T.C
FIRAT ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
ELEKTRİK-ELEKTRONİK BÖLÜMÜ

VPN (SANAL ÖZEL AĞLAR)

BİTİRME ÖDEVİ

HAZIRLAYANLAR

Arif YILDIZ

M. Ali AKDENİZ

DANIŞMAN

Yrd Dç.Dr. Hasan BALIK

Haziran, 2005

ELAZIĞ

T.C
FIRAT ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ

VPN (SANAL ÖZEL AĞLAR)

BİTİRME ÖDEVİ

HAZIRLAYANLAR

Arif YILDIZ M. Ali AKDENİZ

Bu tez ,…….tarihinde aşağıda belirtilen jüri tarafından oybirliği / oyçokluğu ile başarılı / başarısız olarak değerlendirilmiştir.

Danışman:

Üye:

Üye:

Üye:

TEŞEKKÜR

Kıymetli hocamız Yrd.Doç.Dr. Hasan Hüseyin BALIK'a ve çalışmalarımızda bizden yardımlarını esirgemeyen değerli arkadaşlarımıza teşekkürlerimizi sunarız.

Arif YILDIZ
M. Ali AKDENİZ

İÇİNDEKİLER

ŞEKİL LİSTESİ

Şekil:9.1.1. Ondemand VPN yapısı
Şekil.9.1.2. Çoklu protokol/On-demand tünelli VPN yapısı
Şekil.9.1.3. Şifreli oturumlu On-demand VPN yapısı
Şekil.9.2.1. On-demand/Firewall VPN yapısı
Şekil.9.2.2. Çoklu protokol/On-demand VPN
Şekil 9.3.1. İstemci-Fırewall VPN yapısı
Şekil 9.3.2. İstemci-sunucu VPN
Şekil.9.4. Doğrudan VPN yapısı

REFERANSLAR:

- Internet
- [CHM] Building A Virtual Private Network by Meeta Gupta

ÖZET

Günümüzde teknoloji ve bilgisayar kavramları birçok alanda kullanılmaya başlamış ve insan hayatının vazgeçilmezleri arasına girmeyi başarmıştır. Ev elektroniğinin bu denli gelişmesi insanların kendi evleri içerisinde daha güvenli ve konforlu bir yaşam sürmesini amaçlamaktadır. Bu nedenle yapılan çalışmalar gün geç tikçe artmakta ve daha yaygın kullanılır hale gelmektedir.

Bu çalışmada geçmişi günümüzdeki durumu ve geleceği ile akıllı evler incelenmiştir. Bu konu adı altında mikrokontrolörler, bilgisayar haberleşmesi, uzaktan kontrol, ve bu bunların birlikte kullanılması gibi birçok konu ele alınmıştır.

Bu çalışma sırasında örnek olarak ele alınan sıcaklık kontrolü yanı sıra projenin güvenlik, otomatik bahçe sulaması, havalandırma, garaj kapısı kontrolü, alarm, ihbar, aydınlatma kontrolü gibi birçok alanda kullanılması mümkündür.

Sonuç olarak; bu çalışma ile insan hayatını kolaylaştıracak ve güvenli bir hale getirecek olan bir alanın küçük bir uygulaması işlenmiştir.

Proje gerek uygulama alanının çok geniş ve gerek geliştirilmeye açık olması bakımından ele alınmış ve incelenmiş büyük uygulamaların temelini oluşturacak sonuçlar elde edilmiştir.

1. VPN (SANAL ÖZEL AĞLAR)

1.1. Giriş

Tüm dünyada yeni bir WAN (geniş alan ağı) çözümü hızla tanınıyor ve her geçen gün daha çok firma tarafından tercih ediliyor; VPN (Virtual Private Network/Özel Sanal Ağ). Bu yeni çözüm daha esnek ve en önemlisi çok daha düşük maliyetler ile geleneksel WAN çözümlerinin tüm işlevlerini yerine getirmektedir.

Ağ teknolojilerindeki düzenli gelişmelere rağmen, kurumların hedefi daha hızlı ve daha verimli haberleşme olanaklarını kullanabilmektir. Personel ve yöneticiler dünyanın neresinde olurlarsa olsunlar, yerel ağlarına sanki ofislerindeymiş gibi erişebilmek isterler.

1980 ortalarında ve 1990 başlarında uzak erişim için telefon hatları kullanıyordu. Şirketler, yöneticilerinin taşınabilir bilgisayarlarına veri sıkıştırabilme yeteneğine sahip hızlı modemler yerleştirip, ofisteki sunuculara bağlanabilmelerini sağlayabilmekteydiler. Çalışanların ve yöneticilerin yapması gereken sadece bulundukları ortamda RJ-11 telefon konnektörünü modemlerine takmak ve uzak erişim sunucularına şifreleri yetkisinde bağlanabilmekti.

1990 sonlarında kurumlar, uzak erişimin şirketlerine sağladığı avantajları daha çok anlamaya başladılar ve bazı büyük şirketler, ülke içinde ücretsiz aranabilecek telefon numaraları ile çalışanlarına bu hizmeti sunabildiler. Uluslar arası ticaret yapan kurumlarda ise, milletlerarası telefon ödemeleri söz konusu olduğu için uzak erişim servisleri şirketlere ciddi bir maliyet getirmekteydi.

VPN teknolojisinin cazip hale gelmesinin sebebi kurum/şirket çalışanlarının LAN sunucularda ve kurumsal ağlarda uzak noktalardan çalışmaya başlamış olmalarıdır. Bu çalışanların işlerini uygun bir şekilde yürütebilmeleri için kurumsal LAN'lara , WEB uygulamalarına ve diğer sunuculara uzaktan erişim sağlamaları büyük önem taşımaktadır.

Günümüzde sadece büyük kuruluşlar değil küçük ve orta ölçekli firmalar da ofislerini, bayilerini, iş ortaklarını kolayca ve ekonomik yoldan birbirine bağlayarak veri, hatta ses veya video iletişimi sağlama ihtiyacı duyuyor. Bu network yapısını firmaların kendi başına kurmaları son derece yüksek maliyetli ve zahmetli olduğundan firmalar, bağlantı ihtiyaçlarını VPN'ler sayesinde daha düşük maliyetler karşılığında, ülke geneline dağılmış erişim noktalarına ve yüksek performanslı bir ulusal omurgaya sahip İSS'ler aracılığı ile karşılamayı tercih ediyorlar.

VPN teknolojisi, firmaların şubeleri ve iş ortakları ile aralarında veri iletişimini güvenilir, kolay ve ekonomik biçimde sağlamasına olanak veren bir tünelleme teknolojisidir. Kurumların yerel ağlarını internet ortamı üzerine taşınmasını sağlar. VPN teknolojisinde, noktalar arası ekonomik ve güvenilir bağlantılar kurulurken
iletişim maliyetini minimum seviyede tutabilmek için internet ortamını "iletişim omurgası" olarak kullanılır. VPN'lerde kullanılan ağ kamuya açık bir ağdır, ancak ileti bir noktadan diğer noktaya kadar özel bir tünel aracılığı ile şifrelenerek ulaşır. Personel ve yöneticiler dünyanın neresinde olurlarsa olsunlar, yerel ağlarına sanki ofislerindeymiş gibi erişebilme imkanına sahip olurlar.

Bu teknoloji sayesinde belirli lokasyonlarda uzak ofisleri bulunan kurumlar, ofislerinin kendi aralarında haberleşmesini, döküman transferi, stok bilgisi sorgulama, satış bilgileri gibi çeşitli uygulamaları bu sanal ağ üzerinden güvenli bir şekilde gerçekleştirebilirler.

Gerek Intranet/Extranet VPN'lerde gerekse remote access/dial VPN çözümlerinde güvenlik, "tünelleme teknolojisi" ile garanti edilmektedir. Temel olarak, VPN trafiği servis sağlayıcının İnternet omurgasında güvenli ve kapsüllenmiş/kapalı bir tüneli içinde dolanır. Bu tünele giriş veya tünelden çıkış noktası sadece kurum tarafındaki güvenli router veya ağ güvenlik sunucusudur.

Geniş Alan Ağ (WAN) oluşturma yollarından biri olan VPN, altyapı olarak Internet'i kullandığından maliyeti en düşük bir WAN çözümüdür. VPN'ler kiralık özel veri hatlarının güvenilirliğine erişebilirmi? Pratik olarak VPN çözümlerinde güvenlik sorun olmaktan çıkmıştır. Tüm VPN çözümlerinde İnternet erişimi üzerinden kurulan güvenli tüneller söz konusudur.

Güvenli tüneller, kriptolama teknikleri ile sağlanır. VPN'ler bir kuruma, bir servis sağlayıcının herkese açık ağının veya Internet'in ölçeğini kullanarak, servis sağlayıcı yerel POP noktaları üzerinden kurum ağına uzaktan bağlanabilme olanağı sağlar. Bu durum, kurumlara merkez ofiste yer alan RAS (Remote Access Server) sunucuya doğru yapılan uzak mesafeli telefon çağrı ücretlerinden tasarruf sağladığı gibi, aynı zamanda kurum içinde RAS tabanlı uzaktan erişim çözümleri barındırmanın getirdiği harcamalar ve yönetim masraflarında da azalmalar sağlar. VPN'ler aynı zamanda, işletmeden işletmeye e-ticaret bağlantılarına yönelik, yeni ekstranet uygulamalarına da olanak tanır. Frame Relay veya özel kiralık hatların bulunmadığı veya çok pahalı olduğu birbirine uzak ofisler için, kurumlar Internet'in her tarafta bulunma ve ekonomik olma özelliğinden yararlanabilir. Internet üzerinden kritik bilgilerin transfer için gerekli olan gizlilik ve güvenlik konuları VPN teknolojileri yardımıyla çözülmüştür.

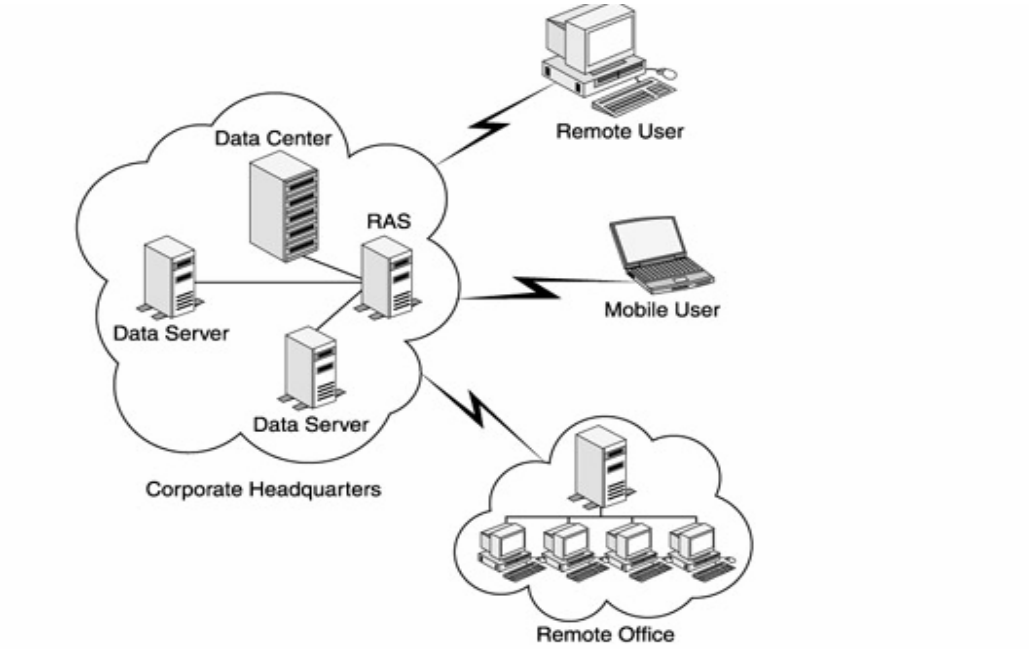
VPN sanaldır:
Her bir VPN bağlantıda networkün fiziksel yapısı transparent özelliktedir. Yani VPN kullanıcısı bağlı olduğu esnada bağlantı yaptığı networkü sahiplenmez, bu network aynı anda birçok VPN kullanıcısı tarafından paylaşılır.
VPN özeldir:
Özel olması VPN üzerinden akan trafiğin özel olması 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 olsada VPN bir network özelliğindedir. VPN, iki uç arasında güvenilir tünel bağlantısı sağlayan bir networktür.

Kimler için VPN?
-Yurtdışında ofisleri bulunan,
-Yüksek seviyede bilgi güvenliğine ihtiyacı olan,
-Yurtiçi veya yurtdışında mobil personeli bünyesinde barındıran kurumlar için VPN en -ideal çözümdür.

2. VPN TİPLERİ

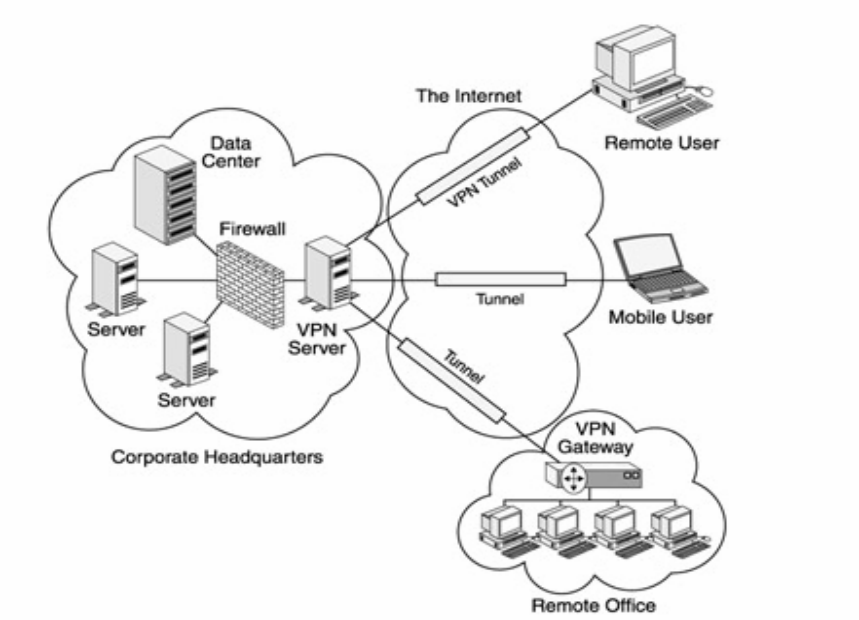
2.1. UZAKTAN ERİŞİMLİ VPN

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



Şekil 2.1.1: VPN olmadığı durumda tipik bir uzaktan erişim yapısı

VPN ile uzaktaki kullanıcılar ISP veya ISP'nın POP noktasına dial-up lokal bağlantı yaparak Internet üzerinden karşı networke bağlanırlar. Bu bağlantının yapısı Şekil 2.2'de görülmektedir.



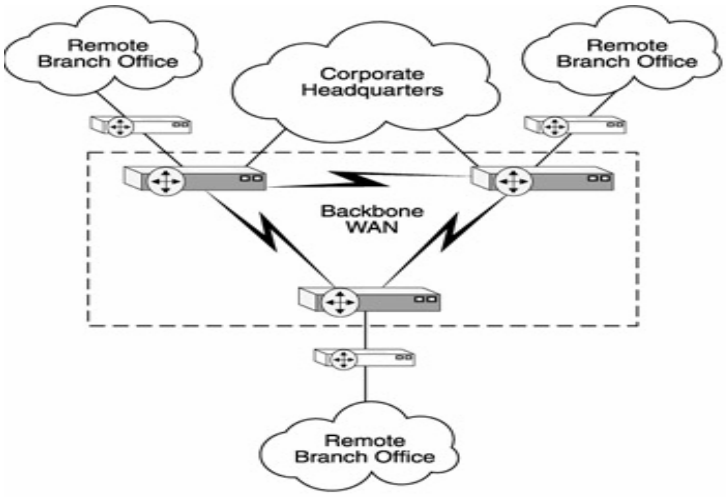
Şekil 2.1.2: Uzaktan erişimli VPN yapısı

VPN ile erişimin diğer erişimlere göre avantajları aşağıda anlatılmaktadır:
-RAS sunucusuna ihtiyaç olmaz ve RAS sisteminin modem pool'unuda kullanmaya gerek kalmaz.
-Uzun mesafe dial-up bağlantılar yapılmaz, bu işlemin yerine lokal dial-up bağlantılar yapıllır.
-Uzak mesafe kullanıcıları için ekonomik bir dial-up lokal bağlantı servisi sağlar.
-Lokal ağa eş zamanlı erişmek isteyen kullanıcılar olursa, bu kullanıcıların sayısı ne kadar artsada VPN bağlantılarda problem olmaz.
-Dial-up bağlantılar lokal olduğu için, modemlerin uzak mesafe erişimlerdede performansı iyidir.

VPN bu kadar avantajlı olmasına rağmen, olumsuz yönleride vardır:
-Data kaybı ve paketlerin iletimi esnasında bu verilerin yapısının bozulma ihtimali vardır.
-Gelişmiş şifreleme algoritmalarından dolayı, protokol yoğunluğu sözkonusu olduğundan bir yük meydana gelmektedir. Bu durum kimlik doğrulama sürecinde gecikmelere yol açmakadır. Ayrıca VPN'deki IP ve PPP tabanlı veri sıkıştırması uzun bir sürede gerçekleşmektedir.
-İletim ortamı olarak Interneti kullandığı için, multimedya içerikli veriler uzaktan erişimli VPN tüneller içinden iletilirken , iletimde gecikmeler sözkonusu olabilmektedir.

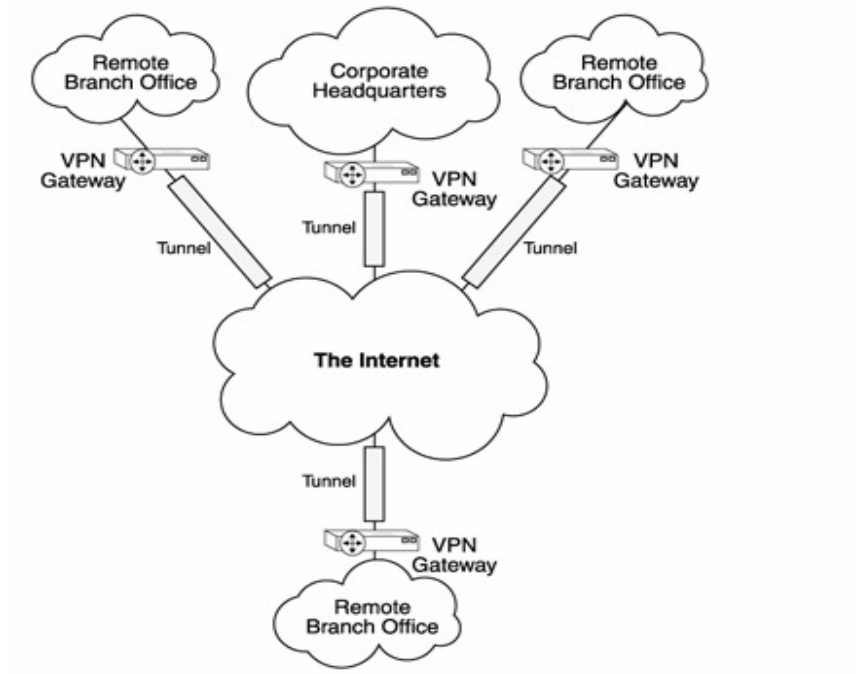
2.2. INTRANET VPN

Intranet VPN, bir organizasyonun uzaktaki branş ofislerinin, organizasyonun ortak intranetine erişip işlem yapabilmesi için kullanılır. VPN olmadan Intranet bağlantlarında herbir kullanıcı merkezdeki router'a erişmek durumundadır. Intranet VPN ile merkez ofis ve bölge veya şubelerin dahil olduğu networkler güvenli bir şekilde birbirine bağlanabilimektedir.



Şekil 2.2.1 : WAN omurgasını kullanan Intranet bağlantısı (VPN olmadan)

Şekilde görülen bağlantı yapısının donanım maliyeti yüksektir. Çünkü organizasyonun intranetine uzaktan bağlantı için en az 2 routera ihtiyaç vardır. Ayrıca tüm lokasyonlardan akan trafiğin intranet omurgasında tanımlanmasının ve yönetimininde maliyeti yüksek ve çözümü karmaşık olmaktadır. Intranet ne kadar geniş olursa maliyet o kadar çok artmaktadır. VPN çözümleri ile intranetler için pahalı WAN omurga bağlantıları,
düşük maliyetli Internet bağlantısı ile ortadan kalkmıştır. Şekil 2.1.3'de VPN çözümü gösterilmektedir:



Şekil 2.2.2: VPN çözümlü intranet bağlantısı

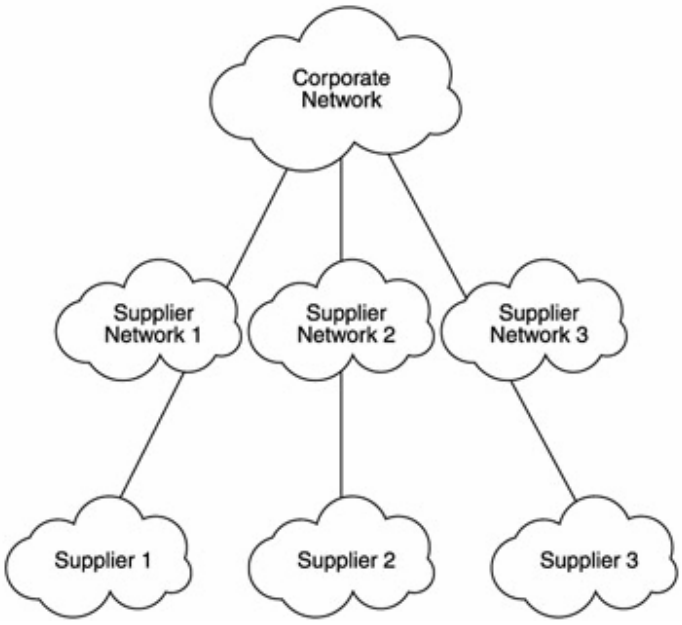
VPN çözümlü intranet bağlantılarının sağladığı avantajlar aşağıda açıklanmıştır:

-Özel bir WAN omurgasına ihtiyacı olmayıp, Interneti kullandığı için donanım maliyeti düşüktür.
-Çok fazla donanıma ihtiyaç duymadığı için bu konuda destek sağlayan personel saysıda az olacaktır, yani daha az bir işgücü gerektirecektir.
-İletim ortamı olarak Interneti kullandığı için uçtan uca bağlantılarda yeni bir uç bağlantı eklenmesi kolaylaşmaktadır.
-VPN tünellemede anahtarlama işlemi hızlı olduğundan VPN bağlantılarda backup özelliği vardır.
-ISP 'ye lokal dial-up bağlantı yapıldığı için, erişim hızı yüksektir.

