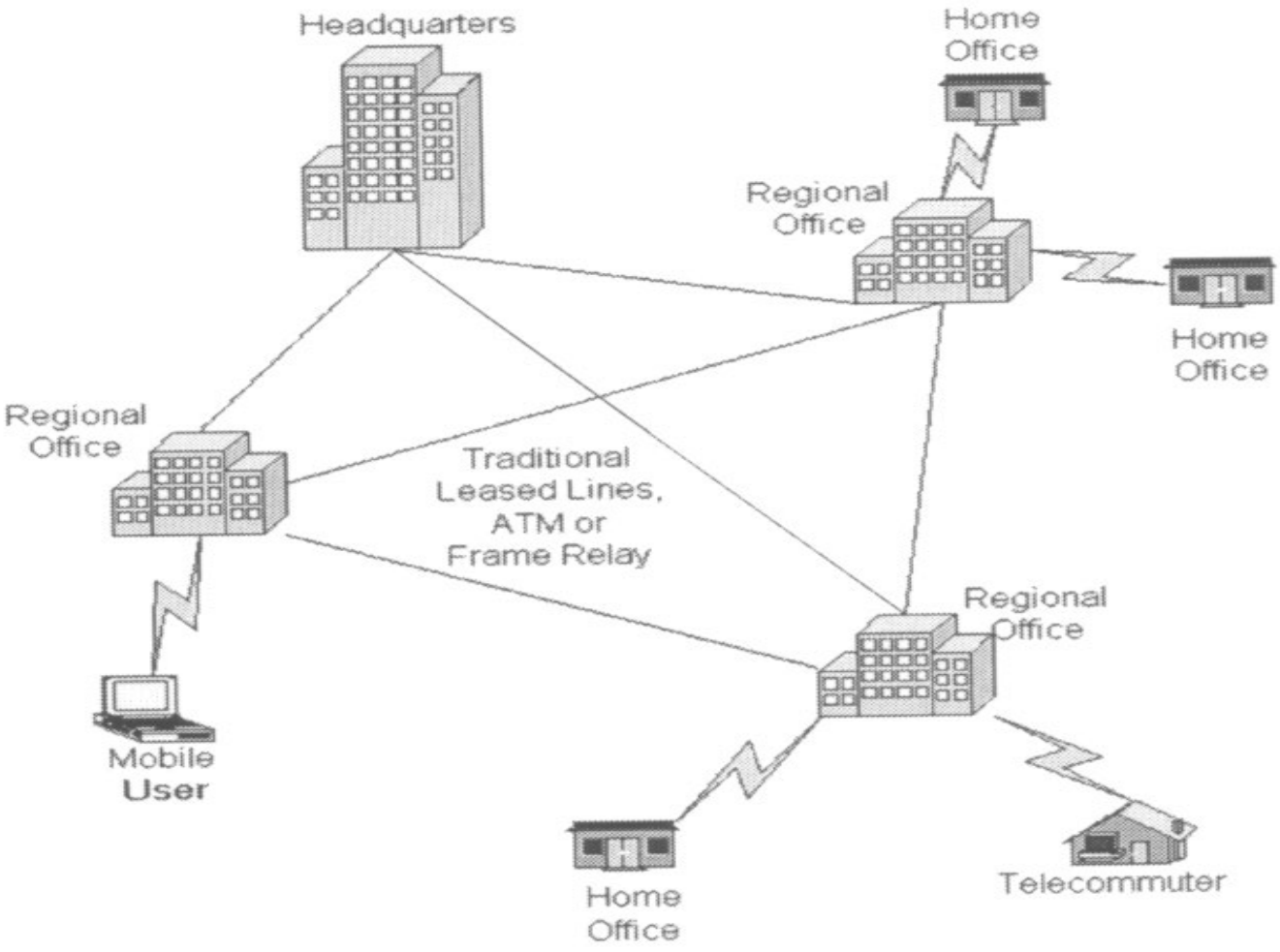
VIRTUAL PRIVATE NETWORKS (VPN - SANAL ÖZEL AĞLAR)

Geleneksel Bağlantı



- https://www.youtube.com/watch?v=_wQTRMBAvzg&ab_channel=vpnMentor

VPN nedir?

•VPN(Virtual Private Network/Sanal Özel Ağ) internet üzerinden sifreli ve güvenli veri iletişimi sağlamak için düşünülmüş bir teknolojidir.

• Kamusal bir iletişim ağı üzerinde, Kiralık hatlar(Lease-line) gibi güvenli, sağlam çözümlerin yerine VPN kullanilmasinin temel nedeni, maliyet ve kolay yapılandırmadır.

•Tüm VPN çözümlerinde İnternet erişimi üzerinden kurulan güvenli tüneller söz konusudur. **Güvenli tüneller, kriptolama teknikleri ile sağlanır.**

• Gartner Group; VPN'i, herkese açık bir iletişim altyapısı üzerinden, iki veya daha fazla doğrulanmış/onaylanmış taraflar arasında güvenli veri iletişimi sağlamak üzere oluşturulmuş sanal ağlar olarak tanımlar.

VPN nedir?

- VPN, İstemci PC'nin başka bir ağdaki **sunucunun önceden belirlenmiş portuna TCP/IP tabanlı protokoller** aracılığı ile mevcut internet veya İntranet bağlantısı kullanılarak yapılan bağlantıdır. VPN bağlantıda giden ve gelen veriler şifrelendiği için güvenlidir.

- Bir İstemci VPN yoluyla bir ağa bağlanacaksa **o ağa ait bir IP adresi alarak** ilgili ağa katılır. O ağın üyesi olarak çalışır. Eğer ağa bağlanmak için havuzda boş IP adresi yok ise bağlantı başarısızdır. IP'ler DHCP protokolü veya elle VPN yapılandırmasıyla sağlanır.

- VPN bağlantıları PPTP(Point-to-Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), SSTP(Secure Socket Tunneling Protocol) isimli protokoller kullanılarak sağlanır. Bu protokollere **TÜNEL protokolleri** denir. Bu protokollerin temelinde PPP (Point to point Protokol) protokolü vardır. PPP protokolü çevirmeli bağlantı ve noktadan noktaya veri aktarımı için geliştirilmişlerdir.

VPN nedir?

- **PPTP** tünel yönetimi TCP bağlantısını (1723. port) ve tünel oluşturan veri için ise GRE (General Routing Encaplusulation- Genel Yönlendirme kapsüllemesi, port:47) kullanır. Kapsüllenen PPP çerçevelerinin payload'ları şifrelenebilir, sıkıştırılabilir.

