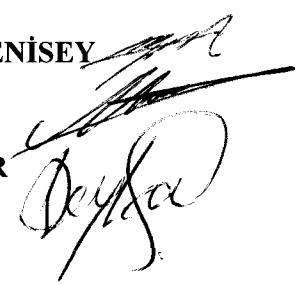
İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL KAYNAK PLANLAMASI SİSTEMLERİNDE SANAL ÖZEL BİLGİSAYAR ŞEBEKELERİ KURULMASI KARARININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ
End. Müh. Mete ÇAVDAR
507001318

Tezin Enstitüye Verildiği Tarih : 5 Eylül 2003
Tezin Savunulduğu Tarih : 10 Eylül 2003

Tez Danışmanı	Y.Doç.Dr. Mehmet Mutlu YENİSEY
Diğer Jüri Üyeleri	Y.Doç.Dr. Ahmet BEŞKESE
	Doç.Dr. Demet BAYRAKTAR



EYLÜL 2003

ÖNSÖZ

Son yıllarda özellikle bilgisayar teknolojisindeki hızlı gelişmeler bu alandaki yeniliklerinin kullanımının sadece akademik, askeri vb. alanlarla sınırlı kalması durumunu ortadan kaldırmıştır. Bu gelişmelerden en önemlisi hiç şüphesiz İnternet'tir. İnternet gün geçtikçe hayatın her alanında etkisini daha fazla hissettirmektedir dahası İnternet'in farklı insanları bir araya getiren, çok çeşitli ve fazla miktarda bilgiye kolay erişilebilmesini sağlayan bir ortam olmasının yanında giderek iş dünyası için de önemi artmaktadır ve İnternet firmaların bu yapı üzerinde faaliyet gösterebilecekleri bir ortam olma özelliği kazanmaya başlamıştır.

Ticari faaliyetlerin yoğunlaşmaya başlamasıyla birlikte güvenlik sorunları ortaya çıkmaya başlamış kötü niyetli kimselerin daha faydalı işler yapılabilmesine olanak sağlayabilme potansiyeline sahip bir ortamı baltalamalarına engel olunması gerekliliği baş göstermiştir. Bankacılık işlemleri, elektronik ticaret, ERP uygulamaları gibi kendisini kullanlar tarafından gizliliğin ve güvenliğin çok önemli olduğu sistemlerin güvensiz bir ortam üzerinde çalışmalarını devam ettirme ihtimalleri yoktur.

Sanal Özel Bilgisayar Ağları sağladıkları gelişmiş güvenlik tedbirleri ile İnternet ortamının sağladığı tüm kolaylıklardan faydalanarak aynı zamanda faaliyetlerin güvenli bir biçimde sürdürülmesine de imkan tanıyan bir teknolojidir. Bu çalışmada bu teknolojinin Kurumsal Kaynak Planlaması Sistemleri ile birlikte kullanımı konusu değerlendirilmiştir. Bu çalışmanın hazırlanması aşamasında desteklerini esirgemeyen danışman hocam Y.Doç.Dr. Mehmet Mutlu Yenisey'e teşekkürlerimi sunarım.

Eylül 2003 Mete Çavdar

İÇİNDEKİLER

KISALTMALAR

ERP :Enterprise Resource Planning
MRP :Material Requirements Planning
MRPII :Manufacturing Resource Planning
JIT :Just in Time
OPT :Optimized Production Tecniques
DRP :Distribution Resource Planning
CRM :Customer Relationship Management
CIM :Computer Integrated Manufacturing
EDI :Electronic Data Interchange
SCM :Supply Chain Management
BI :Business Intelligence
APS :Advanced Planning and Scheduling
API :Application Programming Interface
BAPI :Business Application Programming Interface
GUI :Graphical Use Interface
XML :Extensible Markup Language
VPN :Virtual Private Network
LAN :Local Area Network
WAN :Wide Area Network
RAS :Remote Access Service
İSS :İnternet Servis Sağlayıcı
POP :Point of Presence
VoIP :Voice Over IP
FTP :File Trandsfer Protocol
DMZ :Demilitarilized Zone
DES :Data Encryption Standart
RSA :Rivest Shamir Adleman
PAP :Password Authentication Protocol
CHAP :Challange Handshake Authentication Protocol
RADIUS :Remote Authentication Dial-In User Service
TACACS :Terminal Access Controller Access Control System
HDLC :High-Level Data Link Control
PPP :Point to Point Protocol
LDAP :Lightweight Directory Access Protocol
PPTP :Point to Point Tunelling Protocol
L2TP :Layer 2 Tunelling Protocol
L2F :Layer 2 Forwarding
SDLC :Synchronous Data Link Control
ATM :Asynchronus Transfer Protocol
ISDN :Integrated Subscriber Digital Network

TABLO LİSTESİ

ŞEKİL LİSTESİ

ÖZET

Bu çalışma kapsamında Kurumsal Kaynak Planlaması (ERP) sistemlerinde aynı organizasyona ait birbirinden coğrafi olarak uzak konumlarda bulunan farklı yerleşkelerin bu sistemleri kullanarak birbirleriyle uyumlu bir çalışma düzenini sağlayabilmeleri için aşılması gereken iletişim sorununa Sanal Özel Bilgisayar ağları kullanımı ile nasıl çözüm getirilecebileceği ve bu kararın alınmasında göz önünde bulundurulması gereken karar kriterlerinin neler olduğu incelenmiştir. Çalışmada Kurumsal Kaynak Planlaması sistemlerinin tarihsel gelişiminden bahsedilerek günümüzde gelinen nokta ve geleceğe dönük beklentiler açıklanmış, bu sistemlerin teknik özellikleri ve sağladığı faydalar belirtilmiştir. Daha sonraki bölümlerde Sanal Özel Bilgisayar ağlarının tanımı, fonksiyonu, güvenlik ile ilgili getirdiği çözümler kullanılan protokoller teknik bilgiler de verilerek açıklanmış mevcut alternatiflerle bir karşılaştırma yapıldıktan sonra değerlendirme bölümü ile çalışma tamamlanmıştır.

SUMMARY

Enterprise Resource Planning Systems integrate company's information concerning supply chains, customers, human resources, finance, and accounting. Capabilities of ERP systems are based on information technology. If there are more than one department, store or factory that spread out over a large geographical area, there might be a communication problem that prevent all these parts of organization from working together. Internet provides a free communication environment so it can be used as a communication infrastructure. Virtual Private Networks take Internet as its infrastructure and put away security problems by using cryptographic algorithms and some other security hardwares and softwares. Historical progress of Enterprise Resource Planning Systems, technical details of Virtual Private Networks' working principles and evaluating the decision of establishing a Virtual Private Network is also covered in this study.

1. GİRİŞ

Son yıllarda bir çok ülkede yoğun ilgi gören bilgisayarla endüstriyel yönetim teknikleri uygulamalarının içinde en yaygın olanının ve uygulamada çok başarılı sonuçlar elde edilenin Kurumsal Kaynakların Planlaması (ERP) kavramı olduğu bilinmektedir. ERP, üretimde darboğazların giderilmesine , dağıtım kaynaklarının daha iyi planlanmasına müşteri hizmetlerinin iyileştirilmesine ve stokların minimum seviyede tutularak en iyi şekilde kullanılmasına imkan vermektedir. Ülkemizde ERP yazılımları özellikle büyük ölçekli işletmelerde giderek yaygınlaşmakta ve birçok sektörde aranılır hale gelmektedir. Son yıllarda ilişkilerin, bilginin ve ürünlerin inanılmaz boyutlarda geliştiği ve hızlandığı bir dünya oluşmaktadır. Bu hareket büyük bir değişimi dolayısıyla bir o kadar sorunu iş dünyasına taşıyor. Yönetmek en azından artık eskisi kadar kolay olmuyor. Değişen koşullar, anında uyum ve karar verme yeteneği gerektiriyor. İşyerlerinin ve üretim merkezlerinin, hammadde girdilerinden üretime, ambalajdan sevkiyata, sipariş yönetiminden pazarlamaya kadar entegrasyonunu gerektiriyor, işletmelerin rekabet ortamında ayakta kalabilmeleri ve varlıklarını sürdürebilmeleri üç ana parametreye(kalite, verimlilik ve maliyet) -son zamanlarda hızlı tepki verme de eklenmiştir- bağlanmıştır (Tanyaş 1999). Bütün bunların yapılabilmesi kıt kaynakların etkin kullanılmasına bağlıdır. Bu kaynaklar da hammadde, işgücü, makine ve teçhizat ve finansmandır. Bu kaynakların etkin ve gerçekçi kullanılması üretim planlama ve kontrol faaliyetleri ile mümkündür.

Diğer taraftan günümüzün global iş ortamında şirketler hızlı bir değişim ve değişimin getirdiği yeni fırsatlarla karşı karşıya bulunmaktadır. Rekabet tüm işletmeleri daha yüksek düzeylerde hizmet vermeye iterken, gelişen teknoloji de ürünlerin yaşam döngülerini kısaltarak ve şirketleri yeni teknolojileri benimsemeye ya da pazar paylarını kaybetme riskine katlanmaya zorlamaktadır. Bu sürekli değişim ortamında rekabette başarılı olmak , değişen iş koşullarını önceden tahmin edebilmek ve bunlara hızla yanıt verebilmek demektir. Kurumların bunu yapabilmesi için işin tüm cephelerini güçlü ve esnek bir biçimde destekleyen sağlam bilgi sistemlerine

ihtiyaçları vardır. Bu sistemler iş uygulamalarından ve örgütsel yapılardan lojistik proje yönetimi, finans, servis, dağıtım, nakliye ve imalata kadar her cephede değişimlere uyum sağlama yeteneği kazandıracaktır.

Küreselleşme sürecine giren dünyada Toplam Kalite, Kalite Yönetimi gibi çağdaş kurumsal standartlar oluşmuş durumdadır. Ürün merkezli satış örgütleri müşteri merkezli pazarlama stratejilerine dönüşmüş ve esnek organizasyonlar üretimden satışa tüm firmalar için vazgeçilmez bir koşul olmuş durumdadır. Bu amaçlara ulaşmak için JIT, OPT, MRP, MRPII v.b. araçların hepsinin kullanılması gerekmektedir. Tedarik zinciri planlaması (supply chain planning) yapılabilmesi ihtiyacı duyulmaktadır. Bütün bunlar için bilginin paylaşımı söz konusu olmaktadır. Bu sorunlara cevap vermesi ve bu amaçlara ulaşabilmek amacıyla ERP (Kurumsal Kaynakların Planlanması) ortaya çıkmıştır (Tanyaş,1999). ERP bir kurumun etkin bir şekilde çalışması için gerekli bütün planlama , kontrol ve yönetim fonksiyonlarının doğru bir şekilde yönetilmesini sağlayan entegre bir sistemdir. ERP Değişim Yönetimi Müşteri Yönetimi, Teknoloji Yönetimi, Operasyon Yönetimi, Satış Sipariş Yönetimi Satınalma Yönetimi, Üretim Planlama ve Tezgah Yönetimi, Nakit Akışı Yönetimi Depo Yönetimi, Kalite Yönetimi, Bakım Yönetimi, Ofis Yönetimi, İnsan Kaynakları Yönetimi gibi profesyonel ihtiyaçlara cevap verebilecek bir sistemdir.

Kurumsal kaynakların Planlanmasının kaynağı 1960'lı yılların öncesinde kullanılan Malzeme Listesi(Bill of Material-BOM)-ürün ağaçları- kavramına kadar gitmektedir. 1960'lı yıllarda Malzeme İhtiyaç Planlama(Material Requirements Planning-MRP), 1970'li yıllarda Kapalı Çevrimli Malzeme İhtiyaç Planlama (Closed-loop MRPI), 1980'li yıllarda Üretim Kaynakları Planlaması(Manufacturing Resource Planning-MRPII) ve Dağıtım Kaynakları Planlaması(Distribution Resource Planning), 1990'lı yıllarda ise Kurumsal Kaynakların Planlanması(Enterprise Resource Planning-ERP) sistemleri geliştirilmiştir. Kurumsal kaynakların Planlanması tüm adı geçen sistemleri kapsayan bir yapıya sahiptir. 1960'larda Malzeme İhtiyaç Planlaması (MRP) olarak bilinen planlama tekniği piyasa sunuldu. MRP üretim ve envanter kontrolü alanında çok büyük bir atılım gösterdi. Bu kritik araç ilk kez olarak neyin ve ne zaman sipariş edileceğini görme olanağı sağladı. Çok seviyeli ürün ağaçlarından oluşan karışık ana üretim planları kolaylıkla oluşturulabildi ve bunun sonucu ortaya çıkan üretim ve satınalma planlarına göre mevcut envanter netleştirilebildi. Bu aracı

(MRP) başarıyla uygulayan firmalar azaltılmış envanter seviyeleri , geliştirilmiş müşteri hizmeti ve daha fazla kar gibi yararlar sağladılar. Firmalar iş proseslerini bu aracın çalışmasına uygun olarak düzenlemeleri gerektiğini çok kısa bir sürede öğrendiler. Malzeme ihtiyacının tam olarak hesaplanabilmesi için envanter , ürün ağaçları ve planların MRP için kesin ve doğru olması gerekiyordu. Bir sonraki gelişim MRP'nin geliştirdiği üretim planını onaylayabilmek için kapasite planlamasının yapılabilmesiydi.

Bunu takip eden 10 yıl içerisinde bilgisayarların gücü planlama çevrimine finansal kaynakları dahil etmeye izin verecek kadar arttı ve MRPII (Manufacturing Resource Planning- Üretim Kaynakları Planlaması) otomatik planlama sistemi için doğal bir gelişim olarak ortaya çıktı. MRPII ile MRP'nin sonraki adımı olan kapasite planlama yapılabilmekteydi. Bilgisayarların daha da güçlenmesiyle yazılım bir işi yönetmek için araç olarak daha karmaşıklaştı ve ERP programları bir araç olarak ortaya çıktı. ERP ile MRPII arasında çok önemli bir fark bulunmaktadır. ERP'nin ortaya çıkışından önceki bütün araçlar planlama üzerine odaklanmışlardı , fakat gerçekte planlama bir işi başarabilmenin sadece bir parçasıdır. ERP MRPII'den farklı olarak sadece bir kurumun çalışması için gerekli olan kaynakların planlamasında yeteri kadar iyi olmasının yanında bu kaynakların gerçekten iyi yönetilmesini sağlar. ERP bir kurumun etkin bir şekilde çalışması için gerekli bütün planlama , kontrol ve yönetim fonksiyonlarının doğru bir şekilde çalışmasını sağlar.

1.1. Ürün Ağaçları (Bills of Materials)

Ürün ağacı, ana üretim planında bir ürünü oluşturan bileşenler ve hammaddelerin tanımlanması veya listelenmesidir(Tanyaş,1999). Ürün ağacı bilgisi üretim işletmelerinde geniş bir şekilde kullanılan bir dökümandır. Bu bilgilerin içinde ürün tanımlaması olarak ifade edilen bir ürünün yapımı için gerekli olan parçalar, ürünün yapısında meydana gelen mühendislik değişikliklerinin kontrolü, servis parçaları ve bitmiş ürünler için hangi malzemelerin gerekli olacağını, ana üretim planını karşılamak için hangilerinin üretilip hangilerinin satın alınacağını belirleyen birçok bilgilere sahiptir. Diğer taraftan, ürünün tüm bileşenlerinin geriye doğru dökümünün sistematik çatısını oluşturmak amacıyla bir kodlama sistemi geliştirilmiştir. Bu sistemde son üründen başlayarak her ürün ağacına bir kademe kodu verilir. Yukarıda sayılan işlerin elle yapıldığı düşünülürse işin ne kadar zor olduğu anlaşılır. Özellikle

onlarca ürünün üretildiği bir işletmede durumun çok karmaşık olduğu görülür. Ayrıca ürünlerin stok miktarı, temin süreleri göz önüne alınmadığından yetersiz kalmış ve malzeme ihtiyaç planlamasına geçiş söz konusu olmuştur.

1.2. Ana Üretim Çizelgesi (AÜÇ)

AÜÇ, belli bir planlama ufku içinde üretilecek tüm malzemelerin hangi tarihte ve ne miktarda temin edileceğini gösteren çizelgedir(Tanyaş,1999). MRP ve MRP II'nin girdisidir. Çizelge mamüller veya satılan malzemeler için oluşturulabilir. Bağımsız talebin girildigi bölümdür. AÜÇ nin amacı;

- Belli bir müşteri memnuniyeti seviyesine ulaşmak. Bu, mamul stok seviyelerini belli bir seviyede tutarak ve müşteriye verilen teslimat tarihlerine uyarak sağlanır.
- Malzeme, işçilik ve makinaların en iyi şekilde kullanılmasını sağlamak
- Malzemeye yatırımı istenen seviyede tutmak.

Planlama için gerekli satış tahminleri pazarlama, diğer bilgiler satış tarafından oluşturulur. Genellikle, yakın dönemlere ait satış miktarları gerçek verilere dayanırken, daha sonraki dönemlere ait rakamlar satış tahminlerine dayanır. Üretim planı tahmine dayalı olduğu için hesaplamalar periyodik olarak tekrarlanarak planların güvenilirliği en üst düzeyde tutulmaya çalışılır. Satış ve pazarlama her dönem bekleyen siparişleri ve tahmin rakamlarını günceller. Zaman ilerledikçe planlama ufku da ileriye doğru uzatılabilir. AÜÇ'de geçmiş dönemler silinip, daha ileri dönemlere ait tahminler eklenir. Bu, periyodik olarak tekrarlanması gereken çok önemli bir işlevdir. Ayrıca, AÜÇ müşterilere teslimat tarihi bildirme olanağı sağlar. Bir siparişi karşılamak üzere ayrılmamış olan miktarlar, müşteriye sipariş sırasında söz verilebilir ve müşteriye teslimatlar doğru olarak planlanabilir.

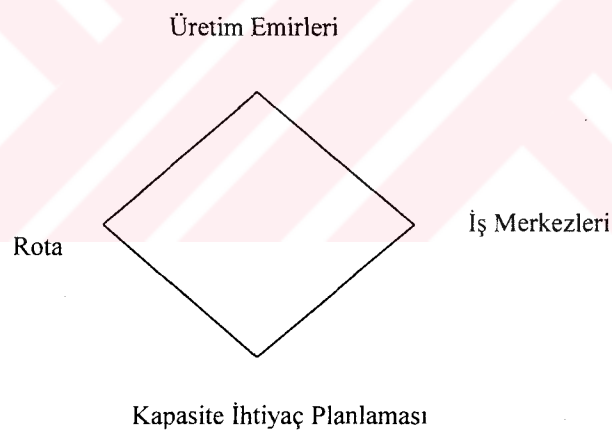
1.3. Kaba Kapasite Planlama (Rough Cut Capacity Planning)

Üretim planını ve/veya Ana Üretim Planını işgücü, makine saat, depolama, envanter seviyeleri ve üretim maliyetleri gibi anahtar (kritik) kaynaklara olan gereksinime çevirme süreci olarak tanımlanır(Tanyaş,1999). Buradaki amaç ana üretim planının uygulanabilir olduğunun denetlenmesidir. Eğer firmanın ihtiyaç duyduğu kapasite, fiili kapasiteden fazla ise alınacak ilk tedbir fiili kapasitenin arttırılmasıdır (iş gücü

arttırma, metot geliştirme, mesai-vardiya uygulama, fasona verme ile arttırılabilir). Eğer fiili kapasite artırımı mümkün olmaz ise işin başka iş merkezlerine verilmesi, üretme yerine satınalmaya gidilmesi veya en son olarak üretim planının değiştirilmesi sözkonusudur. Eğer firmanın ihtiyaç duyduğu kapasite fiili kapasiteden az ise yapılması gereken fiili kapasitenin azaltılmasıdır. Bu da iş gücü azaltma veya mesai vardiyaları kaldırma ile yapılabilir.

1.4. Kapasite İhtiyaç Planlama (Capacity Requirements Planning)

Üretim planının uygulanabilmesi için kapasite seviyelerini,limitlerini oluşturma, ölçme ve ayarlama işlevidir(Tanyaş,1999). Bunun için MRP sistemi tarafından oluşturulan açık iş emirleri ve planlanmış emirler kullanılır. Kritik olan değil, tüm iş merkezlerinin iş yükü dikkate alınır. KİP tüm girdilerle beraber malzeme ihtiyaç planından gelen net ihtiyaç, açık sipariş ve beklenen siparişlere göre her bir iş merkezi için her bir zaman diliminde gerekli kapasiteyi tahmin eder. Gerçek verilerle (makinelerin bakımı, arızalar, mevcut iş yükü)tahmin edilen kapasite karşılaştırılır.



Şekil 1.1 Kapasite İhtiyaç Planlaması

1.5. Dağıtım Kaynakları Planlaması (Distribution Resource Planning)

Bitmiş ürünün son kullanıcıya dağıtımını planlayarak envanterin dağıtımında optimizasyon sağlamaya çalışan bir yöntemdir(Tanyaş,1995). DRP, ihtiyaçlar oluştukça ilk planlamayı yapar ve bununla yetinmeyerek her değişiklik için de planları yeniler. Bölge depolarının taleplerine göre fabrikadan veya merkezi depodan planlanan sevkiyatları kapsar. DRP, periyotlar boyunca dağıtım depolarının

gereksinimlerinin projeksiyonunu yaparak ana depodan planlanmış siparişler oluşturulur. DRP, üretim kapasitesinin ve stokların etkin bir şekilde tahsis edilmesini sağlamak, müşteri servis düzeyini yükseltmek ve stok yatırımlarını düşürmek için, üretim ve dağıtım yöneticileri tarafından ihtiyaç duyulan bilgi akışını sağlar.

1.6. Malzeme İhtiyaç Planlaması(Material Requirements Planning)

MRP, 1960'lı yıllarda bağımlı talep kavramı ile birlikte ilk kez Orlicky tarafından IBM firmasında stok kayıtlarının tutulması ve takibi amacıyla ortaya atılmıştır. Daha sonraki yıllarda üretim planlaması tekniğinin destek alt sistemi olarak gelişmiş bir bilgi sistemi ve benzetim boyutuyla planlama ve kontrol tekniği olarak yerini almıştır (Kobu,1996). Malzeme İhtiyaç Planlaması felsefesi A.B.D.'de 1960'lı yılların sonuna doğru imalatın hızla geliştiği bir dönemde ortaya çıktı. Büyüyen ekonominin getirdiği yoğun talep, üreticileri yüksek hacimli seri üretime yöneltmiş olduğundan temel sorun hedeflenen üretim miktarlarını gerçekleştirmeye yetecek hammadde ve malzemenin tedariki idi.

Bu sorunu çözmek amacıyla işletme yöneticileri parçalara ilişkin statik bilgileri, ürün ağaçlarını, ürünlerin satış tahminlerini bilgisayara girmeye başladılar. Verileri eşleştiren bilgisayarlar önce gereken hammadde miktarını belirleyip sonra da mevcut stoklara ve verilmiş siparişlere bakarak ısmarlanması gereken doğru miktarları verince sorun çözülmüş oldu. Bu yöntem Malzeme İhtiyaç Planlaması olarak bilinmektedir. Malzeme İhtiyaç Planlaması son ürün için hazırlanmış ana üretim programını, burada kullanılan hammadde ve parçaların temini için ayrıntılı bir programa dönüştürmeye yönelik işlemsel teknikler topluluğudur.

Kolay ve anlaşılır bir mantığa sahip olan MRP, işletmenin üretim konusunu oluşturan mamul bileşenlerinin(hammaddeler, parçalar, alt montaj grupları) ihtiyaçlarının kesin olarak ortaya konulması ve planlanması yaklaşımıdır (Kobu,1996). Malzeme İhtiyaç Planlamasının mantığı oldukça basit olmakla birlikte yaklaşımı önemli yapan uygulamadaki veri ve işlem hacminin büyüklüğüdür. Ana üretim planında yer alan her son ürünün yüzlerce parçadan meydana gelmesinin neden olduğu işlem yükünün yanısıra, uygulamada kaçınılmaz olarak karşılaşılan değişimlerde bir dizi işlemin çok kısa zamanda yapılmasını gerektirmektedir.

İlk zamanlarda bu sistemler çok büyük boyutlu bilgisayar yardımıyla, ancak büyük şirketlerce kullanılmaktaydı. Zamanla bilgisayar teknolojisindeki ilerlemeler sayesinde performansı yüksek, fiyatı makul, yüksek hızlı bilgisayarların piyasaya çıkması ve uygulama program ve yazılımlarının geliştirilmesiyle bu sistemlerin kullanımı yaygınlaşmaya başladı. MRP sistemleri ana üretim planı,envanter durumu ve ürün ağacı bilgileri girdi olarak sağlanmadan çalıştırılamaz. Bu nedenle MRP sistemini kullanmak isteyen işletmelerin öncelikle bu girdileri sağlaması gereklidir

Çeşitli bilimsel yayınlarda MRP sisteminin uygulanması sonucu firmaların daha düşük stok düzeyleri, daha az envanter tutma maliyetleri, daha kısa üretim temin süreleri, müşteriye zamanında teslim gibi kazançlara sahip oldukları belirtilmektedir. Ancak bu faydalara rağmen MRP sisteminin bazı eksiklikleri mevcuttur. Örneğin, malzeme ihtiyaçlarını, iş ve satınalma emirlerini üretirken fabrika kapasitesinin bu üretimi gerçekleştirmek için yeterli olup olmadığını incelemez. Bu eksiklik Kapalı Çevrimli Malzeme İhtiyaç Planlamasının geliştirilmesine sebep olmuştur. Kapalı Çevrimli MRP, MRP çerçevesinde kullanılan ve üretim planlanmasının diğer fonksiyonlarını, ana üretim programını ve kapasite ihtiyaç planlamasını da içeren bir sistemdir. Burada önemli olan, atölye düzeyi kontrolün sağlanması, başka bir deyişle kapasite ihtiyaç planlamasının da planlama kapsamına alınmasıdır.

1.7. Üretim Kaynakları Planlaması (Manufacturing Resources Planning)

Ekonomide ve tüketim eğilimlerinde ortaya çıkan sonraki gelişmeler pazarın daha ağırlıklı biçimde müşteri tarafından belirlenir olması sonucunu doğurmuştur. Bunun sonrasında da imalat firmalarında stoğa yönelik üretimden, siparişe yönelik üretim biçimine doğru bir kayma olmuştur. Bu ise daha çok ürün çeşidi anlamına geliyordu ve o yıllara kadar ana sorun olan malzeme ve hammadde tedarikinin yanısıra etkin kapasite kullanımı gereği, küçük miktarlarda da ekonomik üretim yapabilir olma, etkin finansman yönetimi gibi konular büyük önem kazandı. Bu şekilde karmaşıklaşan üretim yönetimi disiplininde MRP yetersiz kaldı.

Firma üretim programını gerçekleştirecek kaynaklara sahip mi? Pazarlama satış tahminlerini gerçekleştirebiliyor mu? gibi soruların MRP kapsamında ele alınmaması yöntemin sınırlı olduğunun diğer göstergeleridir. Bu nedenle MRP'nin yalnızca envanter yöntemini kompüterize eden rolünü artıracak, üretim için gerekli olan tüm kaynakları optimize etmeyi amaçlayacak, üretim ile firmanın diğer fonksiyonlarını

bütünleştirecek bir felsefeye gereksinim olduğu ortaya çıktı. Bir imalat firmasının tüm kaynaklarının etkin olarak planlanması yönetimi olan Üretim Kaynaklarının Planlanması (Manufacturing Resources Planning-MRPII) yaklaşımı bu anlayışın ürünü olarak 1980'lerde yazılım paketleri olarak piyasalarda görülmeye başlandı.

MRPII, firma düzeyinde yürütülen tüm işlevlerin ortak bir veritabanı etrafında bütünleşmesini sağlayan bir yönetim bilişim sistemidir. Bütün üretim planlama, pazarlama, dağıtım, mühendislik ve finansal faaliyetleri kapsayan bir çatı teşkil eder (Tanyaş,1999). MRPII'yi diğer üretim planlama ve kontrol sistemlerinden ayıran özellikler şunlardır:

- MRPII bir toplam yönetim sistemidir. İş planında belirlenmiş amaçlara ulaşabilmek için gerekli tüm fonksiyonları birleştirir ve koordine eder.
- MRPII baştan aşağıya bir sistemdir. Planlama prosesi, bir dizi fonksiyonel operasyonel planlara bölünen stratejik planların formülasyonu ile başlar.
- Stratejik ve operasyonel alternatifler MRPII simülasyonu ile elenirler.
- MRPII tüm firmada aynı rakamların kullanıldığı ortak bir veritabanı oluşturulmasını sağlar.

Aslında bir paket program olan MRP II sistemlerinde bulunan temel modüller şöyle özetlenebilir.

- Satış Tahminlerinin Yapılması
- Satış Siparişlerinin Açılması ve Takibi
- Ürün Veri Yönetimi (Parça Tanımlamaları, Ürün Ağaçları)
- İş merkezleri, Operasyon Planları-Rotalar
- Ana Üretim Programı oluşturulması
- Malzeme İhtiyaç Planlama
- Kapasite İhtiyaç Planlama
- Atölye Üretim Programı
- Satın alma ve Fason Takibi
- Envanter Yönetimi (Stok kontrol)
- Atölye Veri Takip Sistemi (Üretim ve Iskarta takibi)
- Verimlilik Hesaplamaları
- Maliyetlendirme ve Maliyet Kontrol
- Sevkiyat Planlama

- Satış sonrası Müşteri hizmetleri
- Finansman Yönetimi

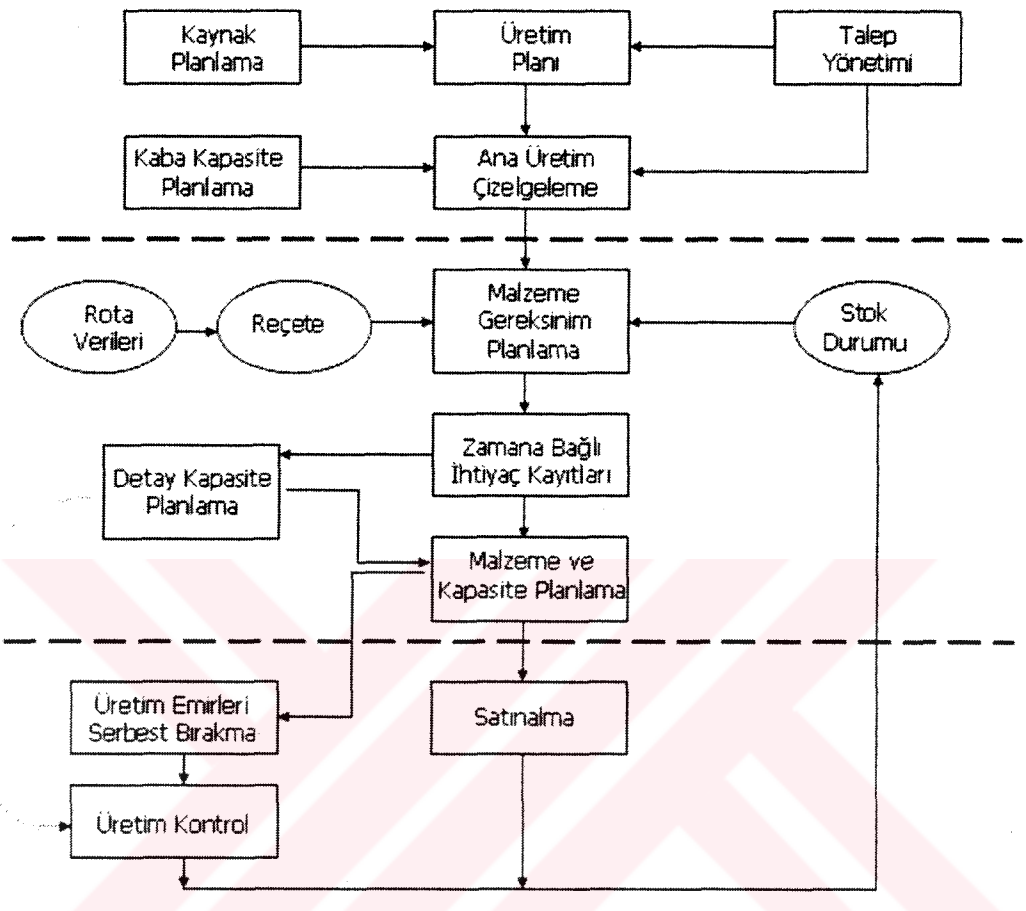
MRPII, malzeme ihtiyaç planlamasının yanısıra, kapasite ihtiyaç planlama maliyetlendirme ve maliyet kontrol faaliyetlerini eş güdümlü olarak gerçekleştirdiğinden MRP sistemini içine alan ve ondan çok daha bütünleşik ve etkin bir sistemdir. Firmaların MRPII'den beklentisi tek kelime ile üretkenlik olarak ifade edilebilir. Stok seviyelerinde azalma, müşteri hizmetlerinde iyileşme, direkt işçilik üretkenliğinde artma, satınalma maliyetlerinde azalma, fazla mesailerde azalma malzeme elde bulundurmama maliyetlerinde azalma, bilgi iletişim ve koordinasyon düzeyinde artma gibi faydalar MRPII'den beklenen faydalardır. MRPII uygulamalarında karşılaşılan maliyet kalemleri şöyle özetlenebilir:

- Donanım Maliyeti
- Yazılım Maliyeti
- İlk veri oluşturma Maliyeti
- Eğitim ve dış danışmanlık Maliyetleri

MRPII yönetimdeki mevcut kaynakların tümü ileri yönetim sistemine dahil edildiği için yönetim kaynakları planlaması olarak ta tanımlanabilir. MRPII'nin prensipleri her yerde geçerlidir. Hemen hemen bütün imalat organizasyonlarında aynı gereksinimler ve aynı yapılar mevcuttur(Kobu,1996). 1970'li yılların sonlarından beri firmalarda uygulanmaya çalışılan MRPII sistemleri firma düzeyindeki tüm kaynakları ortak bir veritabanında toplamakta ve firma içerisindeki tüm çalışanların aynı dilden konuşmasını sağlamaktadır. Ancak yoğun rekabet, uluslararası pazarlara açılması gereksinimini değişik coğrafi bölgelerde merkezi olan işletmeler için uluslararası firmaların genelinde entegrasyonun sağlanması yolunda bilişim teknolojisi için yeni bir gereksinimin doğmasına neden olmuştur.

Son yıllardaki teknolojik gelişmeler, firmaların pazarda tutunabilmelerini zorlaştırmış, klasik yaklaşımların yetersizliğinin açığa çıkması ile beraber yöneticiler kullandıkları üretim teknolojilerini ve yönetimsel yaklaşımlarını tekrar gözden geçirmek zorunda kalmışlardır. Öte yandan gümrük duvarlarının yıkılması neticesinde küresel ekonomi ve küresel rekabet kavramlarının ortaya çıkması tedarikçiden başlayarak, tüm üretim sürecini ve müşteriyi de içine alan tedarik zinciri yönetimi kavramını ön plana çıkarmıştır. Pazardaki güçlü değişimlere ve teknolojik

gelişmelere şirketlerin organizasyonel yapılarındaki kurumsallaşmaya yönelimde eklenince ortaya yeni bir kavram, Kurumsal Kaynakların Planlanması kavramı çıkmıştır.



Şekil 1.2. Standart MRPII

1.8. Kurumsal Kaynakların Planlanması

Son yıllarda birden çok işyerinden oluşan işletmelerde tüm faaliyetlerin entegrasyonu girişimi, bilişim teknolojisi için yeni bir gereksinim yaratmıştır. 1990 ların işletmeleri;

- Coğrafi olarak farklı bölgelerde kurulu fabrikalarda üretim yapan
- JIT tedarik felsefesine uygun çalışan
- Dağınık lojistik ve dağıtım sistemi kullanan bir yapı içerisindedir.