Intranet VPN çözümlerindeki dezavantajlar aşağıda listelenmiştir:
-İletim esnasında paket kaybı ihtimali sözkonusudur.
-Veriler ortak bir network içindeki tünellerden iletildiği için bazı Internet atakları sözkonusu olabilmektedir.
-Multimedia içerikli verilerin iletiminde iletim zamanında gecikmeler olabilmektedir
-Internet ortamından dolayı zaman zaman performans düşüklüğü olabilir ve bu anlarda QoS garanti edilemez.

2.3. EXTRANET VPN

Intranet 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. Şekil 2.3.1'de VPN olmadan Extranet bağlantının yapısı görülmektedir.

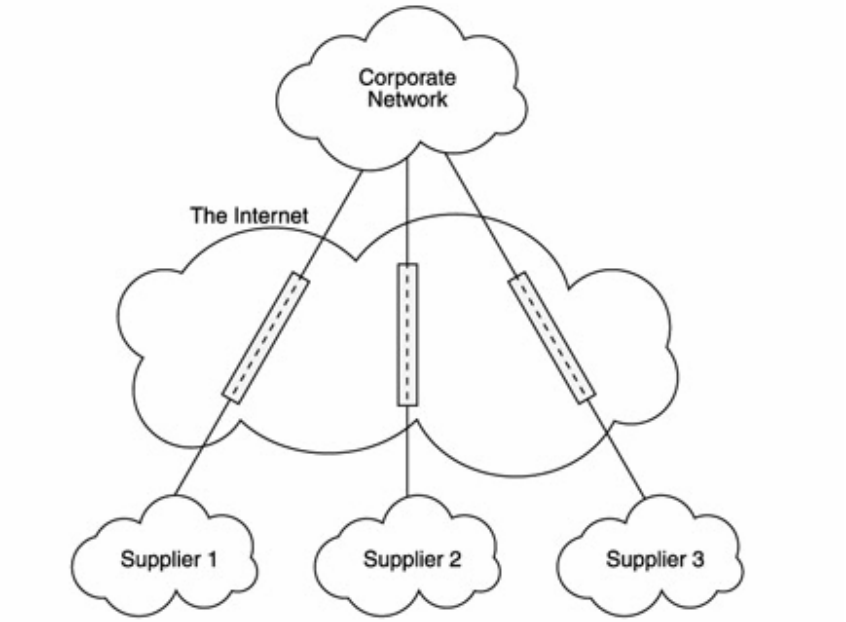


Şekil 2.3.1: Extranet yapısı (VPN olmadan)

Şekilde görüldüğü gibi intranetdeki herbir ağın bağlı bulunduğu networke göre yapılandırılması gerektiğinden bu yapı pahalı, karmaşık ve yönetimi zor bir yapıdır. Bu yapıyı yönetecek olan personel sayısıda fazla olacaktır dolayısıyla extradan bir işgücü gerektirecektir.

Ayrıca bu yapıyı genişletmekte kolay değildir. Bu güçlüklerden dolayı bir network üzerinden bir intranete bağlanılırken problemler yaşanabilir.

Extranet VPN çözümü yukarıda bahsedilen problemlerin yaşanmaması için extranet networklerde ideal bir çözümdür. Şekilde Extranet VPN yapısı görülmektedir.

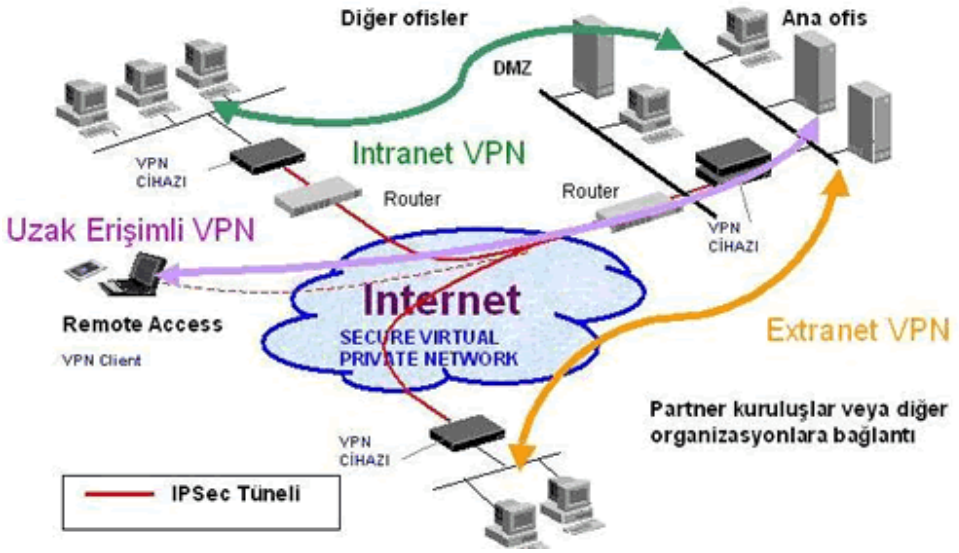


Şekil 2.3.2: Extranet VPN yapısı

Extranet VPN'in sağladığı avantajlar aşağıda anlatılmıştır:
-VPN'siz extranet bağlantılara gore 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.
-Internet üzerinden bağlantı ISP tarafından sağlandığı için ilave bir işgücü gerektirmez dolayısıyla operasyon maliyetide çok düşüktür.

Extranet VPN'in olumsuz yönleride aşağıdaki gibidir:
-Denial-of-service gibi güvenlik tehditleri söz konusu olabilmektedir.
-Intranete bilinmeyen kaynaklardan erişilebilme riski vardır.
-Internet ortamından dolayı, multimedia içerikli verilerin iletiminde zaman zaman gecikmeler meydana gelebilir.
-Internet ortamından dolayı performans değişkendir, zaman zaman QoS garanti edilemeyebilir.

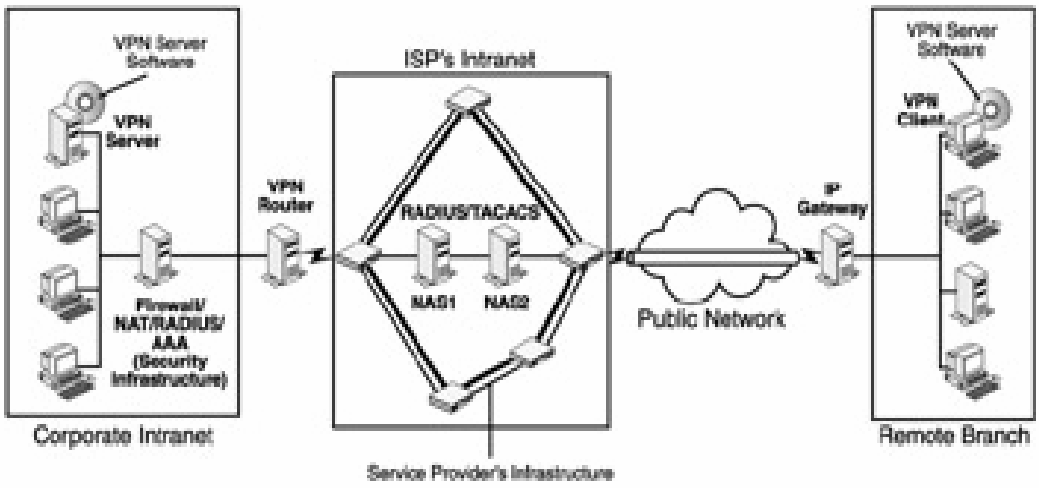
Bazı dezavantajları olmasına rağmen VPN tabanlı çözümün sağladığı avantajlar, dezavantajlarının önüne geçmektedir. Şekil 2.3.3'de VPN tipleri görülmektedir.



Şekil 2.3.3: VPN bağlantı tipleri

3. VPN BİLEŞENLERİ

Aşağıda bir VPN çözümünün şekli görülmektedir :



Şekil 3.a: VPN çözümünde kullanılan bileşenler

-VPN donanım: VPN sunucular, istemci makinalar, VPN yönlendiriciler, gateway'ler ve VPN yoğunlaştırıcılardan oluşur.
-VPN yazılımı: Sunucu ve istemci yazılımı ile VPN yönetim araçlarından oluşur.
-Organizasyon tarafındaki güvenlik: RADIUS, TACACS, NAT ve AAA güvenlik servisleri bu gruptadır.
-Servis sağlayıcı tarafındaki VPN bileşenleri: Servis sağlayıcının network erişimi için kullandığı anahtarlama omurgası ve Internet omurgası bu gruptadır.
-Public network: Internet, PSTN ve POTS bu gruptadır.
-Tüneller: PPTP tabanlı, L2TP tabanlı ve IPSEC tabanlı tüneller bu gruptadır.

3.1. VPN DONANIM BİLEŞENLERİ :

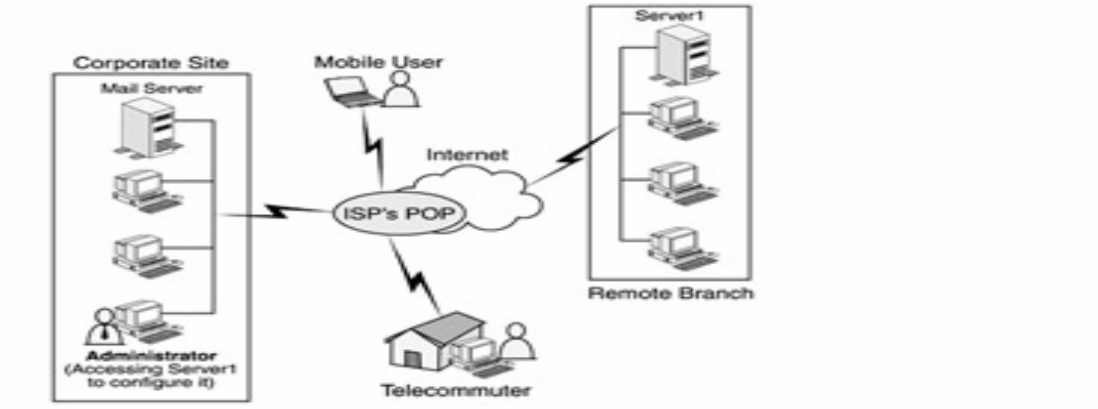
3.1.1. VPN SUNUCULAR

VPN sunucular uzak bağlantı servislerini sağlar. Genel fonksiyonları aşağıdaki gibidir.
-İstemcilerden gelen VPN bağlantı isteklerini dinler.
-Şifreleme ve kimlik doğrulama gibi bağlantı için gerekli olan işlemleri gerçekleştirir.
-VPN istemcilerinin kimlik doğrulamasını ve yetkilendirmesini gerçekleştirir.
-İstemciden iletilen verileri kabul eder / İstemci tarafından beklenen verileri iletir.
-VPN bağlantı ve tünelin son noktasıdır.

VPN sunucularda 2 veya daha fazla sayıda network adaptör kartı kullanılmalıdır. Bu kartlardan biri organizasyonunun intranetine bağlanılırken kullanılmakta olup diğer kart internet bağlantısını sağlar. VPN sunucular aynı zamanda VPN gateway veya yönlendirici görevide yapar. Gateway veya router görevi olan bir VPN sunucu, istemci sayısının az olduğu durumlarda kullanılır (Maximum 20). VPN sunucuların sadece VPN isteklerine cevap vermesi amacıyla kullanılması tavsiye edilen bir durumdur.

3.1.2. VPN İSTEMCİLER

VPN istemciler kimlik doğrulaması yapıldıktan sonra VPN sunucuda VPN bağlantıyı başlatarak uzaktaki bir networke bağlanan uzak veya lokal makinelerdir. VPN sunucu ve istemci ancak başarılı bir log-in işleminden sonra birbiriyle haberleşebilir. Genellikle istemci tarafında yazılım tabanlı bir istemci bileşeni kullanılır. Bununla birlikte istemci tarafında dedicated bir donanımda bulunabilir. Şekilde VPN istemci profilleri gösterilmiştir:



Şekil 3.1.2.1: VPN istemci profilleri

-Evden organizasyonun kaynaklarına Internet üzerinden erişebilen çalışanlar (Telecommuter),
-Internet üzerinden organizasyonun Intranet kaynaklarına erişebilen mobil çalışanlar,
-Yönetim, monitor, problem çözme, konfigürasyon yapma amaçlı Internet üzerinden intranete erişebilen network yöneticileri.

3.1.3. VPN YÖNLENDİRİCİLER, YOĞUNLAŞTIRICILAR

Küçük çaplı bir VPN kurulumu durumunda VPN sunucu yönlendirme görevi yapar. Fakat bu durum büyük ölçekli bir VPN kurulumunda tavsiye edilmez. Büyük ölçekli VPN'lerde yönlendirici görevi yapan ayrı bir donanıma ihtiyaç vardır. Genelde, network firewall arkasında olmadığı sürece yönlendirici o ağın son noktasıdır. VPN yönlendiriciler hedef ağa doğru yolları bulmakta olup en kısa yoldan istemcinin hedef ağa erişebilmesini sağlar.
VPN teknolojisinde ayrıca Add-ons yönlendiricilerde yaygındır. Bu yönlendiriciler gerçekte bir yönlendirici değildir, normal bir yönlendiricinin LAN veya WAN arayüzüne tanımlanır ve bu yönlendiriciye tünelleme ve/veya IPSEC şifreleme ve kimlik doğrulama fonksiyonlarını ekler. Böylece bir organizasyon ek bir yönlendiriciye ihtiyaç duymadan, önceden mevcut olan yönlendiricisine Add-ons özellikler kurarak donanım maliyetini azaltmış olur.

VPN yoğunlaştırıcılar uzaktan erişimli VPN bağlantılarında kullanılır. Bu cihazlar yüksek performans ve gelişmiş şifreleme ile kimlik doğrulama yeteneğine sahiptir. Cisco'nun 3000 ve 5000 serisi VPN yoğunlaştırıcıları yaygın olarak kullanılan cihazlardır.

IP gateway'ler farklı protokolleri IP protokolüne dönüştüren cihazlardır. Bu nedenle gateway cihazları özel bir ağın IP protokolünüde desteklemesini sağlar. Bu cihazlar hem donanım hemde yazılım tabanlı olabilir. Donanım tabanlı bir gateway, genelde intranet tarafında kullanılır, yazılım tabanlı gatewaylerin kurulumu herhangi bir sunucu üzerine yapılabilir ve bu gatewayler farklı protokollerin IP protokollerine dönüştürülmesi için kullanılır. Novell firmasının Border Manager IP gateway ürünü yaygın olarak kullanılan bir yazılım tabanlı gatewaydir.

3.2. VPN YAZILIM BİLEŞENLERİ

VPN yazlımları 3 kategoride sınıflandırılabilir:

1.VPN sunucu yazılımı: VPN sunuculardа, Microsoft Windows 2000 ve Windows NT, Novell-NetWare, ve Linux işletim sistemleri kullanılabilir.
2.VPN istemci yazılımı: Bir ağ içinde VPN sunucuya istekte bulunan herhangi bir makina VPN istemci olarak nitelendirilir.
3.VPN yönetim araçları: Bu tip yazılımlar VPN yönetimi, monitor edilmesi ve problemlerin çözülmesi için kullanılır. Bu amaçla kullanılan en yaygın yazılım Novell firmasının Border Manager ve Cisco Secure Policy Manager yazılımıdır. Windows 2000'de "RRAS snapin for MMC" yazılımıda bu amaçla kullanılabilir.

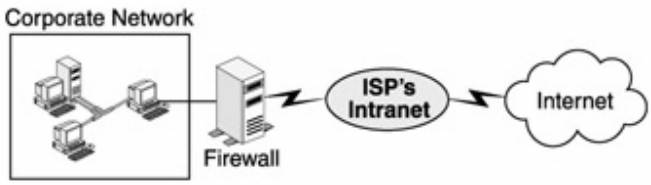
Yazılım tabanlı VPN çözümlerinin maliyeti daha düşük ve konfigürasyonları daha kolaydır. Fakat ilk kurulumları ve yönetimi zordur. Donanım tabanlı VPN çözümlerinin maliyeti yüksek fakat kurulumu ve yönetimi daha kolay olup, performansı daha iyidir. Tek bir donanımda tüm VPN bileşenleri mevcuttur.

4. GÜVENLİK

VPN teknolojisindeki güvenlik çözümleri aşağıda listelenmiştir:
-Firewall
-Network Adres Dönüştürme (NAT)
-Kimlik doğrulama sunucuları ve veritabanları
-AAA mimarisi
-IPSec protokolü

4.1. FIREWALL

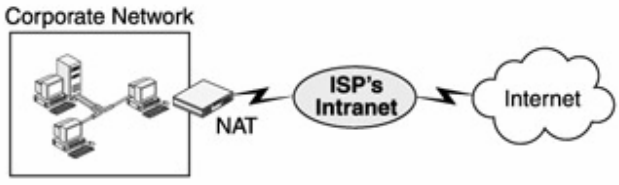
Firewall intranetteki kaynaklara, yetkilendirilmemiş kişilerin erişimini engelleyen bir set rolü oynar. IP adresleri, portların dinlenmesi, paket tipleri, uygulama tipleri ve veri içeriğine göre engelleme yapan firewallar mevcuttur. Aşağıdaki şekilde intranet içinde yer alan bir firewall görülmektedir.



Şekil 4.1: Intranet ve Internet arasındaki firewall

4.2. NETWORK ADRESİ DÖNÜŞTÜRME (NAT)

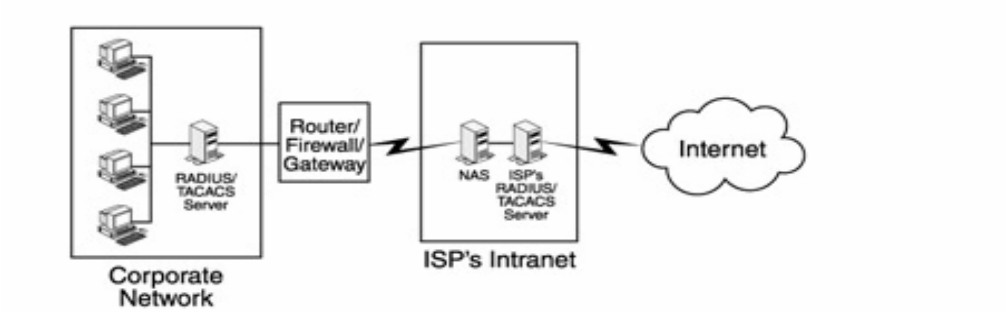
NAT tabanlı cihazlar istemciye intranetin kaynaklarının lokalde sahip oldukları IP adreslerini açığa vurmadan intranet kaynaklarına güvenli erişimini sağlar. Temel güvenliği sağlamanın yanında IP adreslerininde ekonomik olarak kullanılmasını sağlaması bir avantajdır.



Şekil 4.2: NAT yapısı

4.3. KİMLİK DOĞRULAMA

RADIUS ve TACACS kimlik doğrulama amaçlı kullanılan sunucu tipleridir. Bu donanımlar, intranet dışındaki bir istemcinin intranet kaynaklarına erişimini sağlamak için kimlik doğrulama ve yetkilendirme işlemlerini gerçekleşirir.