- **L2TP** Cisco tarafından geliştirilen L2F ve PPTP (layer to forward- İki katmanlı iletim) protokollerinin birleşiminden oluşur. Ayrıca IPSec desteği mevcuttur. IPSec kullanılacaksa hem istemci hemde sunucu Ipsec desteği vermelidir. XP sonrası istemci, Windows Server 2003 ve sonrası Sunucu desteği vardır.

- **SSTP**(Secure Soket Tunel Protokolu) 443.TCP portu üzerinden HTTPS protokolünü kullanan daha yeni bir protokoldür. Bunun nedeni bazı Firewalların PPTP ve L2TP üzerine filtre uygulayarak VPN trafiğini engellemeleridir.

VPN (Virtual Private Network - Sanal Özel Ağ) Nedir?

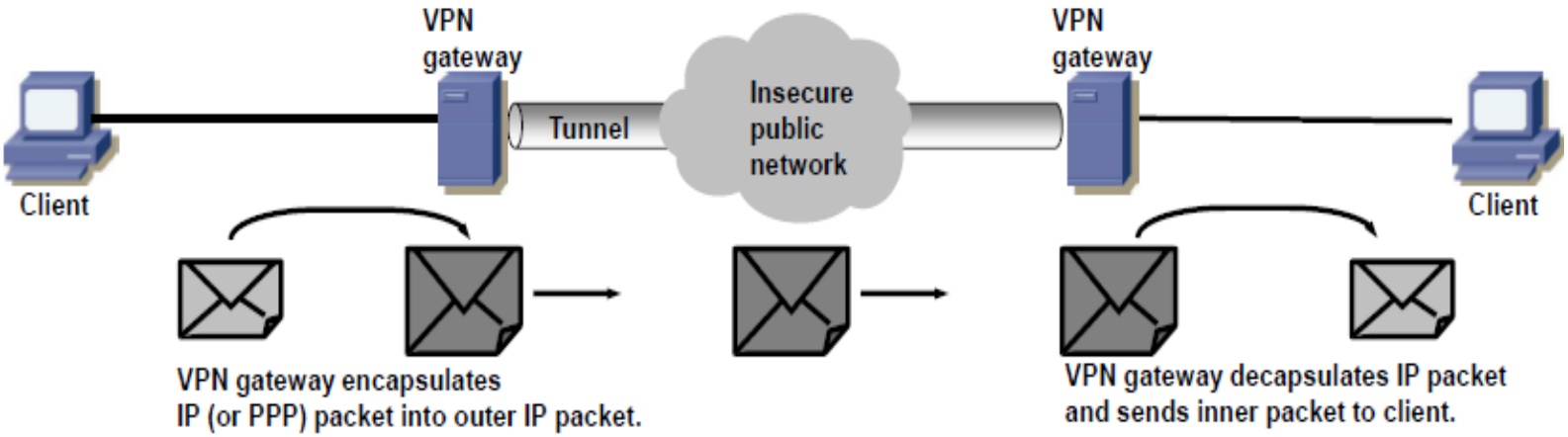
- VPN ağları kullanım alanlarına göre **Access VPN**, **İntranet Tabanlı VPN** ve **Extranet (İnternet) Tabanlı VPN** olmak üzere üç çeşittir. Access VPN gerçek kişiler tarafından bireysel kullanım amacıyla tercih edilirken İntranet ve Extranet Tabanlı VPN ağlar tüzel kişiler (şirketler, üniversiteler gibi kurum ve kuruluşlar) tarafından tercih edilmektedir.

- **VPN'in kullanım alanları:**
  – Evden ofis bilgisayarına bağlanma, çalışabilme, proje ve dosyalara erişim.
  – Kamu ve Özel sektörlerin şubeleri arasındaki iletişim ve denetimini sürdürebilmesi için yüksek güvenlik protokolü altında firmaya bağlanma.
  – Kısıtlama olmaksızın internet üzerinden tüm içeriğe ulaşabilme imkanı.

1. Virtual Private Network VPN amacı

1. Güvenli olmayan bağlantı/networkler üzerinden güvenli iletim.

A. Tunnelling of protocols like PPP:

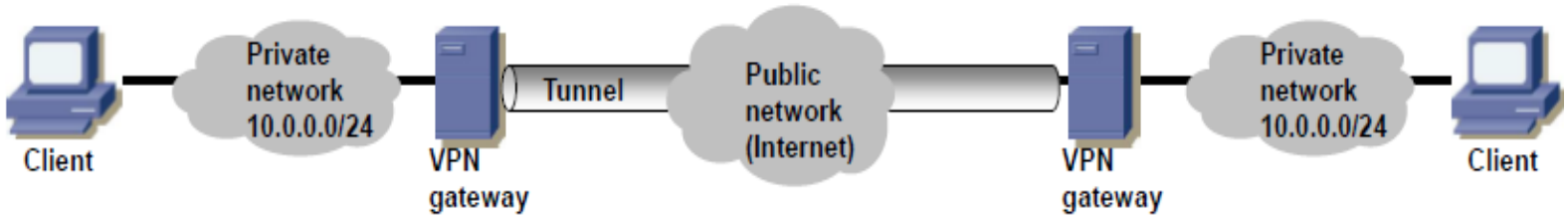


B. Encryption: Tunnel may use encryption to provide secrecy/confidentiality.
C. Authentication: Tunnel may be authenticated thus granting access to VPN only to authorized clients.
D. Access control / authorization: VPN gateways ascertain and enforce level of access for VPN client.
E. Auditing (monitor, log, intervene): VPN gateways monitor usage of VPN and react in case of anomality.

---

2. Özel adres ve protokolları public adresler üzerinde işleme

Tunnelling of private IP addresses (10.0.0.0, 172.16.0.0, 192.168.0.0) through public network (Internet).



VPN sanaldır:
VPN kullanıcısı bağlı olduğu esnada bağlantı yaptığı networkü sahiplenmez, bu network aynı anda birçok VPN kullanıcısı tarafından paylaşılır.

