Ad Soyad: _____ Tarih: _____ Puan: _____

Kurumsal VPN

Sıfır Güven ağ erişimi, özel ağ geçidi düğümleri ve merkezi kurumsal yönetici denetimleri uygulamak.

KURUMSAL VPN AĞLARI 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 kurumsal VPN ağları konusunda rehberlik eder. Sıfır Güven mimarilerini, özel statik IP ağ geçitlerini, yönetici konsollarını, hesap hazırlamayı ve siteden siteye IPsec tünellerini 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/kurumsal/

Kurumsal VPN Ağı Öğrenme Yol Haritan

- Sıfır Güven Ağ Erişimi (ZTNA) çerçeveleri uygula.
- İzin listesi filtreleri için ayrılmış sunucu ağ geçidi IP adreslerini yapılandır.
- Merkezi kurumsal yönetim panellerini ve kullanıcı lisans listelerini yönet.
- Ağ erişim kayıtlarını ve kullanıcı bağlantı geçmişlerini denetle.
- Çoklu oturum açma (SSO) ve çok faktörlü kimlik doğrulama kurallarını yapılandır.
- Şubeden şubeye siteden siteye IPsec tünelleri kur.

KURUMSAL VPN AĞLARI 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: Sıfır Güven ve siteden siteye IPsec. Hızlı Düşün bonus etkinliğiyle bitir.

SIFIR GÜVEN MİMARİLERİ VE ÖZEL AĞ GEÇİTLERİ (GİRİŞ)

Kurumsal VPN'ler, Sıfır Güven Ağ Erişimi (ZTNA) çerçevelerine geçerek ve özel statik IP ağ geçitlerini beyaz listeye alarak kurumsal varlıkları korur. BT yöneticileri, siteler arası IPsec tünellerini ve çoklu oturum açma (SSO) bağlantılarını düzenlemek için merkezi yönetim konsolları kullanır.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1 **1. Eski kurumsal VPN'lerin yerini hangi güvenlik modeli alıyor?**

- A) Zero Trust
- B) Multi-hop
- C) Eşler arası (peer-to-peer)
- D) Tek ağ geçidi

2 **2. Veri tabanı erişimini şirket sunucularıyla sınırlamak için hangi özellik gereklidir?**

- A) Özel IP
- B) Dinamik yönlendirme
- C) Bölünmüş tünel
- D) DNS proxy

3 **3. Kurumsal siteden siteye tüneller için standart olan protokol hangisidir?**

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4 **4. Yöneticilerin çalışan lisanslarını yönetmesini sağlayan merkezi araç hangisidir?**

- A) Yönetici konsolu
- B) Kayıt defteri anahtarı
- C) Yönlendirici donanım yazılımı
- D) Sistem günlüğü

5 **5. Okta veya Microsoft Entra ID üzerinden oturum açmaya hangi kimlik doğrulama standardı olanak tanır?**

- A) Tek Oturum Açma (SSO)
- B) Paylaşılan sır
- C) EPP kimlik doğrulaması
- D) WEP anahtarı

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Sıfır Güvenli Ağ Erişimi, ağa girişi ancak cihaz güveni sürekli doğrulandıktan sonra verir.

Doğru Yanlış

7 Soru 7

7. Özel IP geçitleri, çalışan trafiğini rastgele herkese açık tüketici kullanıcılarıyla birlikte yönlendirir.