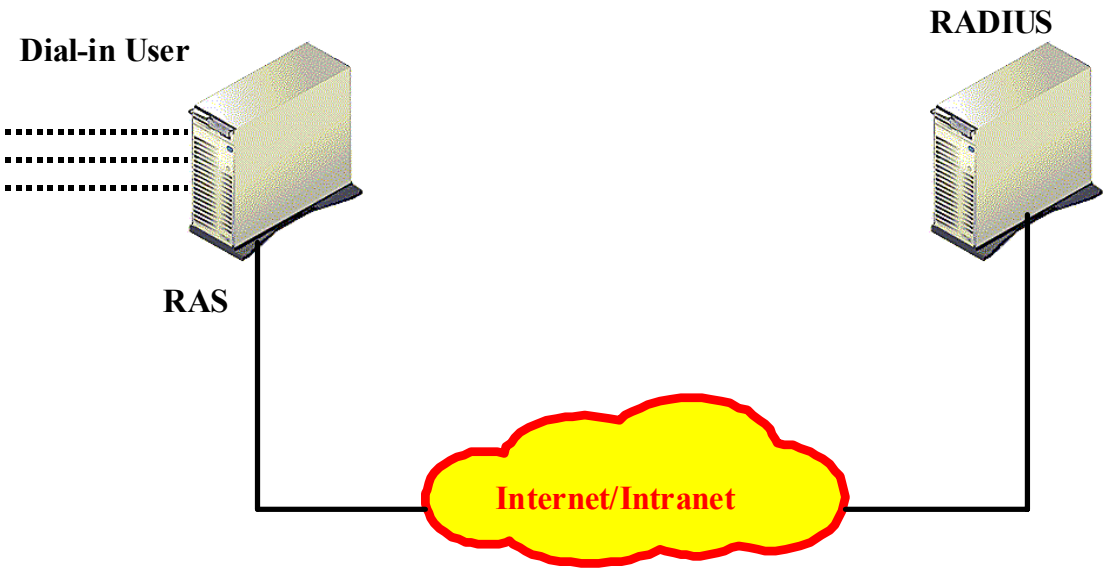
Şekil 4.3.1: RADIUS / TACACS sunucular

RADIUS uzaktan erişimli kullanıcılar ile var olan bilgisayar ağı arasında kullanıcı ID ve parola bilgilerinin güvenli olarak değiş tokuşunu sağlamakla görevlidir. RADIUS açık bir protokol standartıdır ve uzaktan erişimli kullanıcıların merkezi olarak uzaktan erişimini sağlar. RADIUS sunucu, RAS aygıtları ile birlikte çalışır. Bu birliktelikte RAS bir istemci ve RADIUS sunucu bir AAA sunucudur.

RADIUS, Livinston Enterprises (şimdi Lusent Technologies) tarafından geliştirildi ve 3COM, Assend, CISCO gibi ağ teknolojisi sağlayan firmalar tarafından kullanıldı. Pek çok uzak erişim aygıtı RADIUS ile birlikte çalışacak şekilde tasarlanmıştır.

RADIUS istemci/sunucu modeli, CHAP'a benzer yapıda girişim/yanıt protokolünün kullanımını destekler. RADIUS'un kullanılma gereksinimi derhal ortaya çıkan bir görünüm çizmemiştir. Bunun da nedeni; RAS güvenli bir kullanıcı ID 'si ve parola değiş tokuşunu sağlayan özelliğe (CHAP gibi) sahip bulunmaktaydı. RAS yalnız başına , çok az kullanıcı bilgisayar ağına ulaşma ve ağ içinde güvenli noktalara bağlanma isteğinde bulunuyorsa yeterli olabilir.

Buna karşılık pek çok kullanıcı uzaktan erişim gereksinimi gösteriyorsa ve bunların pek çoğu da kişilik belirleme makanizmasının çalışmasını gerektiriyorsa, RADIUS bu gereksinimleri çok basit bir uygulama ile çözer; kişilik belirleme geçit kapısı olarak düşünülebilir ve kapı stratejik olarak uzaktan erişim kullanıcısı ile bilgisayar ağı arasına yerleştirilir. RADIUS'un devreye giriş aşamasında ID ve parolaya sahip kullanıcıların yeniden veya ek olarak parola almalarına gerek yoktur. Zira RADIUS, direkt olarak bilgisayar ağına veya ağa uzak erişimli olarak bağlanma aşamasında parolanın kullanılmasına olanak sağlar. Bu durum özellikle parolaları düzeltmekten sorumlu ağ yöneticisi için büyük bir destektir. Bu sunucular bir kimlik doğrulama isteği aldıklarında, istemcinin lokaldeki veritabanında kayıtlı olup olmadığına bakar ve kayıtlı ise istemcinin intranete erişimine izin verir, istemci kayıtlı değilse merkezdeki veritabanına bakılır. İstemcinin kimlik doğrulaması yapıldıktan sonra RADIUS sunucu ISP tarafındaki NAS (Network Access Server) ile haberleşir, VPN bağlantısı kurulur veya reddedilir.

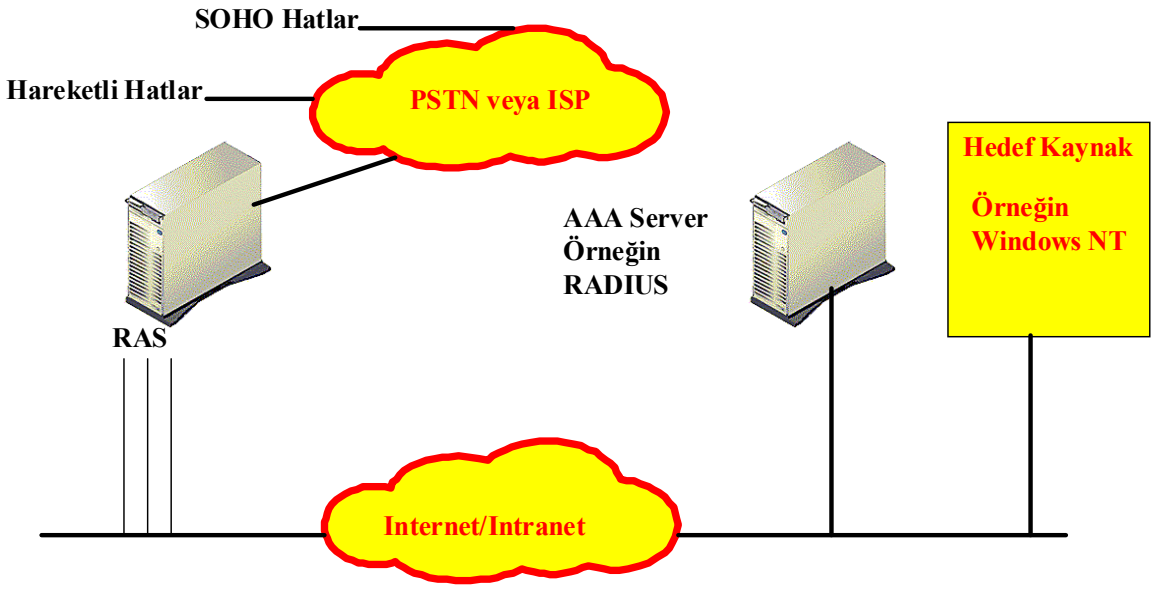


Şekil 4.3.2: RAS sunucu

4.4. AAA

Authentication Authorization Accounting (AAA) lokal kaynaklara erişim için kullanılan bir diğer kimlik doğrulama ve yetkilendirme mekanizmasıdır. RADIUS/TACACS sunucular ile birlikte kullanılan bir tamamlayıcı yapıdır. AAA uzaktan erişim ile ilgili aşağıdaki sorgulamaları yapar:
Networke kim erişmek istiyor?
İstemci networke eriştiğinde hangi yetkilere sahip olacak?
Kullanıcı ağ içinde hangi işlemleri yapmış ve bu işlemleri ne zaman gerçekleştirmiş?

NAS ISP tarafında bulunduğu durumda, uzaktan bağlantı isteğini alır, bu isteği organizasyon tarafında bulunan AAA sunucuya iletir. Bu sunucu istemcinin kimlik doğrulamasını gerçekleştirir veya reddeder, kimlik doğrulanmışsa istemcinin ağda hangi yetkilere sahip olduğunu belirler. Eğer istemci ağda yetkisi dahilinde olmayan bir işlem yapmak isterse bu istek reddedilir ve istemciye uyarı mesajı verilir. Şekilde AAA yapısı görülmektedir:



Şekil 4.4: VPN-AAA yapısı

Şimdi uygulamayı adım adım izleyelim :
Adım-1 : Kullanıcı RAS 'a bağlantı kurar,
Adım-2 : AAA , RAS ile ilişki kurar,
Adım-3 : AAA , RAS 'a yanıt verir,
Adım-4 : Hedef kaynağa ulaşım onaylanır.

AAA; kimlik doğrulama, yetkilendirme ve muhasebe işlemlerinin kombinasyonudur. Aşağıda bu işlemler anlatılmaktadır:

4.4.1. KİMLİK DOĞRULAMA

Kimlik doğrulama, uzaktan erişim söz konusu olduğunda en önemli fonksiyondur. Güçlü bir kişilik belirleme olmaksızın ağa erişimin kontrol altına alınması olanaksızdır ve bunun sonucu olarak kurumsal bilgilerin yetkilendirilmemiş kişilerin eline geçmesi çok kolay olacaktır.

En yaygın kullanılan kimlik doğrulama yöntemi Tek Uygulamalı Parola (One-Time-Password-OTP) dır. Kimlik doğrulama kullanıcı ağın RAS veya yönlendiricisine ulaştığında çalışmaya başlar. Bazı durumda kullanıcı aynı anda bir diğer kısıtlı alana ulaşmak ister, bu durumda ek bir kişilik belirleme uygulaması gerekmektedir. VPN de kişilik belirlemede kullanılan en etkin yöntem iki-faktörlü kişilik belirlemedir. Bu yöntemde ID/Parola kontrolüne ek olarak kişiyi belirlemek için ikinci bir eleman devreye alınır.

Bu uygulama ATM işlemlerine benzetilebilir. Birinci kontrol makinaya okuttuğunuz kart üzerinden yapılır. İkinci kontrol için kişisel ID numarası (PIN-Personel ID-Number) kontrolü devreye girer.

4.4.2. YETKİLENDİRME

Kimlik doğrulama ile yetkilendirmenin sınırı her zaman kesin çizgilerle belli değildir. Yetkilendirme genellikle kimlik doğrulama işlemini izleyerek uygulanır, ancak kimlik doğrulama gerekli değilse birinci uygulama olarak devreye girer. Örneğin WEB sayfasında herkesin kullanımına açık bilgiler gibi verilere ulaşma durumunda yani kimlik doğrulamaya gereksinim duyulmayan durumlarda ve kullanılan ağ servisi gerekli desteği sağladığı durumlarda yetkilendirme işlemi yeterli olacaktır.

4.4.3. MUHASEBE

İş hayatında muhasebe (Accounting) kurumun finansal kayıtlarını yürütmek ve denetlemek amacı ile kurulmuş olan teori ve sistemlerdir. VPN dünyasında iş hayatında olduğu gibi muhasebenin işlevi aynıdır. VPN istemcilere ait kayıtları ve sistemle ilgili hareketleri, faturalama ve güvenlikle ilgili raporların üretilmesi amacı ile tutulmaktadır.

Muhasebe, kullanıcıların ağın hangi noktasından, ne sıklıkla ve ne kadar süre ile işlem yaptığını belirler. Muhasebe işlemi genellikle kimlik doğrulama ve yetkilendirme işleminden sonra gerçekleştirilir, ancak bu iki işlemle her hangi bir bağı yoktur.

5. PUBLIC AĞLAR

Internet bir public network olarak nitelendirilir. Fakat başka public networklerde mevcuttur. Public networklerin listesi aşağıda görülmektedir.

1.POTS (Plain Old Telephone Service): POTS günlük yaşantımızda kullandığımız sabit telefon servislerini sağlayan ağdır. POTS ve POTS olmayan servisler arasındaki temel fark iletim hızıdır. POTS ağlarda en yüksek iletim hızı 56 Kbps'dir.
2.PSTN (Public Switched Telephone Network): PSTN bakır kablo altyapısı üzerinden telefon servislerini sağlayan bir analog teknoloji olup son zamanlarda ADSL, DSL, ISDN, FDDI, Frame Relay ve ATM gibi dijital teknolojilerdede kullanılmaya başlanmıştır
3.Internet: Internet networkü POTS ve PSTN altyapısını kullanır. Bu iki networkden farkı tüm haberleşmeleri konrol etmek ve yönetmek için TCP/IP protokolünü kullanmasıdır.

Public networkler hızlı iletimler için farklı teknolojiler kullanır. Bu teknolojiler aşağıda görülmektedir:
-ADSL (Asymmetric Digital Subscriber Line) : ADSL, PSTN altyapısını kullanarak yüksek hızda dijital veri iletimi sağlar. ADSL, 64 Kbps ve 8 Mbps arasındaki bandgenişliklerini destekler.
-FDDI (Fiber Distributed Data Interface) : FDDI, dijital sinyalleri fiber optik altyapı üzerinden ileten bir LAN teknolojisidir. Veri iletiminde jeton yapısını kullanır. Genelde WAN omurgasında kullanılır. FDDI'in son versiyonu olan FDDI-2'de audio ve video sinyallerinin iletimi daha başarılı olmaktadır.
-ISDN (Integrated Services Digital Network) : Bakır altyapı üzerinden ses, video ve data iletimini fiber altyapı kadar başarılı bir şekilde yapabilen teknolojidir. ISDN, modem yerine uçlarda ISDN adaptör (CSU/DSU) kullanır. ISDN'de BRI ve PRI olmak üzere 2 tip servis vardır. BRI ev kullanıcıları için uygun bir servistir, PRI ise daha çok kurumsal amaçlı

kullanılan bir servistir. ISDN'de 2 tip kanal vardır. B kanalı, data, ses ve diğer sinyalleri taşırken D kanalı kontrol ve sinyalleşme bilgisini taşır. Günümüzde genişband bir ISDN teknolojisi olan B-ISDN yaygın olarak kullanılmaktadır. Aynı kanal üzerinden farklı tipte sinyal gönderme yeteneğine sahiptir ve 1.5 Mbps hızı destekleyebilmektedir. ISDN BRI, 2 adet 64 Kbps B kanalına ve bir adet 16 Kbps D kanalına sahiptir. Bundan dolayı 144 Kbps 'lik bir kapasiteye sahiptir. PRI ise 30 adet B kanalı ve 1 adet D kanalına sahiptir ve yaklaşık 2 Mbps kapasiteye sahiptir.

-Frame Relay : X25 paket anahtarlama teknolojisine dayanır. LAN ağından WAN ağına veri trafiğini taşıyan düşük maliyetli bir çözümdür. Veri transferi için farklı boyutlarda frame'ler kullanılır. Ayrıca kendi içinde hata kontrol mekanizmasıda mevcuttur. FR veri iletiminde PVC ve VCC olmak üzere 2 tip devre kullanır. Bu devreler uç kullanıcıya düşük maliyetli dedicated bağlantı imkanları sağlar.

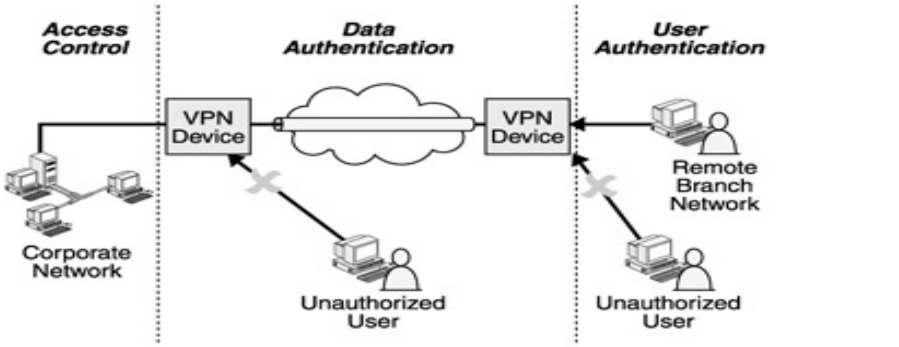
-ATM (Asynchronous Transfer Mode) : ATM, audio, video ve veri sinyallerini dijital iletim ortamından ileten PVC tabanlı bir anahtarlama teknolojisidir. 155 Mbps ve 10 Gbps arasındaki bandgenişliklerini destekler. Veriyi 53 byte uzunluğundaki hücre formunda karşı tarafa iletir. ATM'de CBR, ABR, VBR ve UBR olmak üzere 4 çeşit servis vardır. CBR, kullanıcıya bandgenişliğini garanti eder, ABR trafiğe bağımlı olarak bandgenişliğini belli zamanlarda garanti eder, VBR video konferans uygulamalarında kullanıır. UBR servisinde bandgenişliği garanti edilmez.

6. VPN GÜVENLİĞİ

Internet çok güvenli bir iletim ortamı değildir. VPN teknolojisindeki tünelleme işlemi ile bu ortamdaki risklerin önüne geçilebilmektedir.

6.1. KİMLİK DOĞRULAMA VE ERİŞİM

Güvenlik açıklarını engellemek için en temel işlem kimlik doğrulama ve yetkilendirmedir. Şekilde bir VPN senaryosunda kimlik doğrulama işlemi gösterilmektedir.



Şekil 6.1: VPN senaryosunda kimlik doğrulama

6.2. ERİŞİM KONTROLÜ

Kullanıcıların network kaynaklarına erişimi aşağıdaki kontrollerle sağlanır:

-Login ID ve şifre: VPN erişiminde kullanıcı tanımlanması için İşletim sistemi tabanlı login ID ve şifre sorgulaması yapılır.

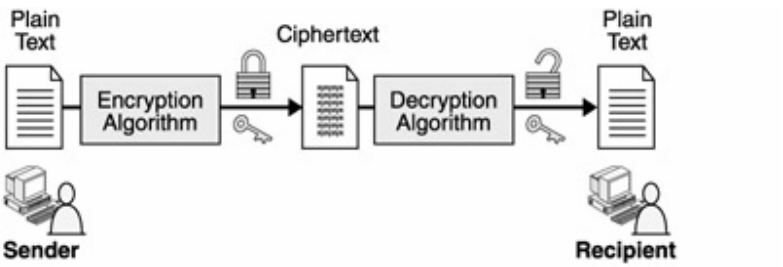
-S/Key şifresi: Kullanıcı şifreyi girişinde kullanıcıya S/KEY ve bir parametre atanır. Bu parametre, şifre için tanımlanan MD4 (güvenli hash fonksiyonu) sayısını belirtir ve sunucuda kaydedilir. İstemci login olmayı denediğinde istemci tarafındaki yazılım şifreye hash fonksiyonunun n-l iterasyonunu uygulayıp sonucu sunucuya gönderir. Sunucu bu cevaba hash fonksiyonunu uygular. Eğer sonuç daha önceden sunucuya kaydedilen sonuç ile eşleşirse istemcinin kimlik doğrulaması başarılı bir şekilde gerçekleşmiş olur ve sunucu daha önceden kayıtlı olan parametreyi istemcinin cevabı ile değiştirir ve şifre sayıcı sistemin değerini bir azaltır.
-RADIUS (Remote Access Dial-In User Service): RADIUS, istemci/sunucu modeline dayanan bir Internet güvenlik protokolüdür. Genelde RADIUS sunucu istemciyi kullanıcı adı ve şifre ile yetkilendirir. Veri güvenliği için istemci ve RADIUS sunucu arasındaki işlem, kimlik doğrulama mekanizması (PAP, CHAP) kullanılarak şifrelenebilir.
-2 faktörlü jeton tabanlı teknik: Kullanıcı bilgilerinin doğrulanması için iki tane kimlik doğrulama aşaması vardır. Kimlik sorgulanması esnasında cihazlar bir jeton ve şifre rolü oynar. Bu tekniği ATM cihazlarından para çekme işlemine benzetebiliriz. ATM kartımızla kimliğimizi siseme tanıtır ve şifre sorgulamasında doğru şifreyi girersek ATM sisteminden başarı ile para çekebiliriz. Sadece bu iki faktör sağlandığı zaman sistemden kendi hesabımıza ulaşabiliriz.

Bir istemcinin kimlik doğrulaması başarıyla yapıldıktan sonra istemci network dahilindeki tüm kaynaklara erişim yetkisi kazanmış olur, buda güvenlik açısından bir tehdittir. Çünkü istemci bilinçli olarak yada olmayarak sistemlerdeki verilerde değişiklik yapabilir. Bu güvenlik açığıda istemcilere limitli yetkiler verilerek kapatılabilir. Örneğin sadece admin olanlar sistemlerde yazma yetkisine sahip olup diğer istemciler sadece okuma yetkisiyle sistemlere erişebilirler.

Erişim kontrolü kullanıcının tanımlanması ile yapılır, bunun yanında kaynak ve hedef IP adresi ve port adresleri, tarih, servis, uygulama ve URL gibi parametrelerle erişim kontrolleride vardır.

6.3. VERİ ŞİFRELENMESİ

Veri şifreleme (kriptolama), veriyi “ciphertext” olarak bilinen anlaşılamayacak bir formata dönüştürme mekanizmasıdır. Böylece iletim esnasında veriler yetkisiz erişimlere karşı korunmuş olur. Data şifrelenmesi ile iletim kayıplarının ve verinin değişikliğe uğramasının önüne geçilmiş olur. Şekilde şifreleme modeli görülmektedir:



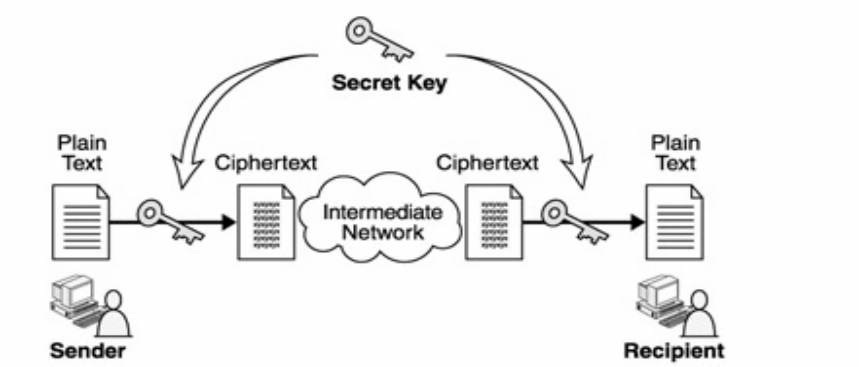
Şekil 6.3: Şifreleme modeli

Gönderen ve alan tarafta simetrik veya asimetrik şifreleme tekniği kullanılır. Şifreleme tekniği (kripto sistemi) kullandıkları anahtarlara göre kategorize edilebilir. Bu anahtar, şifreleme ve çözümleme amaçlı kullanılır ve bir sayı veya kelime formatında olabilir.

