# VPN (Virtual Private Network - Sanal Özel Ağ) Kavramı ve Türleri

## Giriş

Günümüzde internet her yerde ve her zaman kullanılabiliyor. Ancak açık Wi-Fi ağlarında veya genel ağlarda verilerinizin güvenliği risk altında olabilir. Ayrıca, bazı şirket içi kaynaklara (dosya sunucuları, veritabanları) dış dünyadan erişmek isteyebilirsiniz. İşte tam bu noktada VPN (Virtual Private Network - Sanal Özel Ağ) devreye girer. VPN, güvenli olmayan bir ağ (örneğin internet) üzerinden, güvenli ve şifrelenmiş bir bağlantı tüneli (tunnel) oluşturarak iki nokta arasında özel bir ağ bağlantısı kurmanızı sağlar.

## Neden Önemlidir?

VPN'in temel amacı güvenlik ve gizlilik tir. VPN kullanarak:

Verilerinizi Şifrelersiniz: Açık ağlarda verileriniz şifrelenerek gönderildiği için, kötü niyetli kişiler tarafından görülmesi ve ele geçirilmesi engellenir.  
Konum Gizliliği Sağlarsınız: Gerçek IP adresinizi gizleyerek sanal konumunuzu değiştirebilirsiniz. Bu, coğrafi kısıtlamaları aşmak veya anonim kalmak için kullanılabilir.  
Şirket Ağına Uzaktan Erişim: Evden veya seyahat ederken, şirketinizin özel iç ağına (intranet) güvenli bir şekilde erişebilirsiniz.  
Sansür ve Engelleme Aşımı: Bazı ülkelerde veya ağlarda engellenen internet sitelerine VPN ile erişmek mümkündür.

## 

## Temel Bilgiler

VPN Nedir? Güvenli olmayan bir ağ (örneğin internet) üzerinden, iki nokta arasında şifreli ve güvenli bir sanal tünel oluşturarak özel ağ bağlantısı kurulmasını sağlayan teknolojidir.  
Nasıl Çalışır?  
VPN istemcisi (Client), VPN sunucusuna bağlanmak ister.  
Aralarında kimlik doğrulama (Authentication) ve şifreleme anahtarlarının anlaşılması (örneğin RSA, Diffie-Hellman) gibi işlemler yapılır.  
Başarılı bağlantıdan sonra, kullanıcı ile VPN sunucusu arasında şifreli bir tünelleme (tunneling) protokolü (örneğin OpenVPN, IPSec, WireGuard) kullanılarak bağlantı kurulur.  
Artık kullanıcının tüm internet trafiği bu tünel içinden geçer.  
Tünelin diğer ucundaki VPN sunucusu, trafiği kendi IP'siyle internete yönlendirir.  
Dış dünyada görünen IP adresi, kullanıcınınki değil, VPN sunucusununki olur.  
Şifreleme (Encryption): Verilerin okunamaz hale getirilmesi işlemidir. Yaygın algoritmalar: AES, 3DES, SHA.  
VPN Türleri:  
Client-to-Site (C2S) / Remote Access VPN:  
Amaç: Tek bir kullanıcı (istemci) bir VPN istemci yazılımı kullanarak, uzak bir ağdaki (örneğin şirketin iç ağı) bir VPN sunucusuna bağlanır.  
Kullanım: Evden çalışan bir personelin, ofisteki dosya sunucusuna veya yazıcısına erişmesi.  
Site-to-Site (S2S) / Router-to-Router VPN:  
Amaç: İki farklı ağın (örneğin iki farklı ofisin ağı), kendi aralarında VPN tünelleri oluşturarak sanki aynı fiziksel ağdaymış gibi iletişim kurmalarını sağlamak.  
Kullanım: Merkez ofis ile şube ofis arasında güvenli veri alışverişi.

## Örnek Uygulama

Client-to-Site (C2S) VPN Kullanımı - Evden Ofise Erişim:  
Bir çalışan, evinde kendi bilgisayarını (IP: 192.168.10.50) kullanıyor.  
Şirketin ofisinde, çalışanların özel ağı (192.168.10.0/24) ve bu ağa erişim sağlayan bir VPN sunucusu (88.105.125.120) var.  
Çalışan, bilgisayarında bir VPN istemci yazılımı açar.  
Yazılım, 88.105.125.120 IP'li VPN sunucusuna bağlanmak için kullanıcı adı ve şifresini girer.  
Kimlik doğrulama başarılı olursa, çalışanın bilgisayarı ile şirket VPN sunucusu arasında şifreli bir tünel kurulur.  
Artık çalışanın bilgisayarı, sanki ofisteymiş gibi 192.168.10.x IP'li iç kaynaklara (örneğin 192.168.10.5 IP'li dosya sunucusu) erişebilir. Trafik şifreli tünelden geçer.  
Site-to-Site (S2S) VPN Kullanımı - Ofisler Arası Bağlantı:  
Merkez ofisin ağı: 172.16.1.0/16  
Şubedeki ofisin ağı: 192.168.10.0/24  
Her iki ofiste de, kendi ağ geçitlerinde (router/gateway) S2S VPN yapılandırması yapılmıştır.  
Merkez ofisin ağ geçidi IP'si: 212.254.45.81  
Şubedeki ofisin ağ geçidi IP'si: 105.81.21.32  
İki ağ geçidi arasında kimlik doğrulama ve şifreleme anlaşması yapılır.  
Aralarında şifreli bir tünel oluşturulur.  
Bu tünel sayesinde, 172.16.1.20 IP'li DBServer05 ile 192.168.10.5 IP'li FileServer03 sanki aynı ağdaymış gibi güvenli bir şekilde iletişim kurabilir. Şubedeki personel de merkezdeki kaynaklara erişebilir.

## Kapanış / Sonuç

VPN (Virtual Private Network), internet üzerinde güvenli ve özel iletişim kurmanın temel yöntemlerinden biridir. Şifreleme teknikleri ile verilerinizi korur, gerçek IP'nizi gizleyerek gizliliğinizi artırır ve uzaktan erişim ihtiyaçlarınızı karşılar. C2S VPN bireysel kullanıcıların güvenli erişimini, S2S VPN ise ağlar arası güvenli bağlantı kurulmasını sağlar. Güvenli internet kullanımı ve kurumsal ağ yapılandırmaları için VPN kavramını bilmek ve kullanmak son derece önemlidir.  
sibertim.com