant genişliği kapasitesini aştığında hangi sorun ortaya çıkar?**

- A) Bant genişliği boğulması
- B) DNS sızıntısı
- C) El sıkışma geçişi
- D) IP'nin açığa çıkması

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Çok faktörlü kimlik doğrulama, uzaktan oturum açmaları güvenceye almak için ikinci bir doğrulama belirteci ekler.

○ Doğru ○ Yanlış

7 Soru 7

7. Duruş denetimleri, güvenlik duvarı devre dışı olan uzak cihazların özel sunuculara erişmesine izin verir.

○ Doğru ○ Yanlış

8 Soru 8

8. Uzaktan erişim VPN günlükleri, yetkisiz kurumsal ağ girişlerini izlemek için gereklidir.

○ Doğru ○ Yanlış

9 Soru 9

9. OpenVPN ve IPsec, uzak istemci verilerini şifrelemeyen eski protokollerdir.

○ Doğru ○ Yanlış

10 Soru 10

10. Ağ geçidinde bant genişliği darboğazı, uzak trafik bağlantı kartı kapasitesini aştığında oluşur.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Kurumsal portalları korumak için uzaktan girişler _____ kimlik doğrulama gerektirmelidir.

2. Uzak istemciler tünel yükünü standart _____ protokolleriyle şifreler.

3. Cihazlar ağ bağlantısı almadan önce bir güvenlik _____ denetiminden geçmelidir.

4. Denetlenebilir giriş kayıtları sürekli olarak merkezi bir _____ sunucusuna iletilir.

5. Mesai saatlerindeki yoğun trafik, ağ geçidinde _____ tıkanıklığına yol açabilir.

6. Sanal bağdaştırıcı sürücüleri, Windows ve macOS'ta istemciden siteye _____ işlemini yönetir.

KELİME BANKASI

BANT GENİŞLİĞİ · ÇOK FAKTÖRLÜ · DURUŞ · GÜVENLİK DUVARI · OPENVPN · SYSLOG · ŞİFRELEME · TÜNELLEME

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Temel kavram eşleştirme

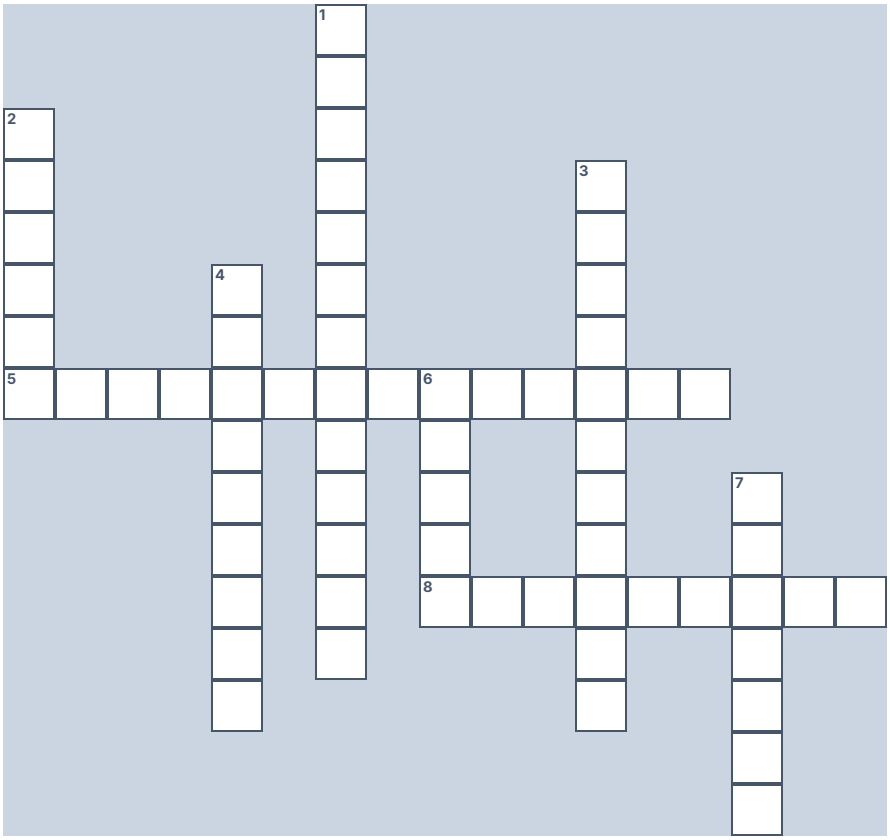
TANIM EŞLEŞTİRME

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

☐	1. ÇOK FAKTÖRLÜ	A	Verileri güvenli bir yola kapsülleme.
☐	2. OPENVPN	B	Merkezi güvenlik günlüğü toplayıcı.
☐	3. DURUŞ	C	Ağ veri kapasitesi sınırı.
☐	4. SYSLOG	D	Standart istemciden siteye protokol.
☐	5. BANT GENİŞLİĞİ	E	Uzak cihaz sağlığı doğrulaması.
☐	6. ŞİFRELEME	F	Trafik filtreleme sistemi kuralları.
☐	7. TÜNELLEME	G	Paketlerin şifreleme yoluyla karıştırılması.
