# VPN

VPN, "Sanal Özel Ağ" anlamına gelir ve genel ağlar kullanılırken korumalı bir şebeke bağlantısı oluşturmaya olanak verir. VPN programları internet trafiğinizi şifreler ve çevrimiçi kimliğinizi gizler. Böylece üçüncü kişilerin çevrimiçi hareketlerinizi takip etmesi ve veri çalması zorlaşır. Şifreleme gerçek zamanlı olarak gerçekleşir.

# VPN nasıl çalışır?

VPN, IP adresinizi VPN ana bilgisayarı tarafından yönetilen özel olarak yapılandırılmış bir uzak sunucu üzerinden yeniden yönlendirerek maskeler. Yani siz internette VPN ile gezinirken VPN sunucusu verilerinizin kaynağı olur. Bu, İnternet Servis Sağlayıcınızın (ISP) ve üçüncü kişilerin ziyaret ettiğiniz web sitelerini veya gönderdiğiniz ve aldığınız verileri göremediği anlamına gelir. VPN, bütün verilerinizi "anlaşılamaz" hâle getiren bir filtreymiş gibi çalışır. Herhangi biri bu verileri ele geçirse bile kullanamaz.

# VPN bağlantısının faydaları nelerdir?

VPN bağlantısı, çevrimiçi veri trafiğinizi gizler ve dışarıdan erişilmelerine engel olur. Şifrelenmeyen veriler, ağa erişimi olan ve görmek isteyen herkes tarafından görüntülenebilir. VPN sayesinde bilgisayar korsanları ve siber suçlular bu verilerin şifresini çözüp verileri kullanamaz.

Güvenli şifreleme: Verileri okuyabilmek için şifreleme anahtarına ihtiyacınız olur. Şifreleme anahtarı olmazsa ve bir kaba kuvvet saldırısı gerçekleşirse bilgisayarın kodu çözümlemesi için milyonlarca yıl gerekir. VPN sayesinde çevrimiçi hareketleriniz ortak ağlarda bile gizlenir.

Konumunuzu gizleme: VPN sunucuları aslında internette sizin vekilleriniz gibi davranır. Demografik konum verileriniz başka bir ülkedeki sunucudan geldiği için gerçek konumunuz tespit edilemez. Ayrıca çoğu VPN hizmeti, yaptıklarınızın kayıtlarını depolamaz. Bazı sağlayıcılar ise yaptıklarınızı kaydeder ancak bu bilgileri üçüncü kişilere aktarmaz. Yani kullanıcı davranışlarınızın muhtemel kayıtları kesin olarak gizli kalır.

Bölgesel içeriğe ulaşma: Bölgesel internet içeriklerine her yerden ulaşmak her zaman için mümkün olmayabilir. Servislerde ve web sitelerinde çoğunlukla dünyanın sadece belli bölgelerinden ulaşılabilen içerikler bulunur. Standart bağlantılar, konumunuzu belirlemek için ülkedeki yerel sunucuları kullanır. Bu da seyahat ettiğiniz sırada kendi ülkenizdeki içeriklere, kendi ülkenizdeyken de uluslararası içeriklere ulaşamayacağınız anlamına gelir. VPN konum yanıltması ile başka bir ülkedeki bir sunucuya geçip konumuzu etkili bir şekilde "değiştirebilirsiniz".

Güvenli veri aktarımı: Eğer uzaktan çalışıyorsanız şirketinizin ağındaki önemli bilgilere erişmeniz gerekebilir. Güvenlik sebebiyle bu tip bilgiler için güvenli bağlantı gerekir. Ağa katılmak için genellikle VPN bağlantısı şart koşulur. VPN hizmetleri, özel sunuculara bağlanır ve herhangi bir veri sızıntısı riskini ortadan kaldırmak için şifreleme yöntemleri kullanır.

Neden VPN bağlantısı kullanmalısınız?

İSS'niz genellikle bağlantınızı internete bağlandığınızda ayarlar. IP adresi üzerinden sizi takip eder. Ağ trafiğiniz İSS'nizin sunucuları üzerinden yönlendirilir ve böylece internette yaptığınız her şey kayıt altına alınıp görüntülenebilir.