Özellikle küreselleşmeye paralel olarak, hızla yaygınlaşan çok uluslu firmalar entegrasyon gereksinimini ciddi olarak yaşamaktadır. Entegrasyon, ancak faaliyetleri

destekleyen bilginin entegre edilmesi ve ulaşılabilir hale getirilmesi ile mümkündür. Bu da MRPII'yi aşan daha üst düzey bir bilgi entegrasyonu demektir ki en iyi şekilde kurumsal kaynakların planlanması kavramı olarak ifade edilebilir. Aslında kurumsal kaynakların planlanması, küresel bilgi entegrasyonunu gerçekleştiren bütünsel bir yazılım stratejisidir. ERP kavramının gelişmesinin nedenlerini şu şekilde özetleyebiliriz:

- Fiziki olarak dağınık imalat operasyonları
- Uluslararası dağıtım zincirleri
- Uluslararası pazarlara açılma gereksinimi
- JIT tedarik sistemi
- Yüksek rekabet
- Değişken dünya pazarı şartları
- Ekonomik duvarların yıkılması
- Yönetim organizasyonlarında sadeleşme

Bu nedenlerin oluşturduğu gereksinim bilgi teknolojisindeki gelişmeler tarafından desteklenince ERP doğmuştur. Bilindiği gibi, istemci/sunucu (client/server) tasarımı, bilgiyi bir ağ üzerinde fiziki noktalara dağıtmakta, değişik bilgisayarlarda saklamakta, oluşan bu dağınık veri tabanı sistemi içinde elektronik işletim teknolojisi ve grafik kullanıcı arayüzler ile bağlantı sağlanmaktadır. Böylece üzerindeki herhangi bir kullanıcı program ve veri tabanlarının fiziki konumuna bakmaksızın, küresel verilere ulaşabilmekte dağınık veri sistemini tek bir birim gibi kullanabilmektedir. Böylece şu fonksiyonlar sağlanmaktadır:

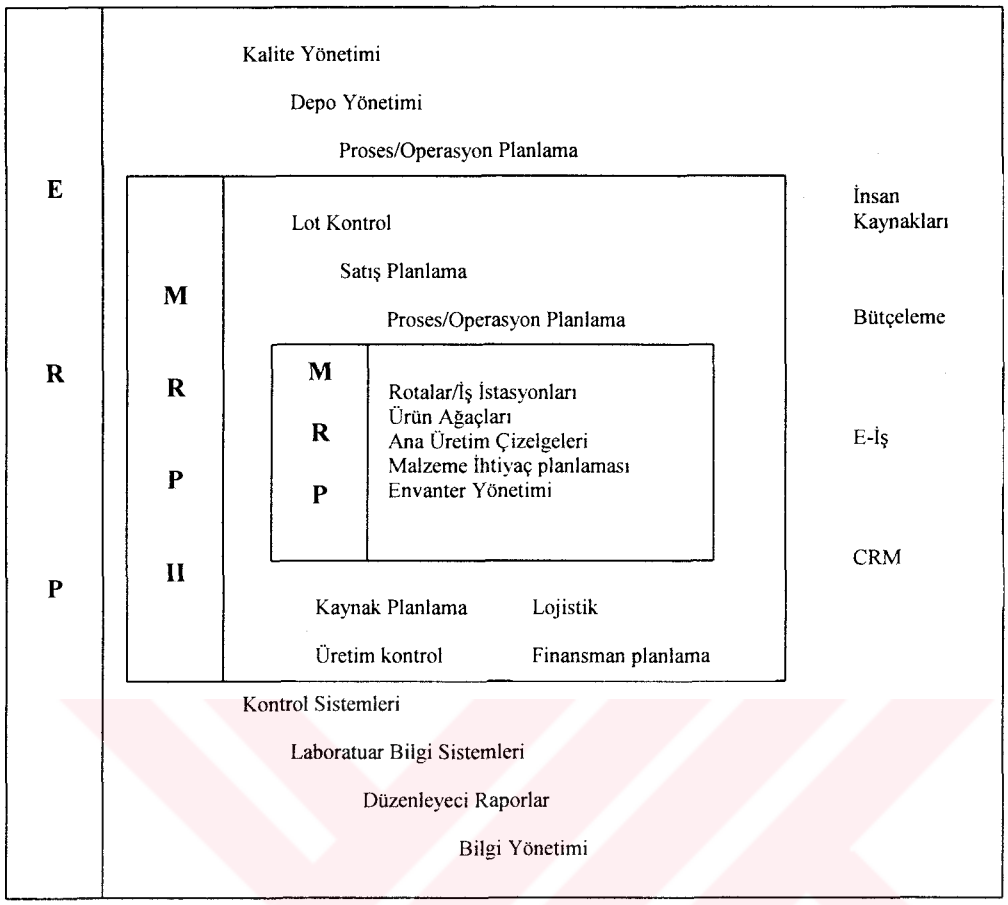
- Üst düzey bilgi entegrasyonu
- En güncel bilgiye hızla ulaşım
- Küresel lojistik, envanter kontrol ve arz/talep entegrasyonu
- Pazar/müşteri/iş dünyası oluşumlarına anında tepki.

Müşteri talebinin sürekli nitelik ve nicelik olarak değiştiği ve bu değişimin tahmin edilmesinin ne kadar zor olduğu bilinen bir gerçektir. Faaliyetlerimizi bu değişime uygun hareket edebilecek hale getirebilmenin yolu ERP yaklaşımından geçmektedir. Hem stratejik planlama çalışmaları ile belirlenen amaç ve hedeflere hem de üretim ve dağıtım kaynaklarımızın kapasite ve özelliklerine gereken ayrıntıda dikkat ederek,

faaliyetlerimizi değişime duyarlı hale getirebilmek ancak ERP yaklaşımı ile olabilmektedir.

ERP'nin diğer bir özelliği, işletmenin coğrafi olarak farklı bölgelerde (yurt içi ve dışı)bulunan fabrikalarının, bunların tedarikçi firmalarının ve dağıtımı merkezlerinin (depo) kaynaklarını eşgüdümlü olarak planlamasıdır. Bu çerçevede hangi müşteriye ait hangi siparişin hangi dağıtım merkezinden karşılanması veya hangi fabrikada üretilmesi gerektiği, tüm fabrikaların malzeme ve hizmet ihtiyaçlarının nereden karşılanmasının uygun olacağı, fabrikaların elinde bulunan makine, malzeme, işgücü, enerji, bilgi vs. üretim ve dağıtım kaynaklarının nasıl eşgüdümlü ve ortaklaşa olarak kullanılabileceği belirlenmiş olmaktadır. Diğer bir deyişle, müşteriye ait siparişin en kısa sürede, istenen kalite ve maliyette karşılanabilmesi için tüm bağlı işletmelerin dağıtım, üretim ve tedarik kaynaklarının kapasite ve özellikleri aynı anda dikkate alınmaktadır.

ERP fabrikalar arası entegrasyonu, fabrikalar bazında esneklik ilkesine uygun olarak gerçekleştiren bir sistemdir. Amaç fabrika bazında ademi merkezi yönetimin avantajlarından yararlanırken fabrikalar arası koordinasyonu ve entegrasyonu işletmenin temel stratejileri doğrultusunda sağlanmaktadır (Esteves ve Pastor 2001). Sonuç olarak, ERP işletmenin stratejik amaç ve hedefleri doğrultusunda müşteri taleplerini en uygun şekilde karşılayabilmek için farklı coğrafi bölgelerde bulunan tedarik, üretim ve dağıtım kaynaklarının en etkin ve verimli bir şekilde planlaması, koordinasyonu ve kontrol edilmesi fonksiyonlarını bulunduran bir yazılım sistemidir. Söz konusu planlama, koordinasyon ve kontroldeki temel ilke ve sistematik Üretim Kaynakları Planlaması (MRPII) ile aynıdır.



Şekil 1.3. ERP Sistemi

1.9. Kurumsal ve Üretim Kaynakları Planlamalarının Karşılaştırılması

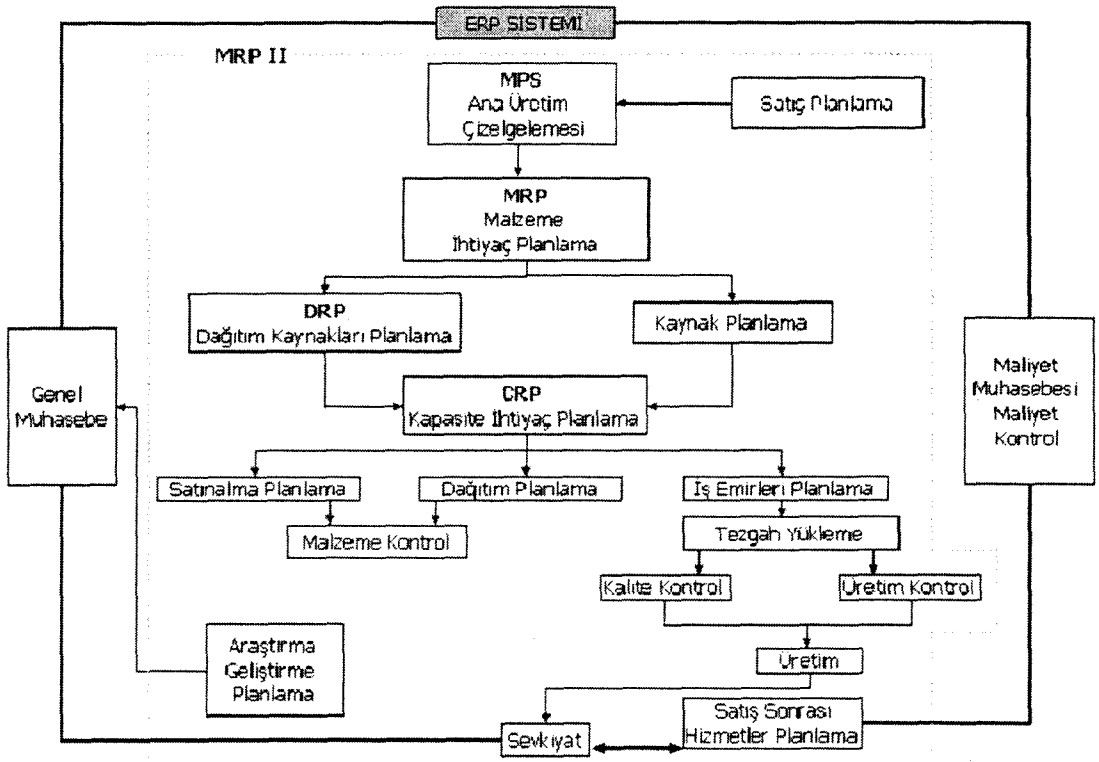
MRPII esas itibariyle bir itme sistemidir. Ekonomik kapasite kullanımını elde edebilmek için müşteri siparişlerinin yanısıra talep tahmini sonuçlarını da dikkate almaktadır. Buna karşılık DRP(Distribution Resource Planning) gerek itme ve gerekse çekme amacı ile çalıştırılabilmektedir. Temin sürelerinin kısa olması çekme uzun olması itme esaslı çalışma şeklini gerektirmektedir. Çünkü işletme hem müşteri talebine kısa sürede cevap verebilmek, hem de fabrikalarını ekonomik ölçülerde çalıştırmak zorundadır. CIM(Computer Integrated Manufacturing) sisteminin sağladığı azaltılmış temin süreleri ile MRPII ve DRP sistemleri tam zamanında yönetim felsefesine uygun olarak çekme amacı ile çalıştırılabilir(Akgeyik,1998). ERP bu entegrasyonu gerçekleştirmektedir. DRP sistemi ile alınan sipariş, MRPII sistemi

ile planlamakta, CIM sistemi ile üretilmekte ve tekrar DRP sistemi ile planlanarak müşteriye iletilmektedir.

ERP ile MRPII arasındaki temel fark MRPII'nin tek bir fabrikaya, ERP'nin daha ziyade birden çok fabrika ve tesisin entegrasyonuna yönelik olmasıdır. Tek fabrikalı işletmelerde ERP, ancak işletmenin değişim mühendisliği (Reengineering) çalışmaları sonucu birbirinden ayrılmış üretim süreçlerinin oluşturulduğu ve bu süreçlerin yönetimin kısmen bağımsız olarak hareket edebildiği durum için söz konusudur. MRPII, üretim sürecinde ve çeşitli yönetim kademelerinde bulunan her çalışanı bir donanım-yazılım sistemi ile birbiriyle doğru ve zamanında iletişim kurulabilir hale getirir. Herkes ortak bir veri tabanında bulunan aynı ve güncel verilere ulaşabilir. Bu şekilde üretim sürecinde MRPII ile sağlanan entegrasyon ERP ile daha üst ve merkezi faaliyetler düzeyinde gerçekleştirilir.ERP, hiçbir zaman MRPII'ye ikame bir sistem değildir. MRPII'nin daha geliştirilmiş bir halidir. ERP birden fazla fabrikada veya tesiste çalışan MRPII sistemlerini entegre eden bu entegrasyondan gerekli bilgileri üreten bir sistemdir. Bir başka deyişle, ERP bu yarı özerk olarak nitelendirebilecek, iş birimlerini stratejik bir şemsiye altında toplayarak kurumsal bazda bir bilgi ve kaynak entegrasyonu sağlamayı amaçlayan bir tümleşik çözümdür.

Dolayısıyla MRPII'de başarılı olmuş işletmelerde ERP etkin sonuçlar verir. MRPII deki modüller yapı ERP için de söz konusudur. ERP daha önce de belirtildiği gibi çok tesisli bir toplu yönetim için uygun bir yaklaşımdır. Fakat ERP tam anlamıyla merkeziyetçi bir sistem değildir. Tesis yöneticilerini kendi birimlerinin yönetiminde belli ölçüde serbest bırakmaktadır. Tesis yöneticilerinin kendi birimlerinde etkin kararlar verebilmesi için tüm topluluğu ilgilendiren temel bilgilere ihtiyacı vardır. ERP bu bilgileri sağlar. Bu amaçla tüm tesislerin bir şebeke halinde birbirine bağlanarak bilgi alışverişini etkin bir düzeye getirmesi gerekmektedir.

ERP işletmelere MRPII yöntem ve sistematiğine bağlı kalarak yeni ufuklar açan yeni bir yaklaşımdır. Sistemde işlenen bilgiler ile elde edilen raporlar organizasyonun plan ve programlarını yönlendirir, karar verme aşaması kolaylaşır.ERP; mali, dağıtım ve üretim yazılımlarının bütünleştirilmiş bir setidir fakat ERP, MRPII değildir. ERP, MRPII'nin genişletilmiş ve bütünleştirilmiş bir setidir. Sonuç olarak ERP, MRPII uygulamalarını içerir ve ona bazı ilaveler yapar.



Şekil 1.4. ERP ve Diğer Sistemler Arasındaki İlişkiler

1.10. Kurumsal Kaynakların Planlanması ve Bilgi İşlem Teknolojisi

Coğrafi olarak farklı bölgelerde bulunan fabrika, tedarikçi firma ve dağıtım merkezlerinin eşgüdümlü olarak planlanması yüksek düzeyde bir bilgi entegrasyonu ve iletişimini gerektirmektedir. Hatta bu entegrasyonun yurt dışı bağlantılar nedeniyle küresel boyutlara taşınması gerekmektedir. Farklı birimler arasında yatay elektronik bilgi değişim hızının yüksekliği ERP'nin temel taşlarından biridir. İstemci/sunucu bilgi işlem teknolojisi, hiyerarşik, dağıtılmış ve ilişkisel veritabanı, standart sorgulama dilleri, farklı ülkelerdeki tesisler veya bu ülkelerle olan ilişkiler nedeni ile çok dilli kullanım, 4. kuşak programlama dili kullanımı, açık sistem mimarisi uygulama programlarına grafiksel bağlantı kurabilme, personel, bakım kalite vs. çok sayıda uygulamayı kapsaması, raporlama esneklikleri, farklı üretim yapılarına (stok için veya siparişe göre üretim) uyum gösterebilme yazılımlarında bulunması gereken diğer özelliklerdir. Özelikle istemci/sunucu teknolojisi, ERP endüstrisinin yükselmesine yardım eden önemli bir etkendir (Loos,2002). Böylelikle, verinin hangi noktada olduğu önemli olmaksızın küresel boyutta veriye ulaşılması ve kullanılması olası hale gelmektedir. Küresel boyutta tasarımlanan ERP veritabanı tek bir noktadan

kullanılabilmektedir. Bir fabrikada yaratılan teknolojik bilgiden diğer fabrikalar anında yararlanabilmektedir.Yine bir bölgedeki yeni tedarikçi firmanın özellikleri diğer bölgelerdeki fabrikalarca da bilinir hale gelmektedir. Tüm stoklar (özellikle yedek parça) merkezi olarak değerlendirildiğinden stok optimizasyonu daha etkin olarak gerçekleştirilebilmektedir.

Bilgi işlem teknolojisi çok hızı bir gelişim içindedir. İşletmelerde bilgisayar kullanmayan hiçbir eleman bırakmayacak biçimde gelişme sürmektedir. ERP'de veriler, genellikle farklı yerlerdeki veri tabanlarına dağıtılmış durumdadır. Bu veri tabanları bir ağ sistemi ile birbirlerine bağlı olmak durumundadır (Loos,2002). Kullanıcının görmek istediği verilerin nerede olduğunu bilmesi gerekmemekte, sistem istenilen verileri istenilen formatta kullanıcının hizmetine sunmaktadır. Bu ilişki istemci/sunucu yapısı ile çok daha etkin bir hale getirilmektedir. Bu yapıda bir çift program aynı anda çalışmaktadır. İstemci tarafında hizmet için istekte bulunulmakta sunucu tarafında ise bu isteklere cevap verebilmektedir. Dolayısıyla müşteri ön tarafta isteklerde bulunurken arka tarafta sunucu istenilenleri gerçekleştirmektedir.

İstemci/sunucu yapısı tasarım, mühendislik, atölye veri takibi, tezgah yükleme gibi uygulamalarda büyük hız ve esneklik sağlamaktadır. ERP yazılımlarında bu yapı kullanım etkinliği ve verimliliğini artırmaktır. ERP, dağıtılmış veritabanları, yani fiziksel olarak farklı yerlerde bulunan veritabanları arasındaki entegrasyonu ile kullanıcıya istediği veriyi istediği anda verebilecek şekilde kurulmakta, veritabanları da tek bir işlemle güncellenebilmektedir(Loos,2002).

2. ERP'NİN TEKNİK YAPISI

ERP'nin en önemli teknik özelliği istemci/sunucu mimarisine uygun olarak çalışmasıdır. Eski bilgisayar sistemleri oldukça kolay anlaşılabiliyordu terminalden bazı datalar giriliyor ve bunlar ana bilgisayara gönderiliyordu. Master/Slave sistem diye adlandırılan sistemde ana bilgisayar verileri saklıyor ve ihtiyacı olan kullanıcılara yeni bir formatta gönderiyordu. Bütün veriler ana bilgisayara gidiyor ve ana bilgisayardan geliyordu. Tabi ki kullanıcı ve ana bilgisayar arasında veya ana bilgisayarda bir sorun olduğunda ana bilgisayarla iletişim kurulamadığından bütün sistem duruyordu.

PC(kişisel bilgisayar)erin fiyatlarının düşmesiyle böyle terminaller yerine PCler kullanılmaya başlandı. Bu PCler çoğu şeyi kendileri yapabilmektedir ve ana bilgisayara hemen hemen hiç ihtiyaçları bulunmamaktadır. Ofis, departman veya şirkette diğer bilgisayarlarla bir network ile bağlı durumdadırlar. Bu istemci/sunucu mimarisi herkese kendi datalarını üretme ve isterse istegi kişilere gönderme imkanı sağlanmış durumdadır.

ERP Sistemi;

- İşletim Sistemi
- Veri Tabanı
- Grafik Ara Yüzü
- Donanım Mimarisi ile çalışan bir sistemdir.

İşletim Sistemi olarak

- Dos/Windows
- UNIX
- Windows-NT
- OS/2
- Novell v.b. kullanılmaktadır.

Veri Tabanı olarak

- Oracle
- SQL-Server
- Sybase
- Informix vb. Kullanılmaktadır.

Grafik Ara Yüzü olarak

- Windows
- Windows 95
- Presentation-Manager
- OSF-Motif
- Windows-NT v.b. kullanılmaktadır.

Donanım Mimarisi olarak

- Bağımsız PC
- Net ile bağlı PC'ler
- İstemci/Sunucu Mimarisi v.b. kullanılmaktadır.

2.1. ERP Sisteminin Genel Özellikleri

İşletmelerde, bölüm içi ve bölümler arasında gerçekleştirilen faaliyetler sonucu oluşan bilgilerin, organizasyon yapısı içerisinde ilgili yerlere anında ve doğru bir şekilde akışın sağlanması "entegre sistemler" ile mümkündür. Böyle bir sistemden beklenen özellikler kısaca şöyle sıralanabilir:

- Entegrasyon
- Modüler yapı
- Kullanım kolaylığı
- Açıklık
- İşlevsellik
- Güvenilirlik
- Esneklik
- Çok dillilik
- Sektör bağımsızlıgı
- Tarihçe takibi
- Kısa kurulum süresi

2.1.1. Entegrasyon

Entegrasyon, şirket genelinde yapılan işlerde verimliliği, güvenilirliği ve kaliteyi artırıcı çok önemli bir unsurdur. Kaydedilmiş tüm veriler, ilişkisel bir veri tabanında tutulur ve tüm kullanıcılar tarafından istenildiğinde erişilebilir. ERP sisteminin sunduğu entegrasyon ile işletmelere şeffaflık ve eşitlik getirilir. İş akış yönetiminin (work-flow management) gerçekleştirilmesine imkan tanıyan bir alt yapı sunulur.

Entegre yapı sayesinde tüm birimlerin birbirleriyle koordinasyonu sağlanır ve işletme amaçlarına ulaşılmasında karşılıklı destek elde edilir. Farklı bölümlerce kullanılacak verilerin sisteme girişi sadece bir defa yapılır. Veriler doğduğu kaynakta ortak kullanıma sunulduğu için hatalı veri girişi ve veri tekrarı engellenir. Tüm bölümlerce kullanılacak verilerde tutarlılık sağlanır.

2.1.2. Modüler Yapı

ERP temel modül çatısı altında tüm sistem modülleri bağımlı ve/veya bağımsız çalışabilirler. Böylece, ERP sistemleri şirketin gelişim hızına ve yatırım kaynaklarına bağlı olarak aşamalı kurulabilir.

2.1.3. Kullanım Kolaylığı

MS-Windows gibi grafiksel ortamlarda çalışabilmenin getirdiği kolay veri girişi ve erişimi imkanı vardır. Sistemde stoklar, iş emirleri, planlama sonuçları ve kapasite yükleri grafiksel olarak izlenebilir ve grafik nesneler üzerinden işlem yapılabilir (drag, click, drop). Kullanıcılar, çok sayıdaki işlemden (transaction) seçim yaparak kendi menülerini oluşturma imkanına sahiptirler. Sıkça kullanılan veri giriş alanları her defasında yeniden açıldığında, en son kayıt edilen veriler otomatik olarak görüntülenir. Bu sayede, kullanıcının işlem yapabilmesi için mümkün olan en az sayıda veri alanını doldurması sağlanır.

İşlemlerin (transaction) her biri içerisinde yer alan yardım menüleri ile sistem kullanıcıya yol göstermekte ve yazılımın kullanımı kolaylaşmaktadır. Sistemde her kullanıcı veya kullanıcı grubu için yapılacak işler listesi (event and to-do list) alınır. Sistemdeki entegrasyonun sağlanması ve işlemlerin gerçekleştirilmesi için

kullanıcıya yapması gereken işler sunulur. Ayrıca sunulan yardım fonksiyonlarıyla (On-line Help) kullanıcının problemleri en kısa zamanda çözmesi sağlanır.

2.1.4. Açıklık

ERP sistemleri tüm ilişkisel veri tabanlarında çalışır. Böylece mevcut sistemlerde yer alan verilerin, ERP Sistemine aktarımı kolaylıkla gerçekleştirilebilir.Sistem açık sistem bağlantısı (OSI) standartlarını sağlamaktadır. Bu nedenle farklı platformlarda ve veri tabanlarında çalışan ve farklı kullanıcı ara yüzlerine sahip diğer uygulamalarla istenildiği şekilde iletişim kurabilme (online real time veya batch) ve tüm elektronik veri değişimi (EDI) imkanları sunulmaktadır. Bilgisayar destekli tasarım (CAD), bilgisayar destekli üretim (CAM), otomatik tanıma ve veri toplama vb. sistemlerle rahatlıkla entegrasyon sağlanabilmektedir.

2.1.5. İşlevsellik

Sistem, büyük küçük tüm işletmelerin ihtiyaçlarını karşılayacak fonksiyonları içerir. Modüllerin çeşitliliği, sistemin işlevselliğinin bir göstergesidir. Bu işlevsellik verilerin hiyerarşik bir yapıda, farklı seviyelerde (1.Holding, 2.Sirket, 3.Tesis, 4. Depo) tutulmasıyla desteklenir. Her seviyede, diğer seviyelere ait verilerin konsolidasyonu sağlanır. Her seviyedeki veri yönetimi kalite standartlarına (ISO 9000-14000) uygun yapılır.Sistemin, büyük çaptaki şirketlerin ihtiyaçlarına da karşılık gelecek ölçüde veri saklaması, çok çeşitli raporlamalara imkan tanımaktadır. Rapor tasarım araçları veya yazılım geliştirme aracı ile kullanıcıların ihtiyaçları doğrultusunda kolayca rapor tasarımı yapmaları ve sistemin işlevselliğini genişletme imkanları da vardır.

2.1.6. Güvenilirlik

Kullanıcılar ve kullanıcı grupları bazında farklı yetki alanları tanımlamak mümkündür. ERP sistemleri çok farklı şekillerde kullanıcı yetki sınırlaması imkânı sunabilmektedir: Kullanıcılara;

- Sistemdeki işlemleri (örn: MRP çalıştırma, stok hareketi yapma, vb.) kullanma (transaction based)
- Ekranlar üzerindeki alanlara veri girme ve değiştirme (field based)
- Verilerin tipleri bazında erişilmesi, silinmesi ve güncelleşmesi (information based) konularında sınırlama getirilebilir.

2.1.7. Esneklik

ERP Sistemi, değişik sektörlerdeki ve farklı yapıdaki firmalara uygun, esnek çözümlere sahiptir. Kontrol tabloları ile firmadan firmaya değişen özellikler, yazılım içerisinde değişiklik yapmadan sisteme yansıtılabilir. ERP sistemlerinde olmayan fonksiyonlar ise, ERP yazılım Geliştirme Aracı ile kısa sürede geliştirilebilir.

2.1.8. Çok Dillilik

ERP sistemleri genelinde, tanımlar çok dilli yapılabilmektedir. Dolayısıyla değişen şartlara göre (örn: tedarikçi ve/veya müşterinin ülkesi) çok dilli raporlar ve çıktılar alma imkanı vardır. Ayrıca, kullanıcılar ERP Sistemine giriş esnasında ekranların hangi dilde görüntülenmesini istediklerini belirtebilirler. Dolayısıyla ERP Sistemi, aynı şirket içerisinde farklı kullanıcılar tarafından değişik dillerde kullanılabilir.

2.1.9. Sektör Bağımsızlığı

ERP Sistemi, sektör bağımsız bir yazılımdır. Sistemin modüler yapısı ve işlevselliği, sektör bağımsızlığını destekleyen özelliklerdir. Üretim yapan şirketlerde ERP Sisteminin tüm uygulamaları, hizmet sektöründe veya ticari işletmelerde finans ve lojistik uygulamaları kullanılabilir.

2.1.10. Tarihçe Takibi

ERP sistemleri içerisinde, ilgili bilgiler kalite standartlarına göre oluşturulmakta ve saklanmaktadır. Sistem içerisinde yapılan bir işlemin veya belgenin kim tarafından, hangi tarihte ve saatte yapıldığına dair kayıtlar sistem tarafından takip edilmektedir. Sistem içerisindeki statik kayıtların (malzeme, ürün ağacı, rota) zaman ekseni üzerindeki değişimlerinin takibi, sistemin diğer bir önemli özelliğidir. Kullanıcılar tarih belirterek, o dönem içinde geçerli olan, önceki ve sonraki kayıtlara ulaşım sağlayabilirler.

2.1.11. Kurulum Süresi

Bu çaptaki entegre yazılımların kurulum süresi birçok faktöre bağlı olmakla beraber, ERP Sistemi, açıklık ve esneklik özellikleriyle çok daha kısa sürelerde şirketlerde üretken kullanıma geçirilebilmektedir.

3. ERP FONKSİYONLARI

ERP fonksiyonları ERP'nin yapabildikleri anlamını taşımaktadır. Tamamen uygulanmış bir ERP sistemlerinde aşağıdaki fonksiyonlar mevcut durumdadır. ERP sistemleri seçiminde de ilk önce ihtiyacınıza göre sistemin bu fonksiyonların hangilerine cevap verebildiği araştırılmalıdır.

Mühendislik

- Parça Bölüm Numarası Kontrolü
- Malzeme Listesi Kontrolü

Tam Mühendislik Değişim Ve Dökümantasyon Kontrolü

- Rotalama
- Tahmin
- Dizayn Mühendisliği

Satın Alma

- Tedarikçi Performansı
- Satınalma Sipariş Yönetimi
- Taşeron Satınalma Siparişleri

Malzeme

- Envanter Kontrol
- Ana Üretim Planı
- MRP
- Kapasite Planlama

Üretim

- Alan Kontrolü
- Kapasite İhtiyaç Planlaması
- Proje Kontrol

Maliyetlendirme

- Maliyet
- Nakit Akış Analizi
- Fiili Maliyetler
- Standart Maliyetler
- Kriz Yapısı

Finans

- Tahsil Edilecek Hesaplar
- Ödenecek Hesaplar
- Ana Hesap Defteri (Defteri Kebir)
- Yabancı Para Çevrimi

Pazarlama/Satış

- Satış Sipariş Yönetimi
- Sipariş Şekillendirme
- Faturalama
- Satış Analizleri
- Yüzde/Komisyon Hesaplama/Raporlama
- Satış Tahminleri
- Kota Hesaplama

4. ERP MODÜLLERİ

ERP Modülleri fonksiyonları yerine getiren yazılım parçalarıdır. Bunlar çeşitli ERP sistemlerinde birleştirilmiştir.

- Sistem Kontrol
- Temel Üretim
- Üretim Mühendisliği
- Envanter Kontrol
- İş Planlama
- Finans
- Tahsil edilecek Hesaplar
- Ödenecek Hesaplar
- Defteri Kebir
- Üretim Maliyet Kontrol (Standart ve Fiili)
- MRP
- Proje Kontrol
- Satınalma
- Satış Sipariş ve Kota Yönetimi
- Alan Kontrol
- Data/Emek Kolleksiyonu
- Tasarım Mühendisliği
- Tahmin
- Merkezileştirilmiş Satış Sipariş Yönetimi ve Kota
- Merkezileştirilmiş Mühendislik
- Merkezileştirilmiş Satınalma
- Döviz
- Mühendislik Değişim Kontrol

5. ERP SİSTEMİNİN AVANTAJLARI

ERP Sisteminin avantajları bir kurumun hemen hemen her bölüm ve faaliyetinde görülebilir. Bu getirilerin bazılarını sayısal olarak ölçmek mümkündür.

5.1. Faaliyetler Açısından Avantajları

Satışlar tahmin edilebilir,geçmiş yıllara yönelik karşılaştırmalı satış raporlarını analiz ederek içinde bulunulan yıla ait satışlar önceden tahmin edilebilir.Siparişler sağlıklı alınır,siparişler sisteme girilirken, aynı anda stok, üretim planı, kapasite, risk ve teklif kontrolü yapılır, sonra onaylanır. Telefon veya Internet üzerinden müşteriler özel şifrelerini girerek siparişlerini çabuk ve sağlıklı şekilde verebilirler.Planlı üretim yapılır,planlama sırasında gereken kapasite, kontrol ve tahsis edilir, hammadde veya malzemeler için stoklar yetersiz ise sistem otomatikman talep yaratır ve üretimin termin tarihini belirler.

Planlama çeşitli şekillerde yapılabilir;

- İnteraktif planlama
- İleriye planlama
- Geriye planlama
- Birden çok iş merkezine paylaştırma
- Alternatif reçete seçim imkanı
- Batch planlama
- Revizyon planlaması

Satınalma ihtiyaca göre yapılabilir, sistem tarafından yaratılan veya ihtiyaç sahiplerinin manuel olarak girdikleri talepler talep tarihi, ihtiyaç tarihi veya son sipariş verme tarihi bazında incelenir. Yoldaki siparişler rezerv edilir. Ne kadar ihtiyaç varsa o kadar alınır. Detaylı ürün izlenebilirliği, hammadde kimden alındı hangi ürün, ne zaman, nerede işlendi, bir önceki aşamadan ne zaman çıktı, nerede idi kim tarafından kontrol edildi, hangi sonuçlar elde edildi, işlemi yaparken iş merkezinde arıza var mıydı, mal iade ediliyorsa sebebi nedir şeklindeki sorulara

cevap verilebilir. Üretim kapasitesi önceden bilinebilir, mevcut üretim planı, boş kapasite izlenebilir veya senaryolara göre kapasite analizi yapılabilir. Enflasyona göre maliyet izlenebilir, ürüne, iş merkezine ve üretilen miktarlara göre sürekli değişen maliyet giderlerini anında kontrol ederek doğru kararlar verilebilir, risksiz fiyat politikaları izlenebilir(Esteves,Pastor,2001).

Kalitede bütünlük sağlanır, satın alınan hammadde ve malzemenin, üretimin ve iade malların kalite kontrolü yapılıp sonuçları saklanır. Satıcıların ve ürünlerin fiyat, teslim süresi, kalite faktörlerine göre değerlendirilmesini sistem yapacaktır. Bakım, onarım planını sistem yapar, bakım, onarım planları, üretim planı göz önüne alınarak yapılır. İş merkezi modülleri, modüllerin parçaları, kullanılacak malzeme bilgileri ve bakımı kimin yapacağı sistemde bellidir.

Telefon/ Internet ile teknolojik hız elde edilir, opsiyonel Telefon /Internet entegrasyonu ile müşteri veya satıcı, araya insan diyaloğu girmeden işlemlerini büyük bir hız ve güvenlik içinde yapabilirler. Otomatik veri toplanabilir, üretim makinaları ve barkod cihazları sürekli olarak sisteme bilgi aktarır. Kriz günleri önceden bilinebilir, ödeme ve tahsilat planları, nakit akış tablosu, sistemden öğrenilebilir, finansman ve ödemeler planlanabilir. Muhasebe işlemleri hızlanır, her işlem kendi muhasebesini kendisi yapar. Elle fiş kesme %98 azalır. Kar zarar tablosu gibi raporlar muhasebe departmanı beklenmeden yapılabilir.

5.2. ERP'nin Fonksiyonlar Açısından Avantajları

Mali Getirileri

Stokta tutma Maliyeti ↓ **%25**

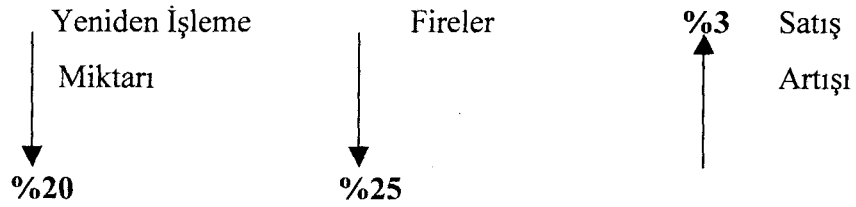
%10 Verimli Depo Kullanımı ↑

Firelerde Azalma ↓ **%12**

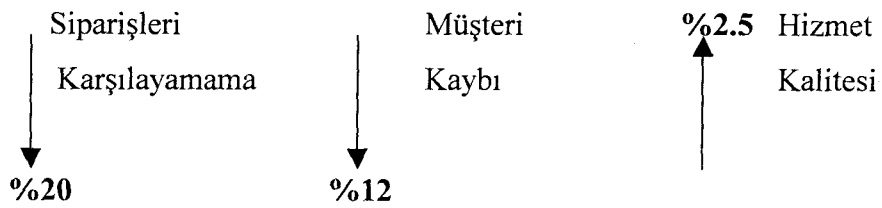
Satınalma Getirileri

Satın alma Masrafları ↓ **%3-5**

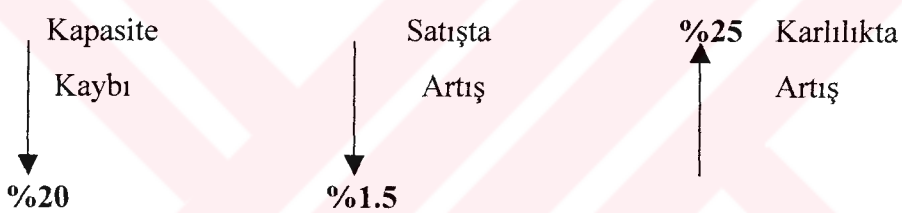
Kalite Kontrol Getirileri



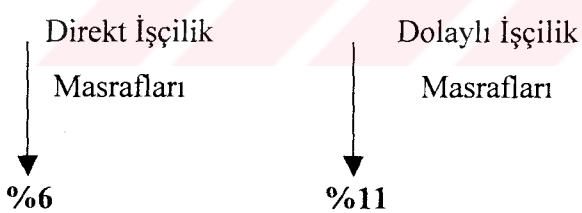
Satış Getirileri



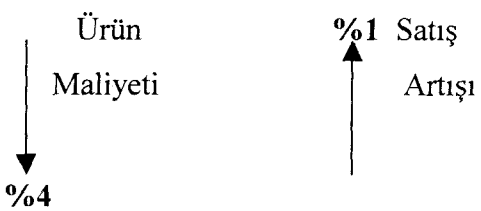
Kapasite ve Kaynak Kullanımı



Verimlilik



Ürün Maliyeti



Nakit Akış Yönetimi

- Faturalama Sürecinde Hızlanma (2 gün)
- Tahsilat Sürecinde Hızlanma (10 gün)
- Şüpheli Borç Kaybında Azalma (%12)

Ürün Alanında

- Kaynak Kontrolünde Artış
- Reaksiyon Gösterme Yerine Planlamak
- Sürekli Performans İyileştirmek
- Pazar hareketlerine Daha Çabuk Uyum
- Tedarik, Üretim Sürelerinde Düşüş
- Geriye Dönük İzleme Yapmak

Yönetim Alanında

- Zamanında ve Doğru Bilgiye Ulaşabilme
- Etkili Kararlar Alabilme
- Tüm İş Süreçlerinin Daha İyi Kontrol Edilmesi
- Daha Fazla Rekabet Gücü
- Etkin Bilgi Dolaşımı ve Paylaşımı

Pazarlama Alanında

- Pazar Payında Artış
- Rekabetçi Fiyat Avantajı
- Daha Fazla Müşteri Memnuniyeti

Finansal Alanda

- Detaylı ve Kesin Ürün Maliyetlendirme
- Geliştirilmiş Maliyet Kontrol
- Paranın Daha Verimli Kullanılması

6. GELENEKSEL ERP SİSTEMLERİ

ERP yazılımı kabaca, bir işletmedeki finans ve insan kaynakları bölümlerinin işlevlerini otomatize eden ve üreticilerin siparişleri işleyebilmesine ve üretim planı yapabilmesine yardımcı olan tümleşik çalışan uygulamalar takımı şeklinde tanımlanabilir. Tipik olarak bir ERP paketi altı temel iş fonksiyonunun yönetimini sağlayan uygulamaların bir topluluğudur. Bu altı fonksiyon şunlardır:

- Muhasebe ve denetim
- İnsan kaynakları yönetimi
- Üretim ve malzeme tedarik yönetimi
- Proje yönetimi
- Kalite yönetimi ve fabrika bakımı
- Satış ve dağıtım

Bu uygulamalar geleneksel veya çekirdek ERP sistemini oluşturur. Bu alanların her birini destekleyen uygulamalar, modüller olarak adlandırılan gruplar şeklinde düzenlenmiştir. Örneğin bir ERP paketindeki tüm muhasebe uygulamaları finans modülünde ve tüm satış gücü uygulamaları satış ve dağıtım modülü içinde içerilmiştir. Üç kategori halinde ERP modülü yaygınlık kazanmıştır:

- Finans uygulamaları:Muhasebecilik işlemleri ve faturaların anında ödenmesi için.
- İnsan kaynakları uygulamaları:İşletmelerdeki yönetici ve çalışanların personel işlemleri ile ilgili konuları yönetebilmek için.
- Üretim ve lojistik uygulamaları:Üretimin planlanması, sipariş alınması ve ürünlerin yüklenerek gönderilmesi işlemleri için.