☐	8. GÜVENLİK DUVARI	H	Ek belirteç gerektiren oturum açma güvenliği.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

5. Trafik filtreleme sistemi kuralları (14)

8. Paketlerin kriptografik olarak karıştırılması (9)

YUKARIDAN AŞAĞI

1. Ağ veri kapasitesi sınırı (13)

2. Merkezi güvenlik günlüğü toplayıcısı (6)

3. Ek belirteç gerektiren oturum açma güvenliği (11)

4. Veriyi güvenli bir yola kapsülleme (9)

6. Uzak cihazın sağlık durumunu doğrulama (5)

7. Standart istemciden siteye protokolü (7)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

5 soldan sağa: Trafik filtreleme sistemi kuralları (14 harf):

8 soldan sağa: Paketlerin kriptografik olarak karıştırılması (9 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Ağ veri kapasitesi sınırı (13 harf):

2 yukarıdan aşağı: Merkezi güvenlik günlüğü toplayıcısı (6 harf):

3 yukarıdan aşağı: Ek belirteç gerektiren oturum açma güvenliği (11 harf):

4 yukarıdan aşağı: Veriyi güvenli bir yola kapsülleme (9 harf):

6 yukarıdan aşağı: Uzak cihazın sağlık durumunu doğrulama (5 harf):

7 yukarıdan aşağı: Standart istemciden siteye protokolü (7 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

ÇOKFAKTÖRLÜ OPENVPN DURUŞ SYSLOG BANTGENİŞLİĞİ ŞİFRELEME TÜNELLEME GÜVENLİKDUVARI

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. ÇOKFAKTÖRLÜ**
- **B. OPENVPN**
- **C. DURUŞ**
- **D. SYSLOG**
- **E. BANTGENİŞLİĞİ**
- **F. ŞİFRELEME**
- **G. TÜNELLEME**
- **H. GÜVENLİKDUVARI**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Merkezi güvenlik günlüğü toplayıcısı.
2. Trafik filtreleme sistemi kuralları.
3. Veriyi güvenli bir yola kapsülleme.
4. Paketlerin kriptografik olarak karıştırılması.
5. Standart istemciden siteye protokolü.
6. Ağ veri kapasitesi sınırı.
7. Uzak cihazın sağlık durumunu doğrulama.
8. Ek belirteç gerektiren oturum açma güvenliği.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Alan adı aracılığının temel kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. A T L O K Ö Ç R K Ü F
2. D Ş U R U
3. A B İ L Ş Ğ İ N N G E İ T
4. L E M E E L T Ü N
5. V N N E O P P
6. O L S S G Y
7. L Ş M E E R İ E F
8. E K A L D U Ü I G İ V R V N