İSS'niz güvenilir gibi görünebilir ama göz atma geçmişinizi reklam firmaları, polis, hükûmet ve/veya üçüncü kişilerle paylaşabilir. İSS'ler ayrıca siber suçluların saldırılarına maruz kalabilir: Servis sağlayıcınız ele geçirilirse kişisel ve özel verileriniz tehlikeye girebilir.

Düzenli olarak herkese açık Wi-Fi ağlarına bağlanıyorsanız bu ihtimali göz önünde bulundurmalısınız. İnternet trafiğinizi kimin izlediğini ve sizden ne çalabileceklerini bilmenize imkân yoktur; şifreleriniz, kişisel verileriniz, ödeme bilgileriniz veya kimliğinizin tamamı bile çalınabilir.

# İyi bir VPN'nin görevi nedir?

VPN'ninize bir veya birden çok işlem yapmak için güvenebilmeniz gerekir. VPN uygulaması da güvenlik açıklarına karşı korumalı olmalıdır. Kapsamlı bir VPN çözümünden beklenen özellikler şunlardır:

IP adresinizin şifrelenmesi: VPN'nin ana görevi IP adresinizi İSS'nizden ve diğer üçüncü kişilerden gizlemektir. Bu durum, siz ve VPN sağlayıcısı dışında kimsenin görme riski olmadan çevrimiçi bilgi göndermenizi ve almanızı sağlar.

Protokollerin şifrelenmesi: VPN'nin arkanızda internet geçmişiniz, arama geçmişiniz ve çerezler gibi izler bırakmanızı da engellemesi gerekir. Çerezlerin şifrelenmesi özellikle önemlidir çünkü üçüncü kişilerin kişisel verileriniz, finansal bilgileriniz ve internet sitelerindeki diğer içerikleriniz gibi gizli bilgilerinize erişimlerini engeller.

Kill Switch: VPN bağlantınız aniden kesintiye uğrarsa güvenli bağlantınız da kesintiye uğrar. İyi bir VPN, böyle ani kesintileri tespit edebilir ve daha önceden seçilen programları sonlandırarak verilerin çalınma riskini azaltır.

İki faktörlü kimlik doğrulama: Güçlü bir VPN, çeşitli kimlik doğrulama yöntemlerini kullanarak oturum açmak isteyen herkesi kontrol eder. Örneğin, sizden şifre girmeniz istenebilir ve sonra da cep telefonunuza bir kod gönderilir. Bu işlem, istenmeyen üçüncü kişilerin güvenli bağlantınıza erişim sağlamasını zorlaştırır.

# VPN ile nasıl güvende kalınır?

VPN'ler internette gezinirken yaptıklarınızı şifreler ve bu şifre sadece bir anahtarla açılabilir. Bu anahtarı sadece bilgisayarınız ve VPN programınız bilir, böylece İSS'niz nerede gezindiğinizi izleyemez. Farklı VPN'ler farklı şifreleme süreçleri kullanır ama genellikle üç adımda işlev gösterirler:

1. İnternete bağlandığınızda VPN programınızı açın. VPN, internetle sizin aranızda güvenli bir tünel görevi görür. İSS'niz ve başka üçüncü kişiler bu tüneli tespit edemez.
2. Cihazınız artık VPN'nin yerel ağındadır ve IP adresiniz VPN sunucusunun vereceği başka bir IP adresiyle değiştirilebilir.
3. Artık internette istediğiniz gibi gezinebilirsiniz çünkü VPN, bütün kişisel verilerinizi korur.

# DEZAVANTAJLARI

## Performans ve Hız Kaybı:

Yavaşlama: VPN kullanımı internet hızını yavaşlatabilir. Çünkü verileriniz, VPN sunucusuna ve ardından hedef sunucuya gitmek zorundadır.

Ping Süreleri: Özellikle çevrimiçi oyunlarda, artan ping süreleri nedeniyle gecikmeler yaşanabilir.

## Güvenlik ve Gizlilik:

Güvenilirlik: Bazı VPN sağlayıcıları, kullanıcı verilerini kaydedebilir veya üçüncü taraflarla paylaşabilir. Güvenilir bir sağlayıcı seçmek önemlidir.