ERP paketleri, toplam olarak 40-50 farklı uygulama içeren 12 taneye kadar farklı modülden oluşabilir. Tablo 6.1'de standart hale gelmiş bazı modüller listelenmiştir:

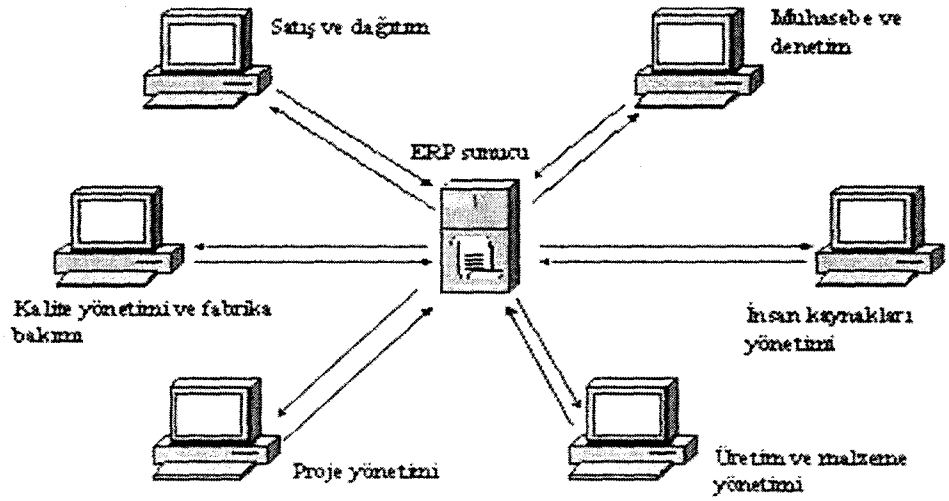
Tablo 6.1. ERP Sistemi Modülleri

Modül ismi	Açıklaması
Çalışan haklarının yönetimi	Çalışanlara yönelik hakların esnek bir şekilde yönetimi; üst düzey yönetici haklarının, emeklilik planlarının ve hisse senedi opsiyonlarının yönetimi
Denetim	Genel masraflar muhasebesi; masraf merkezi muhasebesi; kar merkezi muhasebesi; genel işlemlere yönelik siparişler; etkinliklere dayalı maliyet muhasebesi; ürün maliyeti denetimi; karlılık analizi
Çalışanların gelişimi	Çalışanların gelişimlerinin izlenmesi; işe almaların gözden geçirilmesi; işe alma ve eğitimlerin yönetimi; ücret ve kıdem ilerlemelerinin planlanması; regülasyonlarla uygunluk
Çevre sağlık ve emniyet yönetimi	Ürün emniyeti ve düzenlemelerle uygunluk
Finans muhasebesi	Genel muhasebe; alacaklar ve ödemeler; sabit kıymet muhasebesi ve yönetimi; yasal konsolidasyon yazılımı; seyahat ve masraf raporlama
Yatırım yönetimi	Kurum bütününde bütçeleme ve amortisman tahmini yapabilme
Malzeme yönetimi	Malzeme satın alma; malzeme listesi; envanter yönetimi ve denetimi; tedarikçi zaman programı(takvimi); ambar yönetimi; faturalama
Bordro	Brütten nete ve netten brüte işlemleri; düzenli ve düzensiz bordro işlemlerinin yönetimi
Fabrika yönetimi	Bakım planlaması; bakım özkaynak planlaması; bakım maliyeti muhasebesi
Ürün verisi yönetimi	Master veri ve doküman yönetimi; mühendislik değişim yönetimi; malzeme listesi yönetimi; proje yönetimi
Üretim planlama ve kontrolü	Satış ve operasyonların planlaması; kısıtlamalara dayalı planlama; malzeme özkaynak planlaması; istek yönetimi; üretim denetimi; devam eden işlerin yönetimi; kapasite planlama
Proje yönetimi	İşin kesintiye uğramasını dikkate alan proje yönetimi; takvim oluşturma ve izleme; maliyet toplama ve hesaplama; proje maliyetleri ve varlıkların kapitalizasyonu
Kalite yönetimi	Kalite planlama; kalite gözlemleme; kalite denetimi; kalite hakkında uyarı ve sertifika verme
Satış ve dağıtım	Satış siparişi yönetimi; satış siparişi girme; ürün konfigürasyonu; faturalandırma ve kesme; satış gücü yönetimi; yükleme yönetimi; satış gücü kompanzasyonları; satış analizleri
Servis yönetimi	Servis kontrat yönetimi; çağrı yönetimi; servis faturalandırma; müşteri servis ve çağrı merkezlerinin yönetimi; uzaktaki saha servis operasyonlarının yönetimi; bakım, arıza yönetimi
Zaman yönetimi	Zaman ve işten ayrılmaların yönetimi (toplam çalışma süresi, işten ayrılma durumlarına yönelik raporlar, işe gelmeme zamanlarının çetelesinin tutulması, vs.)
Hazine	Nakit yönetimi; hazine yönetimi; pazarlık/anlaşma yönetimi; sermaye/fon yönetimi; risk yönetimi; bankalarla ilişkilerin yönetimi; banka hesap raporlarının işlenmesi.

Tüm ERP sistemleri aynı modüllere sahip değildir. Ayrıca, farklı ERP üretici/satıcıları benzer modülleri farklı şekillerde adlandırmaktadır. Örneğin bazı üreticiler hazine yönetimi modülünü nakit yönetimi olarak adlandırmaktadır. Ayrıca

tüm modüller aynı uygulamaları içerecek diye bir şey yoktur. ERP sistemlerini, bir sürü uygulamanın bir araya getirildiği bir küme olarak düşünmek, konuyu hafifletmek anlamına gelebilir. ERP paketlerindeki yazılım, işletmenin çapraz fonksiyonel görünüşünü ortaya koyacak şekilde tümleşik bir yapıdadır. Bunun tersi bu uygulamaların kendi başlarına, adacıklar halinde çalışmasıdır. ERP sistemleri çekirdek iş süreçlerini, birden fazla bölümü kapsayan ve ortak verilerin kullanıldığı görevler olarak değerlendirir. Örneğin ERP sistemleri, sipariş işlemenin envanter yönetimini, envanter yönetiminin malzeme satın alma ile ilgili olduğunu ve malzeme satın almanın muhasebe ile ilişkili olduğunu varsayar.

Üretim için ham maddelerin satın alınması, bir çapraz fonksiyonel süreçtir. Çalışanlardan biri ERP içindeki satın alma uygulmasını kullanarak, şirkete gelen sipariş emrini ilgili ham maddeyi sağlayan kuruma gönderir. Ham maddeler şirkete geldiğinde, malzemeler ERP'nin malzeme yönetim uygulamasına kaydedilir ve aynı anda, satın alınan malzemelerin bedeli otomatik olarak şirketin genel muhasebesinden çıkar. Tüm bu satın alma sürecinde, belki ERP'nin kalite kontrol uygulaması da tetiklenebilir. Örneğin, bir ilaç fabrikasının malzeme yüklemeleriyle ilgili bölümü yeni bir ilaç numunesi aldığında, bu numunelerin ertesi sabah test edilmesi için laboratuvara gönderileceğine dair ilgili çalışana otomatik olarak uyarı gönderebilir. Özetle, işletme içinde bir çok süreç diğer birçok süreçle ilintilidir. ERP sistemleri, ortak bir veri takımı ile birbirine bağlı bu çapraz fonksiyonel süreçleri destekleyebilir(Esteves,Pastor,2001) .



Şekil 6.1. ERP Uygulamaları Arasındaki İlişkiler

ERP sistemleri olmaksızın iş süreçlerinin nasıl oluştuğunun analiz edilmesiyle, ERP yazılımlarının etkinlikleri daha iyi bir şekilde ortaya çıkacaktır. ERP yazılımları kullanmayan işletmelerde, tipik olarak, farklı bölümlere dağılmış çok sayıda, birbirinden ayrık olarak çalışan sistemler mevcuttur. Bu sistemler arasında bağlantı olmadığından, bölümler kolayca bilgilerini paylaşamazlar. Sonuç olarak, bölümler birbirlerinin yaptığı şeylerden haberdar olamaz ve belirli konularda eşgüdümü sağlamakta zorluklarla karşılaşır. Bu tür şirketlerde, bilgiye karşı kurumsal bir görüş ve anlayış yoktur. Çapraz fonksiyonel olmayan süreçler bile, çok sayıda kaynaktan veri elde edilmesini gerektirebilir. Dünya çapında çok sayıda yerleşkesi bulunan bir şirkette, ay sonunda finansal göstergelerin toplu sayımının yapılması hali, böyle bir durum için örnek oluşturabilir. ERP sistemi olmadığı durumda, her bir yerleşke kendi finansal durumunu izleyecek ve ay sonunda merkeze aylık rapor gönderecektir. Merkez ofiste, diğer yerleşkelerden gelen aylık raporlar kendi finans yazılımına girilerek, şirketin o dönemdeki toplam finansal performansı hesaplanır. ERP sistemi olması halinde, tüm şubeler düzenli bir şekilde kendi finansal bilgilerini kurum bütününde kullanılan aynı ERP sistemine girer. Ay sonunda ise, şirket, diğer birçok veri kaynağından veri derlemek yerine, sadece tek bir sistemi kullanarak ay sonunda defterlerini kapatabilir.

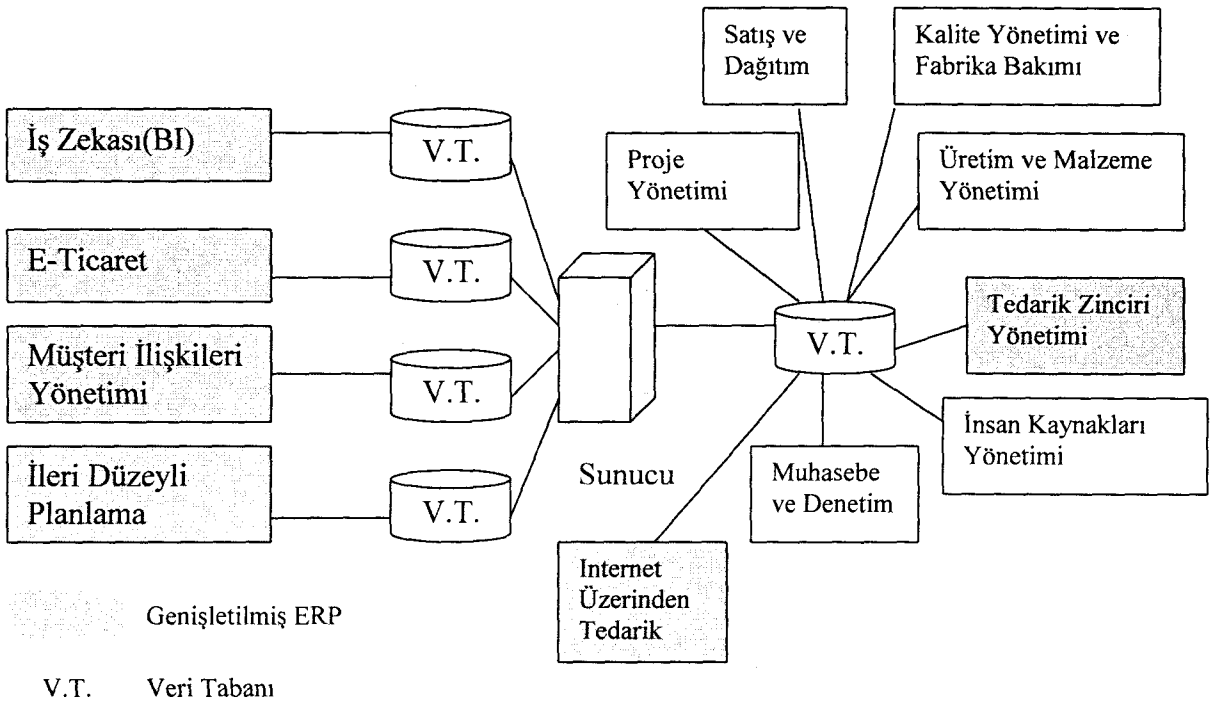
7. YENİ NESİL ERP

Genişletilmiş ERP uygulamaları olan, E-ticaret, CRM(Customer Relationship Management), SCM(Supply Chain Management), BI (Business Intelligence) Internet üzerinden tedarik, APS(Advanced Planning & Scheduling) ve portallar geleneksel ERP sistemleri tanımının dışına düşer.

Tablo 7.1. Geleneksel ve Genişletilmiş ERP Karşılaştırması

GELENEKSEL ERP	GENİŞLETİLMİŞ ERP
Muhasebe ve denetim	E-Ticaret
İnsan kaynakları yönetimi	Tedarik zinciri yönetimi
Üretim ve malzeme yönetimi	İş zekası
Proje yönetimi	Müşteri ilişkileri yönetimi
Kalite yönetimi ve fabrika bakımı	İleri düzeyli planlama
Satış ve dağıtım	Internet üzerinden tedarik

ERP yazılımı sağlayan şirketler, sözü edilen genişletilmiş özellikleri yansıtmak üzere, bir sonraki nesil uygulamalarına yeni etiketler yakıştırmışlardır. Örneğin, dünyanın başlıca ERP sağlayıcısı olan SAP, ilk başta yeni ERP sistemi uzantısını New Dimensions(Yeni Boyutlar) şeklinde adlandırmıştır. Daha sonra ise bu adlandırmayı terk ederek, SAP'ın tüm e-iş stratejisini yansıtan mySAP.com'a geçmiştir. SAP, bu stratejisini gerçekleştirebilmek için yazılım birimini, yeni gelişmeler, bakım ve ürün iyileştirme şeklinde üç iş birimi halinde yeniden yapılandırmıştır. Şimdilik, tüm ERP sistem üreticileri yukarıda sözünü edilen genişletilmiş uygulamaları sunamamaktadır. Ayrıca, ERP uzantılarının (veya genişletilmiş uygulamalar) her zaman, geleneksel ERP uygulamaları için uygun olan tek veritabanı modeli ile iyi tümleşememektedir. Bunun nedeni, genişletilmiş ERP uygulamalarının çekirdek ERP sistemi içinde oluşan hareketsel (transactional) süreçlerden farklı çalışmakta oluşudur. Bu uygulamalar, çekirdek sistemin dışında ayrı bir veritabanında yönetilmelidir.

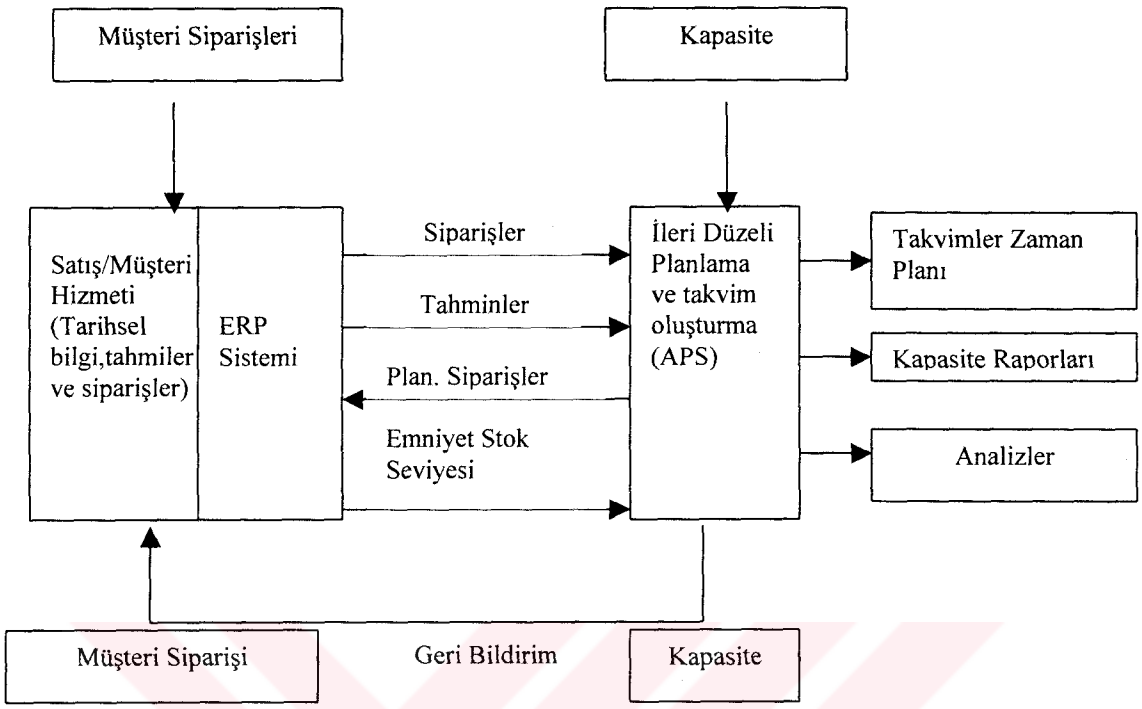


Şekil 7.1.Genişletilmiş ERP Yapısı

Örneğin APS sistemleri, diğer ERP uygulamaları ile aynı veritabanında çalıştırılamayan, şirketlerin üretim süreçlerini etkin bir şekilde planlamalarına yardımcı olabilecek yeni nesil ERP uygulamalarıdır. ERP'den farklı olarak APS emek gücü ve makinaların kapasitesini gözönüne alırken, aynı zamanda malzemelerin var olup olmadığını da kontrol eder. Malzemelerin olup olmaması ve ürünü üretebilme durumu arasında ortaya çıkan herhangi bir çelişki, plan yaratılırken çözümlenmiş olur. Çözümlenme planın yaratılmasından sonra gerçeklenmez. Üretim yöneticileri APS işlem birimi(motoru) ile deneyler gerçekleştirerek, çok sayıda eğer şu yapılırsa ne olur(what-if) senaryoları ile, farklı değişkenlerin(örneğin beklenmedik büyük bir sipariş isteği gelirse) üretim takvimini nasıl etkileyeceğini görebilir. Örneğin, sert/fırtınalı bir hava durumu veya kaza nedeniyle malzeme tedarikinde gecikme olması gibi beklenmedik olaylar halinde, gerçek(değişikliğe uğrayan) üretim takvimi derhal hesaplanabilir. Şirketler bu bilgileri anında müşterileri ile paylaşarak iletişimi ve dolayısıyla müşteri hizmet ve memnuniyetini üst düzeyde tutabilirler(Fui Hoon Nah,2001).

APS sistemleri ERP sistemlerine göre farklı mantıkla çalıştığından, ERP sisteminin dışında yer almalıdır. APS sistemi, örneğin envanter, müşteri siparişleri bilgileri ve ERP sisteminden gelen geleceğe yönelik tahminleri(forecast) elde ettikten sonra, potansiyel üretim takvimleri oluşturabilmek için kendi planlama işlem

birimini(motorunu) kullanarak analizler yürütür. APS sistemi daha sonra elde ettiği bilgileri ERP yazılımına geri gönderir.



Şekil 7.2. APS Sisteminin İşleyişi

7.1. Farklı Veri Tabanı Modellerinin Etkisi

Müşterilerin şu noktanın farkına varmaları gerekmektedir: bazı hallerde, ERP uzantı fonksiyonları (veya uygulamaları), çekirdek ERP veritabanının dışında yer alabilir. Bu model, ERP sistem sağlayıcı/entegratörünün farklı kısımları birbiriyle tümleştirmedeki başarısına(veya başarısızlığına) bağlı olarak topyekun sistemin performansını etkiler. Tabii ki ERP sistem sağlayıcıları, yazılımlarının, çekirdek uygulamalarla tümleşik olduğunu ve genişletilmiş (uzantı) ve geleneksel ERP uygulamalarının kolayca birbirine bağlanabileceğini ileri sürecektir. Uygulamalar farklı yollarla birbirine bağlanabilir. Bu nedenle şirketler, uygulamaların ne derecede biribiriyle tümleşik olduğunu ve bunların birbirine nasıl entegre edildiğini ayrıntılı olarak sorgulamalıdır.Aşağıdaki yöntemlerden birisi ile tümleşim sağlatılmış olabilir: ERP sisteminin açık API'leri mevcuttur ERP sistemindeki uygulamalar özel bir kod katmanı ile sarmallanmıştır. Bu katman onların diğer yazılımlarla iletişim kurmasına yardımcı olur. API'lerin varlığı, uygulamaların basitçe birbirine bağlanabileceği

anlamına gelmez. Bir programcı, iki uygulamayı birbiri ile konuşturabilmesi için gene de bir parça kod yazması gerekir. API'ler sadece işlemi basitleştirir.

ERP sistemi ve uzantı uygulamaları, birbirine veritabanı seviyesinde bağlanmıştır. İki sistem aynı veri yapısını paylaşır. Aynı veri yapısını paylaşan uygulamalar, örneğin genel muhasebe kısmındaki belirli alanlarda aynı sayıda karakteri veya master müşteri dosyalarını kayıt ederken aynı biçemi kullanabilirler. Bağlantının veritabanı seviyesinde sağlatılmış olması, uygulamaların birbiri ile gerçek zamanda iletişim kurduğu veya ortak bir grafiksel kullanıcı arayüzü(GUI) kullandığı anlamına gelmez. Eğer bir uygulamadaki veri değişirse, sistemler yeniden tümleştirilmelidir.

Uygulamalar, veri elde etme tekniği ile veriyi paylaşır. Bir uygulamadaki veriler elde edilerek, başka bir uygulamanın anlayabileceği bir formata çevrilmek üzere bir dosya içine yerleştirilir ve ilgili uygulamaya yığınsal bir şekilde(batch) sağlanır. Verinin yığınsal olarak bir uygulamadan diğerine gönderim sıklığı, her dakikada bir olabileceği gibi, günde bir kez de olabilir.

Uygulamalar ortak bir kullanıcı arayüzünü paylaşır. Uygulamalar birbirine o kadar çok benzer ki, kullanıcı bir uygulamayı durdurup diğerini başlattığının farkına varmaz. Genellikle, tümleşik uygulamalar ortak bir kullanıcı arayüzüne sahip değildir. Uygulamalardan biri kullanıcıya, örneğin gömülü bir link veya özel bir ikon yardımı ile diğer uygulamayı başlatma veya erişime olanağı verir.

Uygulamalar gerçek zamanda veri paylaşır, bu tekniğe, olay düzeyinde(event-level) tümleşim adı da verilir. Bu tür bağlantı olması halinde sistemlerden biri diğer uygulamadaki bilgileri anında, ya asenkron(tek yollu) ya da bisynchronous(çift yollu) iletişim kurup iki uygulama arasında mesaj alışverişi ile güncelleştirir.

Tümleşim terimi, bir ERP sistemi ile üçüncü şahıs bir firmanın ürünü arasında ya son derece gevşek ya da sıkı bir bağlantı anlamına gelebilir. Gevşek bir bağlantıda ERP sistemi gerekli API'lere sahiptir, fakat diğer uygulama ile ortak bir arayüzü veya veri yapısını paylaşmaz ve veri değiştokuşunu sadece yığınsal olarak(batch) gerçekleştirebilir. Sıkı bir tümleşimde ise, iki uygulama müşteriye hazır olarak veri tabanı düzeyinde tümleşik olarak sağlanır. Uygulamalar ortak bir kullanıcı arayüzünü paylaşır ve veriler gerçek zamanda mesaj değiştokuşu ile uygulamalar arasında gidip gelir. Bu durum, arzu edilen kesintisiz tümleşim olarak bilinir(Fui Hoon Nah,2001).

Tümleşim seviyesi üründen ürüne değişir. ERP üreticileri, yatırımın geriye dönüşü(ROI) açısından, sadece en çok kullanılan ve en büyük müşterilerinin(veya en önemli) kullandığı uygulamaları tümleştirme eğilimindedir. Böyle bir durumda bile çok derin(sıkı) bir tümleşim için geliştirme çalışmaları yürütmek, zaman alıcı ve masraflıdır. Anlaşılacağı üzere, bir ERP üreticisinin, uygulamalarının tümünün çekirdek ERP sistemi ile tümleşik olduğunu iddia etmesi, oldukça temkinli olarak karşılanması gerekir ve bilinçli bir inceleme ve analizi gerektirir.

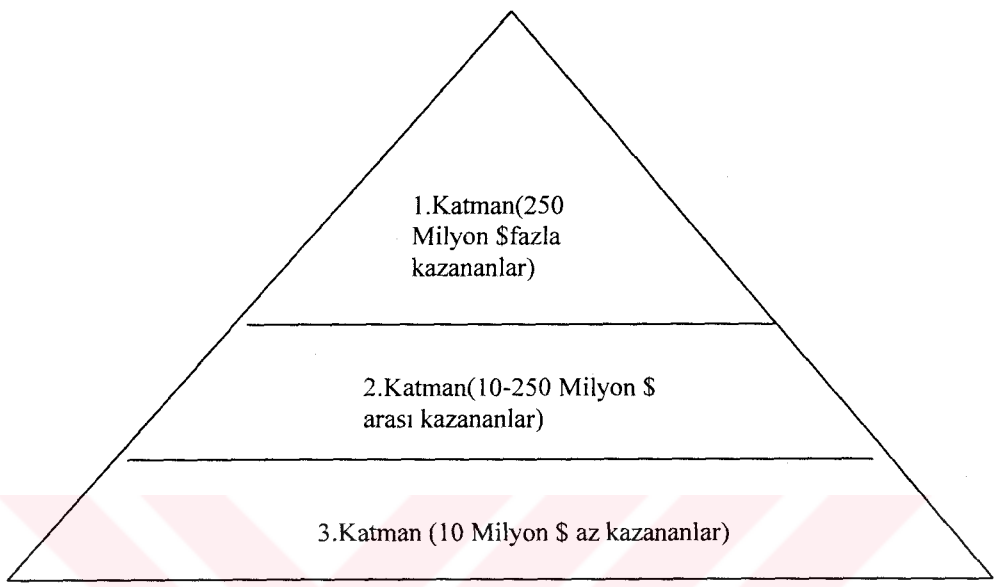
7.2. ERP Yazılımı Üreticileri

ERP yazılım pazarı teknoloji endüstrisi içindeki en büyük ve en karmaşık olanlardan birisidir. AMR Research firması her yıl hazırladığı Enterprise Resource Planning Software raporunda en büyük ERP yazılımı üreticilerini listelemektedir. Bu liste sürekli olarak değişmektedir. Aşağıdaki tabloda son yıllardaki en büyük 34 ERP üretici firması sıralanmıştır.

Tablo7.2. ERP Yazılımı Üreticileri

1. SAP	18. Scala International
2. Oracle	19. Systems Union Group
3. PeopleSoft	20. Deltek Systems
4. Baan	21. MAI Systems
5. JBA International	22. Fourth Shift
6. SSA	23. PSI AG/Psipenta
7. SCT	24. Glovia International
8. Geac Computer(1999 yılında JBA International tarafından satın alındı)	25. Lilly Software Associations
9. Intea International	26. Solomon Software
10. Epicor Software	27. Damgaard
11. IBS Group	28. Kewill Systems
12. Lawson Software	29. Navison Software
13. QAD	30. Made2Manage Systems
14. Cincom Systems	31. Western Data Systems
15. IFS	32. Visibility
16. InterBiz(CA International'ın bir bölümü)	33. FlexiInternational Software
17. MAPICS	34. Macola

1998'lerde ERP pazarının dinamikleri oldukça açık ve öngörülebilir idi. Üreticiler, 1-katman (Tier 1), 2-katman ve 3-katman üreticiler olarak pazarı paylaşmışlardı. 1. Katmandaki ERP üreticileri en büyük ERP sağlayıcıları olup ürünleri en büyük müşterileri hedefliyordu. Buna karşılık 2 ve 3. katmandaki üreticiler, ürünlerini tipik olarak yıllık gelirleri 250 milyon USD'nin altındaki müşterilere satmaktaydılar.



Şekil 7.3. Kazançlarına Göre ERP Üreticileri

1990'lı yılların ortaları ile sonlarına doğru, temel olarak Y2K(2000 yılı sorunu) nedeniyle ERP pazarında bir patlama yaşandığı söylenebilir. İşletmelerin önemli bir kısmı, eski sistemlerini Y2K uyumlu hale getirmek için yeniden programlama işine girişmek yerine, yeni bir sisteme geçmeyi tercih etmiştir. Bu geçişte diğer önemli bir etken, Web temelli iş hareketlerinin (yani e-ticaret, B2B, B2C etkinlikleri) olmazsa olmaz bir hale dönüşmesi ve eski (legacy) ERP sistemleri ile böyle bir şeye kalkışmanın zor oluşu diyebiliriz.

7.3. ERP Pazarında Ortaya Çıkan Yeni Satış Taktikleri

1998 yılından başlayarak, yavaş yavaş 1.katmandaki ERP üretici firmaların pazar büyüme hızları düşmeye başlamış ve 1999 sonlarına gelindiğinde pazar doyuma ulaşmıştır. Bundan sonra, ERP pazarında önemli bir değişime tanık olunmuştur. Bu tarihe kadar büyük müşteriler dışındaki diğer şirketleri hedeflemeyen 1. katman ERP üreticileri birdenbire orta katman müşterilere odaklanmaya başlamıştır. Birdenbire ortaya çıkan bu ilginin nedeni ise, AMR Research'ün bulguları ile anlaşılmıştır. AMR raporuna göre, tüm dünyadaki üretim yapan şirketlerin (60-70 bin adet) ancak

yüzde 20'sinin yeni ERP sistemlerine terfi ettiği ortaya çıkmıştır. Bu sayıya, üretim yapan işletmeler dışındaki diğer sektörlerden küçük ve orta düzey kuruluşlar da eklenecek olursa, potansiyel pazarın büyüklüğü iştah kabartacak boyuta ulaşmaktadır. AMR'nin vardığı neticelere paralel diğer endüstri analistlerinin bulguları, KOBİ lerin varlığının, ERP üreticileri için bir can simidi rolü oynayabileceğini ortaya çıkarmıştır. Bunun üzerine büyük ERP üreticileri, orta ve küçük işletmelerin ilgilerini çekmek üzere, sistemlerini belirli sektörlere hizmet edecek şekilde, önceden konfigüre ederek sağlama yoluna gitmişlerdir. SAP'nin Ready-to-Run ve Oracle'ın Fast Forward programı bu yönde atılmış adımlardır. Tüm bu girişimlerin yanında, IBM gibi bazı firmalar da, belirli ERP sistemleri kurulmuş hazır donanım sistemleri sağlamaktadır. Örneğin IBM AS/400, RS6000 ve Netfinity sunucuları üzerinde hazır yüklenmiş olarak 6 adet ERP yazılımı satmaktadır. Özetle 1998'lerin sonlarına doğru ERP pazarında aşağıdaki satış taktiklerinin oluştuğu gözlenmektedir.

Tablo 7.3. ERP Satış Taktikleri

Taktik	**Özellik**
Önceden konfigüre edilen sistemler	Satıcı, belirli bir endüstriye hizmet edecek yazılımı geliştirir
Toplu halde(bundle) satılan sistemler	Satıcı, yazılımı donanım üzerine önceden kurarak satar
Önceden tümleşik hale getirilerek satılan sistemler	Satıcı, ERP yazılımını diğer üçüncü şahıs yazılımları ile tümleşik hale getirerek satar
Sabit fiyatlı sistemler	Satıcı; yazılım, donanım ve hizmeti önden aldığı sabit fiyata satar
ERP yazılımı kiralama	Satıcı sistemi, aylık, kişi başına sabit bir ücret karşılığında kiralar

7.4. Orta Kademe Pazarında ERP Satış Taktikleri

Orta kademe müşterileri karakterize eden en önemli özellik, bu firmaların geleneksel ERP yazılımlarının gerektirdiği yüksek lisanslama ücretleri ile başedemiyeceğidir. Bunu farkeden ERP üretici/satıcı firmaları bu firmaları kazanabilmek için, daha baştan yüksek bedeller gerektirmeyen ve kiralamaya kadar uzanan değişik taktikler geliştirmişlerdir. Bu arada daha da ilginç bir yaklaşım olarak, ERP yazılımlarını kiralayan firmalardan bazıları(Oracle Business Online) uygulamalara Internet

üzerinden erişim olanağı sağlamışlardır. Yani uygulamalar müşterinin kendi yerinde koşmamakta, sistemler kiralama sağlayan firma (ASP Application Server Provider) tarafından barındırılmaktadır (hosting).

7.5. ERP Üreticileri ve Genişletilmiş Uygulamalar

Büyük ERP üretici firmalarının pazar paylarını artırabilmek için, sadece yeni fiyat politikaları gütmeleri veya kullanımı kolay yazılımlar yaratmaları yeterli görülmemektedir. Yeni pazar segmenti daha farklı yazılımlar istemektedir. Bu yeni istemler sonucunda ERP'nin tanımı da yeni bir boyuta dönüşmüştür. Bu yeni yazılımlar/uygulamalar, APS, BI, CRM, SCM, e-ticaret, Internet üzerinden tedarik ve portallardır. Peki işletmeler ERP çekirdek yazılımının üzerine, bu yeni genişletilmiş uygulamaları neden istiyorlar? Ne de olsa bir ERP sistemi, kuruluşlar için başlı başına büyükçe bir yatırım sayılabilir. Çekirdek ERP sistemleri, genel olarak arka ofis(back-office) yazılımları olarak bilinir. Bu yazılımlar, bir işletmenin günlük iş hareketlerini destekler. Her ne kadar çekirdek ERP sistemleri bir işletme için oldukça yararlı ve önemli ise de, kuruma kattığı katma değer fazla değildir. Buna karşılık, APS, BI, CRM, SCM ve e-ticaret gibi uygulamalar şirketin iş süreçlerine fazladan değer katmaktadır.

Daha önceden de belirttiğimiz üzere, geleneksel ERP sistemleri bu uygulamaları içermemektedir. Bu tip uygulamalar üçüncü şahıs firmaların yazılımlarınca sağlanmaktadır. Artık ERP üretici firmaları da bu uygulamaları çekirdek ERP yazılımları ile birlikte sağlamaktadır. Katma değer sağlayan genişletilmiş uygulamalar normal olarak kendi başlarına çalışabilirlerse de, bu şekilde çalışmak kuruma fazla bir değer sağlamaz. Genişletilmiş ERP uygulamalarının işletmenin iş süreçlerine katma değer katabilmesi ve etkin olabilmesi için, çekirdek ERP işlevleri ile veri alışverişi yapması gereklidir.