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	VPN'lerle ilgili efsaneler			
2	Sıfır Güven'i anlatan sözcükler			
3	Bildiğin ofis programları			
4	Güvenli uzaktan çalışma kuralları			
5	İnternet sağlayıcının görebildiği şeyler			
6	Bildiğin VPN hizmetleri			
7	Çalışanların çalıştığı yerler			
8	Bir şirketin her gün kullandığı araçlar			
9	BT departmanındaki roller			
10	Bir çalışanın sahip olabileceği cihazlar			
11	Bir şirketin korumak zorunda olduğu veriler			
12	Güvenlik ihlalinden sonra yapılacaklar			
13	Görüntülü toplantıyı aksatabilecek şeyler			
14	Güvenli oturum açma yolları			
15	Çalışanlara VPN verme nedenleri			

Kontrol Noktası 8: VPN ve ağ vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: MFA ZORUNLULUĞU



Senaryo: Bir iş analisti uzaktan çalışırken kurumsal veritabanına giriş yapmaya çalışıyor. Kullanıcı adını ve parolasını doğru giriyor, ancak VPN portalı erişimi engelliyor ve fiziksel bir token kodu istiyor.

Tartışma sorusu: Hangi güvenlik ilkesi bu çift doğrulama adımını zorunlu kılıyor?

VAKA ÇALIŞMASI 2: DURUŞ UYUMLULUĞU



Senaryo: Bir yüklenici kişisel dizüstü bilgisayarını uzak kurumsal ağa bağlıyor. VPN istemcisi bağlantıyı hemen kesiyor ve kullanıcıya antivirüs tanımlarının güncel olmadığını bildiriyor.

Tartışma sorusu: Bu bağlantı girişimini hangi özel VPN ağ geçidi denetimi engelledi?

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

25 29 1 14 24 1 17 6 21 12 23 12 16 27 20 17

5 1 9 11 24 11 14 14 25 21 25 16 22 1 15

25 4 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: Uzaktan erişim VPN'i nedir?

Saha dışında çalışan çalışanların özel kurumsal sunuculara doğrudan bağlanmasını sağlayan güvenli bağlantı yöntemi.

Q2: İstemciden siteye bağlantı, siteden siteye bağlantıdan neden farklıdır?

İstemciden siteye, tek tek kullanıcı cihazlarını bağlar; siteden siteye ise tüm fiziksel ofis konumlarını birbirine bağlar.

Q3: Cihaz duruş kontrolü nedir?

Erişim vermeden önce uzak bir cihazın güvenlik durumunu (antivirüs, işletim sistemi yama düzeyi) kontrol eden tarama.

Q4: OpenVPN uzaktan erişim için neden kullanılır?

Güçlü güvenlik protokolü, çapraz platform uyumluluğu ve bireysel bağlantıları yönetebilme yeteneği nedeniyle.

Q5: MFA uzaktan erişimi nasıl korur?

İkincil bir doğrulama belirteci ekler ve çalışan parolaları sızdırılsa veya çalınsa bile erişimi engeller.

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: Syslog sunucusu nedir?

Uyumluluk denetimleri için bağlantı olaylarını, oturum açmaları ve sistem uyarılarını saklayan merkezi günlük deposu.

Q7: Bant genişliği tıkanmasına ne yol açar?

Uzaktan çalışanların toplam bant genişliği talebi, şirket ağ geçidinin internet hızı sınırını aştığında.

Q8: Ev bilgisayarımı iş VPN'ine bağlayabilir miyim?

Yalnızca cihaz kurumsal duruş denetimlerini geçerse ve BT yöneticileri tarafından yetkilendirilmişse.

Q9: Ağ kapsüllemesi nedir?

İletim güvenliğini sağlamak için aktarım sırasındaki veri paketlerinin şifreli protokol başlıklarına sarılması.

Q10: Bölünmüş tünel uzaktan erişimi nasıl optimize eder?