Şifreleme: Düşük kaliteli veya ücretsiz VPN'ler, zayıf şifreleme yöntemleri kullanabilir ve bu da verilerinizi risk altına sokar.

## Maliyet:

Ücretli Hizmetler: Güvenilir ve yüksek performanslı VPN hizmetleri genellikle ücretlidir. Ücretsiz VPN'ler genellikle sınırlı bant genişliği, hız ve güvenlik sunar.

## Kullanım Kısıtlamaları:

Engellemeler: Bazı web siteleri ve hizmetler, VPN kullanımını tespit ederek erişimi kısıtlayabilir veya tamamen engelleyebilir.

Yasal Kısıtlamalar: Bazı ülkelerde VPN kullanımı yasaklanmış veya sıkı bir şekilde düzenlenmiştir. Bu durumlarda VPN kullanmak yasal sorunlara yol açabilir.

## Teknik Sorunlar:

Bağlantı Sorunları: VPN bağlantıları bazen istikrarsız olabilir ve sık sık kesintiler yaşanabilir.

Kurulum ve Yapılandırma: VPN kurmak ve yapılandırmak, teknik bilgi gerektirebilir ve bazı kullanıcılar için zor olabilir.

## Güvenlik Riskleri:

VPN Sağlayıcılarının Hedef Olması: VPN sağlayıcıları, saldırganlar için çekici hedefler olabilir. VPN sunucuları hacklendiğinde, kullanıcı verileri tehlikeye girebilir.

Malware ve Phishing: Kötü niyetli VPN uygulamaları, kullanıcı cihazlarına malware bulaştırabilir veya phishing saldırıları düzenleyebilir.

## Kısıtlı Servis Erişimi:

Coğrafi Engeller: Bazı VPN'ler, belirli coğrafi bölgelerde hizmet vermeyebilir veya performansları düşük olabilir.

# IPSEC VPN NEDİR?

IPsec VPN, ağlar arasında veya cihazlar arasında güvenli veri iletimi sağlamak amacıyla IPsec protokollerini kullanan bir VPN türüdür. Bu tür VPN'ler, verilerin şifrelenmesini, kimlik doğrulamasını ve bütünlük kontrolünü sağlar.

## IPsec'in Temel Bileşenleri

AH (Authentication Header):

Verinin kaynağını doğrular ve verinin bütünlüğünü sağlar.

Verinin kendisini şifrelemez, sadece doğrulama ve bütünlük kontrolü yapar.

ESP (Encapsulating Security Payload):

Veriyi şifreler ve bütünlük kontrolü sağlar.

Hem veri gizliliği hem de bütünlük ve kimlik doğrulama sağlar.

IKE (Internet Key Exchange):

IPsec'in iki uç nokta arasında güvenlik ilişkisi kurmasını sağlar.

Anahtar değişimini ve güvenlik parametrelerinin müzakeresini gerçekleştirir.

## IPsec VPN Çalışma Şekli

Güvenlik İlişkisi (Security Association - SA) Kurulumu:

İki uç nokta arasında güvenlik politikaları ve anahtarlar üzerinde anlaşma sağlanır.

IKE protokolü kullanılarak güvenlik ilişkisi oluşturulur.

Veri Şifreleme ve Doğrulama:

Veri, ESP protokolü ile şifrelenir ve kimlik doğrulaması yapılır.

Alternatif olarak, sadece kimlik doğrulaması ve bütünlük sağlanması gerekiyorsa AH protokolü kullanılır.

Tünelleme veya Taşıma Modu:

Taşıma Modu: Verinin sadece yük kısmı şifrelenir. Daha çok uç cihazlar arasında kullanılır.

Tünel Modu: Verinin tamamı (başlık ve yük) şifrelenir. Genellikle ağlar arasında kullanılır.

## IPsec VPN'in Sağladığı Güvenlik Özellikleri

Gizlilik:

Veriler, şifreleme sayesinde sadece yetkili taraflarca okunabilir hale getirilir.

Kimlik Doğrulama:

Gönderenin kimliği doğrulanır, böylece verinin sahte bir kaynaktan gelmediği garanti edilir.

Veri Bütünlüğü:

Verinin iletim sırasında değiştirilip değiştirilmediği kontrol edilir.