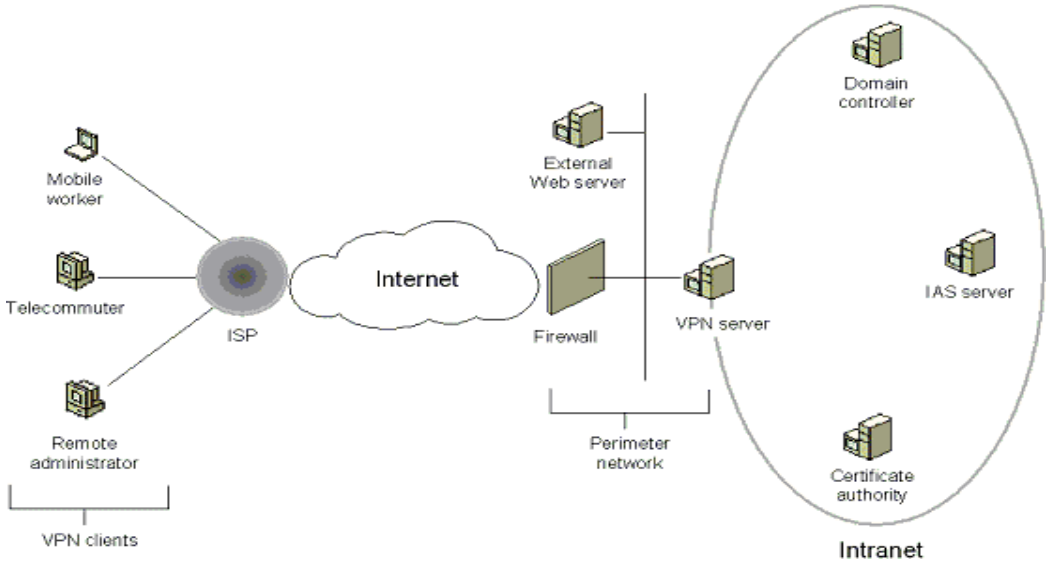
VPN özeldir:
Özel olması VPN üzerinden akan trafiğin özel olması anlamındadır. VPN trafiği Internet (public network) üzerinden geçer. VPN trafiğinin Internet üzerinden güvenli geçişini sağlamak için özel network önlemlerine ihtiyaç vardır, Örneğin data kriptolama, data doğrulaması (data authantication), yetkilendirme (authorization) ve adres spoofing'in önlenmesi gibi.

VPN bir Networktür:
Fiziksel bir varlığı olmayıp sanal olsa da VPN bir network özelliğindedir. VPN, iki uç arasında güvenilir tünel bağlantısı sağlayan bir networktür.

Virtual Private Networks

Temelde iki tip VPN teknolojisi vardır. Amaca göre bu iki VPN teknolojisinden biri seçilebilir. Bu teknolojiler

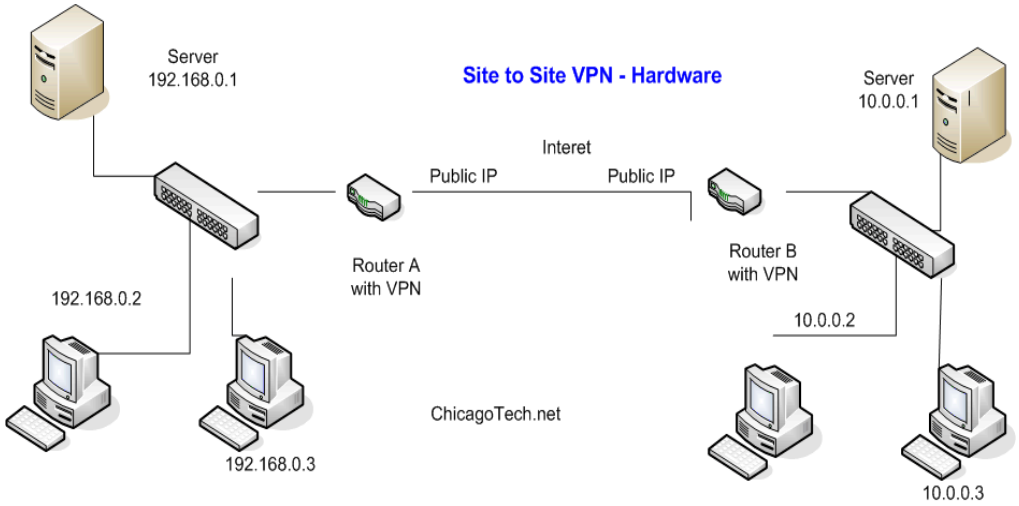
1- Remote Access VPN (Uzaktan erişim VPN),



Uzaktan erişim VPN bağlantıları, evinde çalışan ya da seyahat esnasında ofisinde olamayan kullanıcıların İnternet üzerinden özel ağ üzerindeki sunucuya erişme imkânı sağlar. Remote Access VPN'nin en önemli özelliği kimlik sorgulaması ile uzak ve gezgin kullanıcıların kimliklerini doğrulamasıdır. Kullanıcılar uygun erişim ve teknolojiye sahipse ISP ile bağlanabilir.