6.4. SİMETRİK KRİPTO SİSTEMLER

Sabit uzunlukta bit dizisinden oluşan tek bir anahtar kullanılır. Bundan dolayı bu sisteme "tek anahtarlı şifreleme" de denir. Anahtar gizlidir ve şifreleme ile çözümleme işleminde görev alır.

Her iki taraftada veri iletilmeden önce, anahtar iki taraf arasında paylaşılır. Gönderen taraf bu özel anahtarı kullanarak orjinal veriyi şifreler ve karşı tarafa gönderir. Veri karşı tarafta şifreli formatta alındığında, aynı anahtar kullanılarak verinin şifesi çözümlenir. Şekil'de simetrik kripto tekniği görülmektedir:



Şekil 6.4: Simetrik kripto tekniği

Anahtar değişim tekniklerinin tam anlamıyla güvenli olabilmesi için anahtarın mümkün olduğunca uzun bir formatta olması gerekmektedir. Daha uzun bir anahtarın şifrelenmesi, çözümlenmesi ve kırılması zorlaşır, böylece yetkisiz istemciler anahtarı ele geçirdiklerinde kullanamazlar yani güvenlik sağlanmış olur. Anahtarın uzunluğuna bağlı olarak birçok simetrik şifreleme algoritması geliştirilmiştir. Aşağıda VPN çözümlerinde yaygın olarak kullanılan simetrik şifreleme algoritmaları görülmektedir:

6.4.1. DES (Data Encryption Standard): DES tekniği 128 bite kadar anahtar uzunluğunu destekler. Fakat bu sayı algoritmanın daha hızlı olabilmesi için 56 bite düşürülmüştür. Bu sayının azaltılmasıyla bu teknik "Brute Force" ataklarına karşı açık hale gelmiştir. Bu tip ataklarda, rastgele bir anahtar üretilir ve doğru anahtar belirlenene kadar orjinal veriye uygulanır. Anahtar ne kadar kısa olursa, bu anahtarı tespit etmek ve kripto sistemini kırmak o kadar kolaylaşır.

6.4.2. 3DES (Triple Data Encryption Standard): 56 bit'lik anahtarlar kullanılır. DES tekniğine göre daha güvenlidir çünkü veriyi şifrelemek için 3 farklı anahtar kullanır. Birinci anahtar veriyi şifreler, ikinci anahtar bu şifreyi dekript eder, üçüncü anahtarda bu veriyi ikinci bir defa şifreler. Bu teknik DES tekniğine göre daha güvenli fakat 3 kat daha yavaştır.

6.4.3. RC4 (Ron's Code): 256 byte'a kadar anahtar uzunluğunu destekler. Hızlı ve güvenli bir şifreleme tekniğidir. Rastgele byte dizisi üretir ve sonuç ile orjinal veri arasında XOR işlemi yapar.

Simetrik kripto sistemlerde 2 temel problem vardır. Birincisi şifreleme amacıyla tek bir anahtar kullanılması, diğer problem bağlantı sayısının fazla olması durumunda anahtar yönetiminin zorlaşmasıdır. Ayrıca, istemciye ilk anahtar atanması ve peryodik anahtar değişimleri zaman kaybı ve yüksek maliyete sebep olmaktadır.

Asimetrik kripto sistemlerde bu tip problemler meydana gelmez, ayrıca daha yüksek güvenlik sağlar.

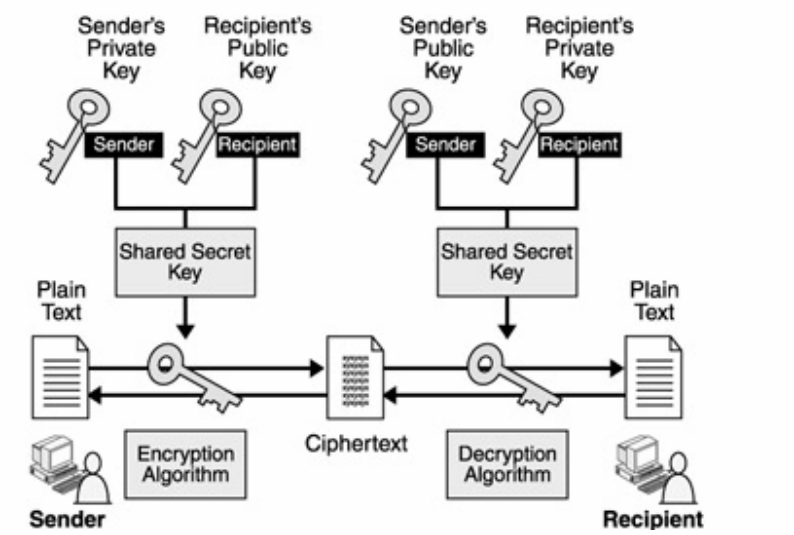
6.5. ASİMETRİK KRİPTO SİSTEM

Asimetrik sistemlerde anahtar çiftleri kullanılır. Bu anahtarlardan biri sadece istemcinin bildiği özel bir anahtar, diğeri ise public bir anahtardır. Public anahtar şifreleme amaçlı kullanılır, özel anahtarlar ise şifeli mesajları çözümlemek için kullanılır. Asimetrik kripto sistemler genelde "public key kripto sistem"ler olarak bilinir. VPN çözümlerinde daha çok Diffie-Hellman (DH) ve Rivest Shamir Adleman (RSA) asimetrik kripto algoritmaları kullanılır.

6.5.1. DIFFIE HELLMAN ALGORİTMASI

Her bir bağlantı, bir tanesi public, diğeri özel olmak üzere bir anahtar çifti alır. Aşağıda bu algoritmanın çalışma mantğı anlatılmıştır:
1. Gönderen taraf istemcinin tüm bağlantılarında kullanacağı public anahtarını öğrenir.
2. Gönderen taraf özel anahtar ve istemcinin public anahtarını birleştirerek bir hesaplama yapar ve bu hesabın sonucu ortak gizli bir anahtarda saklanır.
3. Mesaj bu ortak gizli şifre kullanılarak şifrelenir.
4. Şifrelenmiş mesaj istemciye gönderilir.
5. Şifreli mesaj alındığında, istemci kendi özel anahtarı ve gönderen tarafın public anahtarı ile bir hesaplama yapar gizli anahtarı üretir.

Bu algoritmanın temel mantığı, yetkisiz bir istemci şifreli mesajı ele geçirse bile özel anahtar saklı olduğu için orjinal bilgiye ulaşamayacak olmasıdır. Şekilde bu algoritma gösterilmektedir:



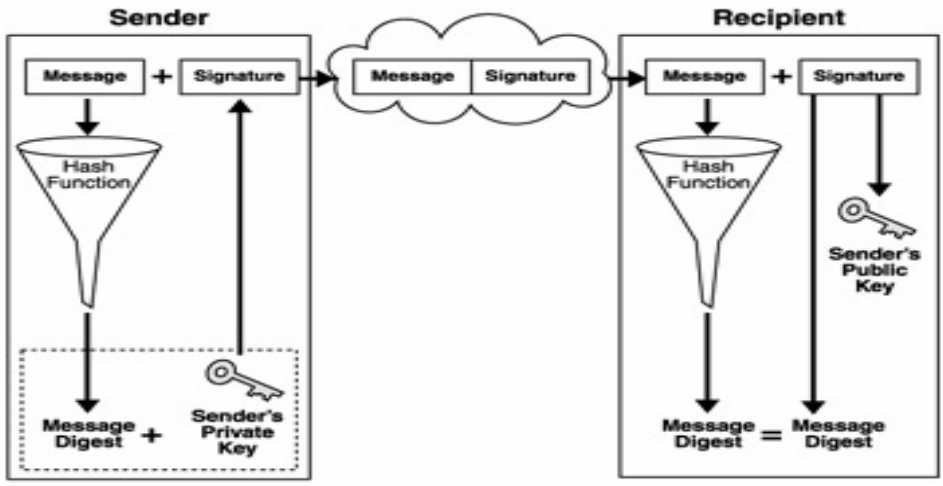
Şekil 6.5.1: Diffie-Hellman algoritması

6.5.2. RSA ALGORİTMASI

Diğer teknikten farklı olarak istemcinin public anahtarı kullanılarak şifreleme yapılır. İstemci gönderen tarafın public anahtarını kullanarak orjinal mesajı elde eder. Dijital imza kullanarak kimlik doğrulaması yapan RSA algoritmasının çalışma mantığı aşağıdaki gibidir:

-İstemci taraf, bilgi gönderecek olan taraftan public anahtarını öğrenir.
-Gönderen taraf orjinal mesajın boyutunu azaltmak için bir hash fonksiyonu kullanır. Elde edilen sonuç MD (Message digest) olarak bilinir.
-Gönderen taraf özel anahtarla MD mesajı şifreler ve dijital bir imza üretilmiş olur.
-Dijital imza ile mesaj istemci tarafına iletilir.
-Şifreli mesaj istemciye iletildiğinde, istemci MD mesaja hash fonksiyonunu uygular ve istemci, gönderen tarafın public anahtarını kullanarak dijital imzayı çözümler. Bu iki sonucu karşılaştırır ve eşleşme sağlanırsa veri iletilmeye devam eder, sağlanmadığı durumda ise bağlantı sona erer.

Aşağıdaki şekilde RSA algoritması görülmektedir.



Şekil 6.5.2: RSA algoritma mantığı

İstemci taraf verinin doğruluğunu 3 aşamada konrol ettiğinden RSA daha güvenli bir veri iletimi sağlar. Ayrıca bu teknikte anahtar yönetimi daha kolaydır.

6.6. PUBLIC ANAHTAR YAPISI

PKI veri iletiminde güvenli bir bağlantı kurma ve anahtar yönetimi politikalarını belirler. Dağıtık sistemlerde açık anahtarlar (public key) ve X.509 dijital sertifikaların kullanımını sağlayan güvenlik hizmetleri kümesidir. Açık anahtar altyapısı (PKI) kişilerin sahip olduğu açık ve özel anahtarları kullanarak oluşturulan bir bilgi altyapısıdır. Açık anahtar altyapısının temel görevi, Internet/intranet üzerinde haberleşen, çalışan kişiler veya kurumlar arasında güvenilen dijital birimler oluşturmaktır.
Açık anahtarlı şifreleme sisteminde açık anahtar ve özel anahtar bulunmaktadır. Bu anahtarlar tek yönlü çalışmaktadırlar fakat birbirlerini tam
amlarlar. Açık anahtar şifrelemek için, özel anahtar da açık anahtarın şifrelediğini deşifre etmek icin kullanılır. Özel anahtar sadece ait olduğu kişide bulunmakta ancak açık anahtar ceşitli şekillerde insanlara iletilebilmektedir, yani açık olarak dağıtılır. Bu altyapıda anahtarların oluşturulması, yetkili bir kurum tarafından onaylanması, sertifikaların saklanması ve dağıtılması, gerektiği durumlarda onayın geri alınması, sonlandırılması gibi işlemler vardır. PKI tekniği organizasyon çapında, ülke çapında veya zon çapında kullanılabilir. PKI fonksiyonları aşağıda anlatılmaktadır:

-PKI istemciler için özel ve public anahtar üretir.
-Dijital imzaları üretir ve bu imzaların doğrulanmasını sağlar
-Yeni kullanıcıların kaydını ve kimlik doğrulamasını yapar.
-Her bir anahtarın geçmiş değerlerini kaydeder ve tutar.
-Geçersiz olan ve süresi dolan kullanıcıların sertifikalarını iptal eder.

6.6.1. PKI BİLEŞENLERİ

-PKI istemci
-CA (Certification Authority)
-RA (Registration Authority)
-Dijital sertifikalar
-CDS (The Certificate Distribution System)

PKI istemci CA veya RA sisteminde tanımlı olan bir dijital sertifikaya sahip olur. PKI istemci CA veya RA'dan sertifika alır ve bu sertifikayı dijital bir kimlik olarak kullanır.

6.6.1.a. Certification Authority (CA)

CA, PKI istemcilerin dijital kimlikleri olan sertifikalarını sağlar, günümüzde yaygın olarak kullanılan CA Verisign'dır.

6.f.1.b. Registration Authority (RA)

CA'daki dijital sertifika istekleri yoğun sayıda olduğunda, CA bazı istekleri RA'ya yönlendirir. Bu durumda RA istekleri alır ve sertifikaları geçerli hale getirir. RA kullanıcıların sertifikalarını tanımladıktan sonra istekleri CA'ya gönderir ve CA kullanıcıların sertifikalarını RA' ya iletir. Bu durumda RA, PKI istemciler ve CA arasında görev yapar.

6.f.1.c. Dijital Sertifikalar

Sertifikalar temel olarak açık anahtar için bir taşıyıcı görevi görürler. Ancak açık anahtardan daha fazla belirleyici bilgiye sahip oldukları için çok daha işlevseldirler. Dijital sertifikalar, sahibinin anonim anahtarını, adını, son kullanma tarihini, dijital sertifikayı hazırlayan sertifika mercii'nin adını, seri numarasını e-posta adresini ve diğer bazı bilgileri içerir.
Dijital sertifikalar ID kartların elektronik ortamdaki eşleniğidir. Aynı zamanda dijital ID, dijital pasaport, X.509 sertifikası ve public anahtar sertifikası olarakta isimlendirilirler.
Dijital sertifika aşağıdaki bilgileri içerir.
-Sertifikanın seri numarası
-Sertifikanın süresi
-CA dijital imzası
-PKI istemcinin public anahtarı
Gönderici taraf kendi kimliğini belirtmek için karşı tarafa şifreli mesajla birlikte dijital sertifikasını gönderir. İstemci taraf aldığı mesajın içinde mevcut olan göndericinin public anahtarının geçerliliğini CA'nın public anahtarını kullanarak tespit eder. İstemci taraf gönderici tarafın kimlik doğrulamasını yaptıktan sonra, istemci taraf mesajı çözümlemek için gönderen tarafın public anahtarını kullanır.

6.6.1.d. CDS (Certificate Distribution System)

CDS public anahtarların geçerliğini sağlar, anahtarları üretir, anahtarların kaydını tutar ve süresi dolmuş anahtarları iptal eder.

6.6.2. PKI TABANLI KİMLİK DOĞRULAMA

1. Anahtar çiftinin tanımlanması : Gönderen taraf istemciye veri iletirken her iki taraf içinde bir özel ve birde public anahtar tanımlanır. İlk önce özel anahtar tanımlandıktan sonra bu anahtara hash fonksiyonu uygulanarak public anahtar üretilir. RSA tabanlı iletimlerde olduğu gibi PKI iletimlerdede özel anahtar mesaja eklenir, public anahtar ise bu imzanın doğruluğunu tespit eder.

2. Dijital İmza tanımlanması: Anahtar çifti tanımlandıktan sonra, dijital imza tanımlanır. Bu imza gönderen tarafın kimliğini tanımlar, dijital imza tanımlanması için orjinal mesaja hash fonksiyonu uygulanır. Bu işlemin sonucunda MD mesaj üretilmiş olur ve bu mesaj gönderen tarafın özel anahtarı ile şifrelenir ve bu şifreli mesaj dijital imza olarak isimlendirilir.

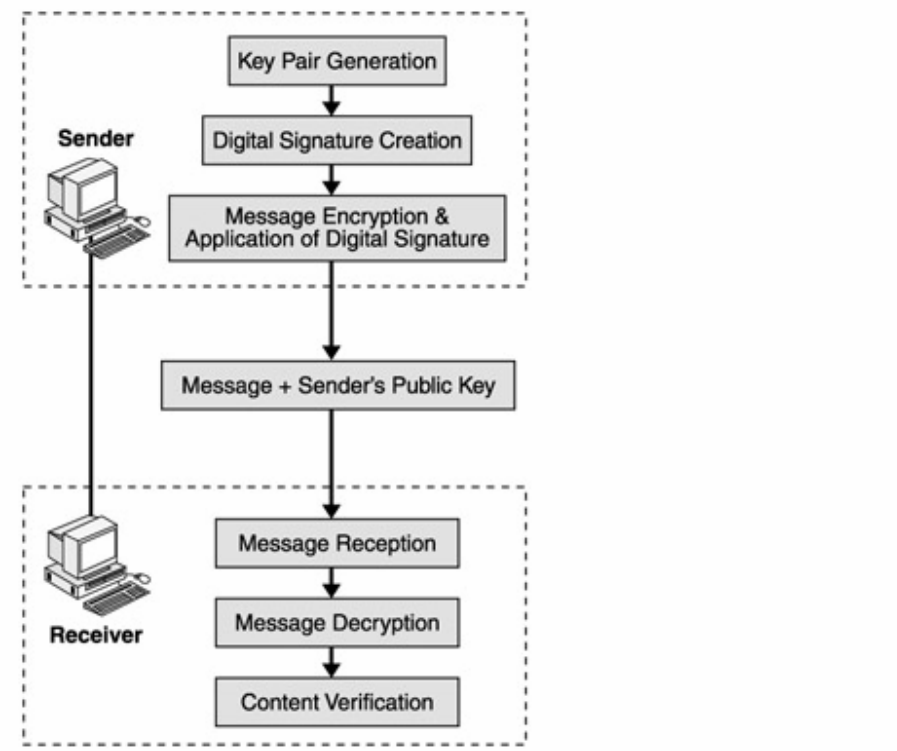
3. Mesaj şifreleme ve dijital imza uygulaması: Dijital imza türetildikten sonra orjinal mesaj, gönderen tarafın public anahtarı ile şifrelenir.

4. Şifrelenmiş mesaj ve gönderen tarafın public anahtarı : Şifrelenmiş mesaj gönderen tarafın public anahtarı ile birlikte istemciye iletilir. Public anahtar istemciye gönderilmeden önce istemcinin public anahtarı ile şifrelenir ve karşı tarafta bu şifrenin çözümlenebilmesi için istemci kendi özel anahtarını kullanır. Gönderen tarafın anahtarı aynı zamanda oturum anahtarı olarakta bilinir.

5. Gönderen tarafın kimlik doğrulaması : Şifrelenmiş mesaj ve public anahtar iletildiğinde, istemci göndericinin kimlik doğrulamasını yapmak için CA parametresine bakar. Dijital imza başarı ile doğrulanırsa, istemci mesajı çözümler, kimlik doğrulaması yapılamazsa alınan mesaj reddedilir ve VPN bağlantısı sonlandırılır.

6. Mesaj çözümlemesi : Gönderen tarafın kimlik doğrulaması yapıldıktan sonra istemci özel anahtarını kullanarak gönderen tarafın public anahtarını elde eder ve ardından mesajı çözümler.

7. Mesaj içeriği doğrulaması : Son olarak istemci alınan mesajın içeriğine bakar, gönderen tarafın public anahtarını kullanarak dijital imza çözümlenir ve MD mesajı elde edilir. Çözümlenmiş olan mesaja hash fonksiyonu uygulanır ve yeni bir MD mesaj türetilir. İletilen MD ve yeni türetilmiş olan MD karşılaştırılır.



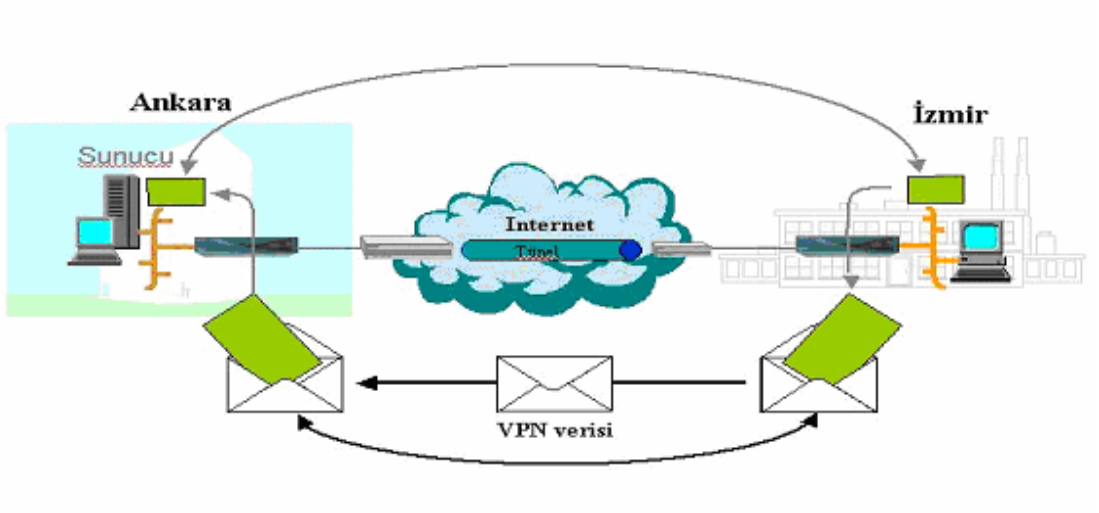
Şekil 6.6.2: PKI tabanlı iletim

7. TÜNELLEME TEKNİĞİ

VPN, şifreleme, kişilik belirleme ve yetkilendirme uygulamaları ile güvenliği sağlamak üzere geliştirilmiş bir ağ modelidir. Ancak tam bir güvenliğin sağlanması için VPN ayrıca tünelleme protokollerini kullanır. Bu protokoller Internet temelli VPN kullanıcılarına tam anlamı ile güvenli bir ortam sağlamayı garanti etmektedir. Bu son nokta genellikle LAN da veya kullanıcı ana sistem aygıtlarında özel gateway veya sunuculardır.