Çalışanların standart gezinme için yerel İSS'lerini kullanmasına, işle ilgili dosyaları ise VPN üzerinden yönlendirmesine olanak tanır.

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: Sertifika tabanlı kimlik doğrulama uzaktan erişimi nasıl güçlendirir?

Bağlantı izinlerini önceden kurulmuş yerel dijital sertifikalara bağlar ve yönetilmeyen veya yetkisiz cihazları engeller.

Q2: Uzaktan çalışma için bölünmüş tünelin güvenlik riski nedir?

Ele geçirilmiş bir yerel cihazın dış tehditleri özel ağa yönlendirebileceği olası bir köprü oluşturur.

Q3: Duruş kontrolleri kayıt defteri ayarlarını nasıl denetler?

VPN istemcisi, kurumsal güvenlik yazılımının etkin olarak çalışıp çalışmadığını doğrulamak için kayıt defteri yollarını sorgulayan yerel betikler çalıştırır.

Q4: Syslog'lar neden varsayılan olarak UDP 514 bağlantı noktasını kullanır?

Günlükleri en az ek yükle hızla iletmek için; ancak güvenli kurulumlar artık TCP üzerinden TLS kapsüllemesini zorunlu kılar.

Q5: Şirketler ağ geçidi bant genişliği darboğazlarını nasıl çözer?

Yük dengeleyiciler uygulayarak ve uzak trafiği bölgesel sunucu düğümlerine dağıtarak.

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: Uzak istemcilerde sanal TAP/TUN bağdaştırıcılarının işlevi nedir?

Sanal ağ kartları gibi davranır ve cihaz düzeyindeki TCP/IP trafiğini doğrudan şifreli VPN tüneline yönlendirirler.

Q7: IKEv2 MOBIKE uzaktan çalışan ekiplerin hareketliliğini nasıl destekler?

IP adresi bağlantılarını dinamik olarak günceller ve kullanıcı Wi-Fi ile hücresel veri arasında geçiş yaparken VPN'i etkin tutar.

Q8: Bölünmüş ve tam tünel yönlendirme arasındaki fark nedir?

Tam yönlendirme cihazın tüm internet trafiğini VPN üzerinden geçirir; bölünmüş yönlendirme ise yalnızca kurumsal hedef IP'lerini gönderir.

Q9: NAT cihazları uzak VPN bağlantılarını nasıl ele alır?

Dönen şifreli veri paketlerini yönlendirmek için yerel port aralıklarını genel ağ geçidi IP adreslerine eşleyerek.

Q10: Hangi uyumluluk standartları uzaktan erişim denetimini zorunlu kılar?

HIPAA, SOC 2 ve PCI DSS gibi standartlar, tüm uzaktan bağlantı oturumlarının kaydedilmesini ve izlenmesini gerektirir.

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

Uzaktan erişim VPN'leri, ofis dışındaki çalışanlar için güvenli istemciden siteye tüneller kurar.

2. VPN İPUCU

Çok faktörlü kimlik doğrulama, uzak iş portallarını korumak için uyumluluk kuralları gereği zorunludur.

3. VPN İPUCU

Duruş denetimleri, özel ağ erişimi vermeden önce yerel istemci güvenlik ayarlarını doğrular.

4. VPN İPUCU

Syslog sunucuları, yetkisiz erişim girişimlerini denetlemek ve tespit etmek için bağlantı kayıtlarını toplar.

5. VPN İPUCU

Ağ geçidinde bant genişliği darboğazları, toplam uzak trafik talebi sunucunun internet sınırlarını aştığında oluşur.

6. VPN İPUCU

Sanal ağ adaptörleri, işletim sistemi ağ sorgularını güvenli protokollerin içine kapsüller.

7. VPN İÇGÖRÜSÜ

MOBIKE desteği, uzak istemcilerin VPN tünelini düşürmeden ağ değiştirmesini sağlar.

