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

KONTROL NOKTASI 10

VPN hakkında sık sorulan sorular

Etkileşimli çalışma kâğıdı ve çalışma rehberi

Kaynak: VPN.com VPN rehberini aç: **https://www.vpn.com/tr/vpn/**

VPN nedir çalışma kâğıdı

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

Olası müşterilerin sanal özel ağları kullanmakla ilgili en sık sorduğu soruları ve cevapları incele.

Q1: VPN nedir ve nasıl çalışır?

Sanal Özel Ağ (VPN) internet bağlantınızı şifreler ve trafiğinizi güvenli bir uzak sunucu üzerinden yönlendirir. Bu, genel IP adresinizi maskeler ve yerel ağ gözlemcilerinin ile İSS'nizin VPN tüneli üzerinden yönlendirilen trafik hakkında görebileceklerini sınırlar.

Q2: Neden VPN kullanmalıyım?

VPN, dijital gizliliğinizi korur, kafeler veya havalimanları gibi herkese açık Wi-Fi ağlarında bağlantınızı güvenceye alır, İSS şifreli trafiğin türünü tanımlayamadığında etkinliğe dayalı kısıtlamayı azaltabilir, küresel içeriğe erişmek için coğrafi kısıtlamaları aşar ve uzaktan çalışma kaynaklarının güvenliğini sağlamaya yardımcı olur.

Q3: VPN beni çevrimiçi tamamen anonim yapar mı?

Hayır. Bir VPN IP adresini gizleyip trafiği şifrelese de tarayıcı çerezleri, açık hesaplar (Google veya Facebook gibi), tarayıcı parmak izi veya VPN sağlayıcının verilerini kaydetmesi yoluyla yine izlenebilirsin.

Q4: VPN internet hızımı yavaşlatır mı?

Evet, hafifçe. Şifreleme süreci ve VPN sunucusuna olan fiziksel mesafe gecikme ve ek yük getirir. Etki; sağlayıcıya, protokole, sunucu mesafesine, cihaza ve ağ koşullarına göre değişir.

Q5: VPN kullanmak yasal mı?

VPN kullanımı birçok ülkede yasaldır, ancak bazı yargı bölgeleri VPN hizmetlerini kısıtlar, düzenler veya engeller. Kullanıcılar kullanmadan önce güncel yerel yasaları doğrulamalıdır. Daha fazla bilgi için VPN.com'daki yasallık kılavuzlarına bak.

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

Olası müşterilerin sanal özel ağları kullanmakla ilgili en sık sorduğu soruları ve cevapları incele.

Q6: Ücretsiz bir VPN kullanabilir miyim?

Ücretsiz VPN'ler reklamlara, sınırlı özelliklere, kullanım analizlerine, veri sınırlarına veya başka gelir modellerine dayanabilir. Kullanıcılar kullanmadan önce sağlayıcının gizlilik politikasını, sahipliğini, denetimlerini ve iş modelini incelemelidir.

Q7: "Kayıt tutmama" politikası nedir?

Kayıt tutmama politikası, bir sağlayıcının hangi etkinlik ve bağlantı verilerini saklamadığını söylediğini açıklar. Kapsam değişiklik gösterir; bu yüzden okuyucular politikayı ve bağımsız denetim bulgularını incelemelidir.

Q8: En iyi VPN'i nasıl seçerim?

Denetlenmiş kayıt tutmama politikalarına, güçlü protokollere (WireGuard, OpenVPN), güvenli sunucu konumlarına, yüksek hızlara, yalnızca RAM kullanan sunuculara, kill switch özelliğine ve istihbarat paylaşım ittifaklarının (5/9/14 Eyes gibi) dışında bir hukuki yargı bölgesine bak.

Q9: Telefonumda ve akıllı TV'mde VPN kullanabilir miyim?

Evet. Modern VPN sağlayıcıları iOS, Android, macOS, Windows, Linux ve akıllı TV'ler için özel uygulamaların yanı sıra ev ağındaki tüm cihazları korumak için yönlendirici kurulumları sunar.

Q10: Kill Switch nedir?

Kill Switch, VPN bağlantısı koptuğunda cihazınızın internet bağlantısını otomatik olarak kesen bir güvenlik özelliğidir. Bu, şifrelenmemiş verilerinizin veya gerçek IP adresinizin sızmasını önler.