2-Site-to-site VPN

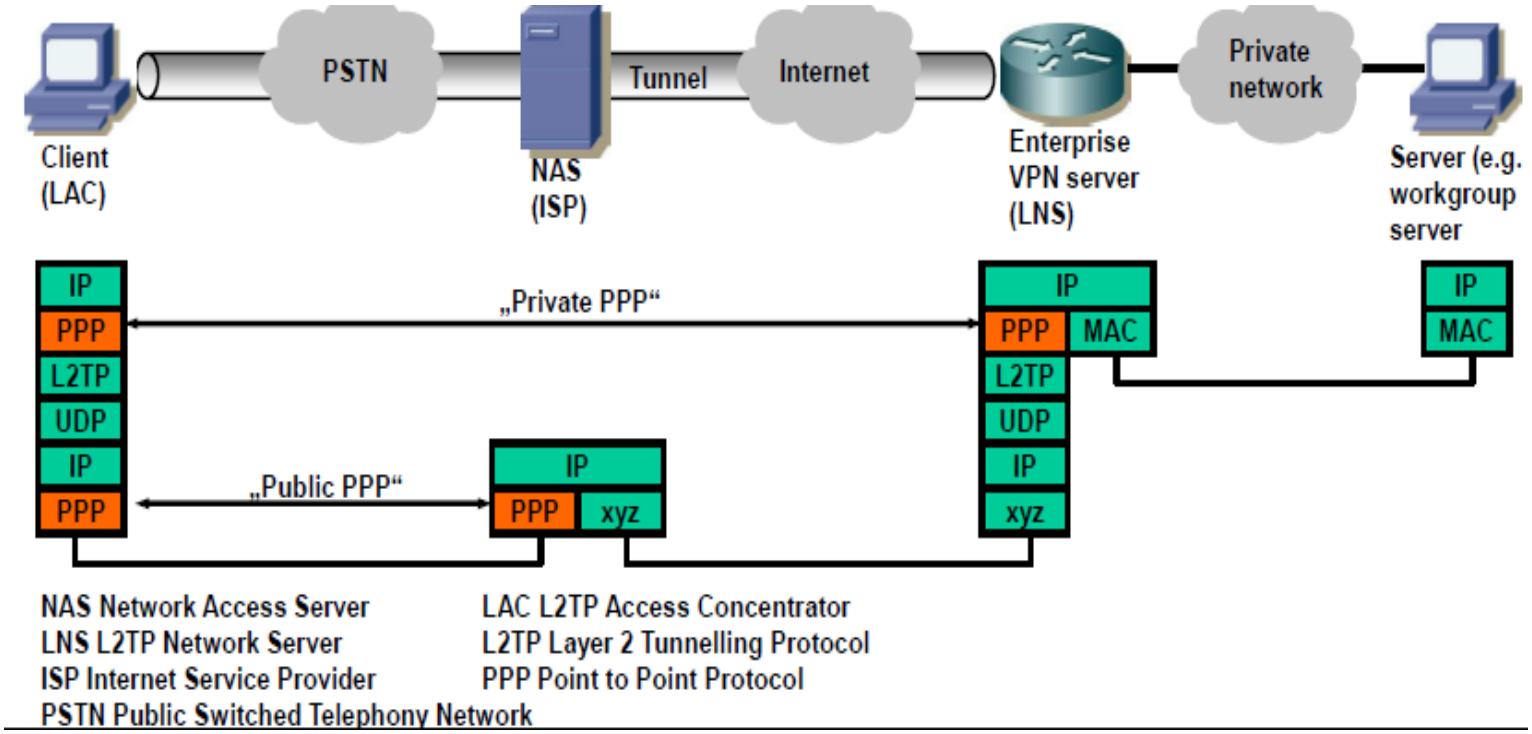
(Siteden siteye VPN:): Bu VPN bağlantısı WAN (Wide Area Network) bağlantısı gibi çalışır. Ağlar, İnternet üzerinden verileri bir yönlendirici ile başka bir yönlendiriciye iletir. Yönlendiricilere göre VPN bağlantısı, veri bağlantısı olarak işlev görmektedir.



1. Remote Acces (Uzak Erişim) VPN (istemcisi tarafından başlatılan (voluntary tunnel = isteğe bağlı -gönüllü tünel)

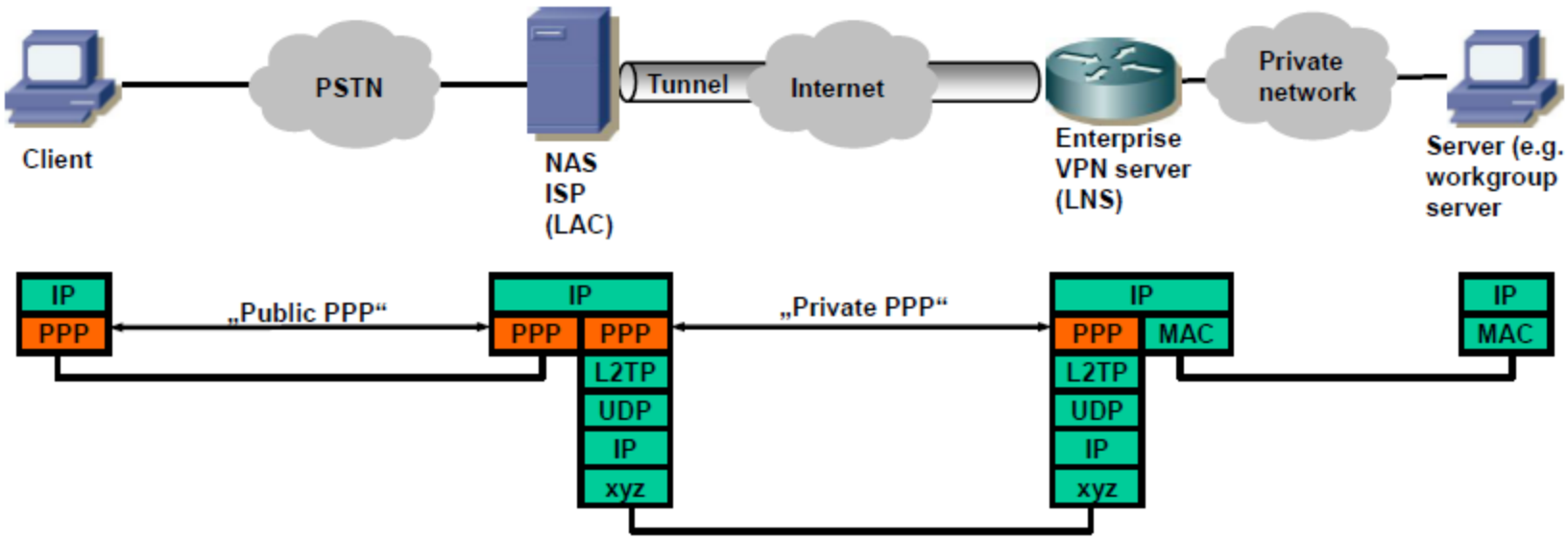
- **VPN istemcisi, istemci makinede** yer almaktadır. NAS sadece PPP aracılığıyla müşteriye ortak IP adresi (istemci ve NAS arasındaki “public PPP oturumu") sunar.
- istemci üst özel IP almak için bir VPN bağlantısı (örn L2TP) oluşturur ve bu şekilde doğrudan (istemci ve sunucu arasında "özel PPP oturumu") özel ağa bağlı gibi, özel ağa bağlanır.

Bu VPN modu (VPN tüneli’nin kurulması ve yönetimi istemcidedir) **voluntary tunnel -** gönüllü tünel " olarak adlandırılır.



Siteden Siteye VPN (Access VPN NAS initiated)

•NAS, istemci adına kurumsal VPN sunucusuna VPN tüneli açar.
•Uzak erişim VPN istemcisinin aksine erişim kısmı (hiçbir şifreleme, hiçbir özel IP) özel değildir.
• VPN istemcisi kendisi kontrolü altında olmadığından , Bu VPN modu (-VPN tüneli istemci kontrolundan bağımsız olduğu için) “ **compulsory tunnel –**zorunlu tunel " denir.