7.1. TÜNELLER NE YAPAR?

Tünelleme VPN teknolojisinde en önemli işlemdir. Bu teknik organizasyonlara Internet üzerinden kendi sanal networklerini oluşturma imkanı sağlar. Intranet dışından hiç bir yetkisiz kullanıcı intranete erişim yetkisine sahip değildir.



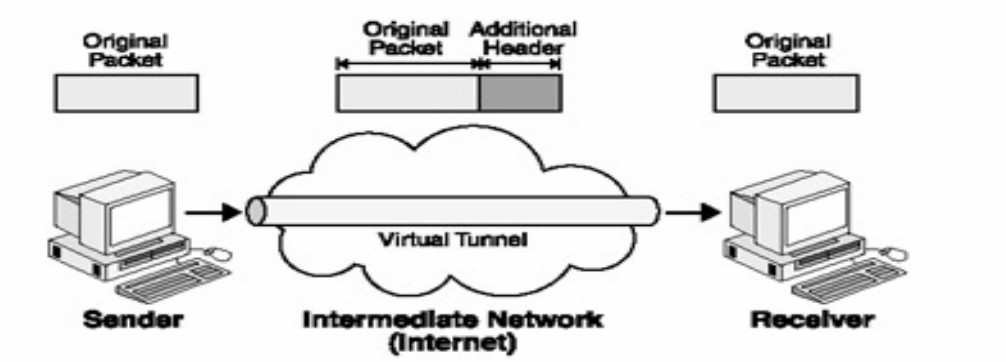
Şekil 7.1: Basitçe bir VPN tünel

Tünelleme tekniğini mektup gönderme işlemine benzetebiliriz. Şekil 7.1'de görülen İzmir'deki VPN yoğunlaştırıcıda (concentrator) mesaj kriptolanır, sonra gönderilmek üzere kapsüllenir. Bu kapsülleme sırasında, mesaj bir "zarf" içine yerleştirilir ve Ankara VPN yoğunlaştırıcısına doğru adreslenir. Ankara VPN yoğunlaştırıcısı mesajı aldığında en dıştaki zarfı yok eder ve verinin kriptosunu çözer ve mesajı hedef sunucuya aktarır. Tünelleme tekniğindede payload mesajı mektuba benzetebiliriz ve zarfda payload mesajı enkapsüle eden protokoldür. Zarfın üzerindeki adres bilgiside pakete eklenen yönlendirme bilgisidir.

Tünellemede paket hedef networke iletilmeden önce bu pakete tünelleme protokolünün başlık bilgisi eklenir. Payload olarakda isimlendirilen orjinal paket internetin desteklemediği bir protokolü kullanıyor olabilir, bu durumda tünelleme protokolü tünel içindeki pakete başlık bilgisini 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 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.

VPN tünelleri tarafından hedeflenen güvenlik seviyesinin gerçekleşmesi için, tüneller çok dikkatli oluşturulmalıdır.Tüneller iki grup altında toplanabilir. Bazıları sabit olarak kurulurken, bazıları ihtiyaç durumunda oluşturulabilir. Class-C IP adres alanı için en fazla 256 tünele izin verilmektedir. Tünel kurulduğunda, tünel aygıtları bilgi (kullanıcıya ait parola, şifreleme metotları ve anahtarlar ve tünelleme protokolleri ve ayrıca paketlere ait birbirini izleyen numaralar, paket belirleyiciler, kaynak ve varılacak ağ adresleri vb.) alışverişini başlatır.
Paket hedef noda yönlendirildiğinde, Internet üzerinde mantıksal bir yoldan iletilir. Bu mantıksal yol tünel olarak isimlendirilir. Alıcı taraf tünellenmiş paketi aldığında tekrar paketi orjinal formatına dönüştürür. Şekilde tünelleme işlemi görülmektedir.



Şekil 7.1.2: Tünelleme tekniği

7.2. TÜNELLEMENİN AVANTAJLARI

-Kolay tanımlanması
-Güvenlik: Bir tünel yetkisiz kişilerin erişimine kapalıdır, bundan dolayı tünel içinden iletilen veri, her ne kadar Internet gibi güvensiz bir ortamdan iletilsede güvendedir.
-Düşük maliyet: Tünelleme iletim ortamı olarak Interneti kullandığı için özel ağlar yada kiralık devrelere kıyasla düşük maliyetli bir çözümdür.
-Protokolden bağımsızdır: NetBIOS ve NetBEUI gibi yönlendirme özelliği olmayan protokoller TCP-IP ile uyumlu değildir. Bu nedenle bu tip paketler Internet üzerinde yönlendirilemezler. Fakat tünelleme ile IP olmayan paketlerde Internet üzerinden iletilebilir.
-IP adresi ekonomisi : Tünelleme, IP desteği olmayan paketlerin, IP adresi kullanan pakatlere eklenerek Internet üzerinden iletilmesini sağlayabilir. Böylece network dahilindeki her bir noda IP adresi atanmasına gerek kalmaz, küçük bir IP bloğu ile VPN networkü kurulabilir.

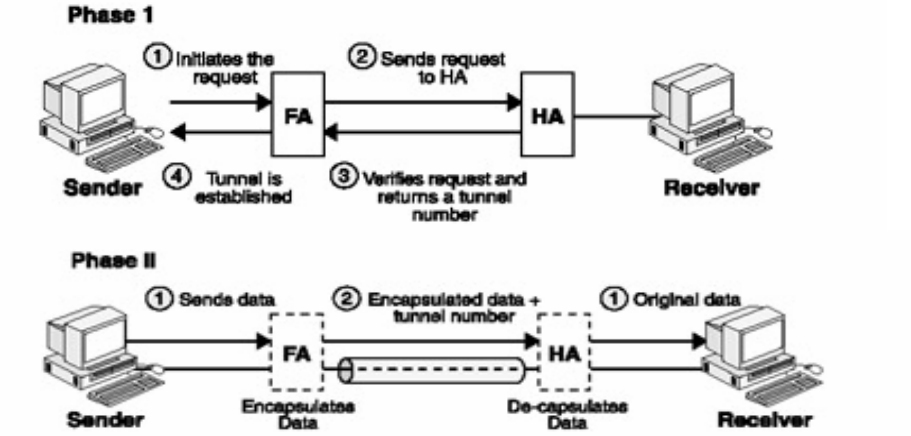
7.3. TÜNELLEME TEKNİĞİNİN BİLEŞENLERİ

Bir tünel kurulabilmesi için 4 bileşene ihtiyaç vardır:
1. Hedef network: İstemcinin erişmek istediği kaynakları bulunduran ağdır.
2. İstemci nod: VPN bağlantısını başlatan istemci veya sunucudur, lokal networkün bir parçası veya laptop kullanan mobil bir çalışan olabilir.
3.HA (Home Agent): VPN isteklerini alır ve bu isteklerin kimlik doğrulamasını gerçekleştirir. Kullanıcıyı yetkilendirdikten sonra tünel kurulmasına izin verir.
4. FA (Foreign Agent): Hedef network tarafındadır, HA sisteminden VPN isteklerini alır.

Tünel tekniğini 2 fazda anlatabiliriz:
Faz1: İstemci VPN isteğini gönderir ve HA sistemi bu istemcinin kimlik sorgulamasını yapar.
Faz2: Tünel içinden veri transferi başlatılır.

Faz1 de bir istek başlatılır, bu istek kabul edildiğinde iki uç arasında tünel kurulur ve FA sistemine bağlantı isteği gönderilir. FA (genelde RADIUS sunucudur) istemciyi kullanıcı adı ve şifresi ile doğrular. Eğer kullanıcının kullanıcı adı ve şifresi yalnışsa VPN isteği reddedilir. Kimlik doğrulaması yapılabilirse bu VPN isteği hedef networkdeki HA sistemine iletilir. İstek HA tarafından alındığında, FA sistemi HA sistemine şifrelenmiş login ID ve şifrelenmiş kullanıcı şifresini gönderir. HA bu mesajların doğrulamasını yapar ve FA sistemine bir tünel numarası gönderir ve FA mesajı aldığında bir tünel kurulmuş olur.

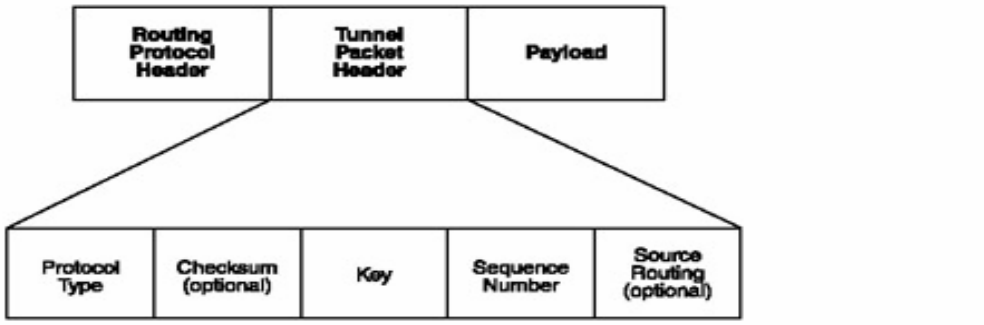
Tünelin kurulmasından sonra veri iletim aşaması olan 2. faza geçilir. Faz2'de veri paketleri FA sistemine iletilmeye başlanır. FA bir tünel başlığı türeterek herbir veri paketine bu başlığı ekler. FA tünel numarasını kullanarak şifrelenmiş verileri HA sistemine gönderir. HA bu verileri aldığında, paketi orjinal formatına dönüştürür. Orjinal veri networkdeki hedef noda gönderilir. Şekilde tünelleme işleminin 1. ve 2. fazı görülmektedir:



Şekil 7.3: Tüneller içinden 2 fazda data iletimi

7.4. TÜNELLENMİŞ PAKET FORMATI

Daha öncedende bahsedildiği gibi paket hedef networke iletilmeden önce orjinal paket FA tarafından enkript edilir. Bu formattaki paket tünellenmiş paket olarak isimlendirilir. Şekilde tünellenmiş paket görülmektedir:



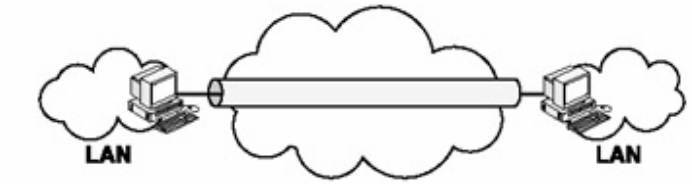
Şekil 7.4: Tünellenmiş paketin yapısı

Yönlendirilebilir protokol başlık bilgisi: Hedef HA ve kaynak FA sistemlerin IP adres bilgisini içeren başlıktır.
Tünel paket başlığı: Aşağıdaki alanları içerir :
-Protokol tipi: Pay-load protokol tipidir.
-Anahtar: İstemcinin tanımlamasını ve kimlik doğrulamasını gerçekleştirir.
-Seri Numarası: İletilen pakaetlerin seri numarasıdır.
-Kaynak yönlendirme: İlave yönlendirme bilgisi içerir, opsiyonel bir alandır.
Pay-load: İstemci tarafından FA sistemine gönderilen orjinal pakettir.

7.5. TÜNEL TİPLERİ

7.5.1. İstemci tarafından isteğe bağlı olarak oluşturulan tüneller:

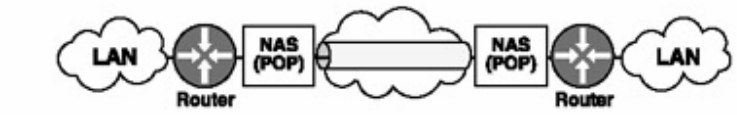
Uçtan uca tünel olarak bilinir. İstemcinin bağlantı isteği üzerine oluşturulur. İstemci nod tünelin son noktasıdır. Bundan dolayı, her bir uç için farklı tüneller oluşturulur ve iki uç arasındaki iletişim sona erdiğinde tünelde sonlandırılır.



Şekil 7.5.1: İsteğe bağlı olarak oluşturulan tünel yapısı

7.5.2. Sunucular tarafından oluşturulan tüneller:

İstemci tarafındaki istekle oluşturulan tünelden farklı olarak, bu tüneller NAS (Network Attached Storage) veya dial-up sunucular tarafından oluşturulur. Uzaktaki istemci ilk olarak bu sistemlerle bağlantı kurar (bu sistemler genelde ISP tarafında bulunur) ve tünel oluşturulur.

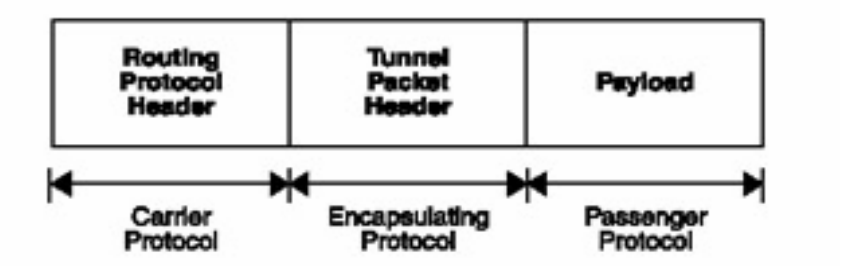


Şekil 7.5.2: Sunucular tarafından oluşturulan tüneller

İstemci tarafından oluşturulan tünel	**Sunucu tarafından oluşturulan tünel**
İstemci tünelin son noktasıdır.	NAS veya dial-up sunucular tünelin son noktasıdır.
Her bir bağlantı için farklı tüneller kurulur.	Çoklu bağlantılar aynı tüneli kullanırlar.
Data iletimi daha hızlıdır.	Aynı anda birden fazla bağlantı durumunda bağlantılar aynı tüneli paylaştığı için data iletimi daha yavaştır.
Tünellerin süresi kısadır.	Tünellerin süresi diğer tekniğe göre daha uzundur.

8. 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 orjinal veriler için bu protokol devreye girer. En yaygın olan iletim protokolleri PPP ve SLIP (serial line internet protocol) protokolleridir.



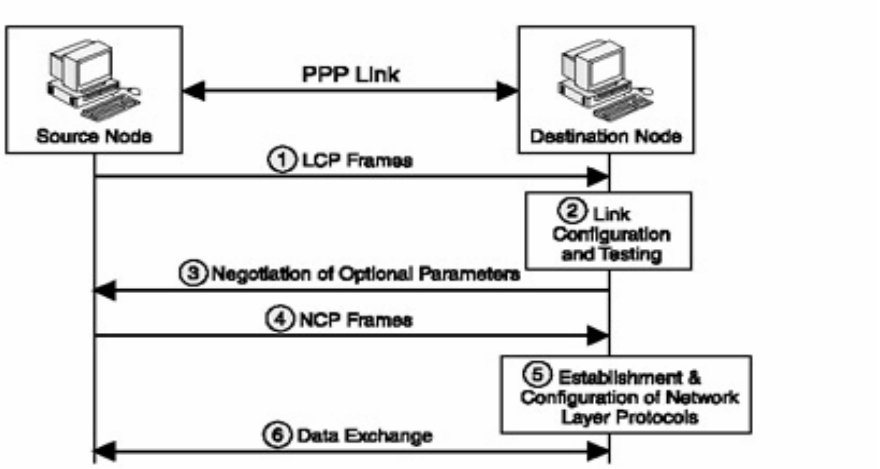
Şekil.8: Tünelleme protokolünü kullanan tünellenmiş paketler.

8.1. POINT TO POINT PROTOKOL (PPP)

Seri ve uçtan uca bağlantılarda kullanılan enkapsülasyon protokolüdür. PPP, EIA/TIA-232-C ve ITU-T V.35 'e sahip olan herhangi bir DTE veya DCE sistemde kullanılabilir. IP ve IP olmayan verilerin enkapsülasyonu ve iletilmesi aşağıdaki gibi gerçekleştirilir:
-IP olmayan datagramlara IP adreslerinin atanması,
-Kurulan bağlantının konfigürasyonu ve test edilmesi,
-Datagramların senkron ve asenkron enkapsülasyonu,
-İletim esnasında hata algılama.
PPP yukarda bahsedilen işlemleri gerçekleştirmek için 3 standart kullanır:
-Uçtan uca bağlantılarda data paketlerini enkapsüle etmek için kullandığı standart. Genelde bu standart HDLC (High Level Data Link Protocol) olarak bilinir ve bu protokol data paketlerini çerçevelere bölerken, PPP paket formatını değiştirmez.
-Uçtan uca bağlantıların kurulması ve test edilmesi için standart olarak LCP (Link Control Protocol) kullanır.
-İletim esnasında hataları yakalamak için standart olarak NCP (Network Control Protocol) kullanır.

8.1.1. PPP TEKNİĞİ

-Data paketleri enkapsüle edildikten sonra istemci, karşı tarafa uçtan uca bağlantı üzerinden LCP frameleri gönderir.
-Karşı taraf bağlantı isteğini aldığında, bağlantı kurulmuş olur,
-Kaynak nod uygun network katmanı protokollerinin seçimi için NCP frameleri gönderir ve iki uç arasında data iletimi başlar.

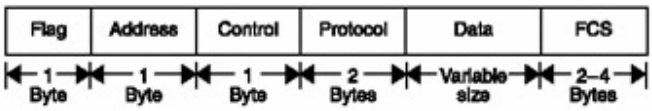


Şekil 8.1.1: PPP bağlantının kurulması

PPP bağlantılar kurulduğunda, bu bağlantılar LCP ve NCP frameler bağlantıyı sonlandırana dek devam eder. Bağlantıda bir problem olduğu durumda da bu bağlantı sonlandırılabilir.

8.1.2. PPP PAKET FORMATI

Bir PPP frame 6 bölümden oluşur:
Flag: 1 byte uzunluğundadır, frame'in başlangıç ve bitimini belirtir.
Adres: PPP uçtan uca bağlantıları kullandığından, broadcast adres kullanır, bu alanın uzunluğu 1 byte'dır.
Kontrol: Bu bilginin uzunluğu 1 byte'dır ve 00000011 serisini kullanır. Frame'in istemci bilgisini taşıdığını belirtir.
Protokol: Frame'in data alanında enkapsüle edilmiş olan verinin protokolünü belirtir. Uzunluğu 2 byte'dır.
Data: Kaynak ve hedef nodlar arasındaki bilgiyi içerir. Maksimum uzunluğu 1500 byte'dır.
FCS (Frame Check Sequence): Uzunluğu 2-4 byte'dır.



Şekil 8.1.2: PPP frame'in formatı

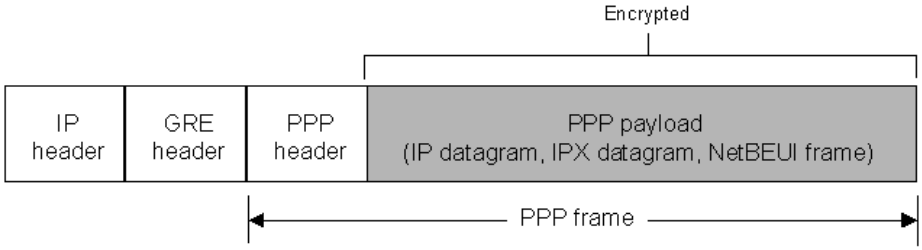
8.1.3. PPP BAĞLANTI KONTROLÜ

PPP, 2 nod arasındaki data iletiminin yanında 2 uç arasındaki bağlantının kontrolünü yapma işlemindende sorumludur. Bu amaçla LCP standartını kullanır. LCP aşağıdaki işlemleri yapar:
-PPP bağlantısının kurulumunda görev alır.
-Kurulu olan bağlantının konfigürasyonunu yapar
-Kurulu olan bir PPP bağlantının düzenli kontrollerini sağlar.
-2 uç arasındaki veri iletimi tamamlandığında, bu bağlantıyı sonlandırır.

LCP tabanlı link kontrolü 4 fazda çalışır: Link kurulumu, link kalitesi, uygun network katman protokolünü belirleme, link sonlandırma fazları. Bu fazların açıklamaları aşağıdadır:
-Link kurulumu: İki uç arasındaki bağlantı LCP tarafından kurulur, LCP bu işlem için bağlantı kurulum frame'lerini kulanır. Her bir uç cevap olarak kendi frame'ini gönderdiğinde bu faz tamamlanmış olur.
-Link kalitesi: Kurulan bağlantının tam olarak hazır olup olmadığını kontrol eder.
-Network-katman protokolünü belirleme: Bu fazda PPP frame'in protokol alanına enkapsüle edilmiş olan datanın Network-katmanı protokolü belirlenir.
-Link sonlandırma: LCP'nin son fazıdır ve iki uç arasındaki mevcut PPP bağlantıyı sonlandırır.