Yeniden Oynatma Saldırılarına Karşı Koruma:

Verinin eski veya tekrarlanmış paketler kullanılarak yeniden oynatılması engellenir.

## IPsec VPN'in Kullanım Alanları

Kurumsal Ağlar:

Şirket içi ağlar arasında güvenli iletişim sağlamak için kullanılır.

Uzak Çalışanlar:

Çalışanların ofis dışından güvenli bir şekilde şirket ağına bağlanması için kullanılır.

Şube Bağlantıları:

Farklı coğrafi konumlardaki şubeler arasında güvenli bağlantı kurulmasını sağlar.

## Sonuç

IPsec VPN, güçlü şifreleme ve güvenlik özellikleri sayesinde internet üzerinden güvenli veri iletimi için ideal bir çözümdür. Özellikle kurumsal ağlarda ve uzak çalışan bağlantılarında yaygın olarak kullanılır. IPsec'in sunduğu gizlilik, kimlik doğrulama, veri bütünlüğü ve yeniden oynatma saldırılarına karşı koruma gibi güvenlik özellikleri, veri güvenliğini üst düzeye çıkarır.

# YAZILIMSAL VPN’ler

## 1. OpenVPN

* Açık Kaynak: OpenVPN, açık kaynaklı bir VPN protokolüdür ve geniş bir topluluk tarafından desteklenir.
* Platform Desteği: Windows, macOS, Linux, iOS ve Android gibi çeşitli platformlarda çalışır.
* Güvenlik: Güçlü şifreleme ve çeşitli güvenlik özellikleri sunar.
* Esneklik: Yüksek derecede yapılandırılabilir ve birçok farklı kullanım senaryosuna uyarlanabilir.

## 2. WireGuard

* Modern Tasarım: WireGuard, hızlı ve verimli çalışacak şekilde modern bir tasarıma sahiptir.
* Güvenlik: Basit ve ince bir kod tabanı ile güvenliği artırır.
* Performans: Düşük gecikme süresi ve yüksek performans sunar.
* Platform Desteği: Linux, Windows, macOS, iOS ve Android platformlarında çalışır.

## 3. SoftEther VPN

* Çok Protokollü Destek: SoftEther, OpenVPN, L2TP/IPsec, EtherIP, ve SSTP gibi birçok protokolü destekler.
* Platform Desteği: Windows, Linux, macOS, iOS ve Android'de çalışır.
* Performans: Yüksek hız ve düşük gecikme süresi sunar.
* Kullanım Kolaylığı: Kullanıcı dostu bir arayüze sahiptir ve kurulum süreci basittir.

## 4. Cisco AnyConnect

* Kurumsal Kullanım: Genellikle büyük şirketler ve kurumlar tarafından kullanılır.
* Güvenlik: Güçlü güvenlik özellikleri ve merkezi yönetim imkanı sunar.
* Platform Desteği: Windows, macOS, Linux, iOS ve Android platformlarında çalışır.
* Entegrasyon: Cisco ağ cihazlarıyla kolay entegrasyon sağlar.

## 5. OpenConnect

* Açık Kaynak: OpenConnect, Cisco AnyConnect VPN protokolüne uyumlu açık kaynaklı bir VPN istemcisidir.
* Platform Desteği: Windows, macOS, Linux ve BSD platformlarında çalışır.
* Güvenlik: Güçlü şifreleme ve kimlik doğrulama özellikleri sunar.

## 6. Shadowsocks

* Gizlilik: İnternet trafiğini gizlemek ve sansürleri aşmak için tasarlanmış bir şifreleme protokolüdür.
* Platform Desteği: Windows, macOS, Linux, iOS ve Android gibi çeşitli platformlarda çalışır.
* Hafif ve Hızlı: Düşük gecikme süresi ve yüksek hız sunar.

## 7. Tinc

* Mesh VPN: Tinc, birden fazla düğüm arasında mesh tarzı bir VPN oluşturur.
* Açık Kaynak: Açık kaynaklı ve esnek bir yapıdadır.
* Platform Desteği: Linux, Windows, macOS, FreeBSD ve Solaris gibi birçok platformda çalışır.
* Güvenlik: Güçlü şifreleme ve güvenlik özellikleri sunar.