Doğru Yanlış

8 Soru 8

8. Merkezi yönetici konsolları, BT yöneticilerinin tek tek çalışan lisanslarını anında iptal etmesine olanak tanır.

Doğru Yanlış

9 Soru 9

9. IPsec, siteden siteye ağ tünellerini desteklemeyen hafif bir protokoldür.

Doğru Yanlış

10 Soru 10

10. Single Sign-On, kurumsal kimlik sağlayıcıları kullanarak güvenli çalışan kimlik doğrulaması sağlar.

Doğru Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Modern güvenlik mimarileri eski tünelleri _____ erişimiyle değiştirir.
2. Veritabanı erişimini kısıtlamak için şirketler bir _____ ağ geçidi adresi yapılandırır.
3. Şube ofisler siteden siteye _____ tünelleriyle güvenli biçimde bağlanır.
4. BT yöneticileri çalışan kullanıcı lisanslarını merkezi _____ içinde tahsis eder.
5. Okta entegrasyonu, çalışanların kurumsal _____ ile kimlik doğrulaması yapmasını sağlar.
6. Girişleri korumak için kurumsal portallar _____ kimlik doğrulamayı zorunlu kılar.

KELİME BANKASI

AĞ GEÇİDİ ÇOK FAKTÖRLÜ IPSEC ÖZEL IP SIFIR GÜVEN TAHSİS TEK OTURUM AÇMA YÖNETİM PANELİ

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Temel kavram eşleştirme

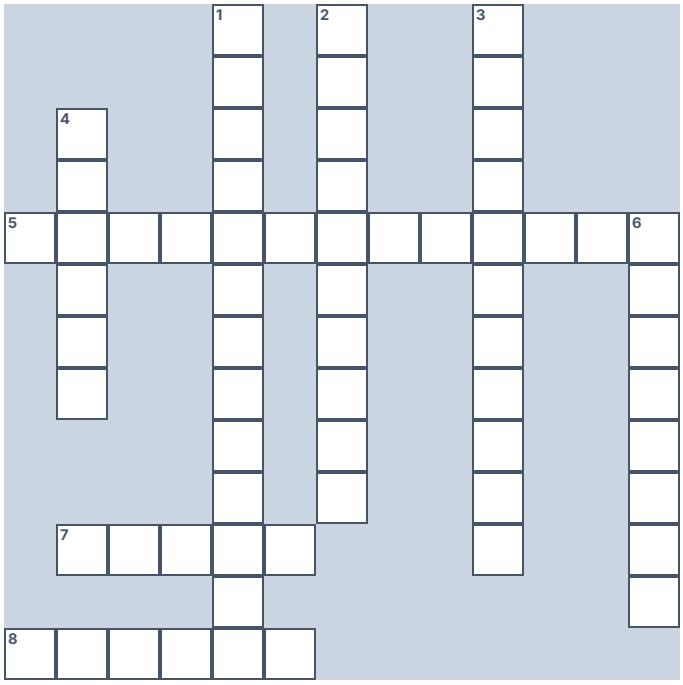
TANIM EŞLEŞTİRME

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

1. SIFIR GÜVEN	A	Çalışan VPN erişim lisanslarını tahsis etmek.
2. ÖZEL IP	B	Okta ve Entra ID kimlik bağlantısı.
3. IPSEC	C	Ek belirteç gerektiren oturum açma güvenliği.
4. YÖNETİCİ KONSOLU	D	Statik beyaz liste ağ geçidi adresi.
5. TEK OTURUM AÇMA	E	Siteden siteye tünel standardı.
6. ÇOK FAKTÖRLÜ	F	Ağ giriş yönlendirme düğümü.
7. AĞ GEÇİDİ	G	Merkezi BT yöneticisi lisans portalı.
8. TAHSİS ETME	H	Sürekli güven doğrulama çerçevesi.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

5. Okta ve Entra ID kimlik bağlantısı (13)

7. Siteden siteye tünel standardı (5)

8. Çalışanlara VPN erişim lisansı ayırma (6)

YUKARIDAN AŞAĞI

1. Merkezi BT yöneticisi portalı (13)

2. Sürekli güven doğrulama çerçevesi (10)

3. Ek belirteç gerektiren oturum açma güvenliği (11)

4. Sabit beyaz liste ağ geçidi adresi (6)

6. Ağ girişi yönlendirme düğümü (8)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

5 soldan sağa: Okta ve Entra ID kimlik bağlantısı (13 harf):