8.2. POINT TO POINT TÜNELLEME PROTOKOLÜ (PPTP)

PPTP bir Layer-2 protokolüdür ve PPP frameleri IP ağı üzerinden (Internet) iletilmesi için IP datagramlar içine enkapsüle eder. PPTP daha çok uzaktan erişimli VPN bağlantılarda kullanılır. RFC 2637'de tanımlı bir protokoldür. PPTP, tünel işlemleri için TCP bağlantı, PPP framelerin enkapsülasyonu için GRE kullanır. Aşağıdaki şekilde bir PPTP paketin yapısı gösterilmektedir.



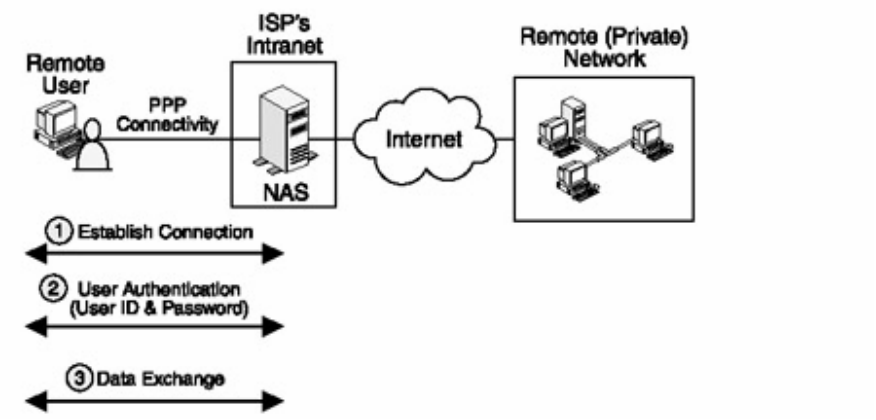
Şekil 8.2: PPTP paketin yapısı

PPTP, IP network üzerinden VPN bağlantısı sağlayarak, istemci ve sunucu arasında güvenli veri transferi yapar. On-demand VPN bağlantıları kurmayı sağlar. PPTP protokolünün avantajları aşağıdaki gibidir:
1. PSTN (Public Switched Telephone Networks) networkünü kullanır: VPN bağlantılarda PSTN networkünün kullanılmasına imkan sağlar ve böylece VPN konfigürasyonları daha kolay bir hale gelir. Bu kolaylığından ve düşük maliyetinden dolayı günümüzde yavaş yavaş kiralık devre networklerinin yerini almaktadır.
2. IP tabanlı olmayan protokolleride destekler: IP protokolünün yanında TCP/IP, IPX, NetBEUI ve NetBIOS standartlarınıda desteklemektedir. Bundan dolayı sadece Internet üzerinden değil, özel networkler üzerindende VPN bağlantıları kurulabilir.

8.2.1. PPTP PROTOKOLÜNDE PPP PROTOKOLÜNÜN ROLÜ

PPTP, PPP protokolünün gelişmiş bir versiyonudur. Temel olarak PPP protokolünün tekniklerini kullanır. Farkı ise sadece PPP trafiğini public networkler üzerinden farklı bir yöntemle geçirmesidir. PPTP protokolüde PPP gibi, çoklu bağlantıları desteklememektedir. PPTP kullanan tüm bağlantılar uçtan-uca bağlantılardır. PPP protokolü PPTP tabanlı iletimlerde aşağıdaki fonksiyonları destekler:
-Uç noktalar arasında fiziksel bağlantının kurulması ve sonlandırılması,
-PPTP istemcilerin kimlik doğrulamasının gerçekleştirilmesi,

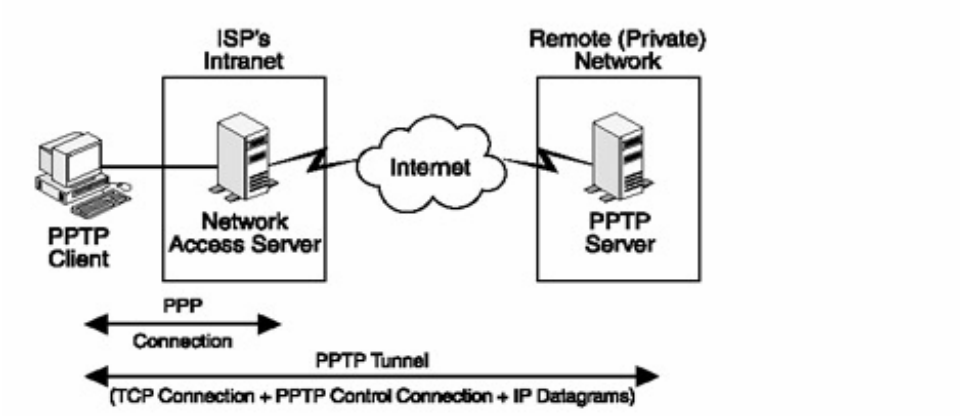
-PPP datagramlarının oluşturulabilmesi için IPX, NetBEUI, NetBIOS ve TCP/IP datagramlarının şifrelenmesi.



Şekil 8.2.1: PPP işlemleri

8.2.2. PPTP BİLEŞENLERİ

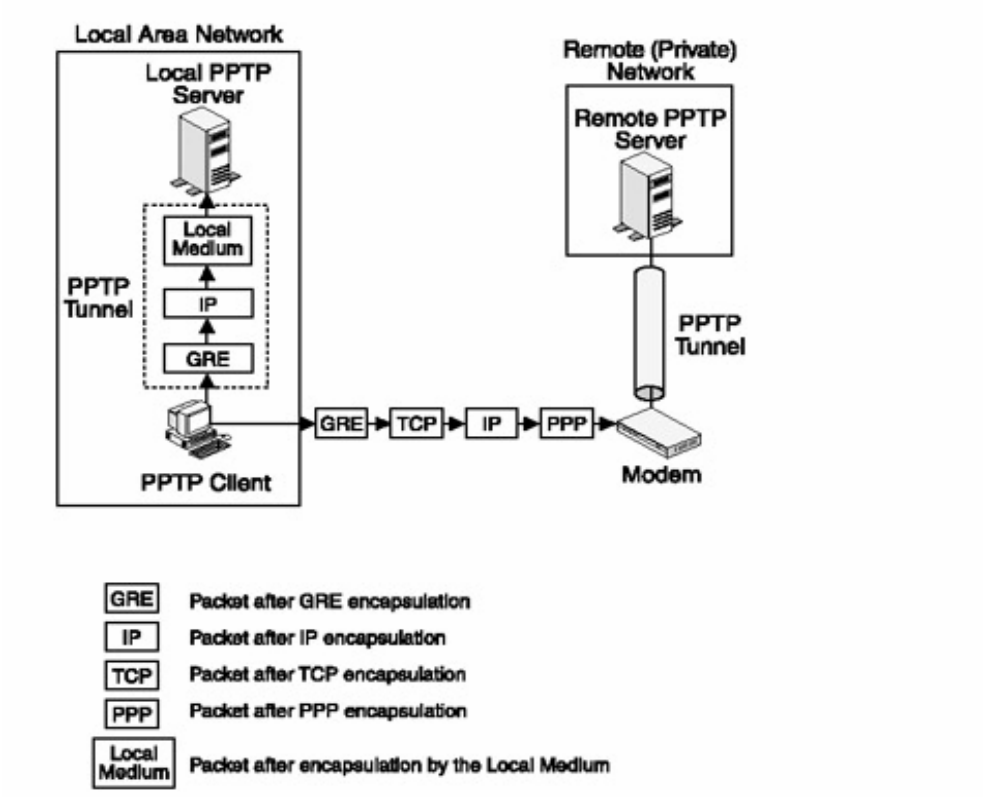
-PPTP istemci
-Network Access Server (NAS)
-PPTP sunucu



Şekil 8.2.2: PPTP tünel ve PPTP bileşenleri

8.2.2.1. PPTP İSTEMCİLERİ

PPTP istemci uzak bir sunucuya bağlantı isteği gönderdiğinde ISP tarafındaki NAS sisteminin servislerini kullanır. İstemci ilk olarak ISP tarafına dial-up PPP bağlantı kurabilmek için bir modeme ve bir tünel oluşturulması için VPN cihazına bağlanır. VPN cihazları Internet üzerinden tünel oluşturmak için ISP tarafındaki NAS sistemine dial-up olarak bağlanırlar.



Şekil 8.2.2.1: PPTP paketlerinin karşı networke iletimi

8.2.2.2. PPTP SUNUCULAR

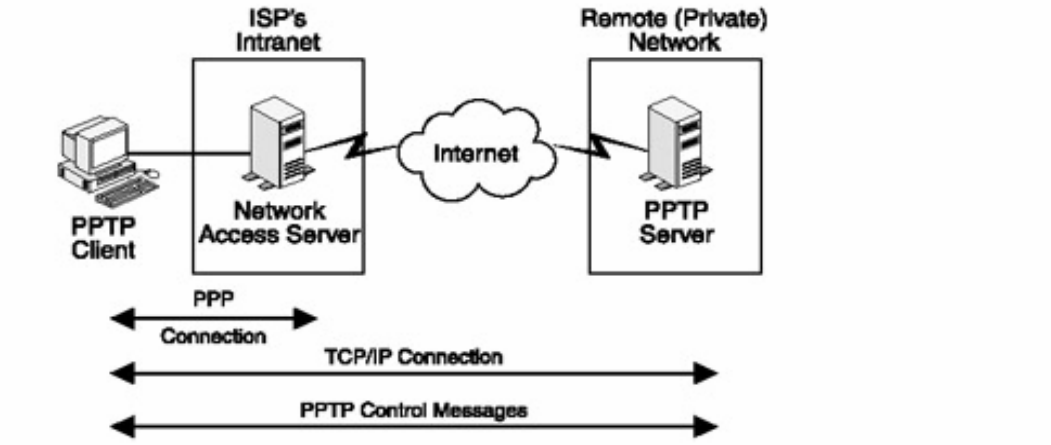
Uzaktaki veya lokaldeki bir noddan diğer bir noda VPN isteklerini iletme yeteneğine sahip sunuculardır. Uzak isteklere cevap verebilen PPTP sunucuların yönlendirme özelliğine sahip olması gerekmektedir. RAS (Remote Access Server) sunucular ve Windows NT 4.0 sunucular günümüzde yaygın olarak kullanılan PPTP sunuculardır.

8.2.2.3. PPTP NETWORK ERİŞİM SUNUCULARI (NASs)

İstemcilerin PPP/dial-in olarak internet bağlantısını sağlayan ve ISP tarafında bulunan sunuculardır.

8.2.3. PPTP GÜVENLİĞİ

PPTP güvenli bir iletişim için aşağıdaki özelliklere sahiptir:
-PPP tabanlı bağlantı kurma
-Bağlantı kontrolü
-PPTP tünelleme ve PPTP veri transferi
-PPTP bağlantı kontrolü
PPTP sunucu ve istemci arasında PPP tabanlı bir fiziksel bağlantı kurulduktan sonra PPTP bağlantı kontrolü yapılır. Bu kontrol tipi Şekil ‘de görülmektedir:



Şekil 8.2.3: PPP bağlantı üzerinden PPTP kontrolünün yapılması

PPTP kontrol mesajları TCP datagramlara enkapsüle edilir. Bundan dolayı, uzak sunucu veya istemciyle PPP bağlantısı kurulduktan sonra bir TCP bağlantı başlatılır. PPTP kontrol mesajları bu bağlantı üzerinden iletilir.

8.2.4. PPTP TÜNELLEME

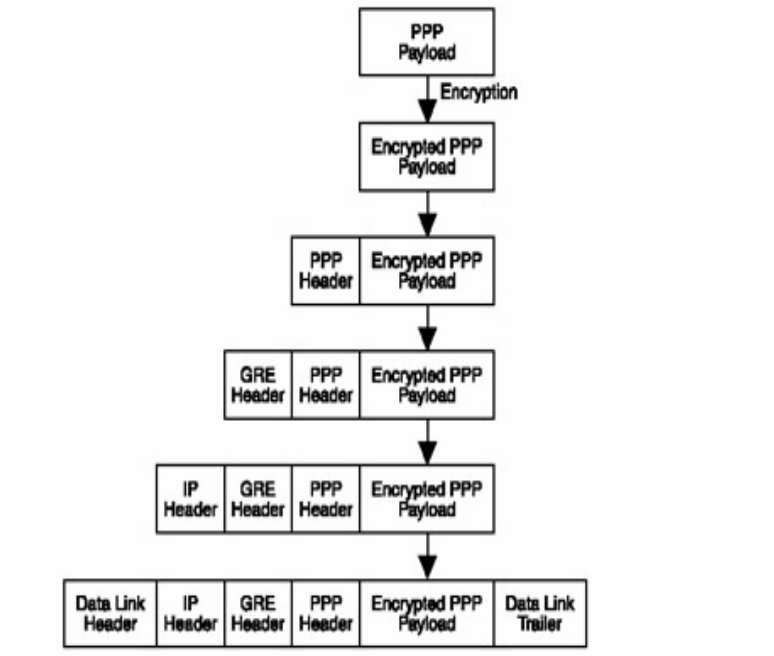
Bir PPTP veri paketi aşağıdaki enkapsülasyon işlemlerinden geçirilir:

-Verinin Enkapsülasyonu: Payload şifrelenir ve bir PPP frame içine enkapsüle edilip bu frame'e bir PPP başlık eklenir.

-PPP frame'lerin enkapsülasyonu: Başlık bilgisi eklenmiş olan PPP frame, GRE içine enkapsüle edilir.

-GRE paketi enkapsülasyonu: GRE paketin içine enkapsüle edilmiş olan PPP frame'e bir IP başlık eklenir ve bu başlıkta PPTP istemci ve hedef networkdeki sunucunun IP adresleri taşınır.

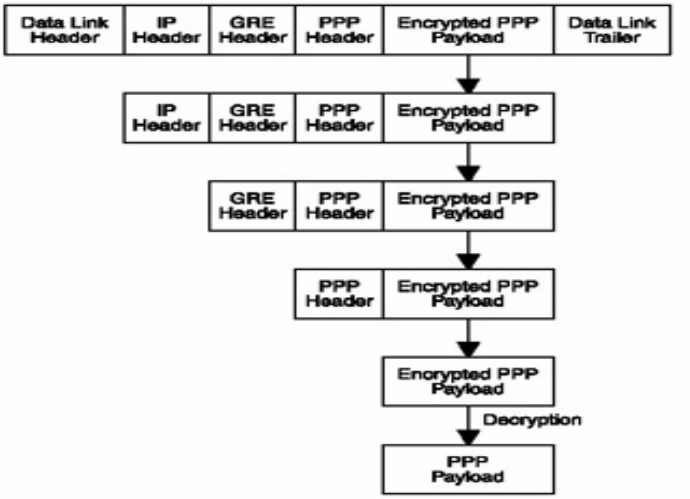
-Data Link Layer Enkapsülasyonu: PPTP bir Layer 2 tünelleme protokolüdür. Bundan dolayı data link layer başlığı tünellemede büyük öneme sahiptir. Bu layer datagramlara kendi başlık bilgisini ekler. Eğer bu datagram lokal PPTP tünelinden geçecekse, bir LAN teknolojisi başlığı ile enkapsüle edilir. Eğer bir WAN tünelini kullanacaksa bu datagramda değişiklik yapılmaz.



Şekil 8.2.4.a: PPTP veri tünelleme işlemi

PPTP data transferi istemciye başarıyla yapıldığında istemci tünellenmiş paketleri orjinal paketlere dönüştürmeyi isteyecektir. PPTP tünellenmiş paketin geri dönüşümü, PPTP tünelleme işleminin tam tersidir. Orjinal paketlerin elde edilebilmesi için aşağıdaki işlemler takip edilir:

-İstemci pakete gönderen tarafından eklenmiş olan Data Link başlığını kaldırır,
-GRE başlık kaldırılır,
-IP başlık kaldırılır,
-PPP başlık kaldırılır,
-Son olarak şifre çözümleme yapılır.



Şekil 8.2.4.b: Tünellenmiş paketin orjinal pakete dönüştürülmesi

PPTP bağlantıların kontrolü TCP 1723 portu üzerinden PPTP istemcinin ve sunucunun IP adresi ile yapılır. Kontrol mesajları ile PPTP tünellerin devamlılığı ve sonlandırılması sağlanır, PPTP sunucu ve istemci arasındaki bağlantıda bir problem olup olmadığı kontrol edilir.
PPTP protokolündeki güvenlik işlemleri aşağıda görülmektedir:
-Veri Şifrelemesi
-Kimlik doğrulama
-Erişim kontrolü
-Paket filtrelemesi
-PPTP Veri şifrelemesi

PPTP, PPP tarafından desteklenen MPPE (Microsoft Point-to-Point Encryption) şifreleme servislerini kullanır. Anahtar üreten algoritma RSA-RC4 hash algoritmasıdır. Bu anahtar tünel içinden iletilen verilerin şifrelenmesi için kullanılır. Anahtarın uzunluğu 40 bittir. Fakat yakında 128 bitlik anahtarlarda desteklenecektir.

8.2.5. PPTP KİMLİK DOĞRULAMASI

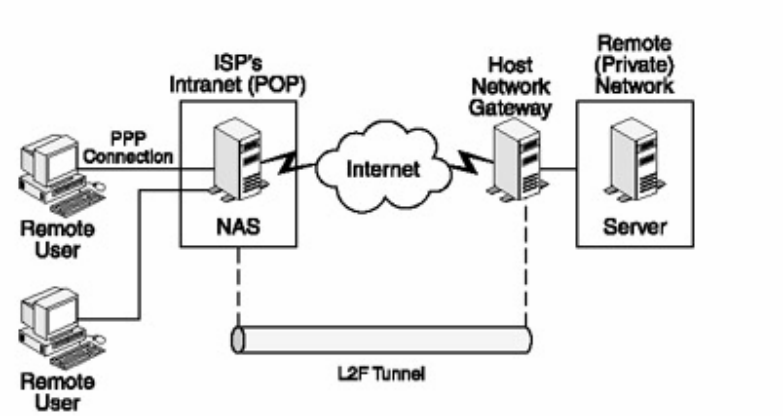
PPTP aşağıda anlatılan kimlik doğrulama mekanizmalarını kullanır:
-MS-CHAP (Microsoft Challenge Handshake Authentication Protocol): PPP tabanlı kimlik doğrulamalar için kullanılır. CHAP tekniğine benzemektedir. Tek farkı, MS-CHAP tekniği RSA RC4 algoritmasını, CHAP tekniği ise RSA MD5 algoritmasını kullanır.
-PAP (Password Authentication Protocol): En yaygın dial-in kimlik doğrulama protokolüdür. Ayrıca PPP tabanlı bağlantılardada kimlik doğrulamada kullanılır.

PPTP protokolünün temel avantajları aşağıdaki gibidir:
-PPTP yaygın olarak kullanılan bir built-in Microsoft çözümüdür.
-IP tabanlı olmayan protokolleride destekler.
-Unix, Linux, Apple’s Macintosh desteği vardır.

PPTP Protokolünün dezavantajları ise aşağıdaki gibidir:
-L2TP ve IPSEC protokolüne göre güvenliği daha azdır.
-PPTP platform bağımlı bir protokoldür.
-PPTP sunucudaki tanımlamaları zordur.
-PPTP protokolünün en büyük dezavantajı güvenlik mekanizmasının çok sağlam olmamasıdır. Çünkü anahtarın kullanıcı şifresinden elde edildiği simetrik şifreleme tekniğini kullanır.

8.3. L2F (LAYER-2 FORWARDING) PROTOKOLÜ

L2F uzak bağlantılarda birçok avantajlara sahiptir. Bir tünel içinde birden fazla oturum açabilir. Yani tek bir dial-up bağlantı ile birden fazla kullanıcı intranete erişebilir. Bu nedenle L2F ile VPN çözümlerinin maliyeti daha düşük olacaktır, çünkü uzak lokasyon ile ISP arasında ve ISP POP noktası ile intranet arasındaki bağlantıların sayısı azalacaktır. Şekilde L2F tünelleme yapısı görülmektedir.