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

Sanal özel ağların ve güvenli tünelleme protokollerinin teknik ve yapısal yönlerini keşfet.

Q1: WireGuard, OpenVPN ve IKEv2 arasındaki fark nedir?

WireGuard, hızlı hızlar ve kısa bağlantı süreleri sunan modern, hafif bir protokoldür (yalnızca yaklaşık 4.000 satır kod). OpenVPN, son derece güvenli ve sınanmış açık kaynaklı bir protokoldür. IKEv2, ağlar arasında geçiş yaparken hızla yeniden bağlanabildiği için mobil cihazlar için mükemmeldir. [4]

Q2: Çift VPN veya Multi-Hop yönlendirme nedir?

Çoklu atlama, trafiğini art arda iki veya daha fazla VPN sunucusu üzerinden yönlendirir. Bu, ikinci bir şifreleme katmanı ekler ve bir sunucunun ele geçirilmesi durumunda gerçek IP adresinin ikinci atlamadan gizli kalmasına yardımcı olur.

Q3: WebRTC sızıntısı nedir ve VPN bunu nasıl önler?

WebRTC, VPN etkinken bile gerçek yerel ve genel IP adreslerini ortaya çıkarabilen bir tarayıcı protokolüdür. Premium VPN'ler masaüstü/mobil uygulamalarında ve tarayıcı uzantılarında WebRTC isteklerini engeller veya taklit eder.

Q4: Yalnızca RAM kullanan sunucular nedir ve neden önemlidir?

Geleneksel sunucular verileri ele geçirilebilen veya tehlikeye atılabilen sabit disklere yazar. Yalnızca RAM kullanan (disksiz) sunucular tamamen geçici bellekte (RAM) çalışır. Sunucu yeniden başlatıldığında veya kapatıldığında bellekteki veriler silinir.

Q5: Gizleme (obfuscation) VPN engellerini nasıl aşar?

Gizleme (veya "Stealth VPN"), VPN trafiğini sıradan HTTPS trafiği (443 numaralı port) gibi gösterir. Bu, hükümetlerin veya okul/ofis ağlarının VPN'leri engellemek için kullandığı Derin Paket İncelemesini (DPI) aşmasına yardımcı olabilir.

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

Sanal özel ağların ve güvenli tünelleme protokollerinin teknik ve yapısal yönlerini keşfet.

Q6: Bölünmüş Tünel (Split Tunneling) nedir ve ne zaman kullanmalıyım?

Bölünmüş tünelleme, hangi uygulamaların şifreli VPN tüneli üzerinden yönlendirileceğini ve hangilerinin doğrudan internete bağlanacağını seçmeni sağlar. Hassas bankacılık uygulamalarını VPN üzerinden yönlendirip yerel oyunları doğrudan bağlayarak VPN'in eklediği gecikmeyi önlemek için kullan.

Q7: İleri Gizlilik (Mükemmel İleri Gizlilik) nasıl çalışır?

PFS, her oturum için benzersiz ve geçici bir şifreleme anahtarının üretilmesini sağlar. Özel anahtar gelecekte ele geçirilse bile, bağımsız anahtarlar kullanıldığı için geçmiş veya gelecek oturumların şifresini çözmekte kullanılamaz.

Q8: 5/9/14 Eyes ittifakları nedir ve neden önemsemeliyim?

Yargı yetkisi, bir sağlayıcının karşılaşabileceği yasal süreci etkileyebilir; ancak pratik gizlilik riski ayrıca sağlayıcının hangi verileri sakladığına, teknik mimarisine, sahipliğine, şeffaflık raporlamasına ve denetim geçmişine bağlıdır.

Q9: DNS Sızıntı Koruması nedir?

DNS sızıntı koruması, cihazının web sitesi arama sorgularını (DNS sorguları) İSS'nin sunucuları yerine VPN'in özel, şifreli DNS sunucuları üzerinden göndermesini sağlar. Bu, İSS'nin hangi siteleri ziyaret ettiğini izlemesini engeller.

Q10: Bir VPN, İSS'in internet hız kısıtlamasını aşabilir mi?

Bazen. Bir İSS belirli etkinliklerin hızını seçici olarak düşürdüğünde VPN yardımcı olabilir, ancak tıkanıklığı, veri kotalarını, hesap düzeyindeki hız sınırlarını veya zayıf ağ kalitesini aşamaz.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/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] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637