7 soldan sağa: Siteden siteye tünel standardı (5 harf):

8 soldan sağa: Çalışanlara VPN erişim lisansı ayırma (6 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Merkezi BT yöneticisi portalı (13 harf):

2 yukarıdan aşağı: Sürekli güven doğrulama çerçevesi (10 harf):

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

4 yukarıdan aşağı: Sabit beyaz liste ağ geçidi adresi (6 harf):

6 yukarıdan aşağı: Ağ girişi yönlendirme düğümü (8 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

SIFIRGÜVEN ÖZELIP IPSEC YÖNETİMPANELİ TEKOTURUMAÇMA
ÇOKFAKTÖRLÜ AĞGEÇİDİ TAHSİS

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. ÖZELIP
C. IPSEC
D. YÖNETİMPANELİ
E. TEKOTURUMAÇMA
F. ÇOKFAKTÖRLÜ
G. AĞGEÇİDİ
H. TAHSİS

TANIMLAR VE EŞLEŞTİRME ALANLARI
_____ 1. Sabit beyaz liste ağ geçidi adresi.
_____ 2. Ağ girişi yönlendirme düğümü.
_____ 3. Çalışanlara VPN erişim lisansı ayırma.
_____ 4. Ek belirteç gerektiren oturum açma güvenliği.
_____ 5. Siteden siteye tünel standardı.
_____ 6. Sürekli güven doğrulama çerçevesi.
_____ 7. Okta ve Entra ID kimlik bağlantısı.
_____ 8. Merkezi BT yöneticisi portalı.

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. EÜGRISVNIF
2. ICESP
3. ETUAMMAKRTUÇO
4. EDİİÇAĞG
5. LEPÖIZ
6. TNMİENLAYÖPİE
7. ÖAÇOTÜRLKKF
8. HSTİSA

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

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

Kontrol Noktası 8: VPN ve ağ vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: SIFIR GÜVEN GEÇİŞİ



Senaryo: Bir kuruluş, ağın içindeki hiç kimseye güvenmek yerine cihaz uyumluluk sertifikalarını, güvenlik duvarı durumunu ve kullanıcı konumunu sürekli doğrulayarak yerel sunucularını güvence altına almak istiyor.

Tartışma sorusu: BT güvenlik direktörü bunu başarmak için hangi çerçeveyi uygulamalıdır?

VAKA ÇALIŞMASI 2: AĞ GEÇİDİ KISITLAMASI



Senaryo: Bir şirket gizli finansal veritabanlarını bulutta barındırıyor. Yönetim panellerine tüm herkese açık internet erişimini engellemek ve oturum açmaya yalnızca doğrulanmış şirket uç noktalarından izin vermek istiyor.

Tartışma sorusu: Veritabanı yöneticisi bulut güvenlik duvarında hangi ağ yapılandırmasını kurmalıdır?

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 11 7 11 21 8 26 27 6 17 1 9 1

2 1 9 15 1 17 1 17 10 6 21 3 12 10 1 29 11

5 18 9 21 25 15 1 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: Kurumsal VPN nedir?

Uzaktan çalışanların merkezi yönetimle kurumsal ağlara erişmesine olanak tanıyan, işletmeler için tasarlanmış güvenli ağ tüneli.

Q2: Sıfır Güven geleneksel VPN'lerden nasıl farklıdır?

Geleneksel VPN'ler tünelin içindeki herkese güvenirken Zero Trust her cihaz ve kullanıcı bağlantısını sürekli doğrular.

Q3: İş amaçlı VPN'lerde Özel IP nedir?

Yalnızca işletmenize ayrılmış, güvenli bulut veritabanı erişimi için beyaz listeye almanızı sağlayan statik IP adresi.

Q4: SSO iş amaçlı VPN'ler için neden önemlidir?