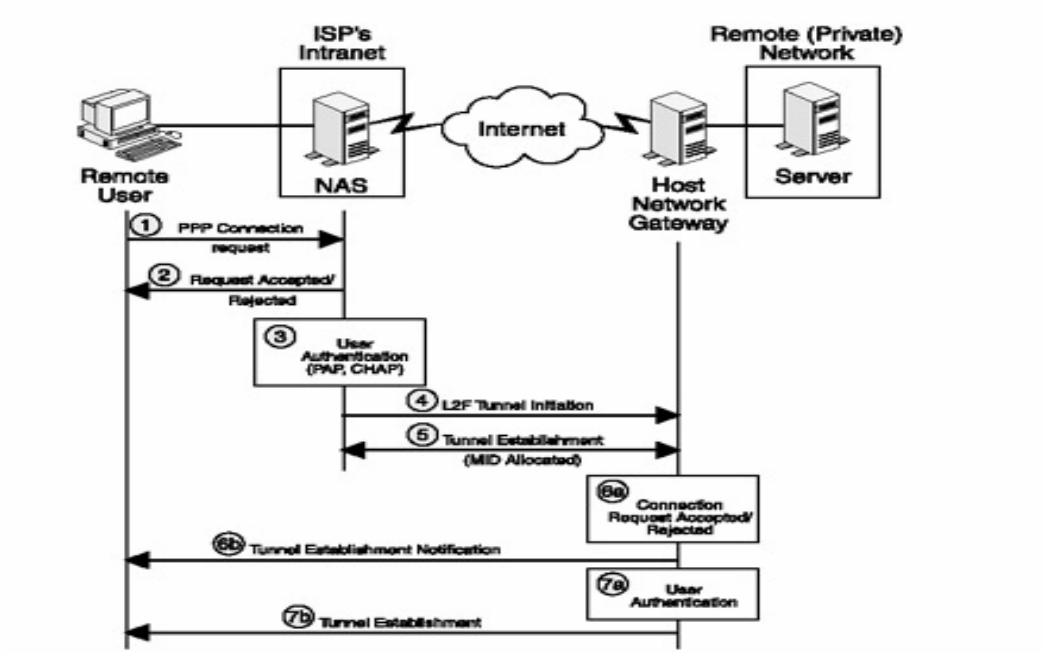


Şekil 8.3: ISP POP noktası ile gateway arasındaki L2F tünel

8.3.1. L2F TEKNİĞİ

Bir istemci intranetteki bir kaynağa dial-up bağlantı ile eriştiğinde aşağıda bahsedilen olaylar gerçekleşir:
-İstemci servis sağlayıcı ile ISDN veya PSTN networkü üzerinden PPP bağlantı başlatır.
-ISP POP noktasındaki NAS sistemi istemcinin bağlantısını kabul ederse, NAS sistemi ile istemci arasında bir PPP bağlantı başlatılmış olur.
-İstemcinin servis sağlayıcıda CHAP veya PAP teknikleri ile kimlik doğrulaması yapılır.
-Eğer hedef ağın gateway'ine mevcut bir tünel yoksa, bir tünel kurulur.
-Tünel kurulumu gerçekleştikten sonra bağlantıya bir MID atanır ve gateway'e uzak bir kullanıcının bağlantı isteği olduğu mesajı gönderilir.
-Gateway bağlantı isteğini ya kabul eder yada reddeder. İstek reddedilirse dial-up bağlantı sonlandırılır, kabul edilirse gateway kullanıcıya bağlantıyı başlatacağına dair mesaj gönderir.
-Kullanıcının gateway tarafından kimlik doğrulaması yapıldıktan sonra kullanıcı ile gateway arasında sanal bir interface kurulur.

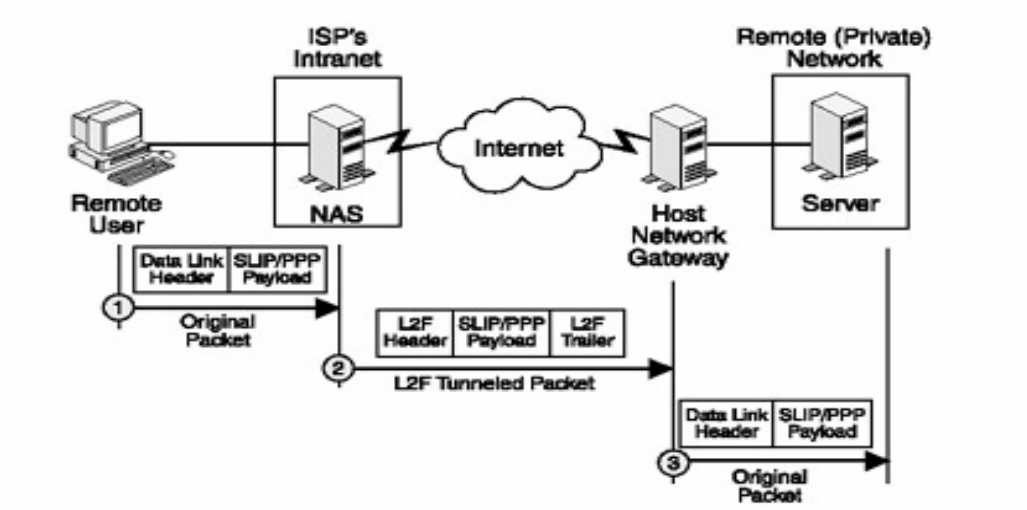
Şekilde iki uç arasında L2F tünelin kurulması işlemleri gösterilmektedir:



Şekil 8.3.1: İstemci ve sunucu arasında L2F tünelin kurulması

8.3.2. L2F TÜNELLEME

İstemcinin kimlik doğrulaması yapılıp bağlantı isteği kabul edildikten sonra, ISP-NAS sistemi ile hedef ağın gateway'i arasında şekilde görüldüğü gibi bir tünel kurulur.

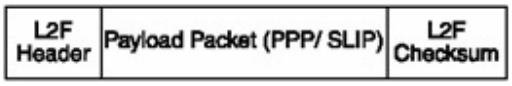


Şekil 8.3.2.1: L2F tünelleme işlemi

L2F tüneller aynı zamanda "sanal interface" olarakta isimlendirilirler. Tünel kurulduktan sonra frame'ler tünel üzerinden aşağıda anlatıldığı gibi iletilir:
-İstemci frameleri ISP-NAS sistemine gönderir.

-NAS sisteminde frame'e bir L2F başlık eklenir, frame enkapsüle edilir ve tünel üzerinden hedef networke gönderilir.

-Gateway tünellenmiş paketleri kabul eder, L2F başlığına bakar ve paketi intranet içinden hedef kaynağa iletir.
-Hedef kaynak aldığı tünellenmiş paketleri orjinal haline dönüştürür.



Şekil 8.3.2.2: L2F paket formatı

Hedef ağdan istemciye cevap gönderilmeside aynı şekilde gerçekleşir, frameler ilk olarak gatewaye gönderilir ve L2F paketlerin içinde enkapsüle edilir, ISP-NAS sistemine iletilir. NAS sistemi frame'in L2F bilgisine göre frame'i istemciye iletir.

8.3.3. L2F VERİ ŞİFRELEMESİ

L2F şifreleme işlemi için MPPE (Microsoft Point-to-Point Encryption) tekniğini kullanır. Fakat bu teknik günümüzde güvenlik açısından yetersiz kaldığı için verinin iletiminde ek olarak IPSEC tekniğinide kullanır. IPSEC, şifreleme amaçlı olarak ESP (Encapsulating Security Payload) AH (Authentication Header) ve IKE (Internet Key Exchange) protokollerini kullanır.

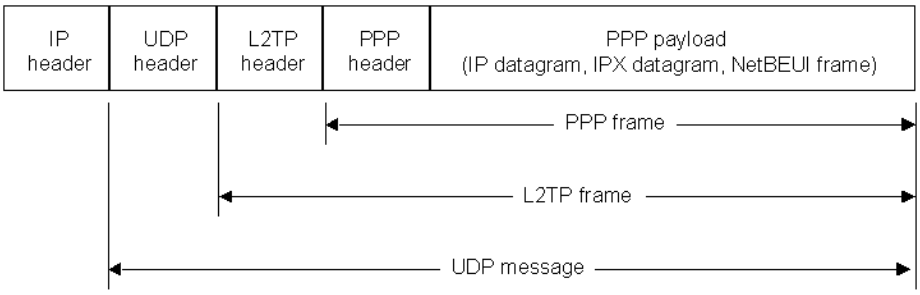
8.3.4. L2F KİMLİK DOĞRULAMA

L2F kimlik doğrulaması 2 aşamada gerçekleştirilir: ilk olarak istemci ISP POP noktasına dial-in bağlantı yapar, kimlik doğrulama geçekleşir ve bir tünel kurulur. İkinci aşamada ise gateway ile NAS sistemi arasında istemcinin kimlik doğrulaması yapılır ve tünel kurulur. L2F, PPTP tekniğinde olduğu gibi, kimlik doğrulama işlemlerinde PPP servislerinden yararlanır. L2F Gateway bir bağlantı isteği aldığında istemcinin kimlik doğrulama işlemi yapılırken PAP tekniği kullanılır. L2F veri güvenliğini sağlamak için ayrıca CHAP, EAP, RADIUS ve TACACS tekniklerindende yararlanır.
L2F çözümlerinin sağladığı avantajlar aşağıdaki gibidir:
-Gelişmiş güvenlik özelliği,
-Platform bağımsız olması,
-ISP tarafında çok fazla tanımlama yapılmaması,
-ATM, FDDI, IPX, NETBEUI ve Frame Relay desteğininde olması.
L2F çözümlerinde aşağıdaki gibi bazı dezavantajlarda sözkonusu olmaktadır:
-Konfigürasyonları kolay olmamaktadır,
-ISP tarafındada L2F desteği olması gerekmektedir.,
-PPTP ile kıyaslayınca L2F tünellerde iletim hızı daha yavaştır.

8.4. L2TP (LAYER-2 TUNNELING PROTOCOL)

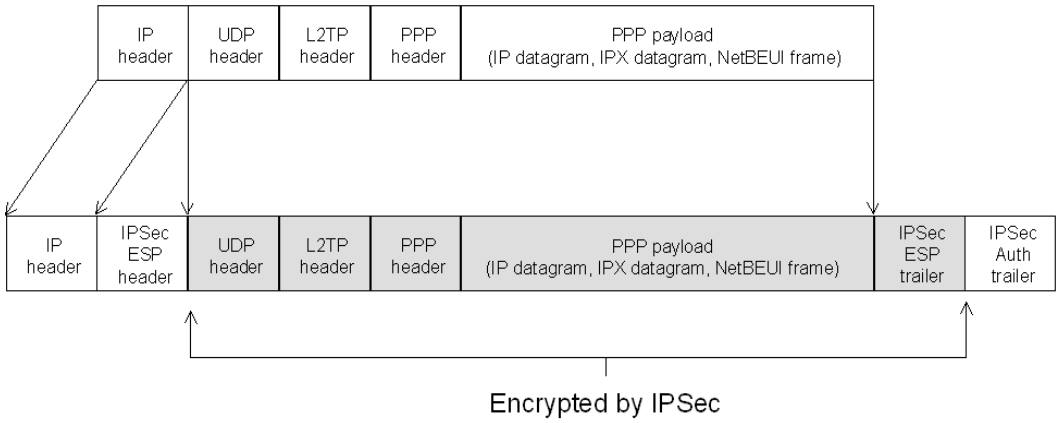
L2TP, PPTP ve L2F protokollerinin birleşimidir. PPTP ve L2F protokollerinin en iyi özelliklerine sahiptir. PPP frameleri; IP, X25, Frame Relay ve ATM networkleri üzerinden iletilebilmesi için enkapsüle eder. Datagram olarak IP kullanacak şekilde tanımlama yapılırsa Internet üzerinden bir tünelleme protokolü olarak kullanılabilir. RFC 2661'de tanımlıdır.

Internet üzerinden, enkapsüle edilmiş PPP framelerin tünellenmiş veri olarak iletilebilmesi için UDP protokolünü kullanır.



Şekil 8.4. L2TP mesajın yapısı

Windows 2000 sisteminde L2TP paketlerin şifrelenmesi için IPSEC/ESP (Encapsulating Security Payload) kullanılır. L2TP paketlerinin ESP ile şifrelenmiş formatı aşağıda görülmektedir:



Şekil 8.4.1: ESP ile şifrelenmiş bir L2TP paketin yapısı

8.4.1. L2TP VE PPTP PROTOKOLLERİNİN KARŞILAŞTIRILMASI

L2TP ve PPTP, OSI modeline gore 2. katmada çalışan protokollerdir. Kullanıcı yetkilendirmesi esasına dayanarak çalışırlar. Örneğin bir PPTP istemcisi, PPTP sunucusuna kullanıcı adı ve şifresini göndererek bağlantı talebinde bulunur. Şayet istemcinin gönderdiği kullanıcı adı ve şifre doğruysa oturum açılır. Artık istemci ile sunucu arasındaki bilgi kriptolu olarak taşınır. Kriptolama için kullanılan anahtar, kullanıcı şifresinden türetilir. Hem L2TP hem de PPTP verinin aktarımını datagram (UDP) paketleri ile yapar. Ancak PPTP, L2TP'den farklı olarak tünelin kurulumu ve yönetimi ile ilgili kontrol işlemlerini, sunucu ile istemci arasında TCP bağlantısı kurarak yapar. Bu PPTP protokolünün, paket geçirme süresinin yüksek olduğu ağlarda L2TP protokolüne göre performansın düşmesine sebep olur. Diğer yandan L2TP'nin bir özelliğide aynı anda iki nokta arasında birden fazla tünel açabilmesidir.

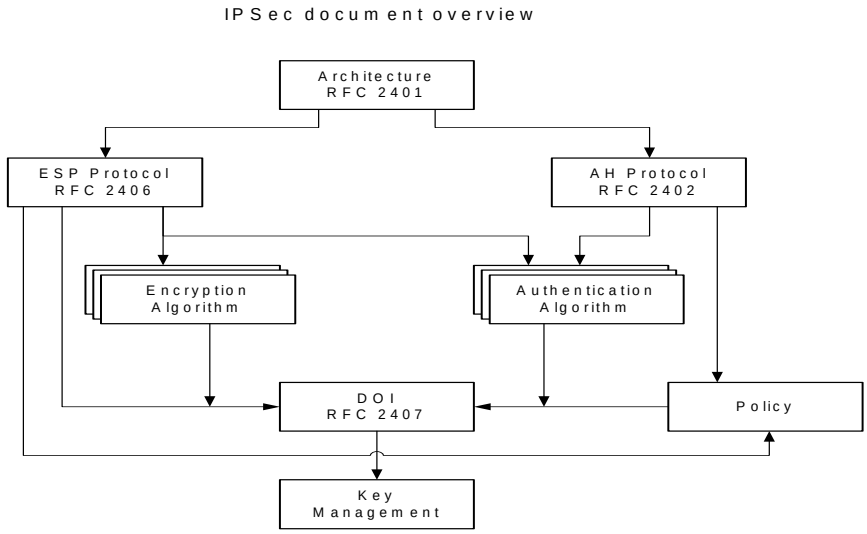
8.5. IPSEC (INTERNET PROTOCOL SECURITY) PROTOKOLÜ

IPSEC, netwok katmanında IP güvenliği sağlamak için IETF (Internet Engineering Task Force) tarafından tanımlanmış protokol takımıdır. IPSec temelli VPN iki kısımdan oluşmaktadır:
1. Internet Key Exchange protokolü (IKE)
2. IPSEC protokolü (AH/ESP/tümü)

Birinci kısım, IKE, ilk görüşme (negotiation) fazıdır. Bu fazda iki VPN uç noktası IP trafiğini hangi metodlarla güvenlik altına alacağı konusunda anlaşır, buna ek olarak IKE, Güvenlik İlişkileri (Security Associations-SAs) kurarak bağlantıları yönetir. SA'ler tek yönlüdür ve böylece her IPSEC bağlantısı için iki adet SA bulunur.
Diğer kısım ise transfer edilen gerçek IP verisidir. Bu transfer IKE görüşmesinde karar verilen şifreleme ve doğrulama metodları (ESP, AH, veya her ikisi) ile yapılır.

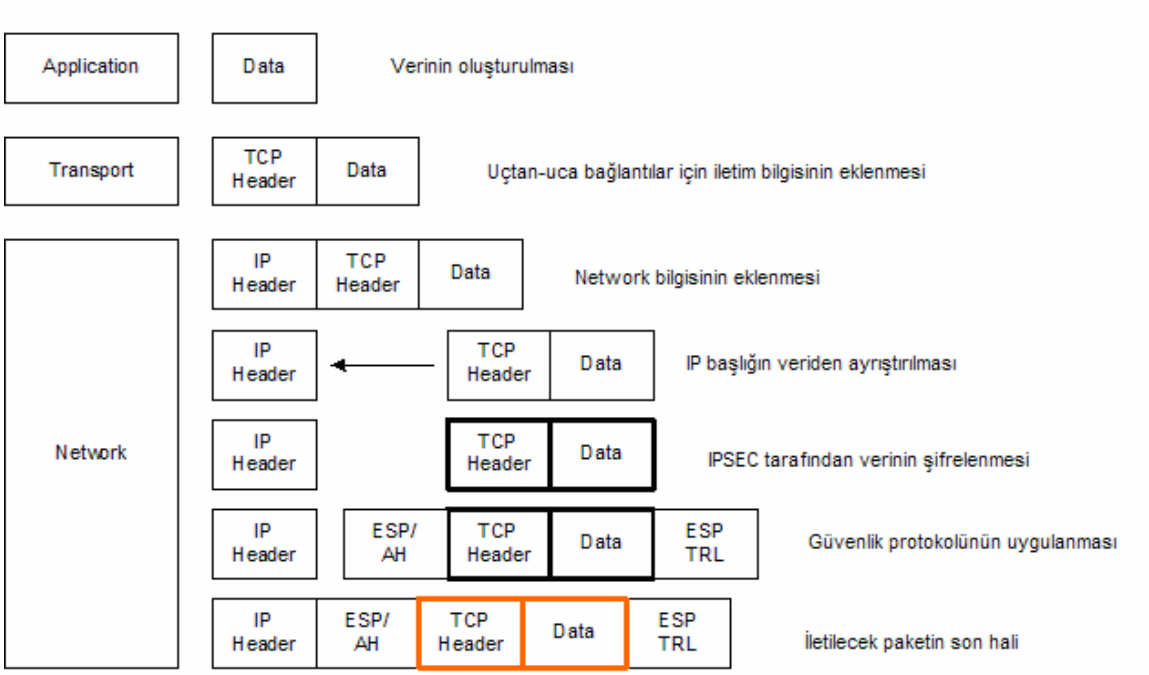
IPSEC Servisleri

	AH	ESP (sadece şifreleme)	ESP (Şifreleme ve kim doğrulama)
Erişim Kontrolü	✓	✓	✓
Connectionless	✓		✓
Veri kimlik doğrulam	✓		✓
Tekrarlanan aynı paketlerin iptali	✓	✓	✓
Güvenilirlik		✓	✓
Trafik akışının limitlenebilmesi		✓	✓



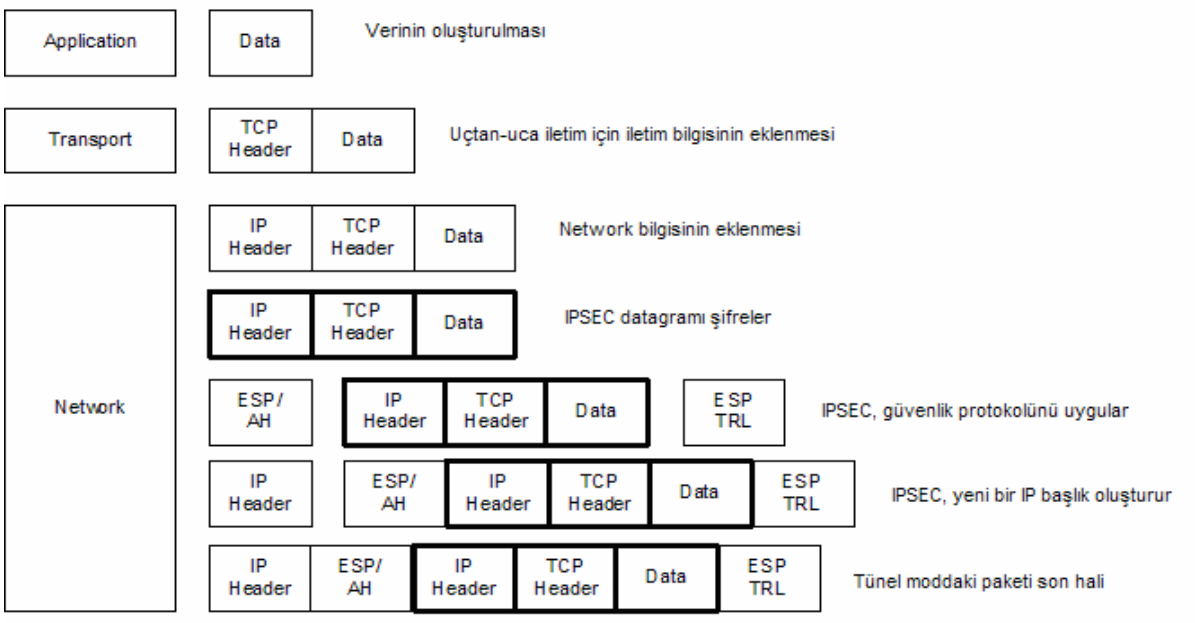
Şekil 8.5: IPSEC mimarisi

IPSEC yapısında 2 mod sözkonusudur;tünel ve iletim modu. Aşağıdaki şekilde iletim modu görülmektedir:



Şekil 8.5.a: IPSEC iletim modu

Bu modda en üst katmandan en alt katmana kadar paketin yönlendirilebilmesi için IP başlık kullanılır.



Şekil 8.5.b: IPSEC tünel modu

Tünel modunda IPSEC paketin son haline gerçek IP adresi eklenir.

8.5.1. IKE (INTERNET KEY EXCHANGE)

Veriyi şifrelemek ve doğrulamak için gerekli işlemler şifreleme ve doğrulama algoritmaları ve bunlar için gerekli anahtarladır. IKE protokolü bu oturum anahtarlarının (session keys) dağıtımını yapmak ve VPN uç noktalarının hangi güvenlik politikalarında anlaşacaklarını kararlaştırmak için kullanılan bir metotdur. IKE üç ana göreve sahiptir:

- Uç noktalara karşılıklı doğrulama için yöntem sağlar ,
- Yeni IPSEC bağlantıları oluşturur (SA oluşturur) ,
- Mevcut bağlantıları yönetir.