Anlaşılacağı üzere, geleneksel ERP üreticileri ile bu zamana kadar işleri genişletilmiş ERP uygulamaları yaratmak olan üçüncü şahıs üreticiler birbirine rakip duruma gelmektedir. ERP üreticileri bu uygulamaları kendi çekirdek yazılımlarıyla tümleştireceğinden, bu işlemi kesintisiz tek bir sistem içinden yapabilme üstünlüğüne sahip gözükmekteler. Buna karşılık üçüncü şahıs firmalar, kendi yazılımları ile çekirdek ERP yazılımlarını arabağlaşım yazılımları (middleware, vs.) aracılığı ile yapmak durumundalar. Diğer yandan, üçüncü şahıs firmaların odaklanmaları tekil

fonksiyonlar(APS, BI, CRM, SCM, e-ticaret, portal) üzerinde olup, bu işleri uzun süredir yaptıklarından, bu konularda daha fazla deneyimli ve bilgilidirler. Geleneksel ERP üreticileri ise, bu uygulamalar konusunda deneyim ve know-how kazanmak durumundalar.

7.6. ERP Sistemlerinin Web Üzerinden Çalışabilirliği

Internet'in çok uzaklara erişim olanağı tanıması ve kesintisiz doğası, onun hızla bir uygulama platformu haline gelmesine yol açmıştır. Birden fazla yerleşkeye dağılmış çalışanlar, kolay bir şekilde Internet üzerinde koşan uygulamaları kullanabilirler. Bu tür uygulamalar aynı zamanda mobil çalışanlara da yarar sağlar. Çünkü, dizüstü bilgisayarlarına hantal büyük yazılımları yüklemelerine gerek kalmaz. Artık, cep telefonu ve avuçiçi bilgisayar gibi küçük mobil ve telsiz aygıtlardan çalıştırılabilecek uygulamalar geliştirmek mümkün olmaktadır. Bu eğilim ve gelişmeler, ERP üreticileri üzerinde de bir baskı yaratmıştır: ERP üreticileri yazılımlarını, Internet ortamı için yeni baştan tasarımlamak durumundadır. Bu durum, işlerin yürütüldüğü geleneksel yerlerin dışında kalan çalışanların önünde yeni ufuklar açmakla kalmaz, aynı zamanda, ticari iş ortaklarına ve müşterilerine Web tarayıcı yardımıyla uygulamalarına erişim olanağı sağlayan şirketler için de, müşteri servisi, SCM ve iş yürütülen ortaklarla ilişkiler açısından, daha önceleri olmayan fırsatlar yaratır.

Yazılımların en baştan Internet üzerinden çalışacak şekilde yazılması(Web temelli yazılımlar) basit bir işlem olmayıp, ERP üreticileri, uygulamalarının Internet üzerinden çalışabilmesi için ürün mimarilerini köklü bir şekilde yeniden gözden geçirmek durumundalar. Geleneksel ERP uygulamaları, bir istemci/sunucu(C/S) ortamında çalışmak üzere tasarımlanmıştır(daha eski, anaçatı sistemlerde çalışan ERP yazılımlarının varlığı da unutulmamalıdır). Bu tür yazılımlar hem sunucu hem de istemcide önemli miktarda kod yazılmasını gerektirir. Bu durumu belirtmek üzere şişman istemciden (fat client) söz edilir. Şişman istemciler Internet ortamı için uygun olmayıp, bu ortamda veri paylaşılmaya kalkışıldığında (C/S uygulamaları sunucu ile istemci arasında büyük oranda veri paylaşımını gerektirir) uygulamanın performansından ödün verilmek durumunda kalınır. Ayrıca, şişman istemcileri dağıtabilmek için yegane yol, kullanıcı makinasına yazılım kurmaktır. Bu durum ise Web üzerinden uygulamaları çalıştırmanın asıl amacını yok eden bir etkendir. Buna karşılık mevcut yazılımların Web üzerinden çalışacak hale getirilmesi(Web enabled)

ise göreceli olarak daha basit bir işlemdir. Bu tür yaklaşımda uygulama kullanıcıların bir Web tarayıcı arayüzünden verileri görmesine ve veri girişine olanak tanımak üzere, uygun hale getirilir(uyarlama işlemi). Yazılımın temel mimari ve tasarımı aynı kalır. Dolayısıyla, uygulama Internet üzerinden iyi çalışmayabilir veya program geliştiriciler, performans düşmesine yol açmamak için uygulamanın belirli(kısıtlı) kısımlarını Web üzerinden çalışır hale getirmiş olabilirler.

Web'e uydurulmuş bir yazılım, mimarisi baştan Internet üzerinden çalışmak üzere tasarlanmış bir yazılıma göre çeşitli sorunlar barındırır. Örneğin, geleneksel ERP uygulamalarında genel olarak, bir müşteri siparişi girmek kadar basit bir fonksiyon için kullanıcının bir sürü adımdan geçmesi gerekir ve göreceli olarak karmaşık kullanıcı arayüzleri söz konusudur. Uygulamanın Internet üzerinden etkin bir şekilde çalışabilmesi için, süreçler ve arayüzler basitleştirilmelidir. Bu arada Web arayüzleri, geleneksel ERP yazılımlarında olmayan, gerçek zamanda sohbet kullanıcı davranışının ve Web sitesi kullanımının izlenmesi, e-posta uyarılarının gönderilmesi ve müşterinin daha önceki ziyaretlerinden elde edilen bilgilere göre müşteriye sunulacak Web sitesinin kişiselleştirilmesi gibi özgün bazı özellikler sunarlar. Web temelli bir ERP yazılımında şu tür yeni özellikler bulunmalıdır:

- Diğer yazılımlara, işaret edip tıklayarak erişme olanağı
- Ya hiç ya da çok az eğitimin gerektiği basit arayüzler
- Sohbet, beyaz tahta uygulaması(whiteboarding) ve uzaktan denetim
- Gerçek zamana yakın bir erişim
- Kolayca konfigüre olabilen masaüstü

Özellikle Internet üzerinden çalışmak için yazılmış yazılımların(Web'e uydurulmamış) mimarisi, C/S yazılımlarından temel olarak çok farklı olup, büyük bir olasılıkla nesne yönelimli(OO: object-oriented) kod ve Java(veya C#) gibi platformdan bağımsız bir dil kullanılarak yazılmıştır. Kod, geleneksel C/S kodundan daha esnektir.

7.7. Yeni Nesil ERP'nin Düşünce Tarzında Yarattığı Değişimler

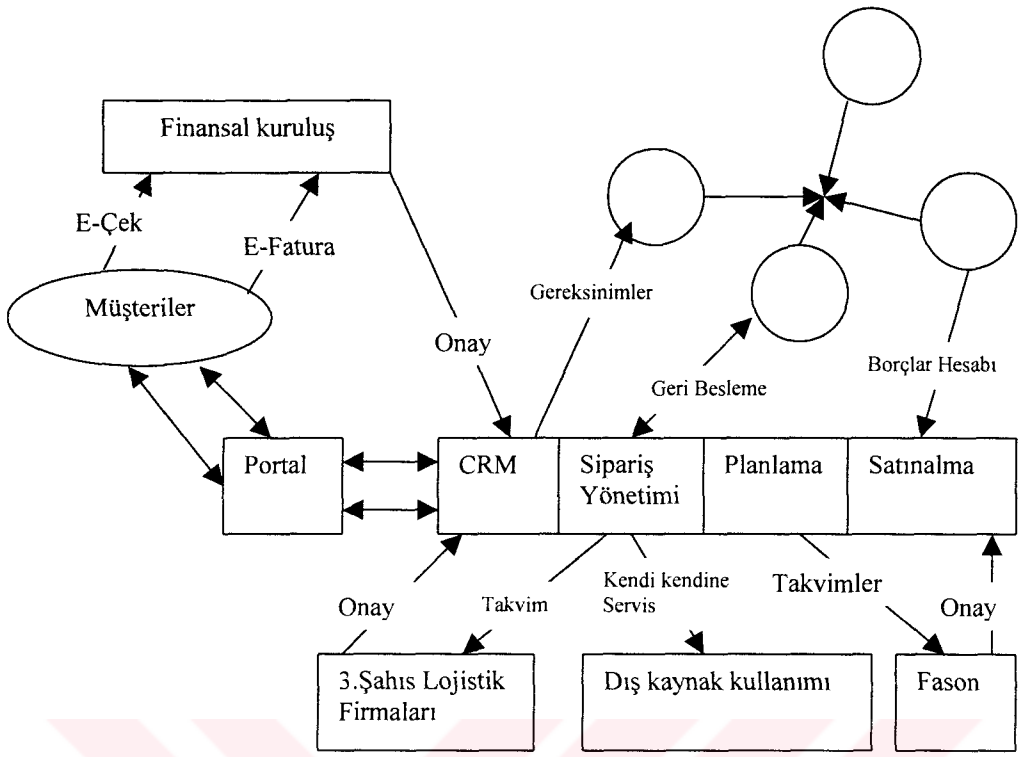
ERP yazılım sağlayıcılar daha genişletilmiş uygulamalar/ürünler, yeni servisler ve yeni arayüzler sağlamalıdır. Daha doğrusu, ERP üreticileri, ERP sistemlerini,

amaçlarını ve sağlama koşullarını nasıl algıladıklarına dair görüşlerini köklü bir şekilde değiştirmelidirler.

Başlangıçta sadece kurum içinde kullanılmak üzere tasarlanmış olan ERP sistemleri, tek bir iş yerinin fiziksel sınırlarının ötesine uzanabilecek özelliklerle donatılmış olmalıdır. Yani, işletmelerin birbiriyle etkileşime girmesine, veri paylaşabilmesine ve iş süreçlerinin tanımlanmasında diğer şirketlerle işbirliği yapabilmesine olanak tanımalıdır. Bu yeni düşünce tarzına, kurumun dışarıya doğru uzatılması/genişletilmesi adı verilmektedir.

EDI:Electronik Data Interchange

Şekil 7.4.Geleneksel ERP Sistemleri



Şekil 7.5.Genişletilmiş ERP Modeli

ERP yazılım üreticilerinin, günümüz dünyasında kurumlarda olup biten şu değişimlerin farkına varması gerekmektedir:

- İşlerin Internet hızında yürütülmesi gereği
- Şirketler arası tümleşim
- Değişen kullanıcı rolleri
- Endüstri toplulukları ve ticaret borsalarının ortaya çıkışı
- İçeriğin uygulamalardaki önemi
- Modern işletmelerin artık sadece iç iş süreçlerine odaklaşarak ayakta kalamayacağı, ayrıca iş ortakları ile işbirliklerinin oluşturması görüşü.

Yukarıda belirtilen etkenler tümüyle yeni uygulama gereksinimleri oluşturmaktadır. Bu yeni dünyada, ERP sistemleri geleneksel satın alma işlemlerini desteklemesinin yanında, ticaret borsaları, müzayedeler(mezat) ve e-bankacılık gibi uygulamaları da desteklemesi gerekmektedir. Örneğin, müşteri hizmetleri uygulamaları sadece müşteri verilerini izlemekle kalmamalı, aynı zamanda müşterilerle Web üzerinde etkileşime de olanak tanımalıdır. ERP sistemleri işbirliği içinde geliştirme ve planlama yapabilmeye ve her bir iş ortağına tüm sürecin görünüşü görebilmesine

imkan tanımalıdır. İş süreçlerinde bu değişimleri gerçekleştirebilmek için ERP yazılım üretecilerinin aşağıdaki yeni teknolojileri yoğun bir şekilde kullanması gerekecektir:

- XML
- İşbirliği olanağı sağlayan araçlar
- Kullanımı kolay iş akış araçları
- Hemen hemen hiçbir eğitim gerektirmeyen kullanıcı arayüzleri ve etkileşimli sohbet gibi özellikler.

ERP yazılımının Web'e uygun hale getirilmesi ile, daha baştan yeniden tasarlanarak(reengineer) Web temelli olması arasında önemli oranda bir fark vardır.

8. GELENEKSEL ERP MİMARİSİ

Modern bir ERP sistemi istemci/sunucu bilgi işlem ortamında çalışmak üzere oluşturulmuştur. Bu mimaride uygulama, uygulamanın büyük bölümünü, işe yönelik mantık kurallarını ve veritabanını içeren bir sunucu ile, uygulama işlemeyi gerçekleştiren, veritabanındaki verilerle etkileşen bir şişman istemciden oluşur. Kullanıcının akılsız terminallerde çalıştığı ana bilgisayar tabanlı sistemlerden farklı olarak, bir şişman istemci C/S uygulamayı çalıştırabilmek için gerekli veri ve mantık kurallarını da üzerinde barındırır. C/S yazılımı masaüstünü akıllı hale getirdiğinden ana bilgisayar tabanlı sistemlere göre önemli oranda bir iyileşme elde edilir. Buna karşılık, C/S yazılımının bazı sakıncaları da vardır:

- Yazılım, her bir masaüstü makinasına elle kurulmalıdır
- Şişman istemci, son kullanıcı makinasının toplam kapasitesinin büyük bir bölümünü yiyip bitirir
- Yazılımda herhangi bir terfi/güncelleştirme olduğunda, istemci yeniden elle kullanıcı makinasına kurulmalıdır
- Yazılım belirli özelliklere sahip bir donanım üzerinde çalışabildiğinden kolayca dışarıdan(kurum dışından) kişiler tarafından erişilemez.

8.1. ERP Sistemine Web Tarayıcı ile Erişim

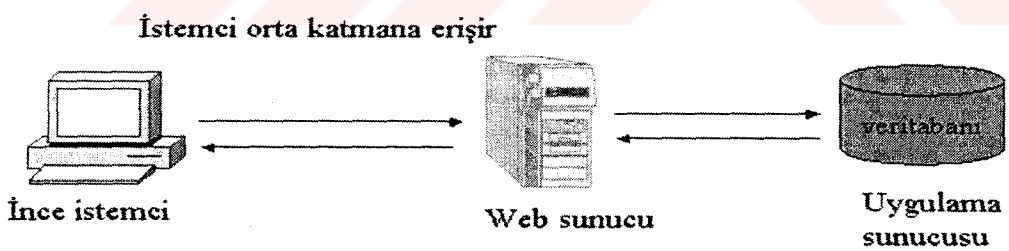
Web tarayıcıların geliştirilmesiyle, kullanıcıların, şişman istemci tarafı uygulaması gerekmeden uzaktan ERP sistemine erişmesi mümkün olmuştur. ERP yazılımı sağlayan firmalar bu uzaktan erişimi ya kendi teknolojileri yardımıyla ya da Citrix,WinFrame gibi çok kullanıcılı uygulama sunucusu yazılımları yardımıyla sağlamışlardır. Citrix, WinFrame gibi bir sunucu yazılımı, herhangi bir donanım üzerinde, herhangi bir bağlantı tipine(modem, Internet , İntranet veya WAN, VPN) sahip bir istemcinin Windows uygulamalarını çalıştırabilmesine olanak tanır. Web tarayıcı ile erişim olanağının eklenmesiyle, ERP ürününün temel mimarisi ve işlevi değişmez. Sadece, kullanıcının uygulama ile etkileşmek için kullandığı araç

değişir. Fakat, geleneksel ERP ürünlerine sadece Web arayüzleri ekleyerek yeni nesil ERP ürünlerine geçilmiş olmuyor. Bundan daha fazlası gerekli. ERP üreticileri Internet 'in olanaklı kıldığı genişletilmiş ürünleri ortaya çıkarmalıdırlar. Bunlardan kastedilen:

- İş süreçlerinin hızlı ve basit bir şekilde yeniden konfigürasyonu
- Hemen hemen hiçbir eğitim gerekmeyen sezgisel arayüzler
- Gerçek zamanda veya gerçek zamana yakın veri erişimleri
- Gerçek zamanda sohbet ve beyaz tahta uygulaması(whiteboarding) gibi etkileşimli ve işbirliğine dayalı özellikler
- Gerçek zamanda analiz
- Herhangi bir iç veya dış kullanıcıya açık erişim

8.2. N katmanlı Mimari

Bir ERP sistemine Web arayüzü eklenmesiyle, yukarıda sözü edilen genişletilmiş özellikler getirilmiş olmaz. Çünkü, ürünün İstemci/Sunucu mimarisi değişmez. Yazılımın, gelecek nesil e-iş yeteneklerini içerecek şekilde yeniden yazılması gerekir. Çok katmanlı bir mimari kullanılmasıyla, uygulama, ince bir istemci(ön yüz), bir Web sunucu ve bir uygulama ve veritabanı sunucusuna dağıtılmış olur.



Şekil 8.1. İstemci Sunucu İlişkisi

N-katmanlı mimari kullanan yazılımlarda şu yararlar sağlanması olasıdır;Uygulama ERP sistemindeki sadece belirli veri parçalarına erişecek şekilde tasarlanabilir. Bu şekilde, eğer sisteme kurum dışından kullanıcılar erişecek ise, bu kullanıcıların tüm ERP verisine erişmesi kontrol altına alınmış ve emniyetli çalışma sağlanmış olur.

Kullanıcılar doğrudan ERP sistemine erişmediğinden, uygulamanın performansı, çalışabilirliği ve yanıt süresi iyileşmiş olur.Yazılım geliştiriciler, uygulama arayüzünü, veri ve fonksiyonları daha basit ve daha mantıklı bir şekilde sunmak üzere yeni baştan tasarlayabilirler.Web uygulama sunucusunda kullanılabilen, kümeleme(clustering), yük dengeleme (load balancing) ve arıza olması durumunda yüksek çalışabilirlik teknikleri sayesinde uygulama daha ölçeklenebilir(scalable) ve güvenilir kılınabilir.

Yazılım üreticileri kolayca N katmanlı bir mimariye geçiş yapamazlar. İlk önce, normal olarak büyük, yekpare ve katı bloklar halinde yazılmış olan geleneksel uygulamalarını, küçük, taşınabilir bileşenler(components) halinde parçalamaları gerekir. Parçalar birbiriyle mesajlaşma ve iş akış teknolojileriyle etkileşir. Çeşitli bileşenlerin kendi veritabanları mevcut olup, bileşenler Business Application Program Interfaces(BAPI) adı verilen arayüzlerle çevrelenmiştir. AMR araştırma kuruluşuna göre, kullanıcılar da bu tür bir mimariden yarar sağlamaktadır. Bu yararlar şu şekilde özetlenebilir:

- Daha hızlı gerçekleme
- Süreç ve organizasyonel değişimlere karşı daha hızlı yanıt
- Daha esnek kullanım
- Daha iyi sistem bakım/onarımı
- Diğer yazılımlarla daha basit tümleşme
- Tedarik zinciri iş ortaklarıyla daha sıkı tümleşim
- Yeni uygulamaların daha hızlı olarak ortaya çıkarılışı
- Daha iyi ölçeklenebilirlik
- Teknolojik değişimlerden daha az etkilenme

9. VPN TANIMI ve GELİŞİMİ

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'lerin ortalarında ve 1990'ların başlarında hedeflerine ulaşabilmeleri için kullanılan teknoloji telefon hatlarını kullanan uzaktan erişim servisleriydi. Şirketler, yöneticilerinin taşınabilir bilgisayarlarına veri şıkıştırabilme yeteneğine sahip hızlı modemler yerleştirip ofisteki sunuculara bağlanabilmelerini sağlayabiliyorlardı. Çalışanların ve yöneticilerin yapması gereken sadece bulundukları ortamdaki telefon hattını modemlerine takmak ve uzaktan erişim sunucularına şifreleri yetkisinde bağlanmaktır.

1990 sonlarında kurumlar, uzaktan erişimin şirketlerinin sağladığı avantajları daha çok anlamaya başladılar ve bazı büyük şirketler ülke içinde ücretsiz aranabilecek telefon numaraları ile çalışanlarına bu hizmeti sunabildiler. Uluslararası iş yapan kurumlarda ise, milletlerarası telefon ödemeleri söz konusu olduğu için uzaktan erişim servisleri şirketlere ciddi bir maliyet getirmekteydi (Scott,Wolfe,and Erwin ,1998). Internet üzerinden paylaşılmış veri ağlarına erişebilmek, o bölgedeki yerel Internet servis sağlayıcının aranması söz konusu olduğundan uzaktan bağlantılarda ödenen ücretlerin büyük ölçüde düşmesine imkan sağlamaktadır. Hatta büyük Internet servis sağlayıcıları, tüm dünyaya yayıldıkları için , aynı kullanıcı adı ve şifre ile dünyanın çoğu yerinden yerel POP (point of presence) numaraları aranarak Internete erişilebilir. Sanal özel ağlar (VPN) yerel Internet servis sağlayıcı ve kurumsal yerel ağlar arasında güvenli bir tünel üzerinden veri iletimi gerçekleştirerek çalışır.Kurumsal ağlarını daha önceden bir takım güvenlik sorunları yüzünden Internete bağlamayan şirketler yeni VPN teknolojileri ile güvenli bağlantılar sağlayabilecekler.

VPN, özel sanal ağ demektir. Büyük ve orta ölçekli kuruluşlar için şube, bayi fabrika ve mağazaları ile güvenli ve ekonomik iletişim kurmak, iş akışını etkin olarak

yönetmek, önemli stratejik avantajları da beraberinde getirmektir. Kurumsal sanal ağlar kuruluşların şube, bölge ofisleri, bayileri, depoları, fabrikalarının Internet üzerinden veya Türk Telekom data şebekesi üzerinden kendi ağlarına (Intranet) erişerek tüm ticari ve kurumsal uygulamalarını ekonomik ve güvenli bir şekilde çalıştırmalarını sağlayan bir hizmettir(Scott,Wolfe,and Erwin ,1998). VPN'de amaç birbirinden uzakta bulunan yerel alan ağlarını Internet veya Telekom'un data şebekesini kullanarak birbirlerine bağlayarak firmaya özel güvenli bir ağ (Intranet - VPN) oluşturmaktadır.

Bugün bilgisayar ağları uygulamaları geniş bir şekilde istemci/sunucu karşılıklı etkileşimli şekle dönüşmüş bulunmaktadır. İstemciler tarafından kullanılan bilgilerin büyük bir bölümü LAN sunucuları üzerinde bulunan dosyalar, dökümanlar veri tabanları veya sayısal bilgilerin diğer şekilleridir.İdeal olan, istemcilerin işlerini gerçekleştirmek için gerek duydukları bütün bilgilerin , istemciler gibi aynı LAN'a bağlanmış bulunan sunucular üzerinde bulunmasıdır. Ancak kurumlar büyüdükçe merkez ve çevre ofislere bölünmektedir. Bu durum da VPN uygulamasını gerekli kılan en önemli etkendir. Sanal özel ağların cazip hale gelmesinde etken olan bir diğer konu da artan oranda elemanların LAN sunucularda ve kurumsal ağlarda uzak noktalarda çalışmaya başlamış olmalarıdır. Bu elemanların işlerini uygun bir şekilde yürütebilmeleri için kurumsal LAN'lara, WEB uygulamalarına ve diğer sunuculara uzaktan erişim sağlamaları büyük önem taşımaktadır. Dışarıda çalışan kişilerin yüzdesi arttıkça bu durum çok daha büyük önem kazanmaktadır. Pek çok çalışan kişi ve yöneticiler küçük ofislerden veya evde kurdukları ofislerden (Small Office and Home Office) yürütmektedirler ve hareketli (Mobile) çalışma geçmiş yıllara oranla inanılmaz boyutta artmış bulunmaktadır.

VPN, ayrı noktalar arasında veri iletimine ihtiyaç duyulan durumlar için ideal bir erişim şeklidir. Bu bağlantı biçiminde, her bağlantı noktası diğer noktalarla veri iletişimini gerçekleştirir. VPN, kurumların Internet omurgasını kendi omurgaları gibi kullanmasına olanak sağlayan bir hizmettir. Güvenlik, bağlantıyı sağlayan yönlendiriciler veya bunlar arkasındaki VPN ağ geçitleri aracılığı ile, kurumsal trafiğin bir noktadan diğerine aktarılırken şifrelenmesiyle gerçekleştirilir (Guichard, Pepellnjak,2000)

Yakın bir zamana kadar genel ve özel ağlar arasında her zaman keskin bir ayrım olmuştur.Yerel telefon sistemleri ve Internet gibi genel ağlar birbirinden bağımsız

uçların birbirleriyle bilgi iletişimini, değiş tokuşunu sağladıkları geniş bir ortamdır.Bu genel ağlara ulaşma imkanı olan herhangi birisi ulaşabileceği toplam kullanıcı sayısı düşünüldüğünde bunların çok küçük bir bölümüne ulaşır.Özel ağ ise bir kurumun sahip olduğu ve sadece kendi organizasyonunun içerisindeki üyelerin birbirleriyle bilgi alışverişine imkan veren bir yapıdır. Bu yapıda bir taraftan gönderilen bilginin ancak bu ortam içindeki kullanıcılar tarafından görülebilmesi temin edilir. Yerel ve geniş alan ağları (LAN,WAN) bu özel ağlara örnektir. Özel ve genel ağlar arasındaki bağlantı bir geçitkapısı üzerinden sağlanır bu noktada kurulan ateş duvarları sayesinde de genel ağdan özel ağa ulaşmak isteyen davetsiz misafirler engellenebilir ayrıca özel ağ içerinde kullanıcıların ulaşım yetkileri sınırlandırılabilir.

Günümüzden fazla uzak olmayan bir dönemde de kuruluşların kendi yerel ağlarının dış çevreden yalıtıldığı adeta izole edilmiş adacıklar şeklinde yapıların oluşturulduğu bilinmektedir. Bu şekilde bir yapı ile aynı kuruma ait bulunan farklı yerlerdeki şubelerin herbirinde diğerlerinden farklı e-posta sistemleri isimlendirme yapıları hatta diğer şubelerle uyumlu olmayan farklı ağ protokollerinin kullanıldığı durumlar ortaya çıkmıştır bunun sonucu olarak bu bilgisayar sistemlerine kuruluşun sahip olduğu kaynaklardan aslında olması gerekenden daha büyük miktarlarda paylar ayrılması mecburiyeti ortaya çıkmıştır. Gelişen teknoloji ve artan müşteri istekleri sebebiyle bir süre sonra bu şubeler arasında bağlantılar kurulması ihtiyacı doğmuştur. Bu sorunda farklı hızlarda çalışan kiralık telefon hatları kullanılarak çözülmüştür. Bu şekilde kuruluşlar her zaman ulaşılabilir ve kendilerine özel bir ağ yapısına kavuşmuşlardır öte yandan bu şekilde bir çözüm pahalı olabilmektedir aylık sabit bir ücret ve hattın kullanımından doğan mesafeye bağlı bir ücretlendirme şekliyle özellikle geniş bir bölgede faaliyet gösteren kuruluşlar için bu yöntem uygun bir seçenek olmaktan çıkmaktadır. Özel ağlar ayrıca işi gereği organizasyonun fiziksel ortamı dışında çalışan ve sürekli dolaşmak zorunda olan satış görevlileri vs gibi çalışanların bulunduğu ve bu kullanıcıların şirketin yerel ağına ulaşabilme imkanının olmadığı durumlarda yetersiz kalmaktadır bu sorun bu kullanıcıların uzak bir noktadan bir modem vasıtasıyla yerel ağa ulaşabilmeleri sağlanarak her ne kadar çözülebilse de bu yöntem bazı durumlarda çok pahalı olabilmektedir (Scott,Wolfe,and Erwin ,1998). Bahsedilen tüm bu sorunların varlığı günümüzde özel sanal bilgisayar ağları adı verilen ve genel bir ağ üzerinden özel bir iletişim

ortamını yazılım, donanım veya ikisinin kombinasyonlarını kullanarak yaratan bir teknolojinin ortaya çıkmasını hızlandırmıştır.

10. VPN TİPLERİ

10.1. İstemci Girişimli VPN

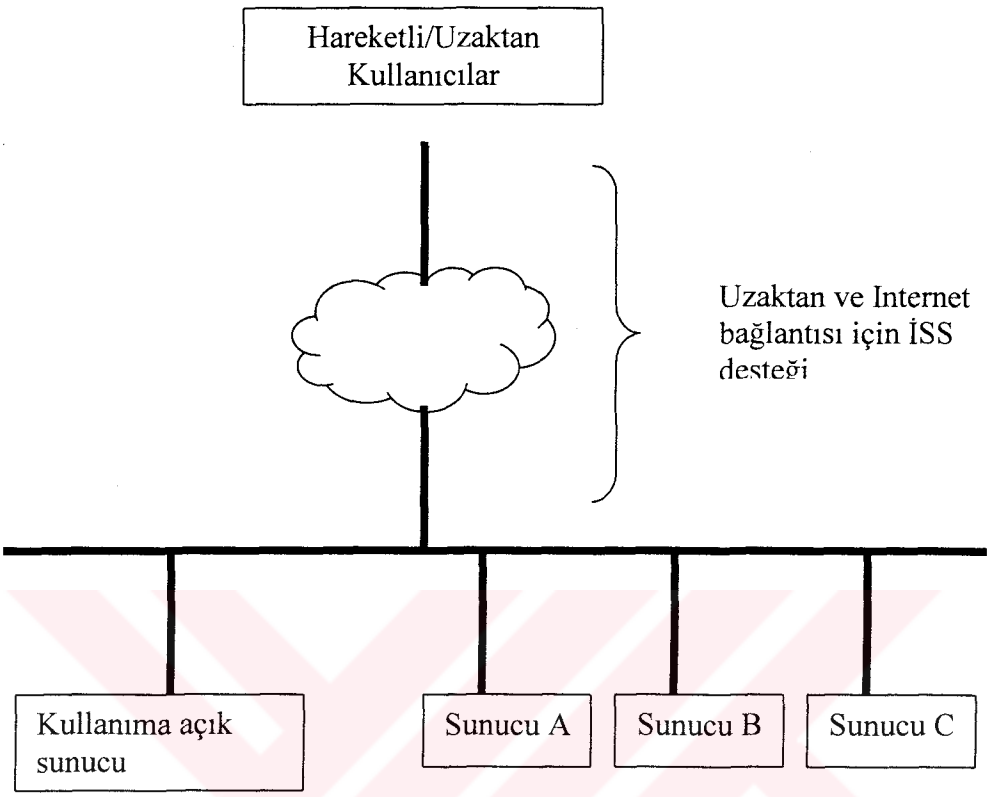
Uzaktan erişim aygıtları kullanıcıların kurumları ile ilişkiye geçmelerini ve gerekli işlemlerini yapmalarını olanaklı kılan arama kapıları (dial-in ports) donatılmıştır. Bu yapıda, yapının sahibi kurumdur, işlemler ve kontrol kurum tarafından yürütülür. Bu organizasyonda İSS'ler çok ender olarak uzaktan erişim noktalarından Internete erişim sağlarlar. Bu yapı uzaktan erişim için kullanılan istemci-girişimli VPN diye adlandırılır. Bunun da nedeni İSS lerin ne ilettiklerinin genellikle farkında olmamasıdır(Manas,2000).

10.2. İSS Girişimli VPN

Bu uygulamada, yapının sahibi İSS dir ve uzaktan işletim aygıtlarının işletimi ve kontrolü İSS lerin elindedir. Bu durumda VPN güvenliğinin sağlanması tümüyle İSS lere aittir. Eğer İSS servisi tüm ülkeye dağılmış durumda ise ve çalışanların hareketleri çok değişken bir durumda ise, bu uygulama yararlı olabilir. Bu durumda bilgisayar ağını ve kurumsal LAN'ı korumak için ek bir güvenlik desteğine gereksinim vardır. Örneğin en azından kurumsal LAN ile Internet arasında bir ateş duvarının bulunması gerekmektedir. Uzaktan erişim kurumsal bilgisayar ağını yetkili kılınmamış ulaşımlara karşı çok hassas hale getirir. Bu durumda VPN nin rolü çok önem kazanır(Manas,2000).

Uzaktan erişim aygıtlarının en bilinen formu, uzaktan erişim dial-in istemcilerine sunucu tipi fonksiyonları sağlayan Uzaktan Erişim Sunucusu (Remote Access Server RAS) dur. Bir RAS , PSTN (telefon ağı) üzerinde anolog ulaşımlar için çeşitli dial-in kapılardan, kullanıcı belirleyicileri (Identifications), paroloları taşıyan veri tabanından ve ağın geri kalan kısımlarına bağlantıdan oluşmaktadır. Sayılan sunucular en az bulunması gerekenlerdir. Bunlara ek olarak e-posta sunucu e-ticaret

sunucu , kullanıcılarla ilgili bilgilerin tutulduğu üye kütüklerini taşıyan sunucu gibi pek çok sunucu ve hattağa bunların bir araya geldiği kümelerden(cluster) oluşur(Norris,Pretty, 2000).



Şekil 10.1. Temel VPN Yapısı

11. VPN NE YAPAR

Sanal olarak nitelendirilmesinin sebebi fiziksel olarak ortada ağı oluşturan özel bir kablolama yapısının olmayıp ağın bazı sanal bağlantılar sayesinde oluşturulmasıdır.Bu sanal bağlantılar iki makine, bir makine bir yerel ağ,veya iki yerel ağ arasında güvenli bir biçimde oluşturulabilirler. Interneti bir uzaktan erişim yöntemi olarak kullanmak önemli maliyet avantajları sağlar Internet servis sağlayıcıların yerel POP noktalarına bağlanılarak özellikle çok geniş bir alanda faaliyet gösteren bir İSS den hizmet alınıyorsa bağlantı maliyetlerinde önemli düşüşler sağlanabilir(Manas,2000).

Uzun mesafeler arasındaki bağlantılar genellikle bir kiralık hat, frame relay veya ISDN teknolojileri kullanılarak yapılır. Yüksek kapasiteli bir kiralık hattın (T1 gibi) kullanılmasını yüksek maliyetler getirdiği daha önce belirtilmişti. Frame relay de ise maliyetlendirme mesafeden çok kullanılacak bant genişliğine bağlıdır. ISDN de ise maliyetler mesafeye bağlı olarak değişir bunun yanında yerel telefon şirketlerinin arama ücretleri de yine maliyetleri yükselten bir unsurdur. Bir kuruluşun farklı şehirlere ayrılmış şubelerinin ve bunların birbirine bağlı olmasının gerektiği bir durum göz önüne alınırsa yukarıda sayılan bağlantı teknolojilerinin şubeleri doğrudan birbirine bağladığı duruma nazaran bu teknolojilerin tüm bu şubeleri İSS lerin yerel POP noktalarına bağladığı ve bağlanan şubeler arasındaki iletişimin İSS nin routerları vasıtasıyla kurulması maliyet açısından daha uygun bir çözüm olacaktır bunun yanında bir telekomünikasyon altyapısı kurulması zorunluluğundan da kurtulunabilir.

VPN'ler kuruluşların kendi intranetlerinin erişilebilirliğini genişletmelerine de imkan sağlayan bir teknolojidir(Çölkesen,1997). Genellikle bir intranetin kapalı bir ağ içinden ulaşılabilir olması istenir ama bazı durumlarda uzak kullanıcıların da bu kaynağı kullanma ihtiyacı ortaya çıkabilir ve bu kullanıcılar Interneti bağlantı şekli olarak kullanmak isteyebilirler. VPN ile yukarıda bahsedilen şekilde bir intranete dışarıdan güvenli bir şekilde bağlanılabilir bu şekilde bir yapı Ekstranet olarakta

adlandırılır. VPN sayesinde kurumların aşağıda sayılan faydalara sahip olabilmesi mümkündür;

- Kurumun birbirinden uzakta bulunan yerel ağlarını güvenli ve kuruma özel bir ağ üzerinde birleştirerek kuruma ait bir Intranet kurulabilir. Böylelikle uzakta bulunan bölge ofisleri ve şubeler firma merkezine ulaşarak iş akışını bu ağ üzerinde kolayca gerçekleştirebilir.
- Internet üzerinden yapılan VPN bağlantılarında VPN'de yer alan her bir yerel ağ Internet'e de bağlı olacağından kullanıcılar web, e-posta, FTP gibi hizmetlerden yararlanabilirler.
- Kurum içi sanal özel ağda kurulacak bir web sunucu ile kurum iş akışını web tabanlı hale getirmek ve iş akışını ekonomik, kolay ve hızlı gerçekleştirmek mümkündür.
- Kurum içi e-posta sunucu ile yerel ve uzak tüm firma ofislerinde bulunan kullanıcılara bir e-posta hesabı açarak haberleşmelerin e-posta ile yaptırılması mümkündür.
- Kurum içi FTP sunucusu ile yerel ve uzak ofislerde bulunan çalışanların bilgi kaynaklarına ortak bir noktadan daha hızlı faydalanabilmelerinin yanı sıra bazı programlara da FTP sunucu üzerinden ulaşarak bilgisayarlarına kurabilmektedirler.
- Kurum içi veri tabanı sunucuları ile veri tabanı uygulamalarının tüm ofisler tarafından aynı ağ üzerinde kullanımı mümkündür. Bu imkan ile uygulamaların bölgesel değil, kurumsal olarak (tüm firma çapında) kullanıma sunulabilmesi mümkün olmaktadır.
- Kurumun merkez ve uzak ofisleri arasında uygun cihazlar (VoIP gateway) kullanılarak VoIP (Voice over IP - IP üzerinden ses) tekniği ile mevcut data hatları kullanılarak ses iletimi mümkün olmaktadır. VoIP ile ek ücret ödemeden data hatları üzerinden mevcut telefon santralleri kullanılarak uzak ofisleri dahili hattan arayıp telefon görüşmesi yapabilmek mümkündür.Böylece telefon maliyetleri VPN yatırımı üzerine ek bir yük getirmeden aktarılabilir. Bu imkan ile yatırımların amortisman giderleri düşer.