Single Sign-On, çalışanların güvenli giriş yapmak için kurumsal kimlik bilgilerini (Okta veya Microsoft Entra ID gibi) kullanmasına olanak tanır.

Q5: Siteden siteye VPN nedir?

İki fiziksel ofisi (şube ofisi ve genel merkez gibi) IPsec kullanarak genel internet üzerinden birbirine bağlayan tünel.

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: Yönetici konsolunun işlevi nedir?

BT yöneticilerinin çalışan lisanslarını eklemesi veya kaldırması, ağ geçitleri ataması ve etkin bağlantıları izlemesi için bir pano.

Q7: MFA iş amaçlı VPN'leri nasıl güvenli hâle getirir?

Ele geçirilmiş parolalarla yetkisiz girişi önlemek için ikincil bir kod (kimlik doğrulayıcı uygulama belirteci gibi) isteyerek.

Q8: Çalışanların bağlantı geçmişini denetleyebilir miyim?

Evet, kurumsal VPN'ler uyumluluk denetimi için bağlantı zaman damgalarını, süreyi ve atanan IP'leri kaydeder.

Q9: ZTNA nedir?

Sıfır Güvenli Ağ Erişimi; tüm ağa değil yalnızca belirli uygulamalara erişim veren bir güvenlik modelidir.

Q10: Ağ geçidi düğümlerinin rolü nedir?

Uzak trafik için güvenli giriş noktaları olarak görev yapar ve verileri doğrudan özel kurumsal sunuculara yönlendirirler.

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: IPsec, siteden siteye kurumsal iletişimi nasıl korur?

IPsec, veri gizliliğini ve bütünlüğünü sağlamak için Encapsulating Security Payload (ESP) kullanarak trafiği ağ katmanında şifreler.

Q2: Eski çevre tabanlı güvenlik, uzaktan çalışan ekipler için neden yetersiz kalıyor?

Çünkü çalışanlar verilere birden çok konumdan ve cihazdan eriştiğinden, tek bir ağ güvenlik duvarı çevresi geçerliliğini yitirir.

Q3: BT yöneticileri otomatik sağlamayı nasıl uygular?

Kullanıcı dizinlerini eşitlemek için kimlik sağlayıcıları (Okta) ile VPN yönetici konsolu arasında SCIM protokollerini eşleyerek.

Q4: Kurumsal ortamlarda bölünmüş tünelin faydası nedir?

Yerel SaaS trafiğini (Microsoft 365 gibi) VPN tünelinin dışına yönlendirir ve kurumsal ağ geçidi bant genişliğini özel veri tabanları için korur.

Q5: Cihaz duruş kontrolleri uç nokta güvenliğini nasıl doğrular?

VPN istemcisi, bağlanmadan önce güvenlik duvarının etkin, virüsten korumanın çalışır durumda ve işletim sistemi yamalarının güncel olduğunu doğrulamak için cihazı tarar.

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: İş amaçlı VPN kurulumlarında NAT geçişinin rolü nedir?

NAT-T, IPsec paketlerini UDP içine kapsülleyerek ev yönlendiricilerinden ve güvenlik duvarlarından bağlantı kopmadan geçmelerini sağlar.

Q7: İşletmeler ağ geçidi bant genişliği tıkanmasını nasıl önler?

Birden çok bölgesel ağ geçidi düğümü dağıtarak ve gelen kullanıcı trafiğini yük dengeleyicilerle bunlar arasında dengeleyerek.

Q8: Statik IP beyaz listeleri neden dinamik olanlara tercih edilir?

Statik beyaz listeler, yetkisiz harici IP'lerin bağlantı el sıkışması denemesini önler ve saldırı yüzeyini önemli ölçüde azaltır.

Q9: Kurumsal VPN'lerde sertifika tabanlı kimlik doğrulamanın rolü nedir?

Şirket tarafından yönetilen cihazlara kurulu benzersiz dijital sertifikaları doğrular ve yönetilmeyen kişisel bilgisayarları engeller.