VPN ağları kullanım alanlarına göre;

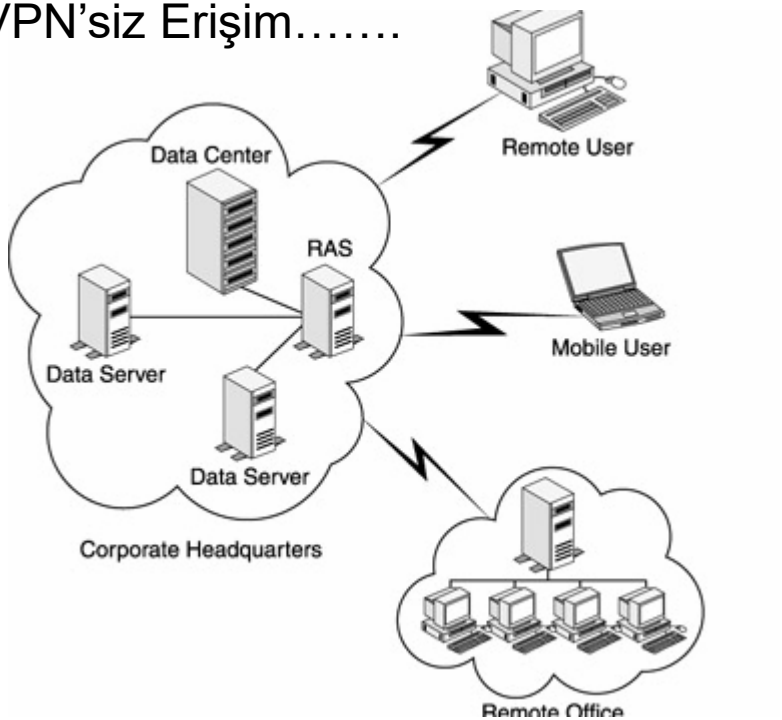
Access VPN,

İntranet Tabanlı VPN,

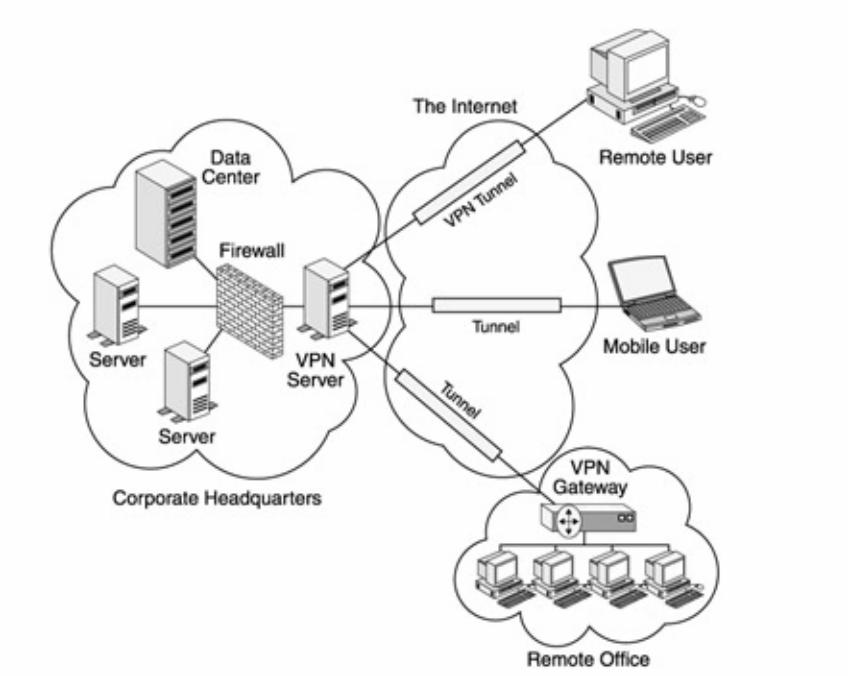
Extranet (İnternet) Tabanlı VPN.

Access VPN gerçek kişiler tarafından bireysel kullanım amacıyla tercih edilir. İntranet ve Extranet Tabanlı VPN ağlar tüzel kişiler (şirketler, üniversiteler gibi kurum ve kuruluşlar) tarafından tercih edilir.

VPN'siz Erişim…….