8. VPN İÇGÖRÜSÜ

Tam tünel yönlendirmesi çalışanların tüm internet trafiğini korur ancak kurumsal ağ geçidi yükünü artırır.

9. VPN İÇGÖRÜSÜ

Sertifika kimlik doğrulaması, VPN bağlantı yetkisini doğrudan şirket tarafından yönetilen donanıma bağlar.

10. VPN İPUCU

SOC 2 ve PCI DSS gibi çerçeveler, uzaktan erişim oturumlarının kaydedilmesini ve izlenmesini bekler.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.

https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.

https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.

https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Oturum Açma Belirteçleri** MFA GÜVENLİĞİ — Doğru cevap: A

ÖĞRETMEN NOTU

Çok faktörlü kimlik doğrulama, oturum açmalar için ikinci bir doğrulama uygular. Kaynak: MFA Uygulaması.

2 **OpenVPN tüneli** İSTEMCİDEN SİTEYE — Doğru cevap: A

ÖĞRETMEN NOTU

OpenVPN, istemciden siteye tünelleri güvenceye almak için kullanılan standart bir protokoldür. Kaynak: OpenVPN Client.

3 **Duruş denetimleri** CİHAZ KONTROLÜ — Doğru cevap: A

ÖĞRETMEN NOTU

Duruş denetimleri, uç noktalarda etkin güvenlik duvarlarını ve virüsten koruma araçlarını tarar. Kaynak: Posture Compliance.

4 **Günlük Toplayıcı** SYSLOG SUNUCUSU — Doğru cevap: A

ÖĞRETMEN NOTU

Syslog sunucuları, erişim ihlallerini izlemek için güvenlik olayı kayıtlarını toplar. Kaynak: Syslog Standard.

5 **Kart Taşması** AĞ GEÇİDİ DARBOĞAZI — Doğru cevap: A

ÖĞRETMEN NOTU

Ağ geçidinde bant genişliği darboğazı, kullanıcı trafiği sunucu sınırlarını aştığında oluşur. Kaynak: Capacity Planning.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Oturum Açma Belirteçleri** MFA KONTROLLERİ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Çok faktörlü kimlik doğrulama, oturum açmalar için ikinci bir doğrulama uygular. Kaynak: MFA Uygulaması.

7 **Soru 7** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Duruş (posture) denetimleri güvenlik duvarı veya antivirüsü kapalı cihazları engeller, bu yüzden bu tür cihazlara erişim reddedilir.

8 **Günlük Toplayıcı** SYSLOG SUNUCUSU — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Syslog sunucuları, erişim ihlallerini izlemek için güvenlik olayı kayıtlarını toplar. Kaynak: Syslog Standard.

9 **Soru 9** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

OpenVPN ve IPsec, uzak istemci trafiğini gerçekten şifreleyen güncel protokollerdir.

10 **Kart Taşması** AĞ GEÇİDİ DARBOĞAZI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Ağ geçidinde bant genişliği darboğazı, kullanıcı trafiği sunucu sınırlarını aştığında oluşur. Kaynak: Capacity Planning.

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

H 1. ÇOK FAKTÖRLÜ	D 2. OPENVPN	E 3. DURUŞ	B 4. SYSLOG
C 5. BANT GENİŞLİĞİ	G 6. ŞİFRELEME	A 7. TÜNELLEME	F 8. GÜVENLİK DUVARI

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 ÇOK FAKTÖRLÜ	2 OPENVPN	3 DURUŞ	4 SYSLOG
5 BANT GENİŞLİĞİ	6 TÜNELLEME		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 D – SYSLOG	2 H – GÜVENLİKDUVARI	3 G – TÜNELLEME	4 F – ŞİFRELEME
5 B – OPENVPN	6 E – BANTGENİŞLİĞİ	7 C – DURUŞ	8 A – ÇOKFAKTÖRLÜ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin ÇOK FAKTÖRLÜ, OPENVPN ve DURUŞ terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