IKE her bağlantıya SA tahsis ederek bağlantıların izini tutar. SA bir bağlantı için atanmış ESP, AH, oturum anahtarları gibi tüm parametreleri tanımlar. SA tabiatı gereği tek yönlüdür.

IKE ve IPSEC bağlantılarının limitli ömürleri vardır. Bu ömürler zaman (saniye) veya veri miktarı olarak tanımlanır. Bu ömürler bağlantıların çok üzün süreler boyunca kullanılmamasını sağlamak için tanımlanırlar. IPSEC bağlantı ömrü genellikle IKE bağlantı ömründen kısadır ve IPSEC bağlantısı kolaylıkla yenilenebilir.

IPSEC bağlantısı başlatan VPN gateway karşı tarafa bir öneri listesi gönderir. Bu listede bağlantının güvenlik altına alınabilmesi için kullanılabilecek şifreleme, doğrulama metodlar/parametreler bulunur. Üzerinde görüşülen bağlantı veri güvenliğini sağlayan IPSEC bağlantısı olabilir veya IKE bağlantısı güvenliğini sağlayan IKE bağlantısının kendisi olabilir. Listeyi alan karşı taraf mevcut politikalarına bağlı olarak kendisine en uygun metodu seçer ve bu seçimini karşı tarafa iletir.

8.5.1.1. IKE PARAMETRELERİ

VPN oluşturabilmek için IKE görüşmesi esnasında kullanılabilecek birçok parametre mevcuttur. VPN bağlantısını oluştururken bu parametrelerin iyice anlaşılması ve bu parametrelere dikkat edilmesi gerekmektedir.

Uç NoktaTanımlamaları:
-Tünel/transport modu
-Main/agresif mod
-IKE şifreleme
-IKE DH grup
-PFS açık/kapalı/kimlik
-IPSEC şifreleme
-IPSEC ömrü
Yerel ve Uzak Ağlar/Bilgisayarlar:
-Uzak gateway
-IPSEC protokolü (ESP/AH/tümü)
-IKE doğrulama
-IKE ömür
-IPSEC DH grup
-IPSEC doğrulama

8.5.1.2. IKE KİMLİK DOĞRULAMA

a. Manuel anahtar girişi :VPN konfigürasyonunun en basit yolu manuel anahtar girişinden geçer. Bu metodda IKE hiç kullanılmaz ve karşılıklı iki VPN uç noktasına şifreleme, doğrulama anahtarları ve diğer parametreler manuel girilir.

Avantajları: Düz bir mantığa sahip olduğu için kısmi birlikte-çalışabilir (interoperable) bir yapıya sahiptir. Birlikte çalışabilirlik problemleri çoğunlukla IKE'de yaşanır. Manuel anahtar girişi IKE'yi tamamıyla baypas eder. SA tanımları bizzat tanımlanır.

Dezavantajları: IKE kullanımından önce geliştirilmiştir ve ilkel bir metoddur, böylelikle IKE'nin fonksiyonelliklerinden uzaktır. Bu yüzden bazı limitlemeleri vardır, örneğin her zaman aynı anahtarlar kullanılır ve İnkar Edememe özelliği eksiktir. Bu tip bağlantı "reply attacks" olarak adlandırılan saldırılara karşı açıktır, 3. bir şahıs belirli bir zamanda gönderilen şifreli paketleri kaydeder ve bir müddet sonra tekrar gönderir. VPN uç noktası paketin sonradan gönderildiğini algılayamaz ve gerekli tedbiri alamaz. IKE bu güvenlik açığını kapatmaktadır.

b. Ön tanımlı anahtarlama (Pre-Shared Keying- PSK): VPN uç noktaları gizli bir anahtarı paylaşır. Bu servis IKE tarafından sağlanır ve bu servis PSK metodunu Manuel anahtar girişi metoduna kıyasla esnek kılar.

Avantajları: Manuel anahtar girişi metoduna kıyasla bir çok avantajı vardır, örneğin, uç nokta doğrulaması sağlar, tünel ömürleri tanımlanabilir, yeni anahtar tanımlanabilir. Dezavantajları: Ön-Tanımlı anahtarlama metodunda en ciddi dezavantaj anahtar dağıtımı sorunudur. Gizli anahtarlar uç nokta VPN geçitlerine veya istemcilerine güvenli bir şekilde nasıl dağıtılacak?

c. Sertifika: Her VPN geçidi kendisine özel sertifikaya ve bir veya birden çok kök sertifikasına sahiptir. Her uç nokta, sertifikasında bulunan bir açık anahtara denk gelen bir özel anahtara sahiptir ve bu özel anahtar sadece kendisinde bulunur. Avantajları: Bir çok VPN istemcisi Ön-tanımlı anahtar olmadan yönetilebilir, bir istemcinin sertifikası başkası tarafından ele geçirilmişse, sadece o istemcinin sertifikası iptal edilir veya yenilenir, diğer VPN geçitleri/istemcileri için yeniden sertifikalandırma çalışmasına gerek yoktur. Dezavantajları: İyi bir yönetim yazılımı olmadan yönetilmesi güçtür.

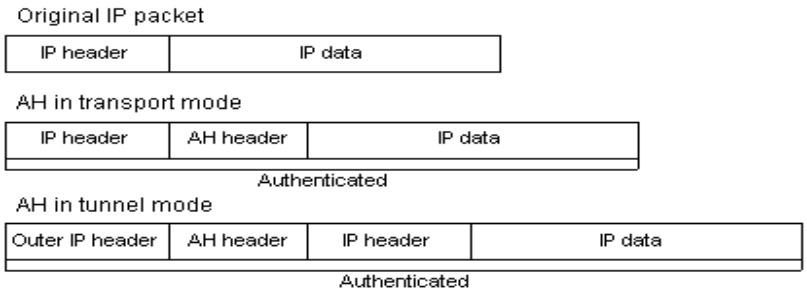
8.5.2. IPSEC PROTOKOLLERİ (ESP/AH)

IPSec protokolleri (AH ve ESP) VPN geçitleri arasındaki gerçek veri trafiğini korumak amacı ile kullanılır.

8.5.2.1. AH (AUTHENTICATION HEADER)

AH data akışını doğrulamak için kullanılan bir protokoldür. IP paketinde bulunan veriden MAC oluşturmak için kriptografik hash fonksiyonu kullanır. Elde edilen MAC, karşı tarafa,

mesajın bütünlüğünün korunduğunun anlaşılması için orijinal paketle birlikte iletilir.

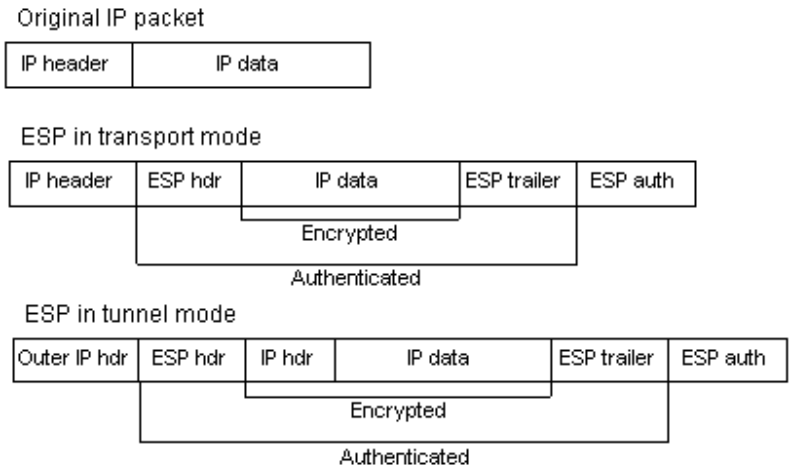


Şekil 8.5.2.1: Pakete AH uygulanması

AH protokolü IP paket verisinin yanı sıra IP başlığının parçalarınıda doğrular. AH protokolü IP başlığından sonra pakete AH başlığı yerleştirir. Bu protokol ile adres spoofing ve replay atakları önlenir. Bu tip atakları bir yetkilendirme fonksiyonu olan ve simetrik anahtar yapısına sahip olan MAC tekniği ile önler. AH, şifreleme işlemi için MD5 hesaplama metodu kullanır. AH protokolünün şifreleme için HMAC-MD5-96 ve HMAC-SHA-1-96 MD5 standartlarını kullanır.

8.5.2.2. ESP (ENCAPSULATING SECURITY PAYLOAD)

ESP protokolü IP paketinin hem şifrelenmesi hem de doğrulanması için veya IP paketinin sadece şifrelenmesi veya sadece doğrulanması için kullanılır.



Şekil 8.5.2.2: Pakete ESP uygulanması

ESP protokolü IP başlığından sonra pakete ESP başlığı yerleştirir. ESP başlığından sonraki tüm veri şifrelenmektedir ve/veya doğrulanmaktadır. AH prtokolünden farkı; ESP protokolü IP paketinin şifrelenmesinide sağlamaktadır. ESP kimlik doğrulama işlemleri için aşağıdaki teknikleri kulanmaktadır:

- DES/CBC
- 3DES

- RC5
- IDEA
- 3 IDEA
- CAST
- Blowfish

8.6. PROTOKOLLERİN KARŞILAŞTIRILMASI

Uygulama, güvenlik ve performans açısından tünelleme protokolleri birbirinden ayrılırlar:

1. IPSEC, en güvenilir olan tünelleme protokolüdür.

2. PPTP protokolü güvenlik açısından L2TP'den daha iyi ancak performans yönünden daha kötüdür. IPSEC daha komplex güvenlik algoritmaları kullandığından, donanım kapasitesi yetersiz olan IPSEC istemci ve sunucular paketlerin gecikmesine neden olabilir.

3. PPTP ve IPSEC protokolü, aralarında mevcut bir IP bağlantısı olan hostlar arasında yapılır. Diğer yandan L2TP, aralarında ISDN, TDM, FR, ATM gibi devreler üzerinde direkt tünel kurup içinden IP, IPX, NETBEUI gibi her türlü trafiği taşıyabilir.

4. PPTP ve IPSEC protokolleri, istemci ile sunucu arasında aynı anda sadece bir tünel kurarlar. Diğer yandan L2TP, birden fazla oturum açabilir. Bu yönüyle, bazı ağ uygulamaları için L2TP oldukça uygun bir tünelleme protokolüdür.

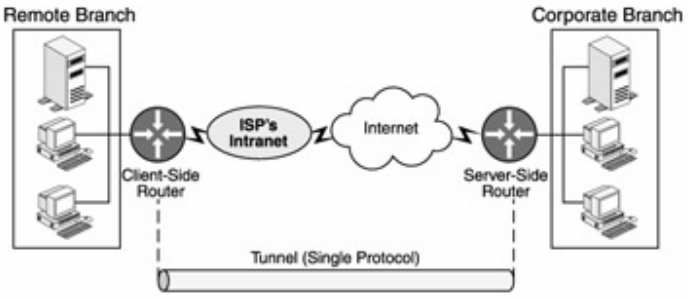
Yukarıdaki maddelerden de anlaşılacağı gibi, L2TP daha çok özel uygulamalar için kullanılan bir protokoldür. Diğer yandan PPTP ve IPSEC protokolleri daha genel uygulamalar için kullanılan protokollerdir.

9. GÜVENLİK AÇISINDAN VPN TİPLERİ

9.1. ROUTER - ROUTER VPN

9.1.1. ON-DEMAND TÜNELLİ VPN

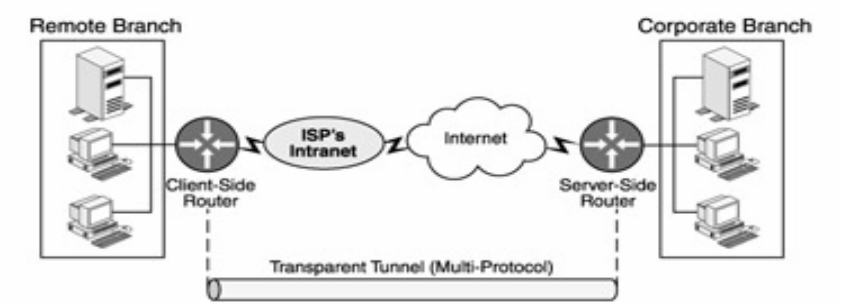
İstemci ve sunucu tarafını birbirine bağlayan yönlendiriciler arasında güvenli bir VPN bağlantısı kurulmasını sağlar. Aynı anda birden fazla bağlantı desteklenir. Her iki taraftaki router, anahtar ve şifreleme algoritmalarını desteklemelidir.



Şekil:9.1.1. Ondemand VPN yapısı

9.1.2. ÇOKLU PROTOKOL ON-DEMAND TÜNELLİ VPN

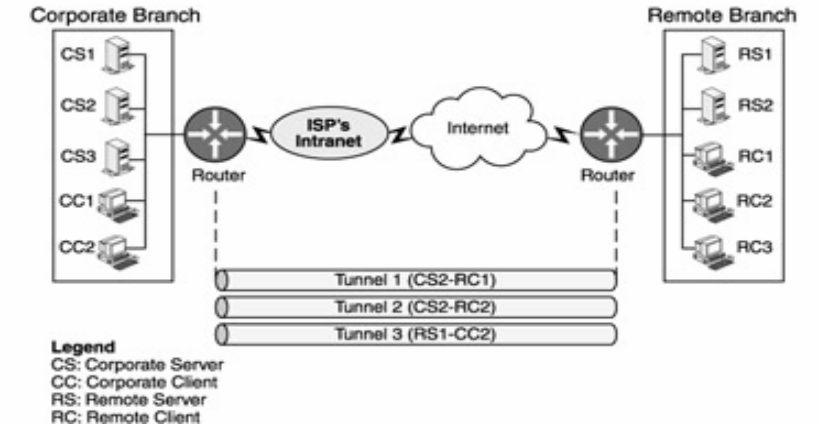
On-demand tünelli VPN'in gelişmiş halidir, tek farkı IP protokolünü desteklemeyen istemcilerinde yönlendiriciler arasında kurulan transparent tüneller üzerinden VPN bağlantılarını sağlamasıdır.



Şekil.9.1.2. Çoklu protokol/On-demand tünelli VPN yapısı

9.1.3. ŞİFRELİ OTURUMLU ON-DEMAND VPN

Bu VPN tipinde yönlendiriciler arasında her bir istek için ayrı bir VPN tüneli kurulur ve her bağlantı (oturum) şifreli bir yapıdadır.

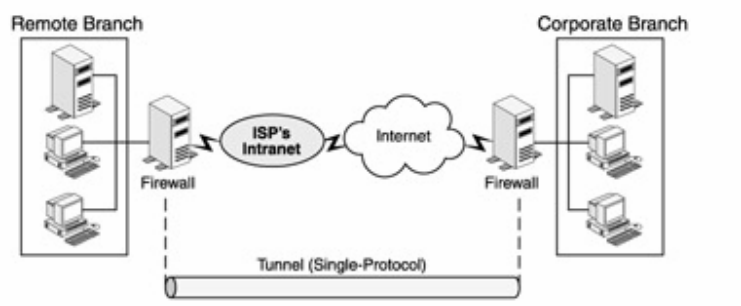


Şekil.9.1.3. Şifreli oturumlu On-demand VPN yapısı

9.2. FIREWALL-FIREWALL VPN

9.2.1. ON-DEMAND/FIREWALL TÜNELLİ VPN

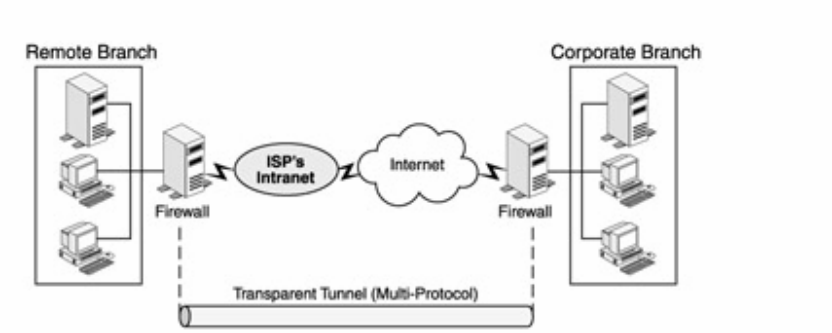
Hem müşteri hemde merkez tarafında firewall mevcuttur.



Şekil.9.2.1. On-demand/Firewall VPN yapısı

9.2.2. ÇOKLU PROTOKOLLÜ ON-DEMAND/FIREWALL TÜNELLİ VPN

Her iki taraftaki yönlendirici aynı prookolü destekleyen yapıda olmalıdır. Protokol olarak çoklu protokol tünel desteği olan IPSEC protokolü kullanılır.



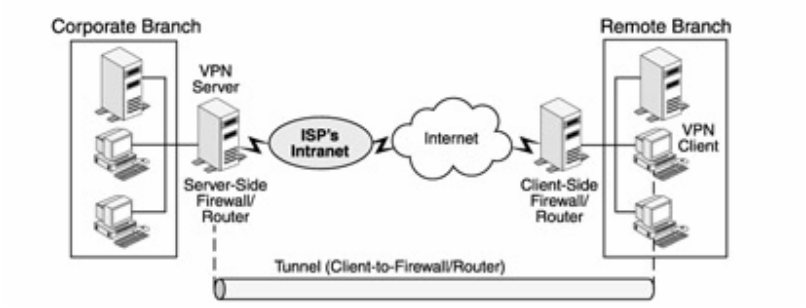
Şekil.9.2.2. Çoklu protokol/On-demand VPN

9.3. İSTEMCİ TABANLI VPN

Diğer iki VPN tipinden farkı, şifreleme ve tünel mekanizmalarının VPN istemci yazılımı üzerinde çalışmasıdır.

9.3.1. İSTEMCİ-FIREWALL VPN

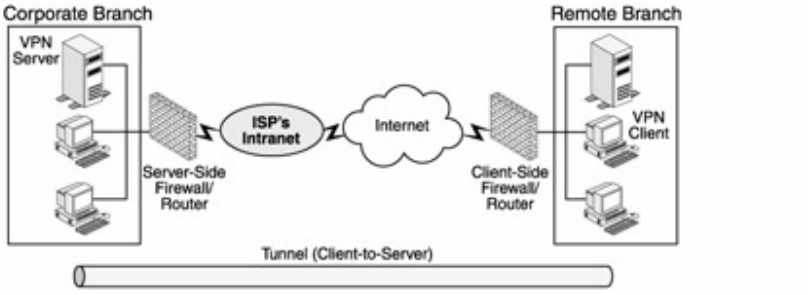
VPN bağlantısı istemci ve firewall arasında gerçekleşir. VPN istekleri firewall tarafından karşılanır.



Şekil 9.3.1. İstemci-Fırewall VPN yapısı

9.3.2. İSTEMCİ-SUNUCU VPN

Uçtan uca bir VPN bağlantısıdır ve istemci-firewall VPN bağlantıya göre daha güvenlidir.

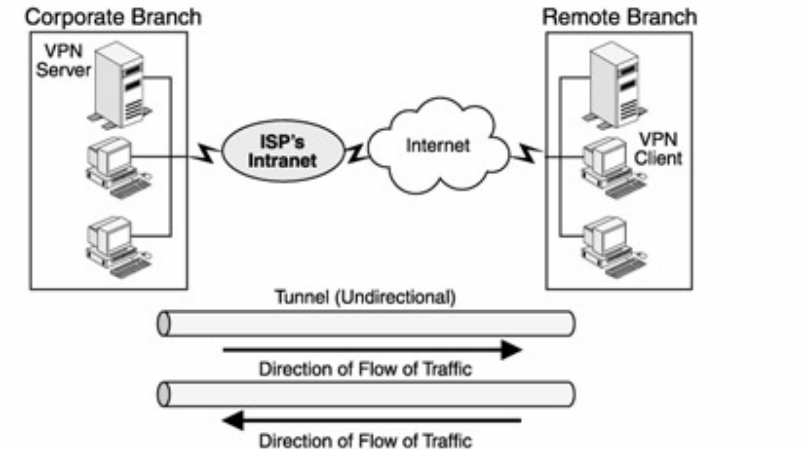


Şekil 9.3.2. İstemci-sunucu VPN

9.4.DOĞRUDAN VPN

Diğer VPN tiplerinden farkı VPN trafik akışının tek yönlü yapılmasıdır. İki uç arasında kurulan VPN bağlantısı tek yönlüdür ve veriler OSI modelinin 5. katmanında (oturum katmanı) enkript edilmektedir. Bu amaçla kullanılan protokol SOCKSv5 protokolüdür. 2 yönlü ve tek yönlü VPN yapısının karşılaştırılması aşağıda anlatılmaktadır:

- Tek yönlü VPN bağlantı yapısı daha güvenlidir.
- 2 yönlü VPN yapısında kaynak ve hedef adresler kullanılır. Tek yönlü (doğrudan) VPN'de sadece hedef ve kaynak adresleri değil, kullanıcı ID, zaman ve uygulama parametreleride kullanılır. Paketlerin içeriğine göre erişim kontrolüde yapılabilir.
- Doğrudan VPN'de IP adres spoofing riski ortadan kalkmıştır, fakat 2 yönlü VPN'ler bu tip risklere karşı açıktır.
- Doğrudan VPN yapısında şifreleme 5. katmada (oturum katmanı) yapılır ve şifreleme mekanizması bu nedenle daha iyidir.



Şekil.9.4. Doğrudan VPN yapısı