12. TEMEL ÖZEL SANAL AĞ TEKNOLOJİLERİ

Bilgisayar ağlarını birbirine bağlama konusunda iki farklı düşünce bulunmaktadır, birincisine göre herhangi bir kullanıcı istediği herhangi bir bilgiye rahatça ulaşabilmelidir, diğer düşünce ise bilginin korunmasının gerekliliğine vurgu yapar buna göre önemli olan bilginin içeriğidir ve yetkilendirilmemiş kullanıcıların bu bilgilere erişimi engellenmelidir. Bu iki birbine zıt düşünceden herhangi birinin gerçek hayatta tek başına uygulama şansı bulması mümkün değildir doğru olan yapılan işin niteliği göz önünde bulundurularak bu iki yöntemin uygun bir karışımının oluşturulmasıdır (Scott,Wolfr,and Erwin ,1998). Bunun yanında her ne kadar mümkün olduğunca fazla bilginin başkalarının kullanımına açılması istense yada gerekli olsa da en azından bu faaliyetlerin sağlıklı bir şekilde sürdürülebilmesi için bile güvenlik konusu her zaman göz önünde bulundurulması gereken bir olgudur.

Internetin çok geniş bir bilgi kaynağına ulaşılmasına imkan sağlaması nedeniyle bu ortamı paylaşan kullanıcıların bilgilerini birbirleriyle paylaşarak kendilerine çok çeşitli faydalar ve gelişme fırsatları sağlamaları mümkündür buna karşın Internete bağlanan herbir kullanıcının yukarıda sayılan son derece yararlı faaliyetler uğruna bu ortama bağlanmakla nasıl bir risk altında bulunduğu yeterince açık olmayan bir husustur. Günümüzde birçok şirket Interneti yeterince kullanılmayan bir sürü potansiyel müşteri ve yeni reklam olanakları ile dolu olan bir pazar gibi görmektedirler fakat herkes böylesine geniş fırsatlar sunan bu ortamının da tıpkı gerçek yaşamda olduğu gibi kendine göre iyi niyetli olduğu söylenemeyecek kişilerden oluşan bir yeraltı dünyası olduğunun farkında değillerdir.Bu gerçekler ışığında kurumların sahip oldukları bilgileri korumalarının günümüzde gelinen noktaya bakılarak bir zorunluluk olduğu söylenebilir,bu noktada özel sanal ağların kullanımı 21. yüzyılda kurumlara büyük faydalar sağlayacaktır çünkü bilginin korunması özel sanal ağ kavramının odak noktasını oluşturmaktadır ve bu korunmayı sağlayan başlıca iki teknoloji bulunmaktadır; ateş duvarları ve şifreleme(encryption).

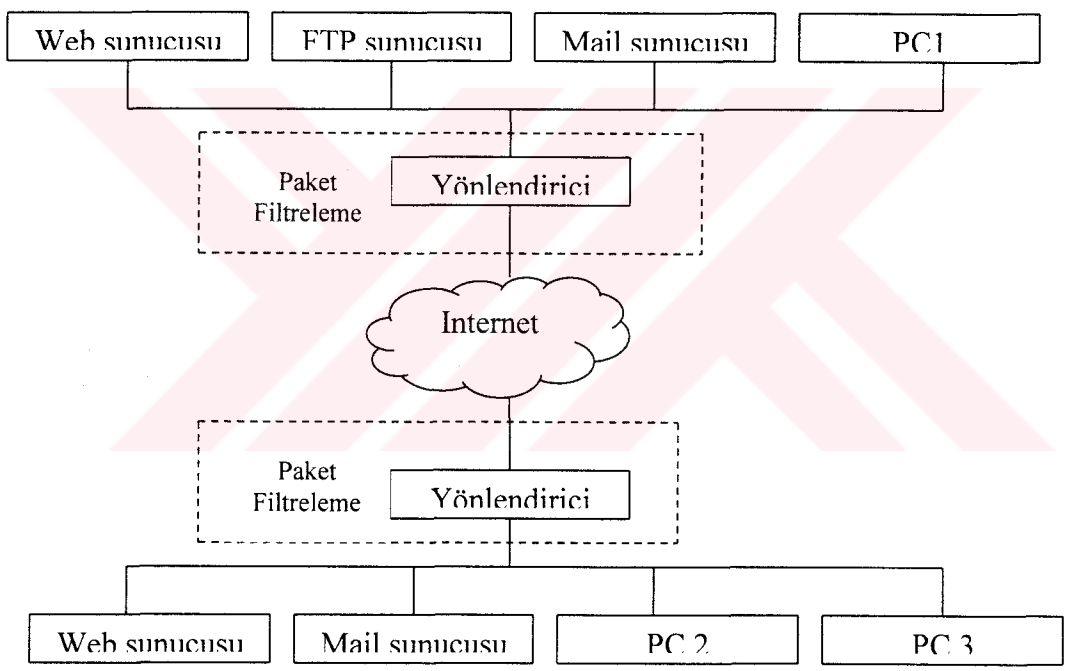
12.1. Ateş Duvarları(FIREWALL)

Bir kurumun yerel bilgisayar ağı veya LAN (local area network) ile Internete bağlandığı her seferde potansiyel bir tehlike ile karşı karşıyadır. Internetin açıklığına bağlı olarak, ona bağlı olan her ağ da saldırıya açıktır. Internet üzerinden kötü niyetli kimseler teorik olarak kurumsal ağa ulaşabilir ve çeşitli şekillerde ona zarar verebilirler. Önemli bir bilgiyi çalabilir ya da yok edebilir, kişisel bilgisayarlara hatta ağın tamamına zarar verebilir; ağ bilgisayarlarının kaynaklarını kullanabilir veya kendini ağın bir üyesi olarak göstererek ağın kaynaklarından faydalanabilir. Bu sorunun en kesin çözümü özel ağ ile Internet arasındaki bağlantıyı kesmek olsa da günümüzde en önemli rekabet avantajı bilgi olduğuna ve istenen bilgiye en çabuk ulaşmanın yolu Internet olduğuna göre özel ağımızı Internete açarken aynı zamanda güvenliği de sağlayacak bir sistem kullanmak yapılacak en doğru harekettir. Bunun yapılmasını ise ateş duvarları kurarak sağlanabilir. Ateş duvarları özel ağdaki herhangi birinin Internete ulaşmasına olanak tanır, ancak Internet üzerinden istenmeyen kimselerin özel ağa girip zarar vermelerine izin vermez (Pohlmann,Crothers,2003).

Ateş duvarı bir iç ağ ile dış dünya arasındaki noktada bulunan bir sistemdir yönlendiriciler(router), sunucular ve değişik yazılımlar kullanılarak kurulan donanım ve yazılım kombinasyonlarıdır. Internet ve iç ağ arasındaki en zedelenebilir noktalarda otururlar ve sistem yöneticilerinin istekleri doğrultusunda oldukça basit yada karmaşık yapılı olabilirler. Bu sistemler uzun yıllardır kullanılmaktadır ve bir güvenlik stratejisi oluşturmak için iyi bir başlangıç noktasıdır çünkü kurumun kendi iç ağı ile herkesin kullanımına açık olan Internet gibi genel (public) ağların kesişim noktasında bulunmaktadır. Mükemmel bir sistem olmamasına rağmen ayar yapılması kolaydır ve sadece bir yönlendirici(router) üzerinde bazı değişiklikler yapılmasına ihtiyaç duymaktadır.Eğer Internete tek bir nokta yerine birçok alternatif yol üzerinden ulaşılıyorsa herbir kesişim noktasına bir ateş duvarı kurulmak zorundadır çok sayıda bağlantı bulunması da bu sistemin yönetimini zorlaştıran bir husustur.

Amerikan savunma bakanlığının kritik öneme sahip devlet bilgilerinin saklanması ve bu bilgilere ne şekilde ulaşılacağının bazı güvenlik seviyeleri oluşturularak belirlendiği sistemi bu ateş duvarlarının ilk örneklerindendir, eğer çok üst düzeyde hassasiyete sahip bilgilerin korunması gerekiyorsa en iyi yolun bu bilgilerin

tutulduğu bilgisayarların ağ ulaşımı olmayan izole edilmiş makinalar olması da düşünülmesi gereken bir husustur. Ateş duvarları bir ağ yöneticisine başlıca yerine getirdiği iki fonksiyon ile hizmet eder; birincisi Internet ortamındaki bir kullanıcının kurumun iç ağında bulunan hangi makinalara ulaşabileceği ve bu makinalar üzerinden verilen hangi servislerden faydalanabileceğidir, ikincisi ise iç ağda bulunan kullanıcıların Internet ortamında hangi noktalara ulaşabileceğinin denetlenmesidir.Buradan anlaşılacağı üzere ateş duvarlarını ağ trafiğini düzenleyen, organize eden bir trafik polisine benzetmek mümkündür(Pohlmann,Crothers,2003). Bu görevi de yönlendirici üzerinden dış veya iç ağa doğru geçen her bir paketi inceleyerek yapar bu sisteme de paket filtreleme adı verilir. Aşağıdaki tipik bir ateş duvarı örneği görülmektedir.



Şekil 12.1. Paket Filtrelemeli Ateş Duvarı

Ateş duvarlarının öncelikli kullanım amacı bir iç ağ ile bir genel ağ arasındaki trafiği denetlemek olsada sadece iç ağ ile Internet arasındaki haberleşmede kullanılmazlar. Aynı zamanda iç ağ içerisindeki trafiği kontrol etmede ve izlemede de kullanılabilir. Dahili ateş duvarları uygulamak iç ağı 'güvenlik alanları'na (security domains-bir güvenlik alanı aynı güvenlik seviyesine sahip makineler grubudur) ayırır. Eğer kurum içerisinde tüm bilgilere erişmemesi gerekli kişiler bulunuyorsa bu tür durumlarda ağı güvenlik alanlarına bölme yöntemi uygulanabilir. Örneğin, kullanıcı

hesapları, pazarlama stratejisi veya ürün geliştirme hakkındaki önemli bilgilerin korunması gerekli olabilir. Bu özellikle çalışanların rakiplere bilgi sızdırmaya eğilimli oldukları durumlarda geçerlidir (FBI'nın bir anketine göre tüm bilgisayar suçlarının %80'i kurum içerisinden gerçekleştirilmiştir). Eğer sadece bir Internete çıkışı denetleyen bir ateş duvarı varsa ve bir saldırgan onu geçmeyi başarırsa ağdaki tüm bilgilere erişebilir. Fakat dahili güvenlik duvarlarları da kullanılıyorsa saldırgan ağın sadece bir bölümüne erişebilir. Bu sebeple saldırganın gerçekten istediği bilgilere erişebilmesi için çeşitli güvenlik duvarlarını aşması gerekecektir. Böyle bir yöntemde olası bir saldırı anında önemli bilgileri çalınması yada zarar görmesi riskini azaltan bir unsurdur (Cheswick.Bellovin.Rubin.2002).

12.1.1. Ateş Duvarı Çeşitleri

Hemen hemen tüm ateş duvarları merkezi kontrola dayanan bir teknik çerçevesinde oluşturulsa da birbirlerine göre bazı farklar gösterebilmektedirler bu kısımda dört ayrı ateş duvarı yapısı incelenecektir.

12.1.1.1. Paket Sınırlamalı veya Paket Filtreleyen Yönlendiriciler

En basit ateş duvarlarından birisi paket filtrelemeden faydalanır. Paket filtrelemede, bir izlenen yönlendirici(screened router) Internet ve iç ağ arasında yol alan her paketin başlığını(header) inceler. Paket başlıkları içinde, gönderen ve alıcının IP adresleri, paketi yollamak için kullanılan protokol ve benzer bilgileri de içeren şeyler yazar. Bu bilgilere dayanarak, yölendirici paketi yollamak için ne çeşit bir Internet servisi kullanıldığını, paketin göndericisi ve alıcısının kimliği gibi şeyleri öğrenir. Bu bilgiler toplandıktan sonra yönlendirici Internet ve iç ağ arasında yollanan bazı paketleri geçirmeyebilir. Örneğin, yönlendirici e-posta dışında her türlü trafiğe engel olabilir. Buna ek olarak, şüpheli hedeflerden veya belirli kullanıcılardan giden veya onlara gelen trafiği engelleyebilir.

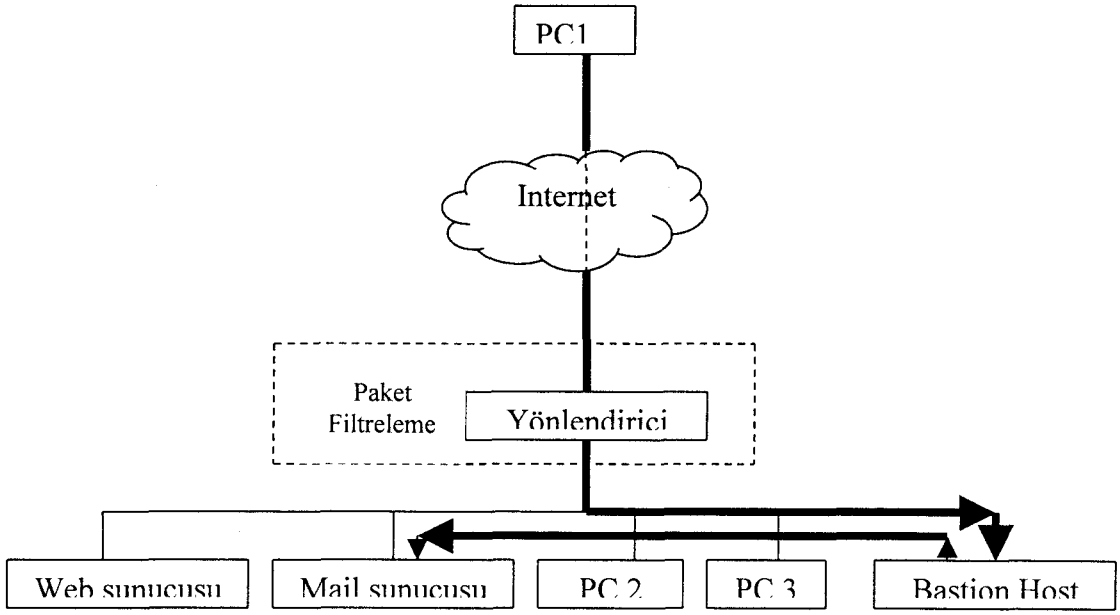
Paket filtreleme yöntemine göre çalışan yönlendiriciler daha önceden belirlenmiş olan bir kurallar bütününe bağlı olarak hareket ederler. Yönlendiriciler paketlerin içeriğine bakmazlar sadece nereden geldiklerine ve nereye gittiklerine bakarlar eğer yönlediricinin temel aldığı ağ trafiğini düzenleyen erişim listesinde o paketin geldiği yer yada gideceği yer ile ilgili bir sınırlandırma varsa yönledirici bu paketin yoluna devam etmesine izin vermez aksi durumda paket yoluna devam eder. Bu erişim listeleri uygulanan güvenlik politikasına uygun olarak ağ yöneticisi tarafından

belirlenir. Paket filtreleme iki değişik şekilde yapılabilir birincisi ağ trafiği tamamıyla serbesttir bu trafik içinden istenmeyen unsurlar ayıklanır bunlar kaynak veya erişim adresi için sınırlandırmalar bulunan paketlerdir, ikincisinde ise ağ üzerinde trafik sınırlandırılmıştır ancak belirli şartları sağlayan paketlere izin verilir telnet,ip trafiğine izin verilip ftp trafiğine izin verilmemesi gibi.

Paket filtreleme yönteminin eksik noktalarından biri ise kullanıcı bazında yetkilendirme yapılamamasıdır, örnek olarak A ağından gelen e-posta trafiğine izin verilir yada izin verilmez kimin ulaşmaya çalıştığına bakılmaz. Bundan başka paket filtreleme yöntemi ile gelen her paketin açılıp incelenmesi performans açısından bir düşüşe yol açar, bir başka engel ise ateş duvarının üzerinde çalıştığı yönlendiricinin ağ teknolojilerinde meydana gelen gelişmeler sebebiyle sık sık yeniden yapılandırılması hatta daha gelişmiş özelliklere sahip olan yeni modellerle değiştirilmesi gerekebilir bu ise zaman ve para kaybına sebep olabilir bu geliştirmeler yapılmadığı durumda ise kurumun tüm ağı henüz kullanılan ateş duvarının engelleme yeteneğine sahip olmadığı saldırı teknikleri sayesinde tamamıyle korunmasız kalabilir (Cheswick,Bellovin,Rubin,2002).

12.1.1.2. Bastion Host

Bastion host yönlendiricinin paket filtreleme mekanizmasına ek olarak kendi işletim sistemi ve üzerinde çalışan çeşitli serviseleri olan bir de güvenlik birimi kullanan bir sistemdir. Bation host diğer makinalar ile aynı şekilde Internete bağlanmış bir güvenlik kontrol makinası olarak işlev görür. Yönlendirici kendi üzerinden bastion hosta doğru olan trafiğe izin verir ve kontrolden geçen paketler yolarına devam ederler. Tipik bir bastion hostun yapısı şekil 12.2'de gösterilmiştir.

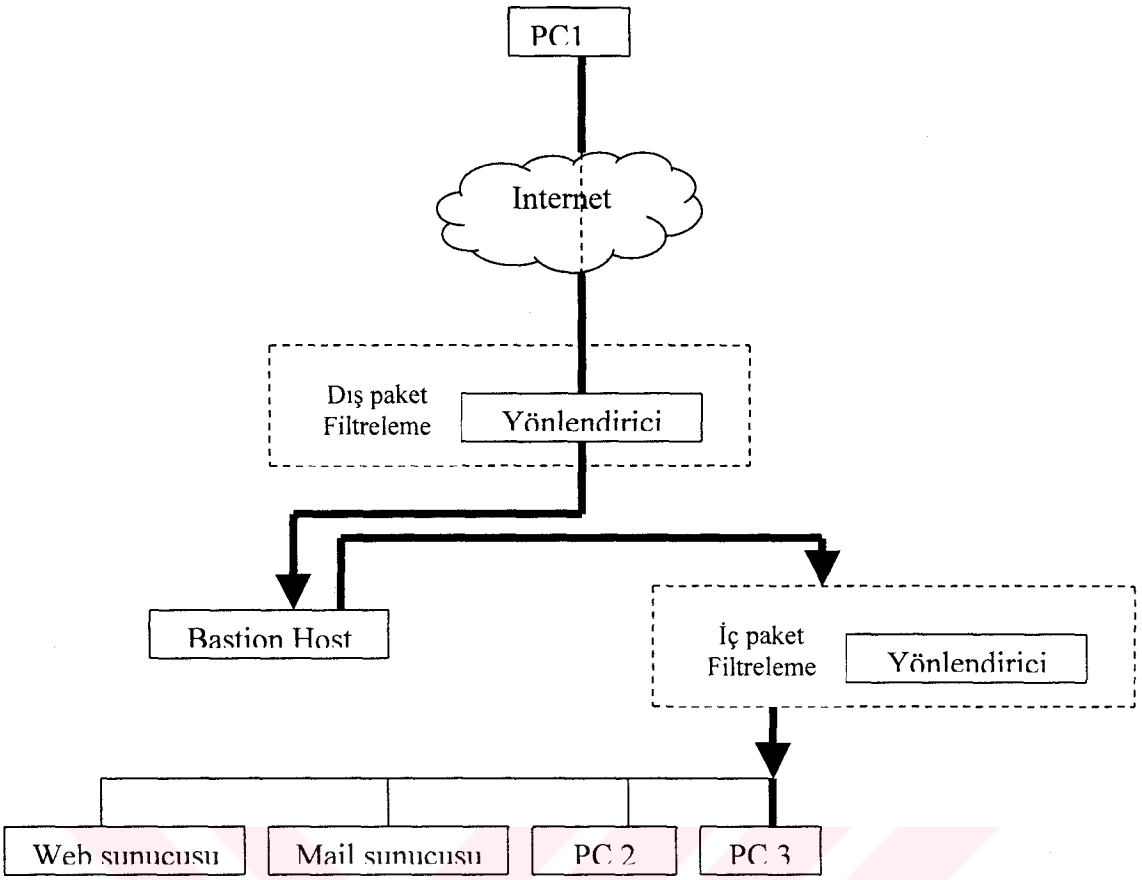


Şekil 12.2. Bastion Host

Ateş duvarındaki bastion host, Internetten e-posta alma, anonim FTP sitesine giriş izni verme gibi servisler için gelen bağlantıların iletişim kurduğu esas noktadır. Bastion host, bir çok güvenlik yöntemleri tarafından yoğun bir şekilde korunan bir sunucudur ve gelen Internet istekleri için tek iletişim noktasıdır. Bu yolda, iç ağdaki hiçbir bilgisayar Internetten gelen isteklere doğrudan bağlanamaz, bu da bir güvenlik seviyesidir. Bastion hostlar aynı zamanda proxy sunucu olarak da kurulabilirler. Bu sunucular Internette gezinme veya FTP yoluyla dosya yükleme gibi iç ağdan Internete giden her türlü isteği düzenlerler(Cheswick,Bellovin,Rubin,2002).

12.1.1.3. Perimeter Zone Network(DMZ)

Geniş kurumsal ağları genel ağlardan gelebilecek tehlikelerden koruma yöntemlerinden birisi de hem içe hem de dışa doğru olan trafiğin üzerinden geçmek zorunda olduğu bir yönlendirici ağ (routing network) kurmaktır. Bu ağ aynı zamanda iç ağa ve dışarıdaki genel ağa bağlı olan yönlendiricilerden oluşur. Oluşturulan bu çevresel ağ(perimeter zone network) zaman zaman, gerçek hayatta birbiriyle sürtüşme içinde olan farklı tarafları birbirinden ayırmak için ara bölgede askerden arındırılmış bir coğrafi alan (DeMilitarilized Zone) oluşturulması uygulamasına benzerliği açısından DMZ olarak ta adlandırılmaktadır.



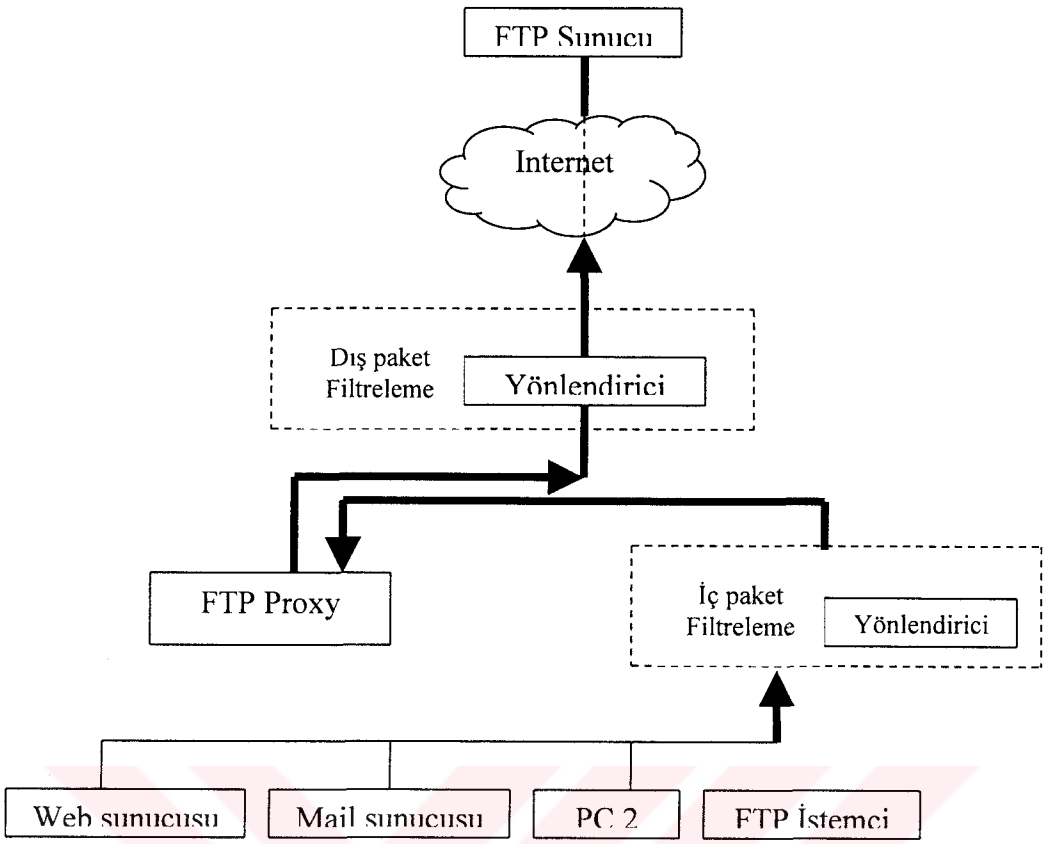
Şekil 12.3. DMZ Yapısı

12.1.1.4. Proxy Servers(Vekil Sunucular)

Proxy sunucular da ateş duvarları içinde sıkça kullanılırlar. Proxy sunucu, ateş duvarı içinde görevini yapan bir sunucu yazılımıdır. Internetle ağdaki tüm bilgisayarların ayrı ayrı etkileşmesi yerine sadece basit bir proxy sunucu etkileştiği için, güvenlik sağlanabilir. Bu basit sunucu, ağdaki yüzlerce bilgisayardan daha kolay korunabilir. İç ağdan Internet üzerinde bir sunucuya ulaşılmak istediğinde bilgisayardan bir istek proxy sunucuya yollanır, proxy sunucu Internetteki sunucuya bağlanır ve sonra proxy sunucu Internetteki sunucudan aldığı bilgiyi iç ağdaki istemci bilgisayara yollar. Böyle arada çalışarak proxy sunucular hem güvenliği sağlar hem de Internet ve iç ağ arasındaki trafiği düzenler(Luotonen,1997).

Sistem yöneticileri, proxy sunucuları çok çeşitli servisler için kullanabilirler: FTP, web ve Telnet gibi. Hangi Internet servislerinin proxy sunucudan geçeceğine sistem yöneticileri karar verir. Her değişik Internet servisi için özel bir proxy sunucu yazılımı gerekir. Proxy sunucular, iç ağ ve Internet arasındaki trafiği izlemek ve kaydetmek için de kullanılırlar. Örneğin, bir Telnet proxy sunucu, her Telnet oturumda basılmış herbir tuşu takip eder ayrıca Internet üzerindeki bağlanılan

sunucunun bu tuş basışlarına nasıl tepki verdiğine de bakar. Proxy sunucular her IP adresi, giriş gününü ve saatini, URL, yüklenen byte sayısını ve benzerlerini kayıt edebilir. Bu bilgiler, ağa karşı yapılabilecek saldırıları analiz etmek için kullanılır. Proxy sunucular ağdaki bir bilgisayar ve Internetteki bir sunucu arasındaki istekleri yollayıp geri almaktan fazlasını yapabilir. Güvenlik tasarıları yürütebilirler, örneğin bir FTP proxy sunucu, Internetten, iç ağdaki bir bilgisayara dosya yollama izni vermek ama iç ağdan Internete dosya yollamamak yada tam tersi için kurulmuş olabilir. Proxy sunucular, caching data(istenen bilgilerin kopyalarını tutma)gibi bazı Internet servislerinin performanslarını hızlandırmak için de kullanılırlar. Örneğin, bir web proxy sunucu birçok web sayfasını cache edebilir. Sonra, ne zaman iç ağdan bir istemci bu web sayfalarından birini istese, bu kişi onları doğrudan sunucudan oldukça yüksek bir hızda edinebilir, böylece ağır bir şekilde onları Internetten almaktan kurtulmuş olur. Proxy sunucusu bir uygulama seviyesi ağ geçidi tipidir. Uygulama seviyesi ağ geçitleri katı bir güvenlik politikasını yürütmek için iyi bir seçimdir çünkü iç ağdan erişilen her servisin kontrol edebilmesine imkan verir. Ayrıca kullanıcı kimlik tanımlamasını desteklerler ve detaylı kayıt (log) bilgisi sağlarlar. Ayarlanmaları bir paket filtreleyici yönlendiriciden daha karmaşık olsa da bakımları daha kolaydır. Paket filtreleyici yönlendiricilerin aksine uygulama ağ geçitlerinin kurulumu pahalıdır ve performansı düşürebilirler(Luotonen,1997).



Şekil 12.4. Proxy Sunucu Yapısı

12.2. Sanal Özel Ağlarda Ateş Duvarı Kullanımı

Sanal özel ağlarda ateş duvarı kullanılması sistemin sağlıklı bir şekilde işleyebilmesi için vazgeçilemez bir öneme sahiptir. Sanal özel ağların açık ağların imkanların faydalanarak iki veya daha fazla ağı birbirine bağladığı göz önünde bulundurulduğunda bu ağların herbirinin dış ortamdan korunmasının gerekliliği daha iyi anlaşılabilir. Her bir sanal ağ kendi kullanıcı ve bağlantıları ile birlikte bir balon olarak düşünülürse her bir balon etrafını saran ve kendisini saldırılardan koruyacak bir duvara ihtiyaç duyar(Pohlmann,Crothers,2003). Sanal özel ağlarda ateş duvarı kullanımının ardındaki düşünce ise her bir balonu sanki diğer ağlardan yalıtılmışcasına güvenli duruma getirmektir. Sistem yöneticileri paket filtreliyici yönlendirici üzerinde belirli kapıları(port) açarak bir balondan diğerine kriptolanmış bilgilerin geçişine imkan tanırlar. Böylece her bir balon arasında bilgi akışını sağlayan güvenli bir kanal oluşturulmuş olunur. Özel sanal ağ yazılımları sağladıkları güvenlik ve uygulama seviyesinde yönlendirme ile sanal ağın her bir ucundaki kullanıcıların ağın tümünü tek bir parçaymış gibi algılamalarını sağlar. Ateş duvarları bir özel sanal ağın bünyesindeki ilk savunma hattıdır ve özel sanal

ağın sağlayabileceği imkanlardan en yüksek oranda faydalanılmak isteniyorsa ihtiyaçlara uygun bir ateş duvarı sistemi geliştirilmeli ve özel sanal ağ kurulumundan önce gerekli testler yapılmalıdır.Bir ateş duvarı kurarken aşağıdaki noktalara dikkat edilmelidir;

- Ateş duvarları güvenlik politikalarını uygularlar .Ateş duvarı kurmak istenildiğinde öncelikle bir güvenlik politikası belirlenmelidir. Eğer güvenlik politikası için kesin kurallar yoksa bunu hazırlamak ve uygulamak oldukça zaman alacaktır. Eğer çok iyi bir güvenlik duvarına sahip olmak isteniyorsa mutlaka çok iyi hazırlanmış bir güvenlik politikasına ihtiyaç vardır.
- Ateş duvarı tek bir sistem değildir. Basit birkaç uygulamanın dışında, ateş duvarı nadiren tek bir cihazdan oluşur. Genellikle birbiriyle uyumlu çalışan cihazlar topluluğudur. Hatta eğer herşeyi kapsayan bir ateş duvarı alındıysa, diğer makinaların (örneğin web sunucu) hala konfigüre edilmesi gereklidir ve bu makinalar da ateş duvarının bir parçası sayılacaktır. Bu yüzden tek bir ateş duvarı yeterli olmayabilir ve bütün güvenlik politikasını tek bir ateş duvarının uygulaması beklenmemelidir.
- Ateş duvarları kullanıma hazır yazılımlar değildir ve çok karmaşık olabilmektedirler bu yüzden devamlı bir bakıma gereksinim duyarlar aksi halde çökmeye mahkumdurlar.Ateş duvarı kurmak ve seçmek çok dikkat ister. Kurabilmek için oldukça fazla kural bilmek gerekmektedir. Bazıları ihtiyaçlara tam uygun iken bir başkası tam tersine oldukça zararlı olabilmektedir.
- Ateş duvarları bütün sorunları tam olarak çözemezler. Ateş duvarlarının bütün güvenlik kurallarını tam olarak yerine getirmesi beklenmemelidir. Dışarıdan, iç ağa gelebilecek belli başlı saldırıları engelleyebilirler. Bunun yanında dışarıdaki zararlı kişilerden birçok atağa karşı ve iç ağda bulunan kullanıcılardan koruyamazlar. Sadece bu saldırıların görülebilmesini sağlayabilirler.
- Standart olarak herşeyi engelle kuralı kullanılmalıdır. Daha sonra güvenli veya gerekli olduğu düşünülünlere izin verilebilir. Her gün yeni açıklar çıkmaktadır, bunların takip edilip, tehlike yaratan kuralların tekrar gözden geçirip kaldırılmaları gerekebilir.

- Kullanıcılar genellikle güvensiz olanları tercih ederler. Eğer bütün isteklere izin verilirse ağ başarısız ve güvensiz olacaktır. Eğer bütün istekler engellenirse, hala başarısız ve güvensiz bir ağ var demektir. Çünkü güvenliğin nerede sağlanması gerektiği hala bulunamamış demektir. Bu sebeplerden çevrede ağ için risk taşıması muhtemel ama ağ kaynaklarından faydalanması gerekli kullanıcılar varsa ortak bir noktada buluşmanın ve onların isteklerini karşılamanın bir yolu bulunmalıdır.
- Aşamalı yaklaşımlar kullanılmalıdır.Böylece tek bir cihaz ve tek bir noktaya bağlılık ortadan kalkacaktır. Böylece tek bir noktadaki başarısızlığın ağın tümünü tehlikelere açık bırakması riski engellenmiş olacaktır.
- Ateş duvarı bilgisayarları, normal makinalar gibi üretici firma tarafından dağıtılan tam bir yazılım desteği gibi kurulmamalıdır. Ateş duvarının bir parçası olan her makina en az çıplaklıkta olmalıdır. Hatta eğer bir makinanın çok güvende olduğu düşünülse dahi eğer gerekmiyorsa sisteme dahil edilmemelidir.
- Ateş duvarları tek kaynaktan gelen bilgiler ışığında kurulmamalıdır eğer bu tek kaynak üretici firma değilse. Birçok kaynaktan yardım alınmalıdır.
- Sadece test edip çalıştığı görülenlere inanılmalıdır, kullanıcı el kitabına bağlı kalmak yeterli değildir. Uygulanan kurallar kontrol edilmelidir mesela bloklananlar bloklanıyor mu? veya serbest bırakılanlar geçebiliyor mu?
- Güvenlik kuralları sık sık gözden geçirilmelidir, daha önce ihtiyaçları karşılayan bir Ateş duvarı bugün tam olarak isteklere cevap veremiyor olabilir.
- Her zaman hatalar beklenmelidir ve bunlara hazırlıklı olunmalıdır. En kötü senaryolar her zaman planlanmalıdır. Makinalar çökebilir, kullanıcılar yapmamaları gereken şeyleri yapabilirler, veya zararlı kişiler tarafından sisteme zarar verilebilir. Fakat bunların ağ için tam bir felaket olmayacağından emin olunması gerekmektedir.

13. KRİPTOLAMA

Kriptografi Romalılar zamanından beri var olup 2. Dünya Savaşı gibi modern savaşlarda da önemli rol oynamıştır. Son zamanlarda kriptografi alanındaki gelişmeler bilgisayar endüstrisinin güvenli bilgi alışverişi, depolama ve işleme ihtiyaçlarını karşılamıştır. Elektronik ticaretin kullanılmaya başlanılmasıyla da kriptografi alanına büyük çapta ticari bir ilgi oluşmuştur. Kriptografik teknikler harddisk, disket ve manyetik teyp gibi medyalar üzerinde depolanan önemli bilgilerin güvenliğini sağlamak için kullanılır. Aynı zamanda Internet üzerinden transfer edilen bilginin güvenliğini sağlamak için de kullanılır. Kriptografi kriptolama ve dekriptolama diye bilinen iki işlem üzerine kuruludur. Kriptolama bir mesajı okunamayacak şekle sokma işlemine denir. Bu kriptolama anahtarı ile gerçekleştirilir. (Bir anahtar rastgele bitlerden oluşur,bit sayısı kripto sistemine göre değişir.) Dekriptolama mesajı orijinal şekline çevirme işlemidir. Bu işlem de bir dekriptolama anahtarı ile gerçekleştirilir. Bir mesaj kriptolanmadan önce düz yazı şeklindedir. Kriptolama işlemi sonrası mesaj şifreli yazı şekline dönüşür. Kriptografi dört ana fonksiyon içerir:

- Gizlilik
- Kimlik tanılama
- Bütünlük
- İnkar edememe

Gizlilik, kriptolanmış bilgi transfer sırasında veya depolanırken dekriptolama anahtarına sahip olmayan kullanıcılar tarafından okunamadığından sağlanmış olur. Kimlik tanılama bilginin doğru kaynaktan alındığını doğrulamak için kullanılır.Bilgi veya mesaj bütünlüğü bilginin ağdaki yolculuğu sırasında değişikliğe uğramadığından emin olmak için gereklidir. İnkar edememe bir mesajı gönderen kişinin o mesajı size gönderdiğini inkar edememesini sağlayan alındı onaylarını sağlar(Stallings,2002).