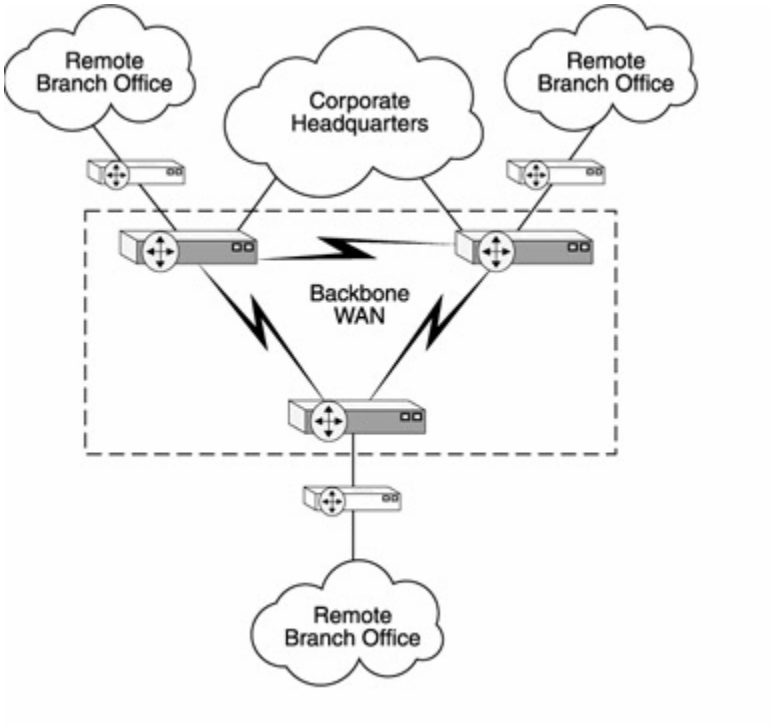
ACCES VPN

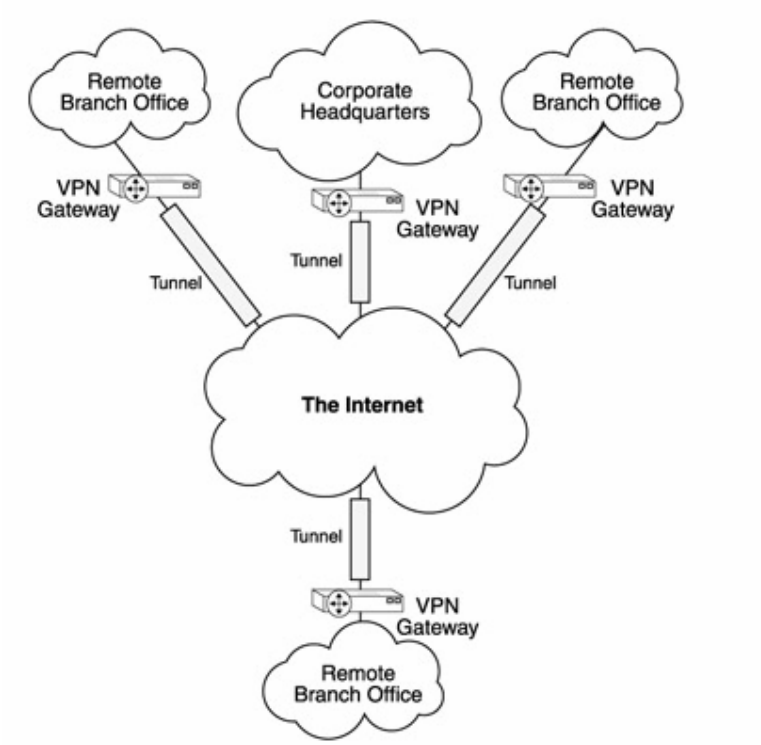


Uzaktan erişimli VPN ile mobil kullanıcılar, küçük/ev uzak ofis (SOHO) merkeze dial-up olarak güvenli bir şekilde bağlanabilirler. Uzaktan erişimli VPN istenilen zamanda network kaynaklarına uzaktan mobil olarak erişim imkanı sağlar. Kurumlarda mobil olarak çalışanlar veya kurumun uzaktaki bir ofisi, bu kurumun intranetine istenilen an erişim yetkisine sahiptir. Uzaktan erişim sunucusu (RAS) uzaktan erişim isteklerinde, kullanıcının kimlik doğrulamasını ve yetkilendirmesini gerçekleştirir. Bu VPN tipinde intranete dial-up bağlantı ile erişir.

INTRANET VPN

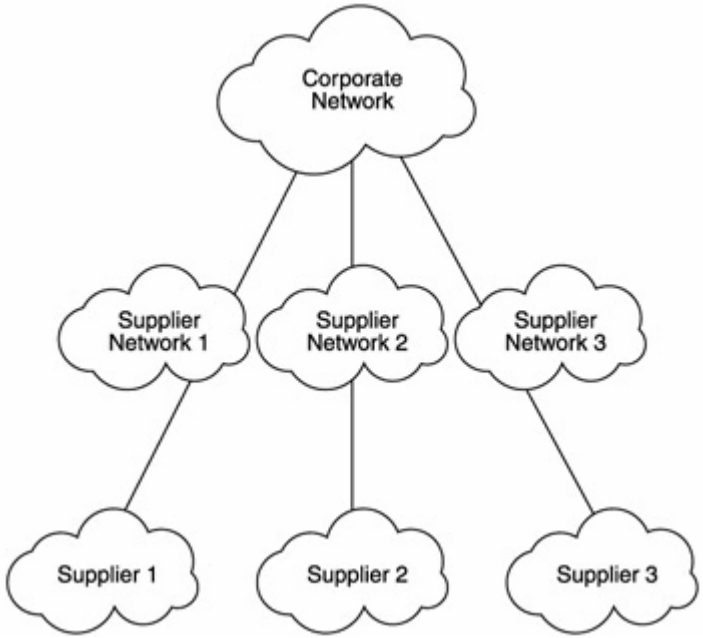
VPN’siz İntranet…



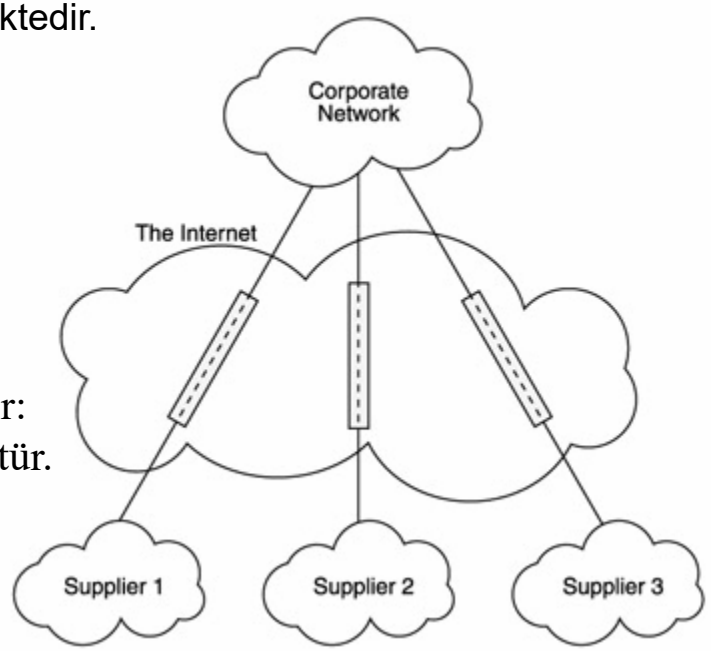


Siteden Siteye VPN bağlantısı özel bir ağın iki bölümünü birbirine bağlar. VPN sunucusu, bağlı olduğu ağa bağlantı sunarken, yanıtlayan diğer sunucu yada yönlendirici (VPN sunucusu) yanıtlayan yönlendiricinin (VPN istemcisi) kimlik bilgilerini doğrular. Karşılıklı doğrulama sağlanır. Ayrıca siteden siteye VPN bağlantısı üzerindeki iki sunucuda gönderdikleri veri transferlerinin başlangıç noktaları tipik olarak yönlendiriciler veya sunucular değildir.

EXTRANET VPN



İntranet ve uzak erişimli VPN çözümünden farklı olarak, Extranet VPN dış dünyadan tam olarak yalıtılmış değildir. İş ortakları, iştirakler, ortak çalışılan şirketler ile yapılan güvenli bağlantılardır. Extranet VPN network kaynaklarına kontrollü erişim sağlar. Şekilde VPN olmadan Extranet bağlantının yapısı görülmektedir.