Q10: ZTNA yanal hareket riskini nasıl azaltır?

Kullanıcı oturumlarını belirli yetkili kaynaklara izole ederek, bir düğüm ele geçirilirse bilgisayar korsanlarının ağda ilerlemesini önleyerek.

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

Sıfır Güven mimarileri, ağ bağlantısı kurmaya çalışan her cihazın güvenlik durumunu sürekli doğrular.

2. VPN İPUCU

Özel IP geçitleri, işletmelerin statik adresleri beyaz listeye alarak bulut veri tabanlarını kilitlemesine olanak tanır.

3. VPN İPUCU

IPsec, güvenli siteden siteye ofis ağ tünelleri yapılandırmak için sektör standardı protokoldür.

4. VPN İPUCU

Yönetici konsolları, BT departmanlarının çalışan VPN erişim lisanslarını sağlamasına, yönetmesine ve denetlemesine olanak tanır.

5. VPN İPUCU

Single Sign-On, VPN erişimini Okta ve Entra ID gibi kurumsal kimlik sağlayıcılarla bütünleştirir.

6. VPN İPUCU

Çok faktörlü kimlik doğrulama, çalınmış parola anahtarlarından kaynaklanan yetkisiz bağlantı girişimlerini engeller.

7. VPN İÇGÖRÜSÜ

Bölünmüş tünelleme, genel SaaS trafiğini şifreli tünelin dışında tutarak kurumsal bant genişliğini optimize eder.

8. VPN İÇGÖRÜSÜ

Cihaz durumu denetimleri, kurumsal sunuculara erişim vermeden önce yerel güvenlik ayarlarını doğrular.

9. VPN İÇGÖRÜSÜ

SCIM dizin senkronizasyonu, çalışanların işe giriş ve çıkışındaki erişim denetimlerini otomatikleştirir.

10. VPN İPUCU

Sıfır Güvenli Ağ Erişimi, kullanıcı erişimini yetkili belirli uygulamalarla sınırlar ve ağ içinde yanal harekete engel olur.

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/

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Sıfır Güven** ZTNA MODELİ **Doğru cevap: A**

ÖĞRETMEN NOTU

Sıfır Güven modelleri, ağa girişten önce cihaz uyumluluğunu sürekli doğrular. Kaynak: NIST Zero Trust.

2 **Özel IP** STATİK IP **Doğru cevap: A**

ÖĞRETMEN NOTU

Özel IP adresleri, herkese açık trafiği engellemek için geçitlerin beyaz listeye alınmasına olanak tanır. Kaynak: Dedicated IP Guide.

3 **IPsec standardı** IPSEC TÜNELİ **Doğru cevap: A**

ÖĞRETMEN NOTU

IPsec, şube siteden siteye tünelleri için kullanılan standart protokoldür. Kaynak: IPsec Tunneling.

4 **BT tahsisi** YÖNETİCİ KONSOLU **Doğru cevap: A**

ÖĞRETMEN NOTU

Merkezi yönetici panoları, BT yöneticilerinin kullanıcı lisanslarını tahsis etmesine olanak tanır. Kaynak: CISA Yönergeleri.

5 **Soru 5** **Doğru cevap: A**

ÖĞRETMEN NOTU

Okta veya Microsoft Entra ID üzerinden oturum açmaya hangi kimlik doğrulama standardı olanak tanır? → Tek Oturum Açma (SSO)

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Sıfır Güven** ZTNA KONTROLLERİ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Sıfır Güven modelleri, ağa girişten önce cihaz uyumluluğunu sürekli doğrular. Kaynak: NIST Zero Trust.

7 **Soru 7** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Dedicated IP'ler tek bir işletmeye ayrılmıştır, bu yüzden trafiği diğer kullanıcılarla karışmaz.

8 **BT tahsisi** BT YÖNETİCİ LİSANSI — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Merkezi yönetici panoları, BT yöneticilerinin kullanıcı lisanslarını tahsis etmesine olanak tanır. Kaynak: CISA Yönergeleri.