Internette yollanan data paketleri birçok halka açık ağdan geçer ve bu da bu paketlere ulaşmanın pek de zor olmadığının bir göstergesidir. Son derece gizli bilgiler, şirket bilgileri ve kredi kartı numarası gibi Internette taşınırken bu durum önemli bir kaygı halini alır. Bu tür bilgileri korumak mümkün olmadıkça, Internet iş yapmak veya gizli, şahsi yazışmalar için asla güvenli bir yer olmayacaktır. Bu kaygılar neticesinde yazılım mühendisleri gizli bilgileri güvenle yollayabilmek için çeşitli yöntemler geliştirmişlerdir. Bilgiler kriptolanarak(encryption) yani gönderilen kişi dışındakilere anlamsız şekiller olarak gözükmesine neden olacak şekilde gönderilir ve karşı tarafa ulaştığında bu kripto çözülerek (decryption) yani sadece alıcı tarafından, orijinal haline dönüştürülebilme haberleşme sağlanır. Kripto sistemlerinin özünde anahtar(key) kavramı yatmaktadır. Anahtar bilgisayarların algoritmalar kullanarak uyum içinde mesajları kriptolamak ve dekriptolamak için kullandıkları gizli değerlerdir. Anahtarın ardında yatan fikir, birisi bir mesajı anahtarla kriptoladığında sadece uyan anahtarla bir başkasının mesajı dekripto edebilmesidir. İki tür yaygın kriptolama sistemi vardır; secret-key cryptography(gizli anahtarlı kriptolama), diğer adı symmetric cryptograph(simetrik kriptolama)dir, ve public-key cryptography(açık anahtarlı kriptolama), diğer adı asymmetric cryptography(asimetrik kriptolama)dir. En yaygın kapalı anahtar sistemi Data Encryption Standart (DES)'dir. En iyi bilinen açık anahtar sistemi RSA'dır (Stalings,2002).

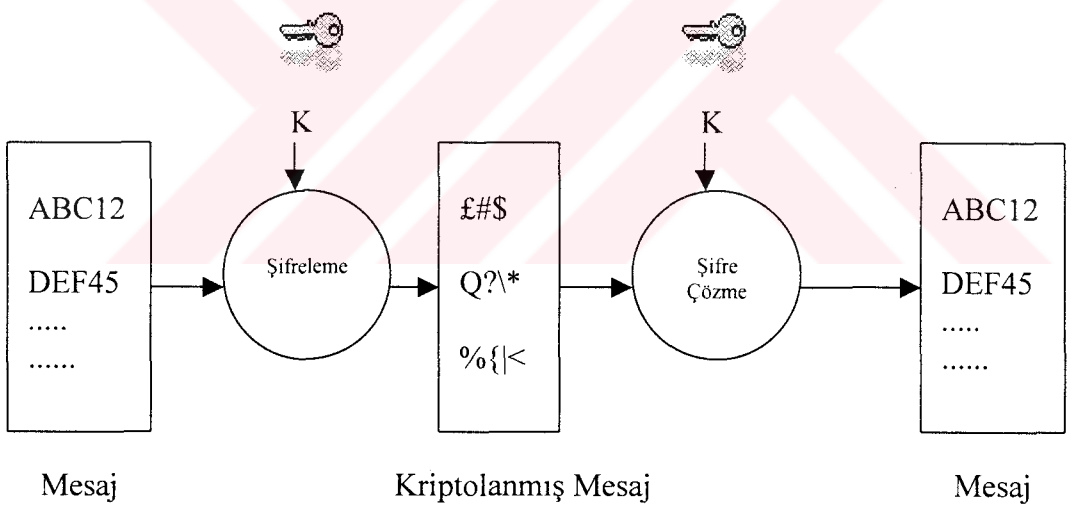
Kriptografi alanındaki en önemli dönüm noktalarından biri, 1976 yılında Diffie ve Hellman'ın açık anahtarlı kriptografi kavramını önermesidir. Bu tarihten önce uzun yıllar boyunca kullanılan tüm kriptolama algoritmaları simetrik algoritmalardı. Simetrik kriptolama algoritmalarında, haberleşen taraflar aralarında önceden belirledikleri bir anahtarı hem şifreleme, hem de şifre çözme amacı ile kullanmaktadırlar. Simetrik algoritmalar hızlıdırlar fakat en önemli problemleri kullanılacak simetrik anahtarın taraflar arasında önceden belirlenmesi gerekliliği ve bu işlemn pratiklikten uzak oluşudur

13.1. Kriptografik Algoritmalar

13.1.1. Secret Key Systems

Gizli anahtar algoritmaları hem şifreleme hemde şifre çözmek için aynı anahtarı kullanırlar veya biri diğerinden türetilebilir. Bu, veri şifreleme için daha kestirme, matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve uzun zamandan beri kullanılmaktadır. Simetrik şifreleyiciler incelenirken aşağıdaki terimler sıksık kullanılırlar (Güncan,Sönmez,1999);

- *S-kutuları*: *n* adet biti *m* adet bite adresleyen tablolar (genelde n ve m denktirler).
- *Feistel ağları*: Bir Feistel ağı, basit fonksiyonlardan blok şifreleyiciler inşa eden bir genel cihazdır, standart Feistel ağı n adet bitten n adet bite bir fonksiyon alır ve 2n adet bitten 2n adet bite tersinebilir bir fonksiyon üretir.



Şekil 13.1. Gizli Anahtar ile Kriptolama

13.1.1.1. DES

Veri Şifreleme Standardı (DES- Data Encryption Standard) 1970'lerin ortalarında geliştirilmiş bir algoritmadır. ABD Ulusal Teknoloji ve Standartlar Enstitüsü (NIST) tarafından bir standart haline getirilmiş, ve ayrıca dünya çapında pek çok hükümet tarafından da kullanılmıştır. Geçmişte ve şimdi özellikle finans sektörlerinde yaygın olarak kullanılmaktadır. DES 64 bit blok genişliğine sahip bir blok şifreleyicidir. 56

bit anahtarlar kullanır. Onun bu özelliği, modern bilgisayarlar ve özel amaçlı donanımlar ile yapılan ayrıntılı anahtar taramalarına karşı kuşku duyulmasına sebep olmaktadır.DES'in bir çeşidi üçlü DES (3DES) , DES'in üç kere kullanılması temeline dayalıdır Üçlü DES tekli DES'e göre çok daha güçlüdür, ancak yeni blok şifreleyiciler ile karşılaştırıldığında oldukça yavaş kalmaktadır. Bununla birlikte, DES günümüzün uygulamaları için az öneme sahip olsa da, bunun hala önemli olduğunu düşünmemizi gerektiren pek çok sebep vardır. Sektörde en çok yayılmış blok şifreleyicidir. DES in çok güçlü bir şifreleyici olduğu kanıtlanmıştır ve herhangi bir ilginç kriptanalitik saldırının ortaya çıkması için on yıldan fazla bir zaman geçmesi gerekmiştir. Diferansiyel ve lineer kriptanalizin gelişmesi, blok şifreleyicilerin tasarımının gerçekten anlaşılmasında çok faydalı olmuştur. DES'in tanıtıldığı zaman tasarım felsefesi gizli tutulmuş olmasına rağmen, bu karşı tarafın analizle uğraşmasını engellememiştir.

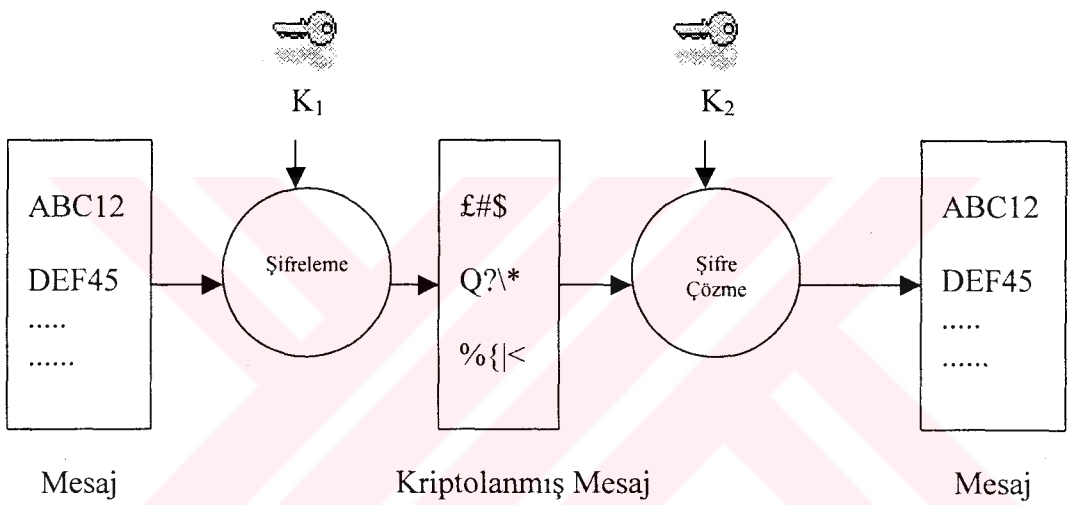
13.1.1.2. One Time Pad

One-time pad (OTP) mutlak güvenli ve uygulamada kırılamaz olduğu ispatlanabilen tek şifreleyicidir. Aynı zamanda, ispatlanmıştır ki herhangi bir kırılamaz, mutlak güvenli, şifreleyici prensipte bir one time pad olmalıdır. 1917 de G. Vernam tarafından keşfedilen Vernam şifreleyicisi OTP nin iyi bir örneğidir. Bu şifreleyici oldukça basittir; düzmetin mesajını içeren bitlerin bir akışını(stream) alır ve mesajın uzunluğuyla aynı uzunlukta bir anahtar alır, ama anahtarın bir bölümü asla iki kez kullanılmamalıdır aksi halde şifreleyici kırılabilir.

13.1.2. Public Key Systems

Açık anahtar kriptosistemleri, algoritmaların karmaşıklık teorisinin geliştirilmesinin yardımıyla 1970 lerde bulundu. Çözümü binlerce yıl alabilecek çok zor probleme dayalı, gizli ve açık olmak üzere iki anahtara sahip bir kriptosistemin geliştirilebileceği gözlenmiştir. Açık anahtar ile bir kişi mesajlar şifreleyebilir ve bunları gizli anahtarla deşifre edebilir. Böylece mesajları deşifre edebilecek tek kişi bu gizli anahtarın sahibidir, ama açık anahtarı bilen herkes bu mesajları gizleyebilir. Diğer bir fikir anahtar değiş tokuşudur. İki taraflı bir iletişimde gizli bir anahtar kriptosistemi kullanarak esaslı şifreleme için ortak bir gizli anahtar üretmek yararlı olabilir. Whitfield Diffie ve Martin Hellman açık anahtar kriptosistemler çağını başlantan bir anahtar değiş tokuşu protokolü oluşturmak amacıyla sayı teorisini

kullanmışlardır. Bundan kısa bir süre sonra, Ron Rivest, Adi Shamir ve Leonard Adleman(RSA) şifreleme ve dijital imzalar kullanma kapasitesine sahip ilk gerçek kriptosistemi geliştirdiler. Sonraları farklı fikirleri (knapsack problemleri, sonlu alanlarda farklı gruplar ve latisler) kullanan pek çok açık kriptosistemler geliştirilmiştir. Bunların pekçoğunun güvensiz olduğu ispatlanmıştır. Ancak, Diffie Hellman protokolü ve RSA şimdiye kadar kalanların en güçlüleri olarak görülmektedir. Herhangi bir açık anahtar kriptosisteminin temel içeriği zor bir hesaplama problemidir. Kriptosistemin güvenliği, gizli anahtarın açık anahtardan elde edilebilmesi için bu zor problemin çözülmesi gerektiği ilkesine dayanmaktadır(Maurer,Yakobi,1996).



Şekil 13.2. Açık Anahtarlama ile Kriptolama

13.1.2.1. RSA

RSA (Rivest-Shamir-Adleman) muhtemelen en yaygın kullanılan açık anahtar algoritmasıdır. Hem şifreleme hem de dijital imzalar için kullanılabilir. Henüz kanıtlanmamış olmasına rağmen, RSA nın güvenliğinin çarpanlara ayırmaya denk olduğu düşünülmektedir. RSA hesaplaması, iki gizli büyük p, q asalı için, tamsayı modülosu n = p * q ile yapılmaktadır, m mesajını şifrelemek için, m'nin küçük bir açık üs (public exponent) ile kuvveti alınır. Deşifre etmek için, $c = m^e \pmod n$ şifreli-mesajının alıcısı $d = e^{-1} \pmod{(p-1)*(q-1)}$ çarpılabilir tersini hesaplar ve $c^d = m^{e*d} = m \pmod n$ yi elde eder. Gizli anahtar n, p, q, e, d'den oluşur (öyleki p ve q unutulabilir) açık anahtar sadece n, e' yi içermektedir. Saldırganın sorunu odur ki, e nin tersi d nin elde edilmesinin, n'nin çarpanlara ayrılması probleminden daha kolay

olmadığı düşünülmektedir. Anahtar genişliği (modülüsün genişliği) makul bir güvenlik düzeyi için 1024 bitten daha geniş (örneğin, 10^{300} genişliğinde) olmalıdır. 2048 bitlik anahtar genişlikleri daha onyıllarca yeterli güvenliği verebilecektir. Geniş tamsayıları çarpanlara ayırmadaki çarpıcı ilerlemeler RSA'yı saldırılara karşı güvensiz kılabilir, ama bazı varyantlara karşı diğer saldırılarda ayrıca bilinmektedir. İyi uygulamalar, şifreli mesajın çarpılabilir yapısını kullanan saldırıları engellemek için, gereğinden fazlalığı (veya belirli yapı ile yalandan doldurmayı) kullanır. RSA seçilmiş düz metin saldırıları ve donanım ve hata saldırılarına karşı savunmasızdır. Ayrıca, çok küçük üslere karşı önemli saldırılar olduğu gibi, modülüsün çarpanlara ayrılmasının kısmen ortaya çıkarılmasına karşı da saldırılar bulunmaktadır. Çıplak RSA algortiması hiçbir uygulamada kullanılmamalıdır. Tavsiye edilmektedir ki uygulamalar, pekçok büyük protokol ile ortak çalışmanın verdiği faydalar sebebiyle standartları takip etmelidirler.

13.1.2.2. Hash (Özet) Fonksiyonu

Özet fonksiyonu bir mesajın 16 veya 20 bitlik parmak izini çıkarır. Belli bir mesaj aynı özet algoritması kullanıldığında, aynı mesaj özetini verir. Eğer iyi bir özet fonksiyonu kullanılıyorsa, mesajda yapılan tek bitlik bir değişim bile mesaj özetinin değişmesine sebep olur. Özet fonksiyonu kullanarak, kimlik denetimi amacıyla gizli anahtarla bütün mesajı şifrelemek zorunluluğu ortadan kalkar. Özet fonksiyonları verilen mesajı şifreler, ancak bunun geri dönüşü yoktur, yani eldeki mesaj özeti kullanılarak orijinal mesaj elde edilemez. Kullanılan özet fonksiyonlarına örnek olarak SHA-1, MD2, MD-5 gibi algoritmalar gösterilebilir.

13.1.2.3. Diffie-Hellman

Diffie-Hellman anahtar değiş tokuşu için yaygın olarak kullanılan bir protokoldür. Pek çok kriptografik protokolde iki taraf aralarında bir iletişim başlatmak isterler. Ancak varsayalım ki başlangıçta herhangi bir ortak gizliliğe sahip olmasınlar ve böylece gizli anahtar kriptosistemlerini kullanabilirler. Bu durum için Diffie-Hellman protokolü tarafından sağlanan anahtar değiş tokuşun, güvenli olmayan kanallar üzerinden ortak bir gizli anahtar iletiminin sağlanmasına bir çare bulmuştur. Diffie-Hellman problemi olarak adlandırılan bu yöntem, kesikli logaritmalarla ilgili bir problem üzerine kurulmuştur. Bu problemin çok zor olduğu ve bazı durumlarda kesikli logaritma problemi kadar zor olduğu düşünülmektedir. Diffie-Hellman

protokolünün, uygun bir matematiksel grup kullanıldığında genelde güvenli olduğu düşünülmektedir(Güncan,Sönmez,1999). Özel olarak, üslü ifadelerde kullanılan üretici eleman geniş bir periyoda sahip olmalıdır.

Kesikli logaritma algoritmaları Diffie-Hellman'a saldırmak için kullanılabilir. Eğer alışıldık bir aritmetik modülo asıl sayı kullanılarak Diffie-Hellman uygulanılırsa, yeterince geniş bir asal seçmek ve üretici elemanın seçiminde özen göstermek yeterli olacaktır. Güç algılanan problemler, üreteçin kötü seçimlerinden kaynaklanıyor olabilir. Diffie-Hellman'a karşı yapılan saldırılardan biri de ortadaki adam saldırısıdır. Bu saldırı uyarlanabilir müdaheleye (adaptive intervention) gerek duyar, ama eğer protokol dijital imzalar gibi sayaç-sayıcılar (countermeasures) kullanmazsa uygulamada bunu yapmak çok kolaydır. Genelde Diffie-Hellman donanım üzerinde uygulanmaz, ve böylece donanım saldırıları önemli bir tehdit oluşturmazlar. Gelecekte, mobil iletişim yaygınlaştığında, bu durum değişebilir.

13.2. Anahtar Uzunluğunun Belirlenmesi

Bir anahtarın uzunluğunun ne olması gerektiği sorusunun cevabı gereksinimlere göre değişmektedir ihtiyaç duyulan güvenlik seviyesinin belirlenmesi için bazı sorular sorulması gerekir verilerin değeri nedir? Ne kadar süre ile korunmalıdır? vs. Bir şirkete ait ticari sırlar rakipler için merak konusudur, askeri sırlar düşmanların daima ilgi alanı içerisindedir. İhtiyaç duyulan güvenlik düzeyine göre anahtar uzunluğu öyle olmalı ki, teknolojide yıllık yüzde 30 oranında bir ilerleme olduğu varsayılsa bile, harcayabileceği 100 milyon $'ı olan bir saldırganın sistemi kırma olasılığı 232'de 1'den fazla olmamalı gibi son derece özelleşmiş gereksinimler belirlenebilir. Gelecekte hesaplama gücünün ne olacağını kestirmek güçtür, ancak bunun için mantıklı bir kurala başvurulabili. Hesaplama malzemesinin fiyata bölünen verimliliği 18 ayda bir ikiye katlanır ve beş yılda bir 10 kat artar. Böylelikle, 50 yıl sonraki en hızlı bilgisayar bugünkünden 10 milyar kat hızlı olabilecektir (bu değerler genel kullanım amaçlı bilgisayarlar için sözkonusudur). Tablo 13.1.'de farklı bilgi tipleri için ihtiyaç duyulan güvenlik düzeyleri belirtilmiştir;

Tablo 13.1. Farklı Bilgi Tipleri için Gerekli Güvenlik Düzeyleri

Trafik Tipi	Yaşam Süresi	Asgari Anahtar Uzunluğu
Taktiksel Askeri Bilgi	Dakika/saat	56-64 bit
Ürün duyuları,şirket birleşmeleri,faiz oranları	Günler/haftalar	64 bit
Uzun vadeli iş planları	Yıllar	64 bit
Ticari sırlar	10 yıllar	112 bit
Hidrojen bombası sırları	>40 yıl	128 bit
Casusluk bilgileri	>50 yıl	128 bit
Kişisel bilgiler	>50 yıl	128 bit
Diplomatik Sırlar	>65 yıl	128 bit

Aşağıdaki tabloda ise simetrik ve açık anahtarlı algoritmaların saldırılara karşı eşit dirençte olan anahtar uzunlukları belirtilmiştir;

Tablo 13.2 Anahtar Uzunlukları

Simetrik Anahtar uzunluğu	Açık Anahtar Uzunluğu
56 bit	384 bit
64 bit	512 bit
80 bit	768 bit
112 bit	1792 bit
128 bit	2304 bit

Teorik olarak, bir anahtar kullanan kriptografik algoritmalar, olası bütün anahtarların sırasıyla denenmesi yoluyla kırılabilir. Olası anahtarların denenmesi işlemi de, anahtarın uzunluğu arttıkça güçleşecektir. Örneğin 5 bitlik (5 adet 0 veya 1'den oluşan) bir anahtarın, en fazla 2^5=32 farklı anahtarı olabileceğinden, bu anahtarların sırayla denenmesi, şifrenin çözülmesine yeterli olacaktır. 32 bitlik bir anahtar için 2^{32} deneme yapılması gerekir. Bu bir amatörün kendi ev bilgisayarıyla deneyebileceği birşeydir. 40 bitlik anahtara sahip bir sistem için 2^{40} adım gerekir ki, bu da birçok üniversitenin ve hatta bazı küçük şirketlerin bile sahip olabileceği bir güçle mümkündür. 56 bitlik anahtarlı bir sistem (DES gibi) oldukça fazla bir çaba gerektirir fakat özel bir donanım yardımıyla bu da kırılabilir. Bu özel donanımın maliyeti oldukça fazla olmasına rağmen,organize suçluların, büyük şirketlerin ve hükümetlerin sahip olabilecekleri bir güçtür. 64 bitlik anahtarlı sistemler, büyük hükümetlerce kırılabilmektedir ve yakın zamanda organize suçlular, büyük firmalar ve daha küçük hükümetler tarafından da kırılabilecektir.

Saniyede 3 trilyon anahtarı deneyebilen bir makine ile (yaklaşık 1 milyon dolar yatırımla elde edilebilecek bir makine) 56 bitlik DES algoritmasını 3,5 saat içinde kırılabilir. Aynı makine 80 bitlik anahtar kullanan bir algoritmayı 6.655 yılda, 128 bitlik anahtar kullanan bir algoritmayı ise 2.000.000.000.000.000.000 yılda kırabilir. Gelişen teknoloji ve işlemci hızları ile bu tip işlemlerin daha hızlı gerçekleştirilebileceği açıktır. 250 bitlik anahtar kullanan bir algoritmanın kırılması için gereken çabayı hesaplamak için termodinamik yasaları kullanılabilir. Buna göre bir bit işlemi için gerekli minimum enerji kullanılarak yapılan hesaplamada, 250 bitlik tek bir anahtarı kırmak için güneşin tahmin edilen ömrü boyunca dışarı verdiği tüm enerjinin gerekli olduğu ortaya çıkar. Güneşin sadece bir yıl boyunca dışarıya verdiği enerji ile yetinecek olursak, en fazla 192 bitlik bir anahtarı kırmamız mümkün olur. Görüldüğü gibi, teorik olarak kıralabilir kabul edilen algoritmaların pratikte kırılması, anahtar büyüdükçe imkansızlaşmaktadır. Çift anahtarlı kriptografide kullanılan anahtarların uzunukları simetrik anahtarlı kriptografide kullanılanlardan genellikle çok daha büyüktür. Açık anahtar kriptografisini kırabilmek için, doğru anahtarı tahmin etmek değil, açık anahtardan ona uygun gizli anahtarı elde etmek gerekmektedir. Örneğin RSA için bu, iki büyük asal çarpanı olan büyük bir sayının çarpanlarına ayrılması anlamına gelmektedir. Bu işlem de teorik olarak yapılabilir olmasına karşın, pratik olarak gerçekleştirilmesi günümüz teknolojisiyle imkansızdır. Bir kriptosistemin gücü genellikle en zayıf noktasına eşittir. Dolayısıyla, algoritma seçiminden, anahtar dağıtımına ve kullanım koşullarına kadar hiç bir şey göz ardı edilmemelidir.

13.3. Kişilik Belirleme(Authentication)

Kişilik belirleme. uzaktan erişim söz konusu olduğunda en önemli fonksiyondur. Güçlü bir kişilik belirleme olmaksızın ağa girişin kontrol altına alınması olanaksızdır ve bunun sonucu kurumsal bilgilerin yetkilendirilmemiş kişilerin eline geçmesi çok kolay olacaktır.İçten ve dıştan gelecek her türlü yetkilendirilmemiş girişlere karşı sistemin daima koruma altında tutulması gerekir bunun da en etken silahı kişilik belirlemedir.

En yaygın kullanılan kişilik belirleme yöntemi Tek Uygulamalı Parola (One Time Password-OTP)dır.Kişilik belirleme kullanıcı ağın RAS veya yönlendiricisine ulaştığında çalışmaya başlar. Bazı durumda kullanıcı aynı anda bir diğer kısıtlı alana

girmeyi arzu edebilir. Bu durumda ek bir kişilik belirlemesi uygulaması gerekmektedir.VPN de kişilik belirlemede kullanılan en etken yöntem iki faktörlü kişilik belirlemedir. Bu yöntemde ID/Parola kontrolüne ek olarak kişiyi belirlemek için ikinci bir eleman devreye alınır.

Bu uygulama ATM lerde uygulamalara benzetilebilir. Birinci kontrol makinaya verdiğiniz kart üzerinden yapılır. İkinci kontrol için kişisel ID numarası (PIN-Personel ID-Number) kontrolü işleme girer. VPN ortamındaki iki faktörlü uygulamada Birinci kontrol Elekronik-Jeton ve ikincisi PIN dir.

13.4. Yetkilendirme(Authorization)

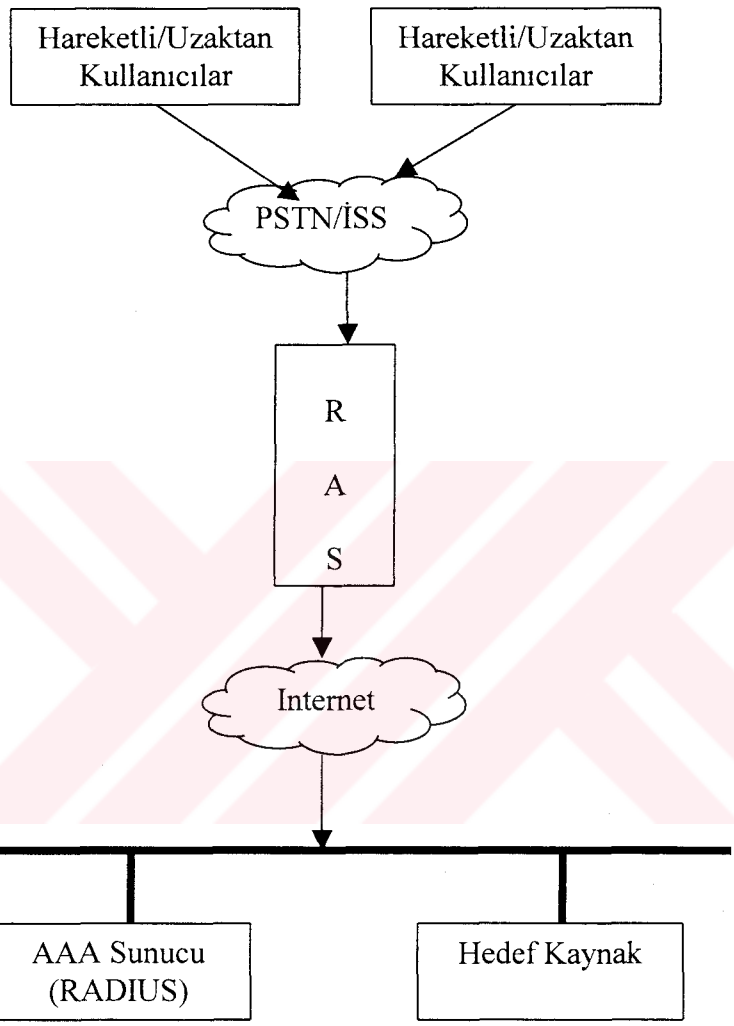
Kişilik belirleme ile yetkilendirmenin sınırı her zaman kesin çizgilerle belli değildir. Yetkilendirme genellikle kişilik belirleme işlemini izleyerek uygulanır ancak kişilik belirleme gerekli değilse birinci uygulama olarak devreye girer. Örneğin WEB sayfasındaki herkesin kullanımına açık bilgiler gibi verilere ulaşmada yani kişilik belirlemeye gereksinim duymayan durumlarda, kullanılan ağ servisinin gerekli desteği sağladığı durumlarda yetkilendirme işlemi yeterli olacaktır. Kişiye özellik, güvenlik ve mahremiyet, kısıtlama yeterli olmadığı durumlarda kolaylıkla bozulabilirler. Ancak kısıtlamalar gerektiğinden çok daha fazla olursa bu kez de yetkilendirilmiş kişilerin gerekli bilgilere ulaşmasında büyük zaman kaybına ve dolayısıyla bu kişilerin çalışma tempolarının düşmesine neden olabilir.Her işte olduğu gibi kısıtlamaların dengeli olarak belirlenmesi kurum için çok büyük önem taşımaktadır. Muhasebe, kullanıcıların ağ'ın hangi noktasından , ne sıklıkla ve ne kadar süre ile devreye girdiğini belirler. Muhasebe fonksiyonu genellikle kişilik belirleme ve yetkilendirme fonksiyonundan sonra devreye girer , ancak bu iki fonksiyonla her hangi bir bağı yoktur.

Özel sanal ağlarda en yaygın olarak kullanılan uzaktan erişimi denetleyen protokollar ;

- CHAP/PAP :Challenge Handshake Authentication Protocol/ Password Authentication Protokol
- RADIUS : Remote Authentication Dial-In User Service

- TACACS: Terminal Access Controller Access Control System . Son iki metot hemen hemen aynı yapıya sahiptirler ve şirket ve İSS'nin RAS'ında görev yaparlar.

Aşağıdaki şekilde RAS üzerinden VPN erişimi yapısı gösterilmiştir;



Adım-1 : Kullanıcı RAS 'a bağlantı kurar
Adım-2 : AAA , RAS ile ilişki kurar
(AAA:Authentication,Authorization,Accounting)
Adım-3 : AAA , RAS 'a yanıt verir
Adım-4 : Hedef kaynağa ulaşım onaylanır

Şekil 13.3. RAS Üzerinden VPN Erişimi

13.4.1. PAP ve CHAP'ın Ortaya Çıkışı

HDLC (High-Level Data Link Control) protokolu temelde veri blokları oluşturmak üzere bitlerden meydana gelen bir çerçeve yapısındadır. Bu çerçevelenmiş verilerin önünde bir başlık(header) bulunur. Bu başlıkta hata kontrol bitleri , adresler ve bir bayrak(flag) bulunur. Bu bayrak çerçevenin başlama noktasını gösterir. Çerçevenin sonunda ise çerçevenin bittiğini gösteren bir bitiş bayrağı da bulunur.PPP (Point-to-Point Protocol), HDLC formatından çıkmıştır. PPP, bu konuda ilk olarak kullanılmaya başlanılan SLIP (Serial Line Internet Protocol) dan çok daha güçlüdür. Örneğin SLIP sadece IP (Internet Protocol) tarafından kullanılabilir. Sadece tek bir protokol tarafından kullanılması ve kişilik belirleme işlemlerindeki eksiklikleri nedeniyle SLIP kullanımı giderek azalmıştır. PPP örneğin IP ve IPX (Internetwork Packet Exchenge) gibi pek çok protokolun tek bir veri bağlantı (Data Link) üzerinden çalışmasına izin verecek şekilde tasarlanmıştır. Ayrıca dinamik adresleme ve kişilik belirleme işlemlerine de destek vermektedir. PPP genellikle Internet'e ulaşmada, ISP lere dial-up bağlanma olanağı sağlamaktadır.

PPP aynı zamanda ana sistemle-yönlendirici , yönlendirici ile yönlendirici ana sistem-ana sistem bağlantılarında çalışır ve VPN ortamında İSS'lere dial-up ulaşmalarda bütün gereksinmeleri karşılayacak şekilde tasarlanmıştır.HDLC de olduğu gibi PPP de 2. katman (Data Link Layer) protokoludur. PPP, veri bağlantı katmanı üzerinden izin vermeden önce iki düzeyde karşılıklı iletişimi gerçekleştirir.Birinci aşamada LCP (Link Control Protocol) paketleri iletişimde bulunan iki uç arasında değiş tokuşa girer Bu safhada sıkıştırma ve çerçeve genişliği gibi özellikler daha önceden belirlenmiştir.İkinci aşamada- bu safha seçimliktir. Örneğin hat eşitliklerini belirlemede kullanılabilir veya ağ katman protokolları , PPP nin Ağ Control Protocol (NCP) özelliğini kullanarak bağlantı üzerinden kullanılabilir.PPP bağlantı yapısı bu tartışmalar sonunda belirlendikten sonra seçimlik PAP /CHAP işlemleri uygulamaya girer.

13.4.2. PAP (Password Authentication Protocol)

PPP ile kişilik belirlemede kullanılan ilk protokol PAP olmuştur. PAP'ı kullanırken bağlanmak isteyen kullanıcıdan kullanıcı ID'si ve parolası hem uzak erişimli kullanıcı ve hem de yönlendirici veya sunucuya gönderilir. Uzak erişimli kullanıcı,

bağlantı sağlanıncaya kadar yönlendirici veya sunucuya dial ederek bağlantıyı sağlar.PAP iki yönlü el sıkışma protokolodur, ancak bugün için özellikle özel sanal ağlarda yeteri kadar sağlıklı güvenlik sağlayamamaktadır. PAP kullanıcı ID ve parolayı şifrelemeden istemciden sunucuya gönderir. Sunucu tarafından sağlanan bilgi kullanılarak , temel kullanıcı bilgileri , ismi ve parolaları taşıyan veri tabanına ulaşır.

SLIP teki kişilik belirlemesinde eksiklik PPP ve PAP kullanılarak giderilebilir. Bununla beraber çok önemli bir problem henüz çözüm beklemektedir, kullanıcı ID/Parola kombinasyonunu playback yöntemi olarak bilinen metodla ele geçirebilir. Bunun için telefon hattına bir saplantı yapmak ve PAP'ı kullanarak ana sisteme bağlanıp tekrarlanan oturumlardan (session) gerekli bilgileri öğrenmek olasıdır. Bu zayıflık nedeni ile, PAP yalnız başına bugünün ağlarında güvenlik için yereli değildir ve bu nedenle PAP ile CHAP birlikte kullanılır. Başka bir deyişle CHAP kişilik belirlemede PAP üzerinden uygulama yapar. Zaten PAP , PPP nin bir parçasıdır CHAP ise PAP'ın bir parçası durumundadır.

13.4.3. CHAP (Challenge Handshake Authentication Protocol)

PAP , ID ve parolaları plaintext formatında gönderdiğinde CHAP bu sorunu tümüyle ortadan kaldırır. CHAP istemci uzaktan erişim yönlendiricisi veya PAP ile bağlanır, daha sonra bu ağ aygıtları ile PPP LCP paremetreleri için pazarlığını yapar ve bunu izleyerek PPP bağlantısı üzerinden kullanıcı ID yi plaintext formunda sağlar. RAS daha sonra CHAP istemci ile bir bağlantı gerçekleştirme girişiminde bulunur. Bu girişim , her bağlantı için tek (Unique) bir bilgi zinciri yapısındadır. Bu zincir gönderilirken RAS, kullanıcı ID için parolayı ekler ve her ikisini de Hash algoritması ile şifreler. Bu tek yönlü şifreleme genellikle MD5 (Message Digest 5) tarafından gerçekleştirilir.

Bu zinciri alan istemci kendi hash değerini kullanarak bu zinciri ve parolayı değerlendirir. Daha sonra belirlediği Hash değerini RAS'a gönderir. Eğer giden ve gelen Hash değerleri uyum sağlarsa RAS bağlatı işlemlerinin başlamasına izin verir. CHAP böylece her bağlantı için tek ve şifrelenmiş bilgi kullanıldığından yalnız kullanıldığında PAP üzerinde etkili olan ve güvenliği bozan playback tekniğini başarısız kılar.Durumu bir örnekle açıklayalım şifrelenmiş bilgilerin kayıt işlemlerinin tamamlandığını var sayalım. Bir playback uygulayıcısı devreye giriyor

ve bir bağlantı kurulması girişiminde bulunuyor ve var sayalım aynı bilgi zincirini kullanıyor. Ancak CHAP ek olarak oturum süresince uzak erişimdeki ana sisteme yeni bir bilgi zinciri gönderir. Bu özellik aynı kullanıcının iki farklı telefon hattını biri büyük bir olasılıkla yetkilendirilmiş kişi, diğeri kaçak sisteme girmek isteyen kişidir, kullandığı durumda aktif hale gelir. Bu durumda CHAP her iki taraftan tek ve şifrelenmiş bilgi zincirinin yeniden gönderilmesini ister.

CHAP bu nedenle üç yönlü el sıkışma protokolu olarak ta kabul edilir. Birinci el sıkışma bilgi zincirinin gönderimi ile, ikinci el sıkışma cevabın alınması ile üçüncü el sıkışma ise kişilik belirleme ile gerçekleşir. CHAP sadece istemciye kişilik belirlemesi uygular, yani sunuculara uygulamaz. PAP ve CHAP , kullanıcı ID/Parola kombinasyonlarını, uzaktan erişimli istemci PC ve NAS (Network Access Server) nın her ikisi üzerine yükler. Böylece yetkilendirilmemiş kişiler sisteme girmeye çalıştığında her iki yönlü kayıt devreye girecektir.