Extranet VPN'in sağladığı avantajlar aşağıda anlatılmıştır:

- VPN 'siz extranet bağlantılara göre maliyeti çok düşüktür.
- Yönetimi, tanımlaması ve tanımlamada değişiklik yapılması kolaydır.
- İletim ortamı internet olduğundan VPN çözümünde organizasyonun ihtiyacına göre çözüm sağlayabilecek birçok servis sağlayıcı seçeneği vardır.
- İnternet üzerinden bağlantı ISP tarafından sağlandığı için ilave bir iş gücü gerektirmez dolayısı ile operasyon maliyeti de çok düşüktür.

VPN Çalışma Yapısı

Tipik bir VPN dağıtımında, istemci, Internet üzerinden uzaktan erişim sunucusuyla sanal noktadan noktaya bağlantı başlatır. Uzaktan erişim sunucusu aramaya yanıt verir, arayanın kimliğini doğrular, verileri VPN istemcisi ile kuruluşun özel ağı arasında aktarır.

Veriler, noktadan noktaya bağlantıyı taklit etmek amacıyla üstbilgi kullanılarak kapsüllenir veya sarılır. Üstbilgi (başlıktaki ek bilgi), verilerin bitiş noktalarına erişmeleri için, paylaşılan veya ortak ağ üzerinden çapraz geçebilmelerine olanak veren yönlendirme bilgileri sağlar.

Özel ağ bağlantısını taklit etmek için, gönderilen veriler gizlilik amacıyla şifrelenir. Paylaşılan veya ortak ağda ele geçirilen paketlerin şifreleri, şifreleme anahtarları olmadan çözülemez. Özel ağ verilerinin kapsüllendiği ve şifrelendiği bağlantı VPN bağlantısı olarak bilinir.

VPN 4 kritik Fonksiyonu yerine getirir

- Authentication – Veriyi gönderen, alanın doğru kişi olduğunu bilir.
- Access control – Yetkisiz kişiler VPN'i kullanamaz.
- Confidentiality – Veri gizliği garanti edilir.
- Data Integrity – Veri bütünlüğü garanti edilir.

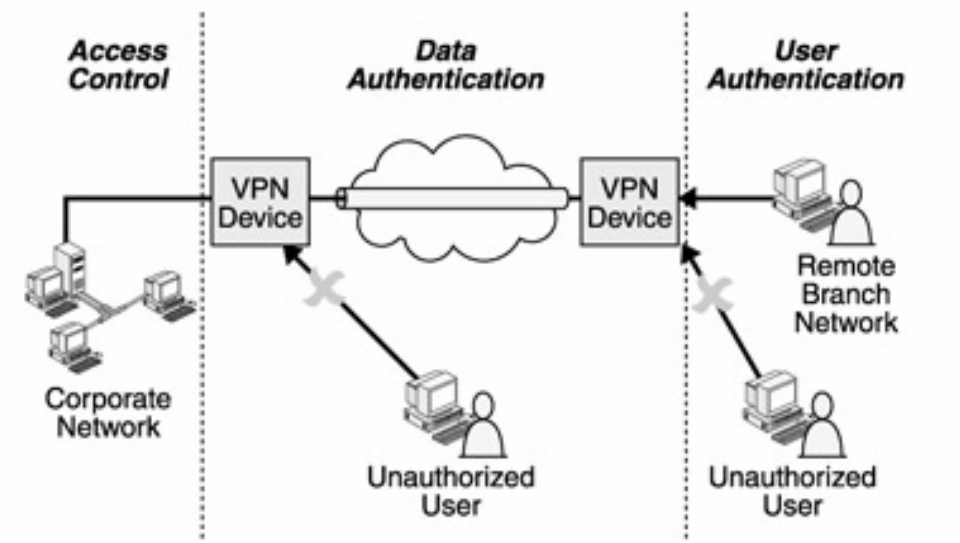
VPN güvenlik açısından sağladığı faydalar;

1- VPN aboneli dışındaki kimseler ilgili VPN'e erişemez.

2- VPN abonesi olmayanlar giriş için VPN tarafından bloklanır

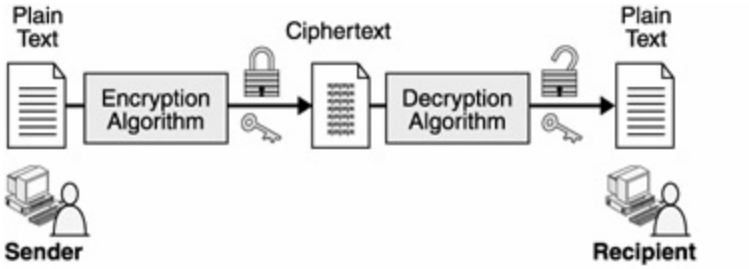
3-Internet üzerinden iletilen verilerin gizliliği ve bütünlüğü sağlanmalıdır

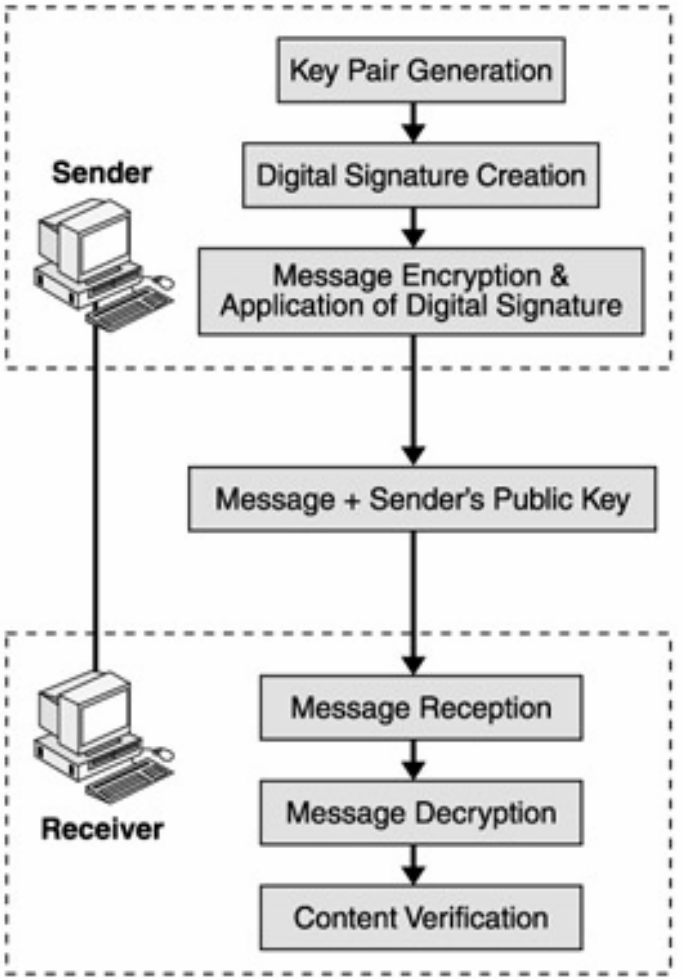
VPN'de, Kimlik doğrulama ve erişim:



LoginID ve Şifre sorgulaması

Verinin kriptolanması





PKI yapısıyla kimlik doğrulama ve mesaj bütünlüğünün kontrolu

VPN ile üç farklı güvenlik tekniği sağlanır.

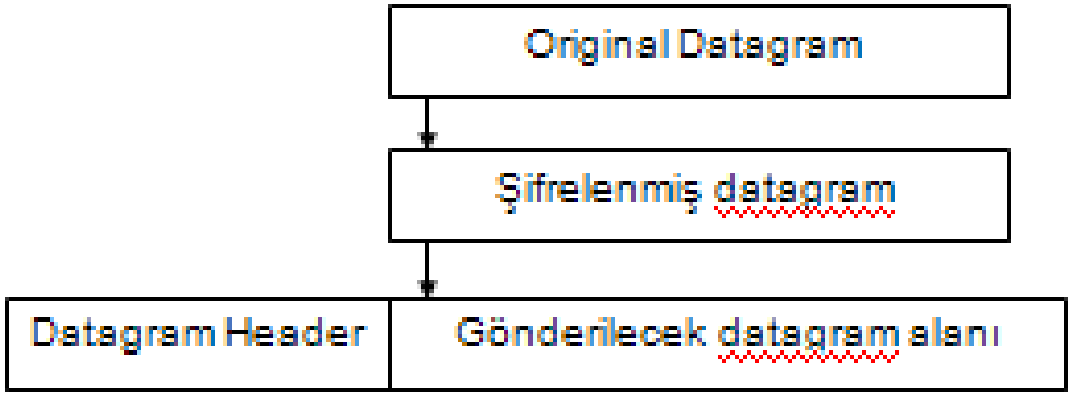
- **Kapsülleme (VPN Tünelleme işlemi)** ile Public ağlar üzerinden, Kiralık hatlar (Lease-line), Frame Relay, ISDN gibi iki nokta arasında daha sağlam, kesintisiz bir bağlantı hizmeti verir. Başka bir deyişle Tünel oluşturma, iletim yapılırken bütünlüğün ve gizliliğin korunması için paketleri diğer paketlerin içine kapsülleme işlemidir. Ancak, Kiralık hat, Frame Relay, ISDN, gibi bağlantı şekilleri kullanılarak şirket ofisleri birbirine bağlandığında aradaki hat özel bir hat olduğu için verilerin çalınması veya değiştirilmesi mümkün olmamaktadır. Fakat internet üzerinden verilerin taşınması söz konusu olduğunda verilerin güvenlik amacıyla şifrelenmeside gerekmektedir. VPN teknolojileri bunu sağlar.
- **Kimlik sorgulaması (Authentication)** ile sadece yetkili kullanıcıların VPN hizmetini alabilmesi sağlanır.
- **Kriptolama (encryption)** ile yapılacak haberleşmenin şifrelenerek başka kullanıcıların haberleşmeyi dinlemesi, veri bütünlüğü (data integrity) ile de kötü niyetli kullanıcıların yolladığınız paketlerin içeriğini değiştirebilmeleri engellenir.

Tünelleme

- **Tünelleme (Enkapsülasyon)** işlemi bir VPN uygulamasının en önemli kısmıdır. Bu teknik organizasyonlara Internet üzerinden kendi sanal networklerini oluşturma imkanı sağlar. Intranet dışından hiç bir yetkisiz kullanıcı intranete erişim yetkisine sahip değildir.
- Tünellemede paket hedef networke iletilmeden önce bu pakete tünelleme protokolünün başlık bilgisi eklenir. Payload olarak da isimlendirilen orjinal paket; internetin desteklemediği bir protokolü kullanıyorsa, tünel içindeki pakete başlık bilgisi tünel protokolü ile ekler.
- Bu başlık yönlendirme bilgilerini içerir ve paket artık Internet üzerinden iletilebilecek hale gelir. Tünelleme protokolleri, tünelin en ucundaki kullanıcı için, oturum yönetimi olarak bilinen işlemleri gerçekleştirmek üzere, tünelleri kurar ve yönetir.

Tünelleme

- Tünelleme protokolleri IP kadar diğer protokollerin kapsülleşmesi işini de yapar ve tünel aygıtları için yetkilendirme yöntemlerini gerçekleştirir. Bu Protokoller genel olarak verileri şifreler ve tünel içine gönderir.
- Bir genel ağ üzerinde sanal bir point-to point bağlantı oluşturmaktır. Tünel tekniğini 2 fazda anlatılabilir:
- Faz1: İstemci VPN isteğini gönderir ve HA (Home Agent) sistemi bu istemcinin kimlik sorgulamasını yapar.
- Faz2: Tünel içinden veri transferi başlatılır.



Data kapsülleme

TÜNELLEME PROTOKOLLERİ

Tünelleme protokolleri üç kategoride sınıflandırılabilir:

1. Taşıyıcı protokoller: Tünellenmiş paketlerin Internet üzerinden iletimini sağlamak için bu paketleri yönlendirir. Tünellenmiş paketler bu protokolün paketleri içine enkapsüle edilir.

2. Enkapsüle protokolleri: Pay-load paketin enkapsüle edilmesini sağlar. Bu protokol ile tünel kurulur ve sonlandırılır. Günümüzde en yaygın olan enkapsüle protokolleri PPTP, L2TP, ve IPSEC'dir.

3. İletim protokolleri: Tünel içinden iletilmesi amacıyla enkapsüle edilmesi gereken orijinal veriler için bu protokol devreye girer. En yaygın olan iletim protokolleri PPP ve SLIP (serial line internet protocol) protokolleridir.