9 **IPsec standardı** SİTEDEN SİTEYE — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

IPsec, şube siteden siteye tünelleri için kullanılan standart protokoldür. Kaynak: IPsec Tunneling.

10 **Okta SSO bağlantısı** SSO GİRİŞİ — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Single Sign-On, VPN girişlerini Okta gibi kurumsal dizinlerle bütünleştirir. Kaynak: Okta SSO.

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. SIFIR GÜVEN	D 2. ÖZEL IP	E 3. IPSEC	G 4. YÖNETİCİ KONSOLU
B 5. TEK OTURUM AÇMA	C 6. ÇOK FAKTÖRLÜ	F 7. AĞ GEÇİDİ	A 8. TAHSİS ETME

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 SIFIR GÜVEN	2 ÖZEL IP	3 IPSEC	4 YÖNETİM PANELİ
5 TEK OTURUM AÇMA	6 ÇOK FAKTÖRLÜ		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 B – ÖZELIP	2 G – AĞGEÇİDİ	3 H – TAHSİS	4 F – ÇOKFAKTÖRLÜ
5 C – IPSEC	6 A – SIFIRGÜVEN	7 E – TEKOTURUMAÇMA	8 D – YÖNETİMPANELİ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin SIFIR GÜVEN, ÖZEL IP ve IPSEC 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

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

BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

5 soldan sağa: TEKOTURUMAÇMA Okta ve Entra ID kimlik bağlantısı (13 harf)

7 soldan sağa: IPSEC Siteden siteye tünel standardı (5 harf)

8 soldan sağa: TAHSİS Çalışanlara VPN erişim lisansı ayırma (6 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: YÖNETİMPANELİ Merkezi BT yöneticisi portalı (13 harf)

2 yukarıdan aşağı: SIFIRGÜVEN Sürekli güven doğrulama çerçevesi (10 harf)

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

4 yukarıdan aşağı: ÖZELIP Sabit beyaz liste ağ geçidi adresi (6 harf)

6 yukarıdan aşağı: AĞGEÇİDİ Ağ girişi yönlendirme düğümü (8 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	E Ü G R I S V N I F	SIFIRGÜVEN	5.	L E P Ö I Z	ÖZELIP
2.	I C E S P	IPSEC	6.	T N M İ E N L A Y Ö P İ E	YÖNETİMPANELİ
3.	E T U A M M A K R T U Ç O	TEKOTURUMAÇMA	7.	Ö A Ç O T Ü R L K K F	ÇOKFAKTÖRLÜ
4.	E D İ İ Ç A Ğ G	AĞGEÇİDİ	8.	H S T İ S A	TAHSİS

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SIFIR GÜVEN AĞA BAĞLANAN HER CİHAZI DOĞRULAR"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Sıfır Güven Geçişi

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kuruluş, ağın içindeki hiç kimseye güvenmek yerine yerel sunucularını cihaz uyumluluk sertifikalarını, güvenlik duvarı durumunu ve kullanıcı konumunu sürekli doğrulayarak korumak istiyor.
- Önerilen Strateji ve Çözüm: Müdür, sürekli bağlama dayalı güvenlik kontrolleri uygulayan Sıfır Güven Ağ Erişimi (ZTNA) modeline geçmelidir.

B Vaka Çalışması 2: Ağ Geçidi Kısıtlaması

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir şirket özel finansal veritabanlarını bulutta barındırır. Yönetim panellerine tüm genel internet erişimini engellemek ve girişlere yalnızca doğrulanmış şirket uç noktalarından izin vermek istiyor.
- Önerilen Strateji ve Çözüm: Yönetici, kurumsal VPN'de bir Dedicated IP ağ geçidi yapılandırmalı ve bu statik adresi bulut veritabanı güvenlik duvarında beyaz listeye almalıdır.