14. VPN PROTOKOLLERİ

14.1. IPSec

Özel sanal ağlar için standart olma yolunda gibi görünen protokol IPSec'tir (Internet Protocol Security). IPSec, Internet Engineering Task Force (IETF) tarafından geliştirilen ve IP tabanlı ağlardaki ağın yapısından gelen güvenlik eksikliği konusuna eğilmek için tasarlanmış olan bir grup kimlik belirleme ve şifreleme protokolüdür. Tünellemeye ilave olarak veri gizliliği, bütünlüğü, kimlik belirleme ve anahtar yönetimi konularına eğilir. IPSec protokolü genellikle güvenlik alanının(domain) uç noktalarında çalışmaktadır. Temel olarak IPSec, bir paketin etrafına başka bir paket sararak şifreler. Daha sonra bütün paketi şifreler. Özel sanal ağ üreticilerinin çoğu ürünlerinde IPSec kullanmaktadır. Her nekadar farklı üreticiler arasında gizlilik, güvenlik, bütünlük ve kimlik belirleme konularında bir uygulamadaki teknolojiler belli protokoller olarak gruplandırılmış olsa da, bunlardan en çok kullanılanları IPsec, tünelleme(PPTP ve LTP) ve Socks5tir(Carlton,2001)

Bu sayıda protokollerin bulunması bazı kurumlar için özel sanal ağ hareketli kullanıcılar ve şubelerin korumalı kurum ağına yerel İSS lerini kullanarak bağlanmasına izin veren uzaktan erişim sunucuların yerine kullanılan bir teknolojidir. Bazıları içinse özel sanal ağlar korumalı yerel ağlar (LAN) arasında Internet üzerinden güvenli tünellerden akan trafiği kapsamaktadır. Özel sanal ağlar için geliştirilen protokoller bu düşünce tarzlarını yansıtmaktadır. IPSec iki yönlü (bidirectional) bir protokoldür, yani Ekstranet konfigürasyonlarının çok dikkatli tasarlanması ve uygulanması anlamına gelmektedir. Bir Ekstranet özel sanal ağ kurarken kullanıcıların bütün ağa erişim sağlamasını veya onlar vasıtasıyla başka kullanıcıların ağa erişmesini istemeyiz.

IPSec göndericinin (veya onun yerine görev yapan geçiş kapısının) her IP paketinin kimlik denetimini yapmasını, şifrelemesini veya her iki fonksiyonu birden pakete uygulamasını sağlar. Bu iki fonksiyonu birbirinden ayırmak IPSec kullanmak için mod denilen iki metodun gelişmesine neden olmuştur. Aktarım modunda, IP paketinin sadece aktarım katmanı bölümüne kimlik dentimi yapılır veya şifrelenir. IP paketinin tamamına kimlik denetimi veya şifreleme yapan öteki yaklaşıma ise tünel

modu denir. IPSec aktarım modu pek çok alanda faydalı olurken, tünel modu belirli ataklara karşı çok daha iyi koruma ve Internette oluşacak trafiği izlemeyi sağlar.

IPSec gizlilik, veri bütünlüğü ve kimlik belirleme için pek çok standartlaşmış kriptografi sistemi üzerine bina edilmiştir. Örneğin IPSec, Diffie-Hellman anahtar değişimlerini iç ağ üzerinde gizli anahtarların karşılıklı taraflara aktarımı için PKC'yi Diffie-Hellman değişimlerini imzalamak, iki tarafın kimliklerini garantilemek, ve man-in-the-middle attackleri engellemek için, DES (data encryption standard) ve diğer bazı şifreleme algoritmalarını veriyi şifrelemek için, anahtarlı hash algoritmalarını (HMAC, MD5, SHA) paketlerin kimliklerini denetlemek için, dijital sertifikaları anonim anahtarları doğrulamak içinkullanmaktadır.

IPSec mimarisi içinde anahtar değişimi ve yönetimi için iki yol vardır; manuel anahtarlama (MK) ve otomatik anahtar yönetimi için IKE(ISAKMP/Oakley IETF standardı olma yolundadır). Her iki metot da IPSec'in zorunlu gereksinimlerindendir. MK az sayıda siteye sahip olan özel sanal ağlar için uygun olurken, fazla sayıda siteye sahip olan veya çok fazla uzak kullanıcıyı destekleyen özel sanal ağlar IKEden daha çok faydalanmaktadır. IPSec sadece IP paketlerini desteklemek için tasarlanmışken, PPTP ve L2TP daha çok NetBEUI, IPX ve AppleTalk kullananlar gibi IP olmayan çoklu protokol alanları için uygun olmaktadır.

14.2. LDAP

LDAP (Lightweight Directory Access Protocol) LAN hizmetlerinin yerelleştirilmesi için ortaya çıkmış bir ikincil sistemdir. X.500 dizinlerinin gerektirdiği 7 katmanlı OSI modeli yerine hafifletilmiş (lightweight) olan 4 katmanlı TCP/IP kullanılmıştır. LDAP bir dizinistemci/sunucu yapısı içinde çalışır. LDAP istemcisi ldap icin yazılmış ve ldap istemcisinin içine gömülmüş APIleri kullanarak aradığı bilginin formatını oluşturarak TCP/IP vasıtasıyla dizin sunucusuna gönderir. Bu isteği alan dizin sunucusu bu isteği dizini içeren bilgisayarı sorgular ve gerekli bilgiyi yine aynı yolla istemciye gönderir. Genel olarak bu dizin ifadesi LDAP'ın yapısı ve içerdiği bilgi itibarı ile veritabanı olarak adlandırılmaktadır. Dizin ifadesi aslında dizinin içerdiği belirli bir sıradaki herbir nesne hakkında bilgi veren bir liste şeklinde açıklanmaktadır. LDAP yapısı genelde sarı sayfalar (yellow pages) ile özdeşleştirilmektedir. Şöyleki sarı sayfalarda bilgi belirli bir sırada dizilmiştir ve bu tip sarı sayfa katalogları bir matbaada basılır(ldap karşılığı write) ve daha sonra

isteyen ya da izin verilen herkes bu listeden aradığını bulur. Bulunan sahşın hakkındaki bilgiler sahşın telefonunu, ev adresini vermektedir.

14.3. RADIUS

RADIUS, uzaktan erişimli kullanıcılar ile var olan bilgisayar ağı arasında kullanıcı ID'si ve parola bilgilerinin güvenli olarak değiş tokuşunu sağlamakla görevlidir. RADIUS açık bir protokol standarttır ve uzaktan erişimli kullanıcılarının 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 protokolunun 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 bulunmakta idi. RAS yalnız başına, çok az kullanıcı bilgisayar ağına ulaşmak ve ağ içinde güvenli noktalara bağlanma isteğinde bulunuyorsa , yeterli olabilir.Buna karşılık pek çok kullanıcı uzakta erişim gereksinimi duyuyorsa ve bunların pek çoğu da kişilik belirleme mekanizmasının çalışmasını gerektiriyorsa, RADIUS bu gereksinimleri çok basit bir uygulama ve birlikte bir nokta ile çözer. Bu birlikte nokta kişilik belirleme geçit kapısı olarak düşünülebilir ve kapı stratejik olarak uzaktan erişim kullanıcı ile bilgisayar ağı arasına yerleştirilir. Pek çok RAS aygıtı ağ içinde kurulmuştur ve coğrafi olarak çeşitli noktalara dağıtılmıştır. Bu durumda , bu kuruluşları izleyerek RADIUS seçimi yapılmaktadır.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.

15. TÜNELLEME

Tünelleme bir ağ ortamında bir protokolun bir diğer protokol üzerinden taşınması işlemi olarak tanımlanabilir. Kendi içlerinde IPX konuşan iki farklı ağ arasındaki bağlantıyı Internet veya başka bir taşıyıcı ortam kullanılarak IP protokolu üzerinden sağlamak tünellemeye örnek olarak gösterilebilir. Bu durumda OSI referans modeline göre IPX paketleri sanki bir yedinci katman (uygulama-application layer-katmanı) verisi(data) gibi işlem görerek tekrar kapsüllenir(encapsulation) karşı tarafın yönlendiricisine ulaştığında ise bu IP paketi açılarak içindeki IPX paketi çıkarılır ve yönlendirme yapılarak haberleşme sağlanır. Tüneller VPN ler için de ayrıca bazı özellikler sağlar . Tünelleme protokolu, tünelin en ucundaki kullanıcı için oturum yönetimi olarak bilinen işlemleri gerçekleştirmek üzere, tünelleri kurar ve yönetir. Tünelleme protokolu IP kadar diğer protokolların kapsüllenmesi işini de sağlar ve tünel aygıtları için yetkilendirme yöntemlerini gerçekleştirir. Protokol genel olarak verileri şifreler ve tünel içine gönderir. Tünelleme protokolunu kullanılmakta olan diğer protokollardan farklılıklarını aşağıdaki gibi özetleyebiliriz(Manas,2001);

- Tünellerin kurulması ve yönetiminin sağlaması
- Çoklu protokol desteği sağlaması
- Tünelin en son noktası için yetkilendirme sağlaması
- Şifreleme sağlaması

Bazı VPN ler tünelleri sadece kendi çoklu protokollarını desteklemek ve Internet üzerinden IP dışında protokolları iletmek üzere kullanılır.VPN tünelleri tarafından hedeflenen güvenlik seviyesinin gerçekleşmesi için tüneller çok dikkatli olarak kurulmalıdır. Tüneller iki grup altında toplanabilir. Bazıları sabit olarak kurulurken bazıları gereksinme duyulduğunda oluşturulabilir. Tünel kurulduğunda, tünel aygıtları bilgi (kullanıcıya ait parola, şifreleme metotları, anahtarlar, tünelleme protokolları, paketlere ait birbirini izleyen numaralar, paket belirleyiciler, kaynak ve varılacak ağ adresleri vb..) alışverişini başlatır. Üç tip tünel yapısından bahsedilebilir;

15.1. Geçitkapısından Geçitkapısına(Gateway) VPN Tüneli

Bu tünelleme yapısı güvenilir olmayan Internet ortamı üzerinden iki güvenli LAN'ı birbirine bağlamayı amaçlamaktadır. Genellikle tüneller LAN'lar üzerine etkili değildirler , zira onlar özel ağlardır. Ancak risk genellikle Internet kullanımı ile hİSSedilmeye başlanır. Bununla beraber risk sadece Internet kullanımı ile değil, tüm şartlarda güvenilir olmayan çalışanlar da bu yapıyı uygunsuz hale getirir. Bu senaryo ancak Internet bağlantılarının desteklendiği kurumsal VPN İntranetlerinin şirketler arasında kiralık hatların devreye alınması ile , güvenlik kazanır.

15.2. Internet Ana Sistemden Geçitkapısına VPN Tünel Bağlantısı

Bu bağlantı da güvenilir kullanıcı ile (kişilik belirlemesinden geçirilmiş) LAN temelli kurumsal tünel geçitkapısı arasında bağlantı söz konusudur. Bu iki senaryo arasındaki önemli fark, bir istemci tarafında LAN'ın bulunmasıdır.. Bu durum, genellikle istemcinin hareketli (mobile) olması yada SOHO (Small Office Home Office) kullanıcılarının arama yaparak ya da İSS kullanarak kurumsal ağa bağlanmaları söz konusu olduğunda ortaya çıkar. Bu senaryoda tüneller Internete direkt olarak bağlanan istemci aygıtlarına kadar genişletilebilir(Manas,2001).

15.3. Ana Sistemden Ana Sisteme (Uçtan uca) Tünel

Bu yapı VPN tünellerinin en gelişmiş şekli olarak görülebilir, ancak bazı PC'ler (ana sistemler) henüz direkt tünelleme yeteneğine sahip değildirler. Önceki iki yapıda kullanıcılar güvenilir olmak zorundadırlar. VPN dikkate alındığında bu güvenilirlik çok kritik bir noktadır. Eğer güvenilir olmayan bir kişiye ağa girmek için izin verilirse veya güvenilir olmayan bir kişi bir yolunu bularak ağa girerse , bu kişiler kolaylıkla ağın her noktasına ulaşabilirler.Ancak belirtilmesi gereken bir nokta vardır ki VPN tünelleri gerçekten çok güvenilir bir yapıdadırlar. Kullanıcı güvenliğinin pek çok kaynağı vardır(Manas,2001);

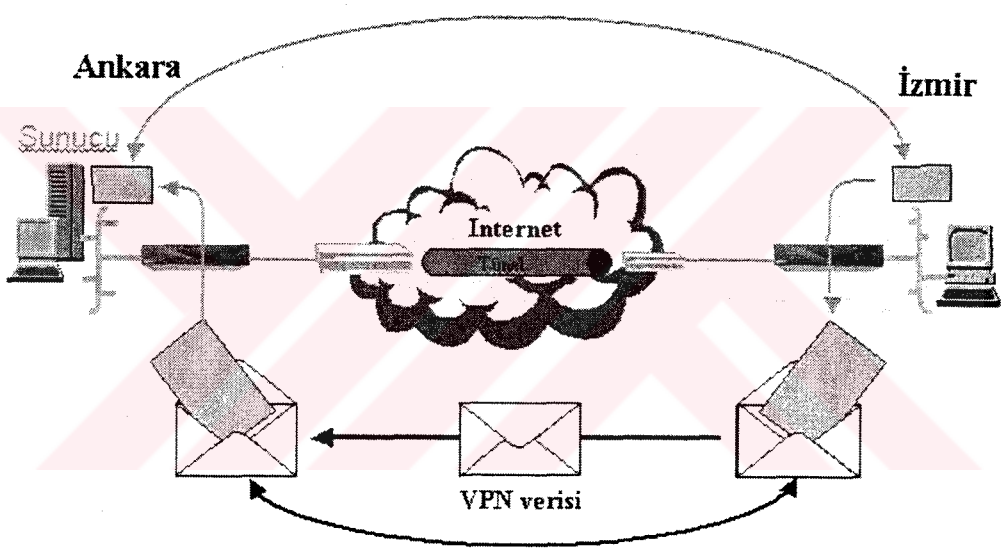
- Kurumsal ağda bulunan kullanıcı güvenilirdir ,çünkü bu özel bir ağdır.
- Uzaktan erişimli kullanıcı güvenilirliğini kişilik belirleme ile kazanır.
- Belirli güvenlik seviyesi sık sık sertifiye(certify) edilir.

Veriler tünel geçitkapısından (kullanıcı ana sistemi) aktarılmadan önce şifrelenir veya kapsül içine alınır. Daha sonra bu paketi alan aygıt bunları şifreden çözer veya kapsül içinden çıkarır. Tünellemede bilgilerin kapsül içine alınma işlemi çerçeve(frame) içindeki paket ve onun içindeki iletilerin (mesaj) kapsül içine alınmasına benzer. Tünelin kapsülleme işlemleri yalnızca tünelin en son noktası tarafından bilinmektedir. Eğer bir saldırgan bir tünelde kapsül içine alınmış bir çerçevenin içine girebilirse göreceği şeyler, çerçeve tipini bilmediği sürece, ona hiç bir şey ifade etmeyecektir. Zaten çerçeve tipi de sadece VPN tarafından bilinmektedir.

VPN'nin kapsülleme ve şifreleme işlemlerini gerçekleştirmesi temel fonksiyonları arasındadır. Ancak temel fonksiyonlar bunlarla sınırlı değildir. VPN ayrıca VPN trafiği içinde özel bir koruma gerçekleştirir. Örneğin yetenekli bir saldırgan ağ içine girip bir kişiyi kullanarak Internet üzerindeki iletilerin içine girerek onları kendi amacına uygun olarak değiştirebilir. Çoğu kez bizzat istemci ve sunucular bu değişmelerin farkına varmaz. VPN tünel ise paketleri belirler ve onlara sıra ile numaralar verir(acknowledgement) ve bunlarda yapılacak değiştirme işlemlerini belirlemek için var olan tüm ölçüm tekniklerini kullanır. Birbirini izleyerek gelen paket numara yapısına etki etmeden tünel içine girip paketi yakalamak, değiştirmek ve yerine yeni bir paket yerleştirmek sanıldığı kadar kolay bir olay değildir. Ancak bu durum gerçekleşirse paket belirleme işlemi tam olarak yerine getirilemez(Manas,2001).

IP de adres yanıltma(IP spoofing) uygulaması giderek artan bir düzeye varmış bulunmaktadır. Ancak adres yanıltma işleminin ilk uygulamalarında saldırganın adresi taşıyan bir IP paketi üretmesi olanaklı idi. Bu durumda paket üretildiği güvenilir ana sistem (veya LAN) veya VPN nin en son noktasında ortaya çıkar. Olayın farkında olmayan istemci ve sunucu paketi kendi ağından gelen bir paket olarak kabul eder ve bunun sonucu her hangi bir kişi olayın farkına varıncaya kadar sistem üzerinde saldırganın arzuladığı bozulmalar gerçekleşir. Ancak bunun gerçekleşebilmesi için, saldırganın kurumsal ağın veya ana sistem sunucu ve kullanıcının IP adresini bilmesi gerekmektedir. Bazı İSS'ler IP adres saklama yöntemini kullanıcıların kendi ağlarının omurgasının ayrıntısını öğrenmesini engellemek için kullanmaktadır. Tüneller aynı zamanda özel kiralık hatlar üzerinde de kurulabilir. Pek çok İSS özel hatlara ek olarak Internet bağlantısı olanağını da

sağlamaktadır. VPN , özel işler veya resmi kurumlar için kendi ağları üzerinden veri transferi yapmak üzere , bir taşıyıcı (örneğin TürkTelekom) kullanarak , yaratabilir. VPN çok genel olarak Internete bağlanmak üzere İSS veya NSP'ler tarafından kullanılan VPN tünelleri yaratılışı İSS veya NSP tarafından dış kaynaklardan istenebilir. Ancak bu durumda tüneller ana sistemlere kadar uzatılmadığı sürece kurumdan İSS ye ulaşım zayıf bir bağlantı olarak düşünülebilir.



Şekil 15.1. VPN Tüneli

16. TÜNEL OLUŞTURMA PROTOKOLLERİ

16.1. PPTP (Point to Point-Tunneling Protocol)

PPTP yönlendiriciler arasında çok yoğun olarak kullanılan PPP(Point to point protocol) nin geliştirilmiş bir şekli olan veri bağlantı protokoludur. PPTP yapımcıları olan 3Com , Ascent , ECI Telamatics , Microsoft , US Robotics 'in oluşturduğu PPTP Forum tarafından geliştirilmiştir. PPTP, IPX, NetBEUI, AppleTalk ve IP gibi protokolların çalışmalarına izin veren GRE protokolunu kullanarak paketleri kapsuller ve Internet aracılığı ile gönderir. PPP ile PPTP çok yakın bağlantı içinde olduğundan, PPTP, PPP de kurulmuş aynı kişilik belirleme yöntemini kullanır. Başka bir değişle PPTP de PPP gibi CHAP (Challenge Handshake Authentication Protocol) ve PAP (Pasword Authentication Protocol) protokollarını kullanır. PPP bir iletişim bağlantısı kurduktan sonra, kişilik belirleme işlemi seçimlik bir safha olarak gelir. Ancak bu safha İSS/VPN yapısı tarafından zorunlu istek olarak hemen uygulamaya sokulmalıdır, aksi halde bütünlüğün sağlanması kesinlikle mümkün olmayacaktır. Microsoft kendi işletim sistemi içinde PPTP için geniş bir destek sağlamaktadır. Windows 95/98 , Windows NT , PPTP yüklenmiş durumdadır ve bu nedenle PPTP nin istemci yazılımında ek bir değişikliğe gerek yoktur. Bu durum Microsoft kullanıcıları için büyük bir üstünlüktür. Zira Widows 95/98 ve Windows NT dışındaki işletim sistemi kullanıcıları, üçüncü parti VPN yazılımları için ek bir ödeme yapmak zorundadır. Windows 95 , PPTP ye kendi dial-up ağ işlem (Dial-Up Networking-DUN) içinde çalışma olanağı sağlar. Windows NT PPTP ile kendi RAS servis yazılımı içinde birlikte çalışır. İlk uygulamalarda istemciden özel ağa tünelleme sadece Windows 95 ve Windows NT de sağlanmıştır. RRAS (Routing ve RAS) devreye girişi ile Microsoft LAN-dan-LANa tünelleme olanağı getirmiştir.

Hareketli istemci ana sistem ile LAN-Temelli sunucu arasında tünel oluştuğunda PPTP tünel kuruluşu için iki bağlantının da sağlanması gerekmektedir birincisi , PPTP istemci ile RAS arasında , ikincisi RAS ile PPTP sunucu arasındadır. Bu iki bağlantı ile PPTP içinde GRE tüneli kurulmuş olmaktadır. PPTP istemci ile PPTP sunucu arasındaki bağlantı GRE tünelidir.Bu tünel oluştuktan sonra, PPP çerçeveleri taşıyan IP paketleri içindeki veriler PPTP istemci ile PPTP sunucu arasında iletilir.

Bu yöntem GRE'nin paket içinde paket yapısından çok daha etkendir. Ayrıca GRE başlığı , dağıtım paketi ile bilgi protokol çerçevesi arasında kullanılır. PPTP kapsülü oluşmasında, eğer istemci uzaktan erişim dial-in istemci değilse dış çerçeve protokolu PPP, Frame Relay veya diğer PPTP yi kullanan bir diğer LAN çerçeve olabilir. PPTP istemci, RAS ve PPTP sunucularının her biri farklı yazılım gereksinimi gösterirler. Örneğin İSS nin RAS'ında (bu bağlantıda Internet kullanılmaktadır) PPTP desteği sağlanmamaktadır. Buna karşılık PPTP yazılımı taşıyan Windows NT kullanmakta ise istemci güvenli bağlantı yapmak üzere PPTP tünellerini kullanma olanağına sahip bulunmaktadır. Bunun tersi bir durumda ise güvenli bağlantı için istemcinin gerekli yazılımı temin etmesi şarttırRAS-PPTP sunucu aracılığı ile sağlanan PPTP desteğini kullanma yerine hareketli istemci üzerine PPTP yazılımının kullanılması halinde VPN'nin çok geniş coğrafik alan üzerinde çoklu İSS bölgelerini desteklemesi olanaklıdır. Geniş bir desteklemesinin nedeni her bir İSS nin PPTP gereksinim duymamasıdır. Bu düzenleme kurumların geniş olarak Windows işletim sistemi kullanması durumunda sorun yaratmayacaktır. Küçük organizasyonlarda eğer bir yerel İSS iş için VPN uzaktan erişim bağlantısının tümünü sağlıyorsa her iki seçenekte geçerli olacaktır.

PPTP sunucusu yazılımında genellikle paket süzme özelliği de vardır. Bu da VPN'ye ek bir güvenlik duvarı özelliği ekler. Microsoft PPTP uygulamasında RFC 40-bit şifreleme algoritması da eklenmiş bulunmaktadır. Bu uygulama özellikle Brute-Force, Play-Back saldırısına karşı korumalarda etken rol oynar. Microsoft PPTP , kendi PPTP sunucusunda 255 bağlantıya kadar olanak sağlamaktadır. PPTP yazılımına istemci yazılımı da eklendiğinde, örneğin 200 den daha az uzak erişim istemcisinin bulunduğu bir VPN uygulamasında Windows 95/98 ve NT kullanıcıları için parasal yönden avantajlı bir durum söz konusu olabilir. Ayrıca , PPTP sunucu ve yönlendirici normal PPP veya çok güvenli PPTP yi desteklemek üzere kurulmuş ise bunlar geniş miktarda uzaktan erişim kullanıcılarını destekler.

16.2. L2TP (Layer 2 Tunneling Protocol)

VPN tünelleri PPTP veya L2F kullanarak kurulabilir. Ancak şunu akıldan uzak tutmamak gerekir ki , Windows işletim sistemleri, Internet omurgasının hemen hemen % 80 ini oluşturan Cisco yönlendiriciler ve diğer Cisco ekipmanları ile birlikte yer almış bulunmaktadır. Microsoft ve Cisco birlikte VPN'de Internet

üzerinde tünelleme protokolunu desteklemek üzere ve her iki şirket ürünleri ile uyumlu olacak bir protokol geliştirdiler. İşte L2TP bu ortak çalışmanın bir ürünüdür.Bu iki şirket Cisco'dan L2F donanım çözümü ile Microsoft'un PPTP yazılım ürünlerinin en yararlı kısımlarını seçerek bir araya getirdiler. Daha sonra da birlikte IETF(Internet Engineering Task Force) ye başvurup bu ürünün standartlık onayını istediler. Pek çok kuruluş daha şimdiden L2TF'yi standart olarak benimsedi ve kullanmaya başladı. Bu durumda L2TF'nin standart olarak kabulünün gerçekleşmesi kaçınılmazdır. Firmaların L2TF'yi hemen benimsemelerinin bir nedeni de bu ürünün L2F ve PPTP'nin üstün özelliklerini birleştirmesi yanında firma bağımlı olmamasıdır(Black,1999).

16.3. Layer 2 Forwarding (L2F)

L2F , Cisco Systems , Nortel ve Shiva tarafından geliştirilmiş firma bağımlı bir protokoldur. L2F , RAS (Remote Access Server) ve ağ yönlendiricileri gibi ağ bağlantı sunucuları arasında tünel sağlamaktadır. PPTP de olduğu gibi L2F de , IPX NetBEUI ve AppleTalk gibi pek çok protokolu desteklemektedir.Ancak L2F bir donanım çözümü iken PPTP bir yazılım çözümüdür. Bu nedenle İSS L2F'yi desteklemek üzere yönlendirici ve diğer ekipmanlarını derece yükseltmesine (Up Grade) gitmeleri gerekmektedir. PPTP, ağ katmanında sadece IP yi desteklerken L2F IP'ye ek olarak pek çok ağ katmanı protokolunu desteklemektedir.L2F özellikleri (specification), L2F paketlerinin nasıl işleneceğini tanımlar PPTP de olduğu gibi kapsülleme için GRE protokolunu kullanmaz. L2F tünel oluştuğunda kullanıcı CHAP/PAP (Challenge Handshake Authentication Protocol/ Password Authentication Protokol) kullanan PPP ile tünel yönlendiriciye ulaşır ve kullanıcının yetkilendirilmesi aşamasında TACACS+ veya RADİUS'tan birini kullanabilir(Black,1999).

17. GENİŞ ALAN AĞLARI(WAN)

Büyük bir coğrafi alana yayılmış bilgisayar ağına Geniş Alan Ağı(WAN) denir. Diğer bir deyişle WAN, iki veya daha fazla yerel alan ağının (Local Area Network) birleştirilmiş halidir. Çoğunlukla açık ağ(public network) olarak isimlendirilen telefon şebekesi, ATM, Frame Relay, uydu, kiralık hatlar, TDM üzerinden oluşturulurlar. Geniş alan ağlarının en temel kurulum amacı geniş bir coğrafyadaki dağınık yerel ağların birbirleri ile haberleşmesini sağlamaktır. Bilgi sistemleri otomasyonunu yazılım, veritabanı ve LAN/WAN entegre olarak tesis etmiş olan ve kullanan bir işletme; iş gücünü, finansmanını ve verimliliğini en üst seviyeye çıkarabilir. Doğru kararları doğru zamanda almanın ve uygulamanın anahtarı doğru parametrelere sahip olmaktan geçer. Alınan ve uygulanan kararların neticeleri de ancak doğru raporlama ve istatistikler ile elde edilebilir.Dünyadaki en büyük WAN, Internet'tir(Çölkesen,1997). WAN standartları aşağıda belirtilen uluslar arası tanınmış otoriteler olarak kabul edilen organizasyonlar tarafından belirlenir ve yönetilir.

- International Telecommunications Union Telecommunication Standardization Sector (ITU/T), formerly the Consultative Committee for International Telegraph and Telephone (CCITT)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- Electronic Industries Association (EIA)

WAN standartları, OSI katmanlarına göre ilk 2 katman olan hem fiziksel hem de data link seviyelerindeki standartları tanımlar. WAN ların belli başlı kullanım amaçları aşağıda belirtildiği şekildedir;

- Veri İletişimi;Farklı yerleşkelerdeki yerel alan ağları arasında veri haberleşmesi yapmak. Bilgi sistemleri otomasyonu ile muhasebe, satış, stok üretim, servis, müşteri ve iş ortağı ilişkilerini yönetmek ve bu parametreleri anlık takip edebilmek.

- Ses/Veri/Faks Entegrasyonu;Kurulu bir geniş alan ağı üzerinden katma değerli servisler tesis ederek işletmenin giderlerini azaltmak ve iş gücünü optimum kullanmak. Örneğin ses entegrasyonu yapılarak ofisler arası telefon giderlerini ortadan kaldırmak. Voice networking uygulamalarını, call center ile entegre B2B ve B2C mantığında tüm ofislerde hayata geçirmek.
- Internet üzerinden e-iş;Internet üzerinden yeni iş olanakları, iş ortakları, yeni ürünler ve yeni pazarlar bulunabilir. Telefon ile anlatılamayacak pek çok şey e-mail ile detaylandırabilir. Firma ile iş ortakları ve müşteriler arasında B2B ve B2C uygulamaları geliştirilebilir.

Bir WAN kurmak için öncelikle fiziksel katman için modem kurulmalıdır. 2. katman data link servis sağlayıcının olduğu katmandır. 2. katmanda Türkiye'de Türk Telekom tarafından sağlanan Frame Relay, Kiralık Hatlar, sayısal (ISDN) ve analog telefon hatları gibi şebekeler veya uydu gibi kablosuz şebekeler vardır. 3. katman için router veya multiservice switch kurulmalıdır.

17.1. WAN Prokolleri

SDLC(Synchronous Data Link Control):IBM tarafından geliştirilen bit oriented bir protokoldür. Temel olarak IBM ağlarını geniş alan ağlarına bağlamak için geliştirilmiştir.

HDLC(High Level Data Link Control):Paket anahtarlamalı ağlarda bir yönlendiriciyi başka bir yönlendiriciye bağlamak için kullanılan ve en yoğun kullanılan WAN data link protokolüdür.

LAP-B(Link Access Protocol-Balanced):X.25 ile kullanılır. Ancak basit bir data link transport olarak da kullanılabilir.

PPP(Point-to-Point ProtocolPPP):RFC1548 ile tanımlanmıştır. Internet Engineering Task Force (IETF) tarafından geliştirilmiştir. PPP, network layer protocol tanımlamak için bir protokol alanı içerir.

ATM(Asynchronous Transfer Protocol):Genel olarak omurga ağın anahtarlar arası haberleşmesinde kullanılan 53 oktet boyutunda sabit paketler temelli bir protokoldür. Network to Network Interface(NNI) ile ATM ağının bir parçası olacak şekilde ve User to Network Interface(UNI) ile ATM ağının bir kullanıcı ucu olacak şekilde

tanımlama yapılabilir. ATM, servis kalitesi olan, her trafik türünü destekleyen hizmet sınıfları olan hücre (cell) tabanlı bir ağ teknolojisidir. Hücre tabanlı olduğundan, yani aktarım için kullanılan paketlerin sabit uzunlukta olmasından dolayı hızlı aktif cihazlar, daha az elektronik aksam kullanılarak tasarlanabilmektedir. Üstelik bu teknoloji ile üretilmiş cihazlarda porttan porta olan gecikmeler ve herhangi iki uç düğüm arasındaki geçikme hesaplanabilmektedir.

X.25(Packet Level Protocol PLP): Bir terminal ile paket anahtarlamalı ağ arasındaki bağlantıyı tanımlar.

Frame Relay:Frame Relay LAP-B tarafından yapılan hata kontrol mekanizmasına ihtiyacı ortadan kaldıran yüksek kalitede dijital bir ortamdır. Hata düzeltmesinin olmadığı basitleştirilmiş çerçeveleme kullanır. Frame Relay diğer WAN protokolleri ile karşılaştırıldığında 2nci katman bilgilerini çok daha hızlı gönderebilir.

ISDN(Integrated Services Digital Network):Ses ve datanın varolan bakır telefon kabloları üzerinden taşındığı, dijital servisler topluluğudur.

17.2. En Çok Kullanılan WAN Haberleşme Yöntemleri

Kiralık Hatlar (Leased Lines):Point to Point bir haberleşmedir. Time Division Multiplexing ile 1 adet 2.048Mbps, 32 adet 64Kbps kanala (2 kanal işaretleşme ve yönetim-30 kanal nx64Kbps veri iletişimi) bölünür ve taşınır. Merkez ofis TDM modem ve yönlendirici V.35 port sayısını artırır. Kanallı E1(ChE1) kullanma imkanı vardır. Merkez ofis yatırım maliyeti fazladır. Türk Telekom A.Ş. aylık işletme/kira bedelleri yüksektir. Performans yüksektir ve ses/veri/video entegrasyonu amacı ile rahatlıkla kullanılabilir. Ancak yüksek bant genişliği ister. Türk Telekom A.Ş. altyapısında NewBridge ve Tellabs olmak üzere iki şebeke vardır.

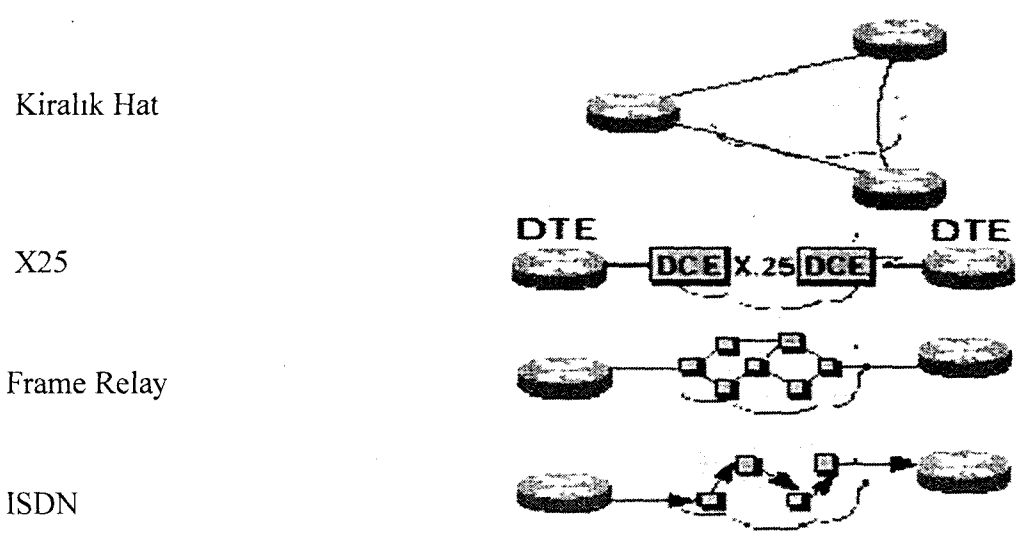
X.25:Paket anahtarlamalı bir şebekedir. 1970'li yılların teknolojisi ve zamanının en iyi çözümlerindendir. Her bir X.25 nodeda error detection/correction yapılması ve kullanıcı yoğunluğuna bağlı olarak daha uzun yönlendirme seçimi gibi nedenlerden dolayı performansta düşmeler ve gecikmeler oluşur. Bu nedenle ses/veri/video entegrasyonu için uygun bir ortam değildir. Servis kalitesi (Quality of Service) garantisi yoktur.

Frame Relay:Paket anahtarlamalı bir şebekedir. Kiralık hatlar ile karşılaştırıldığında aylık işletme/kira bedelleri (yaklaşık %50) oldukça düşüktür. Performans yüksektir

ve ses/veri/video entegrasyonu amacı ile rahatlıkla kullanılabilir. Türk Telekom A.Ş. TURPAK Frame Relay şebekesi tamamen Nortel Networks PASSPORT 6400/7400/ 15000 serisi multiservice anahtarlar ile kurulmuştur. FRF-5 ve FRF-8 desteği ile kendi aralarında ATM, access tarafında Frame Relay çalışabilmektedir. Servis kalitesi vardır. Frame Relay, kurumlara geniş alan ağları üzerinden yüksek hızlarda servis alma imkanı verir, esnek bant genişliği kullanımını sağlar. Frame Relay, uç noktalar ve ağ arasında veri taşınması ve sinyalleşmesi ile ilgili arayüzü tanımlar. Bu arayüz birden fazla kullanıcının haberleşme kaynaklarını paylaşması esasına dayanır ve ağa bağlanan tek bir fiziksel hat aracılığıyla birden fazla nokta ile görüşmelerine olanak tanır. Bu noktada artık iki uç arasında sürekli ayrılmış bantgenişliği yerine gereksinim duyuldukça kısa zaman aralıklarında kullanılan daha yüksek bantgenişlikleri söz konusudur. Bu fiziksel hat üzerinden birden fazla nokta ile yapılacak sanal bağlantılar değişik topolojilere sahip ağlardaki kiralık devrelerle karşılaştırıldığında, gereksinim duyulan devre sayısının azalması ile maliyet etkin bir alternatif olarak kullanılmaktadır. Frame Relay, günümüzün iyileştirilmiş hat kapasitesi ve uç kullanıcı cihazları (PC, iş istasyonları vs.) üzerindeki TCP/IP temelli uygulamaların hata denetim ve düzeltme mekanizmaları dikkate alınarak X.25'deki çoğu denetleme fonksiyonu en aza indirilerek geliştirilmiş ve bu nedenle Frame Relay servisi ile çok yüksek işlem hızlarına çıkmak mümkün olmuştur.