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

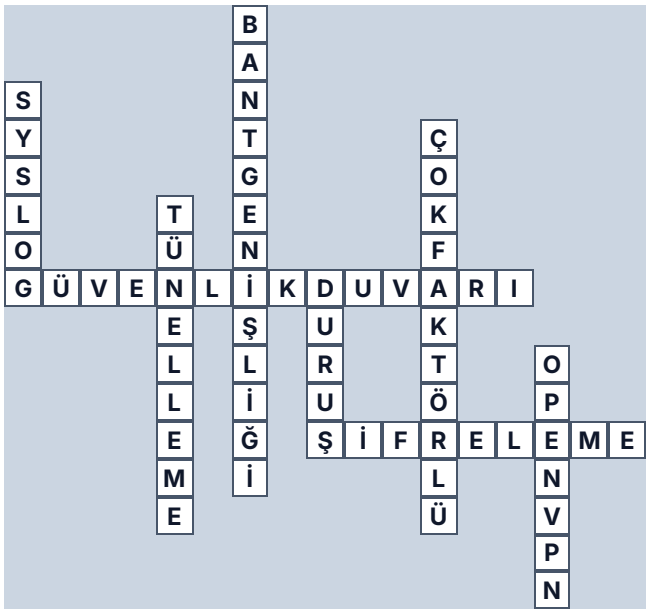
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

5 soldan sağa: GÜVENLİKDUVARI Trafik filtreleme sistemi kuralları (14 harf)

8 soldan sağa: ŞİFRELEME Paketlerin kriptografik olarak karıştırılması (9 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: BANTGENİŞLİĞİ Ağ veri kapasitesi sınırı (13 harf)

2 yukarıdan aşağı: SYSLOG Merkezi güvenlik günlüğü toplayıcısı (6 harf)

3 yukarıdan aşağı: ÇOKFAKTÖRLÜ Ek belirteç gerektiren oturum açma güvenliği (11 harf)

4 yukarıdan aşağı: TÜNELLEME Veriyi güvenli bir yola kapsülleme (9 harf)

6 yukarıdan aşağı: DURUŞ Uzak cihazın sağlık durumunu doğrulama (5 harf)

7 yukarıdan aşağı: OPENVPN Standart istemciden siteye protokolü (7 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. ATLOKÖÇRKÜF	ÇOKFAKTÖRLÜ	5. VNNEOPP	OPENVPN
2. DŞURU	DURUŞ	6. OLSSGY	SYSLOG
3. ABİLŞĞİNNGEİT	BANTGENİŞLİĞİ	7. LŞMEERİEF	ŞİFRELEME
4. LEMEELTÜN	TÜNELLEME	8. EKALDUÜIGİVRVN	GÜVENLİKDUVARI

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"UZAKTAN ERİŞİM VPN DAĞITIK KURUMSAL UÇLARI KORUR"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: MFA Zorunluluğu

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir iş analisti uzaktan çalışırken kurumsal veritabanına giriş yapmaya çalışır. Doğru kullanıcı adını ve parolayı girer, ancak VPN portalı erişimi engeller ve fiziksel bir belirteç kodu ister.
- Önerilen Strateji ve Çözüm: Kurumsal VPN portalı, uzak girişleri güvenceye almak için katı bir Çok Faktörlü Kimlik Doğrulama (MFA) politikası uygular.

B Vaka Çalışması 2: Duruş Uyumluluğu

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir yüklenici kişisel dizüstü bilgisayarını uzak kurumsal ağa bağlar. VPN istemcisi bağlantıyı hemen keser ve kullanıcıyı antivirüs tanımlarının güncel olmadığı konusunda bilgilendirir.
- Önerilen Strateji ve Çözüm: Uzaktan erişim ağ geçidi bir uç nokta durumu kontrolü yaptı ve güncel olmayan güvenlik yapılandırmaları nedeniyle cihazı engelledi.