ISDN: ISDN aynı hat üzerinden, aynı anda, ses, veri, resim ve görüntü aktarma olanağı veren sayısal bir şebeke sistemidir; bulut teknolojisine dayanır. Yani bağlantılar noktadan noktaya değil de anahtarlamalı olarak yapılır; aynı analog telefon şebekesinde olduğu gibi numarası bilinen başka bir noktaya, gerektiği anda bağlantı kurulur ve iletişim bittikten sonra bağlantı koparılarak hat ortamı başka bağlantılar için boşaltılır. Sayısal yapısı ve servis türleri açısından ISDN hem WAN bağlantılarında, hem de küçük ofis ve evden yapılan bağlantılarda esnek performanslı ve kaliteli çözüm sunar. Üstelik küçük ofis veya evden yapılan bağlantılarda var olan telefon hatlarının kullanılması söz konusudur. ISDN, BRI (Basic Rate Interface) ve PRI (Primary Rate Interface) olarak adlandırılan iki tür servis sunar; bu iki servis esnek yapısından dolayı WAN bağlantılarında gereksinim duyulan geniş bir isteğe çözüm sunabilmektedir. Örneğin iki uzak LAN'ın birbirine bağlanması PRI servis türü üzerinden yapılırken, buradaki kaynakları kullanan küçük ofisler BRI servis türünü kullanarak LAN'lara erişebilirler; ve hat ortamından aynı anda farklı

uygulamalara ait veri aktarımı yapılabilir. ISDN şebekede ücretlendirme, kullanıma göre yapılır. Bu özelliğinden dolayı ISDN servis türleri yedek hat olarak ta kullanılır. Halihazırda başka bir teknolojiyle gerçeklenmiş iki LAN bağlantısında, araya bir ISDN bağlantısı eklenerek, iletişimin güvenirliliği sağlanabilir ana hatta olabilecek bir kesilme durumunda, aktarım ISDN servisi üzerinden sağlanır. ISDN BRI servisi herbiri 64 Kbps olan iki tane D kanalı ve 16 Kbps olan bir tane B kanalı sunar. Normalde D kanalları veri aktarımı, B kanalı ise işaretleşme senkronizasyon işlemleri için kullanılır. Bazı uygulamalarda B kanalının işaretleşme dışında kalan (artan) band genişliği veri aktarımı için de kullanılır. B kanalında kullanılan işaretleşme protoklu OSI başvuru modelinin 1, 2 ve 3. katmanları için tanımlı işlevleri içerir. ISDN BRI servisi 2B+D olarak ta gösterilir; toplam band genişliği 144 Kbps olur; fiziksel katman için tanımlamaları, ITU-T I.430 standartı ile belirlenmiştir. ISDN PRI servisi ise, herbiri 64 Kbps olan 30 tane D kanalı ve 64 Kbps olan bir tane B kanalı sunar (30B+D) bu Avrupa standardı olarak bilinir, Amerika ve başka birkaç ülkede kullanılan standartta 23 tane D kanalı ve bir tane D kanalı bulunur (23B+D). Dolayısıyla Avrupa standardında ISDN PRI'ın toplam bant genişliği 2.048 Mbps, Amerika standardında 1.544 Mbps'dir. ISDN PRI için fiziksel katman tanımlamaları ITU-T I.431 standardı ile belirlenmiştir. ISDN servisinin esnekliği, kanallarının aynı anda farklı uygulamalar tarafından kullanılabilmesi ve üstelik tek bir kanalın sahip olduğu bant genişliğinin farklı oturumlar tarafından paylaşılabilmesinden gelir. Bunun yanısıra servis kalitesi sunması, arayan kişinin kimlik bilgilerinin bilinmesi gibi birçok özelliklere sahiptir.



Şekil 17.1. En Çok kullanılan WAN Teknolojileri

17.3. WAN Bağlantı Maliyetleri

Tablo 17.1. ve 17.2.'de yukarıda bahsedilen ve ülkemizde Türk Telekom tarafından verilen WAN bağlantı hizmetlerinin maliyetleri gösterilmiştir;

Tablo 17.1. Frame Relay Bağlantı Ücretleri

		Aylık Ücretler (TL)	
Hız(Kbps)	**Bağlantı Ücreti**	**Port Ücreti**	**PVC Ücreti**
64	170 000 000	33 000 000	349 000 000
128	170 000 000	69 000 000	613 000 000
256	170 000 000	103 000 000	870 000 000
512	170 000 000	170 000 000	1 427 000 000
1024	256 000 000	256 000 000	2 369 000 000
2048	349 000 000	428 000 000	3 498 000 000

Tablo 17.2. ATM Bağlantı Ücretleri

Hız(Mbps)	**Aylık Ücret**
1	1 612 000 000
2	2 784 000 000
4	3 498 000 000
6	4 211 000 000
8	4 912 000 000
10	5 611 000 000
16	7 710 000 000
22	9 824 000 000
28	11 923 000 000
34	14 036 000 000
46	18 963 000 000

17.4. VPN WAN Karşılaştırması

Internetin yaygınlaşması, bağlantı fiyatlarının ucuzlaması ve servis sağlayıcıların belli hizmet kalitesini sunmasıyla birlikte VPN uygulamaları hızla yaygınlaşmaktadır. Güvenlik ve performans en önemli parametrelerdir ve VPN teknolojilerindeki gelişmeler kullanılacıların güvenlik ve performans konulardaki beklentilerini tatmin edecek düzeylere erişmiştir. VPN Geniş Alan Ağlarına (WAN) bir alternatif olarak karşımıza çıkmıştır. Birbirlerine göre üstünlüklerini ve dezavantajlarını anlamak için tablo 17.3.'de özellikleri karşılaştırılmıştır. Karşılaştırma yaparken Türkiye şartları gözönünde bulundurulmuştur;

Tablo 17.3. VPN, WAN Karşılaştırması

	VPN	WAN(kiralık hatlar,frame relay,dial-up bağlantılar ATM)
Güvenlik	Herkese açık olan bir altyapıyı kullandığı için güvenlik VPN uygulama larında en çok üzerinde durulan konudur. Değişik tünelleme, şifreleme ve doğrulama teknikleri ile oldukça güvenli Sanal Ağlar oluşturulabilmektedir.	Taşıyıcı servisin güvenli olması yeterlidir. İstenirse burada şifreleme uygulanabilir ve güvenlikten emin olunabilir.
Performans	Internet Servis Sağlayıcı ile imzalanan bir Servis kalite sözleşmesi herhangi bir performansın garanti edilmesi söz konusu değildir. Ayrıca tüm bölgelerde İSS nin POP noktaları bulunması gerekmektedir.Birden fazla İSSden geçme durumunda performans düşüşleri olabilir.	Performans, sunulan hizmet çeşidine göre değişik parametrelerle garanti altına alınmıştır.
Fiyat	Uzaktan erişimin maliyeti göz önüne alınırken, aramanın nereden kaynaklandığı çok önemlidir. Kullanıcıların kendileri ile aynı şehirde bulunan uzak erişim sunucularını arayarak ağa erişmeleri için en ideal çözüm direkt telefon hatlarını kullanmak olabilir.Söz konusu işlem şehirlerarası veya milletlerarası aramayı gerektiriyorsa, VPN'nin maliyeti çok daha düşük olacaktır.	Türk Telekomun yeni fiyat politikası ile kiralık hat ücretleri oldukça yükselmiştir. Frame Relay servisi teşvik edilmektedir.
Uzaktan Erişim	VPN uygulamalarının en avantajlı olduğu durum uzaktan erişim ihtiyacının fazla olduğu uygulamalardır.	Normal telefon şebekesi üzerinden arama yapıldığından telefon ücretleri oldukça yüksektir.

VPN yada alternatif diğer teknolojileri kullanma kararı verilirken yukarıdaki tabloda belirtilen avantajların değerlendirilmesinin yanı sıra şubelerin konumları performans/güvenlik ihtiyaç derecesi, uzaktan erişim ihtiyaçları, ilave avantajlardan faydalanma istekleri de karar verilmesinde belirleyici olmalıdır.

18. SANAL ÖZEL AĞ KURULUMU

18.1. Sanal Özel Ağ Kurulum Aşamaları

Bir sanal özel ağ kurulumu projesini birbirini takip eden 10 aşama halinde özetleyebiliriz;

Uzaktan erişim gereksinimleri değerlendirilir; Ne tür WAN bağlantıları gerekli olduğu belirlenmelidir. Kullanıcılar kurum ağına LAN/WAN üzerinden mi, yoksa çevirmeli bağlantılar üzerinden mi erişmektedir? Uzaktaki kullanıcılar aynı organizasyonun bir parçası mıdırlar? İntranet'ler aynı organizasyon içinde birbirine güvenen yerleşke ve kullanıcıları birbirine bağlar. Merkez ofise bağlı şubeler uzaktan ve mobil çalışanlar, bu kategoriye girer. İntranet linkleri için VPN, kullanıcı ve şubelere sanki fiziksel olarak kurumsal ağa bağlıymış gibi çalışma olanağı vermelidir. İntranet VPN'sinde, kurumsal güvenlik politikalarından daha fazlası aranmaz. Yani, uzaktaki kullanıcılar kurum ağına giriş yapabilmek için onaylandıktan (authentication) sonra, geçerli olan kurumsal güvenlik politikaları uygulanır; daha fazlası değil. İntranet VPN'lerinde, şube ofislerin fiziksel güvenliği önem kazanmaktadır. Fiziksel güvenlikten, şubedeki kilit ve anahtarlardan, bilgi işlem ve ağ aygıtlarına erişim ve şirkette çalışmayanların aynı unsurlara erişiminin denetlenmesine kadar bir çok etken anlaşılmalıdır. Eğer bu sayılanlardan hiçbirisi sorun değilse, bu durumda VPN tabanlı kullanıcı onayı bulunmayan LAN'dan LAN'a tünel oluşturmak yeterli olur. Eğer fiziksel güvenlik sorunluysa, bu durumda güçlü onay mekanizmaları çalıştırılmalı, uzak kullanıcıların kurum ağı üzerinden sadece yalıtılmış alt ağlara(subnet) erişmesine izin verilmelidir(Quiggle,2001). Ekstranet güvenlik gereksinimleri daha sıkı tutulmak durumundadır. Kuruma özel gizli bilgilere erişebilme yasak olmalı, ancak istendiği zaman izinle erişim sağlatılmalı, iş sona erdikten sonra erişim yine yasaklanmalıdır. Ekstranet bağlantıları normal olarak kurum dışından kişiler anlamına geldiğinden, bunların yönetimi oldukça zordur.

Üst yönetim işin içine erken bir aşamada sokulmalıdır.Bir organizasyonun güvenlik politikaları, hangi tip uzaktan erişimlere izin verilip hangi tip erişimlere izin verilmediğini açıkça tanımlamalıdır. Bu tür yönergeler yazılırken, kuruluşun üst yönetim kadrosu işin projenin erken aşamalarında işin içine çekilmeli ve ortak bir konsensüs oluşturulmalıdır. Yönergede, kullanılacak VPN donanımının tipi(model ve üretici kastedilmiyor) ve gerçekleme seçenekleri ve kullanıcıların nasıl onaylanacağı gibi konuların yer alması yararlı olur. Yönergede içerilebilecek diğer konular arasında, uzak erişim için uygunluk, yönetimsel sorumluluk, ekstranet bağlantıları için sorumluluk, VPN kullanımının gözlenmesi, seyahatteki kullanıcılara erişim hakkı verilmesi gibi konular bulunmalıdır. Yazılı politikalar arasında, kriptolama anahtarlarının uzunluğu gibi teknik ayrıntılar da olabilir. İşten ayrılan veya görev sorumlulukları değişen kullanıcılar, derhal onay veri tabanlarından çıkarılmalıdır. Bu tür işlemlerin kesintisiz yürüyebilmesi için, kurumların insan kaynakları bölümleri ile VPN yöneticileri arasında eşgüdümün sağlatılması gerekecektir.

En uygun ürünün belirlenmesi:Pazardaki VPN ürünleri üç sınıftan birine sokulabilir. Bunlar;

- Donanım tabanlı sistemler
- Kendi kendilerine yeterli yazılımsal ürünler
- Ateş duvarı (firewall) tabanlı sistemler

Bunların çoğu LAN'dan LAN'a çevirmeli bağlantıları desteklemektedir. Donanımsal VPN ürünleri tipik olarak kriptolama uygulayan yönlendiricilerdir (encrypting routers). Bu tip ürünler kriptolama anahtarlarını aygıt içindeki silikon bir yonga (chip) üzerinde sakladığından, bu ürünlerin şifrelerini kırabilmek, yazılımsal tabanlı ürünlere göre daha zordur. Kriptolama uygulayan yönlendiriciler diğer seçeneklere göre daha hızlı çalışırlar. Eğer 1.5 Mbps ve üzeri bağlantı hızları ile çalışılacaksa, bu tür VPN ürünlerin seçilmesi uygundur. Bu tip ürünlerin başlıca sakıncaları arasında, üreticiye özgü standart olmayan donanımlar nedeniyle her iki uçta da aynı ürünlerin kullanılma gereği ve ağ topolojisinin değiştiği veya bir kullanıcının şifre anahtarı iptal edildiği her defasında, her uçtaki aygıtlarda el ile değişiklikler yapılmasını gerektirmesidir. Daha yeni nesil donanım tabanlı ürünlerde her masaüstü makine için istemci yazılımı sağlanmaya başlanmıştır. İstemci yazılımı ile değişen bilgiler otomatik olarak işlenebilmektedir. Yani, yeni nesil donanım

tabanlı ürünlerle işler daha kolaylaşmış ve yazılım tabanlı ürünlerle farklar yavaş yavaş ortadan kalkmaya başlamıştır.

Yazılım tabanlı VPN ürünleri daha fazla esneklik sağlamaktadır. Örneğin donanım tabanlı ürünler protokolden bağımsız olarak tüm trafiği tünellemelerine karşılık, yazılım tabanlı olanlar trafiği adres veya protokole bağlı olarak tüneller. Çevirmeli (dial-up) linkler gibi performansın düşük/orta düzeyde olduğu bağlantılar için yazılımsal VPN ürünleri daha iyi bir seçenek olabilir. Yönetimlerinin zor oluşu yazılımsal ürünlerin başlıca sakıncasıdır. Bu tür ürünler için üzerinde çalıştıkları bilgisayar işletim sistemi (OS), uygulamanın kendisi ve uygun güvenlik mekanizmaları hakkında bilgi sahibi olunmalıdır. Bazı yazılımsal paketler yönlendirme tabloları ve ağ adresleme şemalarında değişimler yapılmasını gerektirebilirler.

Güvenlik duvarı tabanlı VPN'ler iç ağa erişimin kısıtlanması da dahil güvenlik duvarının güvenlik mekanizmasından yararlanır. Güvenlik duvarı tabanlı VPN'ler ayrıca, adres dönüştürme, güçlü bir onay mekanizması(strong authentication), gerçek zaman alarmları oluşturabilme ve ayrıntılı loglama olanağı sağlar. Bu arada bazı güvenlik duvarı ürünleri tehlikeli veya gereksiz servisleri iptal ederek OS'nin çekirdeğini(kernel) sağlamlaştırır. Eğer uzaktaki kullanıcı veya ağlar potansiyel olarak saldırgan nitelik taşıyorlarsa güvenlik duvarı tabanlı VPN ürünleri uygun çözüm olur. Bu durumda, güvenlik duvarı üzerinde üçüncü bir arayüz kartı(NIC) ve kendine özgü erişim denetim kuralları ile demilitarized zone(DMZ) segmenti oluşturulur. Saldırganlar DMZ koluna ulaşabilse bile, iç ağdaki segmentlere zarar veremeyeceklerdir. Sadece İntranet amaçlı gerçeklemeler için güvenlik duvarı tabanlı VPN'ler gerçeklenme ve yönetilmeleri en kolay ve en ucuz seçeneklerdir. Bu üç VPN tipi için ağ yöneticilerinin;

- Baş edilebilen protokol tipleri
- IPSec desteği
- Onay/doğrulama sunucusu desteği
- Kriptolama anahtarlarının ihraç edilebilirliği(bazı ülkelere ihraç yasağı bulunmaktadır)

gibi kritik bazı konulara dikkat etmesi gerekir. Kurumların önemli bir kısmında birden fazla protokol kullanılmaktadır. Buna karşılık VPN ürünlerinin çoğunluğu sadece IP'yi desteklemektedir. IPX veya SNA gibi diğer protokollerin geçirilmesi

gereken durumlarda VPN ürününün ya bu protokolleri kriptolaması veya IP üzerinden tünellemesi gerekir.

IPSec, IETF tarafından TCP/IP protokol takımına standartlara dayalı onay ve kriptolama eklemek üzere girişilen bir çalışmadır. IPSec'in yaygınlık kazanmasıyla güvenilir bir çalışma kurmak için illa da aynı üretici firmanın VPN ürününden kullanılması gerekmeyecektir. Her ne kadar bir çok VPN kendi onay/doğrulama veri tabanına sahipse de, ağ yöneticileri mevcut onay/doğrulama sunucularının işlevselliğini arttırmak isteyebilir. Örneğin birçok RAS'da(Remote Access Server) RADIUS(Remote Authentication Dial-In User Server) veya TACACS(Terminal Access Controller Access System) protokollerinden birisine dayalı bir dış sistem kullanılır. Kendi kendine yeterli onay/doğrulama sunucularının avantajı ölçeklenebilirliktir(scalability). Erişim aygıtlarının sayısından bağımsız olarak, tek bir onay/doğrulama sunucusu yeterli olur.

Test etme (sınama) aşaması:İki üç tane VPN ürünü ayrıntılı testlerden geçirilir. Uzak kullanıcılar arasından küçük bir pilot kullanıcı grubu belirlenerek sistem denenir. İlk denemelerde teknik becerisi birbirinden oldukça farklı çalışanlar seçilmesinde yarar vardır. Bu şekilde, VPN ürününün kolay kullanılabilme ve yönetilebilme durumları hakkında fikir edinilmiş olur.

Başarılı bir VPN test süreci altı noktayı kapsamalıdır:

- VPN'nin organizasyonun uzak erişim politikalarına uygun olarak konfigüre edilebileceğini ortaya çıkarmalıdır
- VPN'nin kullanımda olan tüm onay ve yetkilendirme(authorization) mekanizmalarını destekleyip desteklemediğini ortaya çıkarmalıdır
- VPN'nin anahtarları etkin bir şekilde yaratıp dağıtabildiği kanıtlanmalıdır
- Uzaktaki kullanıcı ve yerleşkelerin sanki fiziksel olarak kurum ağına bağlıymış gibi çalışabildikleri kanıtlanmalıdır
- Sorunlar çıktığında sorunların nasıl giderilebileceği konusunda ipuçlarını sağlar
- VPN'nin teknik veya teknik olmayan personel tarafından kolayca kullanılıp kullanılamayacağını ortaya koyar.

Sistemin ölçeklenmesi:Uygun donanım sistemine karar verme aşamasında toplam kullanıcı sayısı, aynı anda açılan oturumların sayısı gerekli anahtar uzunluğu tahmin edilmeye çalışılır. Sunucu üzerine olabildiğince fazla RAM takılmalıdır. Çünkü daha

fazla RAM, aynı anda daha fazla sayıda bağlantı anlamına gelir.1.5 Mbps 'den daha yüksek hızlara çıkıldıkça donanım tabanlı VPN'lerin dikkate alınması önerilir. Bazı üreticiler ürünleri ile ilgili performans (başarım) kıyaslama(benchmarking) raporlarını sunarlar. Bu kıyaslamaların hangi koşullarda yapıldığının bilinmesi ve farklı üretici ürünlerinin aynı koşullar altında birbiriyle kıyaslanması doğru olur. Bu kıyaslamalar yapılırken, çerçeve (frame) uzunluğu, kriptolama algoritması ve anahtar uzunluğu, sıkıştırma ve mesaj onayının kullanılıp kullanılmadığı gibi konulara dikkat edilmesi gerekir. Ağ yöneticilerinin göz önüne alması gereken iki kritik konudan birisi, sistemlerin yedeklenmesi (birinde arıza çıktığında diğerinin üzerinden çalışma), diğeri ise çok sayıda sunucu üzerinden yük dengelenmesidir (load balancing).

VPN sunucu için yer belirlenmesi:Uzaktaki kullanıcıların kurum ile yakın ilişkisi VPN aygıtının nereye yerleştirileceğini belirler. Merkez ofis ortamındaymış gibi çalışmak isteyen uzaktan erişen kullanıcılar için, VPN sunucuyu ateş duvarı arkasında özel(kurumun korunan iç ağı) ağın üzerine yerleştirilebilir. Fakat bunun saldırganlar için potansiyel bir hedef olacağı unutulmamalıdır. Eğer uzaktaki kullanıcıların çoğu dış organizasyonlara ait ise, VPN aygıtlarının DMZ ağı üzerine yerleştirilmesi daha uygun kaçar. Ayrıca, güvenlik duvarı DMZ kolu üzerindeki aygıtları korur. Eğer onay/doğrulama sunucusu kullanılacaksa, DMZ altağına yerleştirilmelidir. Bu şekilde, gerek dışarıdan ve gerekse içerden gelebilecek tehditlere karşı korunup, yönetilebilir. Şube ofislerle linkler kurulması en kolay yöntemdir. Link ile kastedilen, yerleşkelerdeki bir çift sunucu arasında kriptolanmış tünel oluşturulmasıdır. Seyahat eden çalışanlar veya evlerinden çalışan kullanıcıların onaylanması gerekir. Bu tür çalışmada, kullanıcılar VPN sunucu ile bağlantı kurar ve VPN sunucu kurum güvenlik duvarının dışındaki DMZ kolunda yer alan bir onaylama sunucusuna onay isteğini iletir. En kritik bağlantılar, iş ortaklarıyla oluşturulan bağlantılardır. Bu durumda, bağlantı istekleri ilk önce ikinci DMZ kolunda yer alan VPN sunucusuna gider. Daha sonra, istekler ilk DMZ kolunda yer alan onaylama sunucusuna gönderilir. Bundan sonra, kabul edilen bağlantı istekleri istek yapılan kaynağa doğru yönlendirilir.

Diğer ağ aygıtları yeni baştan konfigüre edilir:VPN kurulması halinde, IP yönetimi ve ateş duvarları söz konusu olduğundan, ağ üzerindeki diğer aygıtların yeniden biçimlendirilmesi (konfigürasyon) gerekecektir. VPN tasarımlarında genellikle ağ

adres dönüşümü(NAT: Network Address Translation) tekniği kullanılır. NAT'da, ağ içindeki özel adresler, Internet tarafından bakıldığında tek veya az sayıdaki bir grup yasal adrese karşı düşürülür. Ağ yöneticileri, hangi adreslerin ağın içinde kullanılmak üzere ayrıldığını belirlemek üzere VPN cihazlarını konfigüre etmelidir. Güvenlik duvarı tabanlı VPN'lerin çoğu DHCP (Dynamic Host Configuration Protocol) tekniğini desteklemektedir. DHCP ağa bağlı istemcilere dinamik olarak IP adresleri atayan bir yöntemdir. Ağ yöneticileri DHCP ve VPN fonksiyonlarını koordine etmelidir. Aksi halde istemciler ya sadece Internet'e veya sadece iç ağa doğru yönlendirilirler. Halbuki her ikisine doğru yönlendirilmelidirler. Eğer VPN güvenlik duvarının arka tarafında kalıyorsa, güvenlik duvarında da konfigürasyon yapılmalıdır. Bu yüzden, güvenlik duvarı için ya doğal bir Proxy veya kapsüllenmiş VPN trafiği geçiren bir kural tanımı yapılmalıdır. Ayrıca trafiği VPN aygıtına ulaştıran bir izin verme kuralı yazılmalıdır. Ekstranet'ler halinde VPN aygıtı DMZ kolunda yer alır. Bu durumda güvenlik duvarına, Internet'ten gelen kriptolanmış trafiği DMZ'ye ve uygulama trafiğinin DMZ'den iç ağa geçmesini sağlayan ek kural satırları yazılmalıdır. Eğer iç ağda bir de onay sunucusu (authentication server) mevcutsa, güvenlik duvarının DMZ ile iç özel ağ arasında onay isteklerinin gidip gelmesine izin verecek şekilde biçimlendirilmesi gerekir. Bilgisayar isimlerini IP adreslerine eşleştiren DNS(Domain Name System) sunucusunda herhangi bir değişikliğe gidilmesine gerek yoktur. Fakat, eğer DNS sunucusu Internet tarafından görülebiliyorsa, saldırganlar için özel kurum ağının planını ortaya çıkarmada hizmet edebileceği unutulmamalıdır.

VPN kurularak konfigüre edilir:Yazılım ve güvenlik duvarı tabanlı VPN'lerde, işe güvenli bir sistem ile başlanmalıdır. VPN'nin kurulacağı sistemin üzerinden tüm gereksiz servisler, uygulamalar ve kullanıcı hesapları kaldırılmalıdır. Sistem üzerine en son hataları(bug) ve güvenlik sorunlarını gideren yamalar kurulmalıdır. Ağ yöneticilerinin VPN üzerinde ayarlaması gereken parametreler arasında, anahtar uzunluğu, birincil ve ikincil onay/doğrulama sunucuları, bağlantı ve atıl (idle) zaman aşımları (timeout), sertifika yaratma, anahtar yaratma ve dağıtma bulunmaktadır. Sayısal sertifikalar kullanıcılar yerine diğer uçtaki VPN aygıtının kimliğini yoklar. Bazı üreticilerin ürünlerinde, tüm bu sayılan bilgiler merkez ofisteki VPN aygıtına girilir ve uzak uçtaki aygıtlar çevrimiçi hale geldikçe bu bilgileri merkezden indirirler. Uzaktan bağlanan kullanıcılar için, şifrelerin yönetilmesi, bağlantı

betiklerinin(script) hazırlanması ve onay yönteminin oluşturulması gerekecektir. Ağ yöneticileri ayrıca, karşı uçtaki onay ve yetkilendirme (authorization) programlarını senkron kılmalıdır. Onay/doğrulama işlemi kullanıcının kendisinin iddia ettiği kişi olduğunu ispat ederken, yetkilendirme işlemi uzaktaki kullanıcının hangi ağ kaynaklarına erişim hakkı olduğunu tanımlar. Bazı hallerde onay sunucusu aynı zamanda grup yetkilerini kontrol edebilir. Böyle durumlarda grup bilgisinin sunucu ile VPN aygıtı arasında düzgün bir şekilde haberleşilmesi gerekir.

VPN'nin gözlenip yönetilmesi:Internet bağlantısının gözlenebilmesi gerekir. Bu VPN'nin ağ trafiği ve veri akış hızı üzerindeki etkisini ölçebilmek için gereklidir. VPN sadece ağ yöneticisi tarafından çalıştırılıp anlaşılmamalı, uzaktaki son kullanıcılar bile bazı temel kullanım kuralları ve yapılabilecek basit şeyler hakkında bilgilendirilmelidirler.

Yedek sistemler oluşturma:VPN kullanım tecrübesi arttıkça, kurum içindeki diğer kritik iş uygulamaları da VPN üzerinden Internet'e taşınacaktır. Örneğin bir şirket müşteriler için satış mağazası açabilir. Bu tür kritik işler açısından, bağlantıların yedeklenmesi şarttır. Tasarım aşamasında yedek bağlantı ve cihazlar planlanmalıdır. Yüksek trafik yoğunluğuna sahip siteler için yük dengelemeyi destekleyen VPN'ler seçilmelidir. Aksi halde, kullanıcılar erişememe veya yavaşlık gibi şikayetlerde bulunabilirler. Acil durumlar için el altında bazı modemler ve çevirmeli hatlar bulundurulmasında yarar vardır. Tüm bu sayılanlar, maliyeti artıran unsurlardır. LAN'dan LAN'a bağlantılar için, en uygun bağlantı yedekleme seçeneği ISDN hatlarıdır. Yedek bağlantıların düzenli aralıklarla, çalışır durumda olup olmadıklarının kontrol edilmesi unutulmamalıdır. VPN teknolojisi, kurumların bilişim altyapısını(infrastructure) radikal bir biçimde değiştiren ve yeni iş yapma biçimlerini olanaklı kılan yeni bir teknoloji olup, hakkındaki gelişmelerin izlenmesi gereklidir. Bunun yanında konu, sertifikalar, kriptografi, tünel oluşturma protokolleri, mesaj özetleri(message digest) ve diğer bileşenleri ile az çok karmaşıklık oluşturmaktadır.

18.2. Protokol Seçimi

Bu kısımda daha önceki bölümlerde bahsedilen ağ , güvenlik vs protokollerinden gerçek hayattaki ihtiyaçlara cevap verecek uygun kombinasyonların seçimi ile ilgili

olarak bir kontrol listesi oluşturulmaya çalışılmıştır. Aşağıda çalışma kapsamında ele alınan tüm protokoller hakkında kısaca bilgi verilmiştir;

DES: Veri Şifreleme Standardı (DES- Data Encryption Standard) 1970'lerin ortalarında geliştirilmiş bir algoritmadır. ABD Ulusal Teknoloji ve Standartlar Enstitüsü (NIST) tarafından bir standart haline getirilmiş. Geçmişte ve şimdi özellikle finans sektörlerinde yaygın olarak kullanılmaktadır

RSA(Rivest-Shamir-Adleman): Muhtemelen en yaygın kullanılan açık anahtar algoritmasıdır.

Hash Fonksiyonu:Özet fonksiyonu bir mesajın 16 veya 20 bitlik parmak izini çıkarır. Belli bir mesaj aynı özet algoritması kullanıldığında, aynı mesaj özetini verir. Eğer iyi bir özet fonksiyonu kullanılıyorsa, mesajda yapılan tek bitlik bir değişim bile mesaj özetinin değişmesine sebep olur.

Diffie-Hellman :Diffie-Hellman anahtar değiş tokuşu için yaygın olarak kullanılan bir protokoldür, bu yöntem, kesikli logaritmalarla ilgili bir problem üzerine kurulmuştur. Bu protokol tarafından sağlanan anahtar değiş tokuşu, güvenli olmayan kanallar üzerinden ortak bir gizli anahtar iletiminin sağlanması için bir yöntem oluşturulmasını sağlamıştır.

PAP: Kişilik belirlemede kullanılan ilk protokol PAP olmuştur. PAP'ı kullanırken bağlanmak isteyen kullanıcıdan kullanıcı ID'si ve parolası hem uzak erişimli kullanıcı ve hem de yönlendirici veya sunucuya gönderilir.

CHAP: Kullanıcı ID ve şifreleri hash fonksiyonu kullanılarak kriptolanır, PAP ta olduğu gibi bu bilgiler düz metin şeklinde iletilmezler.

IPSec: IPSec, Internet Engineering Task Force (IETF) tarafından geliştirilen ve IP tabanlı ağlardaki ağın yapısından gelen güvenlik eksikliği konusuna eğilmek için tasarlanmış olan bir grup kimlik belirleme ve şifreleme protokolüdür.

LDAP: LDAP (Lightweight Directory Access Protocol) LAN hizmetlerinin yerelleştirilmesi için ortaya çıkmış bir ikincil sistemdir, bir dizinistemci/sunucu yapısı içinde çalışır. Genel olarak bu dizin ifadesi LDAP'ın yapısı ve içerdiği bilgi itibarı ile veritabanı olarak adlandırılmaktadır.

RADIUS: RADIUS, uzaktan erişimli kullanıcılar ile var olan bilgisayar ağı arasında kullanıcı ID'si ve parola bilgilerinin güvenli olarak değiş tokuşunu sağlamakla görevlidir. RADIUS açık bir protokol standarttır ve uzaktan erişimli kullanıcılarının merkezi olarak uzaktan erişimini sağlar.

TACACS: Terminal Access Controller Access Control System, standartlaşmış bir güvenlik protokolür. Bir sisteme erişilme girişiminde bulunulduğunda, TACACS kullanıcı adını ve şifresini merkezi bir sunucuya ilerletir. Bu sunucu gerekli doğrulamayı yapar ve TACACS'a o kullanıcının ya ağa girmesine izin verilmesi ya da reddedilmesi için bir karşılık gönderir.

PPTP: PPTP yönlendiriciler arasında çok yoğun olarak kullanılan PPP(Point to point protocol) nin geliştirilmiş bir şekli olan veri bağlantı protokoludur. PPTP yapımcıları olan 3Com , Ascent , ECI Telamatics , Microsoft , US Robotics 'in oluşturduğu PPTP Forum tarafından geliştirilmiştir, paketleri kapsuller ve Internet aracılığı ile gönderir.

L2TP: L2TP, Microsoft ve Cisco tarafından VPN'de Internet üzerinde tünelleme protokolunu desteklemek üzere ve her iki şirket ürünleri ile uyumlu olacak bir şekilde çalışmak üzere oluşturulmuş bir tünelleme protokolüdür.

Layer 2 Forwarding:L2F , Cisco Systems , Nortel ve Shiva tarafından geliştirilmiş firma bağımlı bir protokoldur. L2F , RAS (Remote Access Server) ve ağ yönlendiricileri gibi ağ bağlantı sunucuları arasında tünel sağlamaktadır.

SDLC:IBM tarafından geliştirilen bit oriented bir protokoldür. Temel olarak IBM ağlarını geniş alan ağlarına bağlamak için geliştirilmiştir.

HDLC: Paket anahtarlamalı ağlarda bir yönlendiriciyi başka bir yönlendiriciye bağlamak için kullanılan ve en yoğun kullanılan WAN data link protokolüdür.

LAP-B: X.25 ile kullanılır. Ancak basit bir data link transport olarak da kullanılabilir.

PPP: Internet Engineering Task Force (IETF) tarafından geliştirilmiştir. PPP, network layer protocol tanımlamak için bir protokol alanı içerir.

ATM: Genel olarak omurga ağın anahtarlar arası haberleşmesinde kullanılan 53 oktet boyutunda sabit paketler temelli bir protokoldür

X.25: Bir terminal ile paket anahtarlamalı ağ arasındaki bağlantıyı tanımlar.

Frame Relay: LAP-B tarafından yapılan hata kontrol mekanizmasına ihtiyacı ortadan kaldıran yüksek kalitede dijital bir ortamdır. Hata düzeltmesinin olmadığı basitleştirilmiş çerçeveleme kullanır

ISDN: Ses ve datanın varolan bakır telefon kabloları üzerinden taşındığı, dijital servisler topluluğudur.

Kiralık Hatlar: Point to Point bir haberleşmedir. Performans yüksektir ve ses/veri/video entegrasyonu amacı ile rahatlıkla kullanılabilir.

Aşağıda, bahsedilen protokollerin kullanılabileceği farklı alanlar olarak düşünülen eğitim kurumları, devlet kurumları, banka/finans kuruluşları ve diğer ticari kurumlar ve bu kurumların ihtiyaçları konusunda bilgi verilmiştir.

Eğitim Kurumları

Bilgisayar teknolojisi eğitim çağındaki insanların niteliğini olumlu yönde artıracak ve etkileyecek, öğrencilerin derslerde dikkatini arttıracak, daha verimli öğrenmeye yardımcı olacak, yaratıcılığı ve başarıyı arttıran bir araç olarak kullanılabilir. BDE (Bilgisayar Destekli Eğitim) denildiğinde ise bilgisayar teknolojisinin eğitimde kullanılması anlaşılmaktadır. Eğitimde bilgisayar teknolojisinin kullanılması ile sadece öğrencilere dönük faaliyetler anlaşılmamalıdır ülke içi ve uluslararası alandaki eğitim ve araştırma kurumları (özellikle üniversiteler) arasında kurulacak iletişim kanalları sayesinde bilgilere ulaşma ve paylaşma imkanlarında hız ve kolaylık anlamında büyük gelişmeler sağlanabilir hatta günümüzde de tüm dünya çapında olmasa da belirli ölçüde sağlanmaktadır. Eğitim kurumları gibi sundukları bilginin -özellikle uzaktan eğitim gibi alanlarda- iletimin belli bir seviyede sürekliliğinin sağlandığı durumlarda anlamlı olabileceği göz önünde bulundurulursa kullanılan iletişim hatlarının kapasitesinin (bant genişliği) yüksek olması bu kurumlar için önemlidir, bunun yanında araştırma/geliştirmeye dönük faaliyetlerde ise güvenlik önem kazanan bir kavramdır.

Devlet Kurumları

Sistem entegrasyonu ve ölçeklenebilirliğin olanakları ve sınırlarını teknolojik kurumsal ve politik olarak araştırarak, birbiriyle uyumlu çalışabilen güvenli sistemler geliştiren, Internet teknolojileri, devlet bilgisine ulaşım, elektronik oy verme ve elektronik vergilendirme sistemini mümkün kılan, vatandaşların demokratik süreçlere katılması için yöntem ve ölçümlemeler geliştiren ve kendini sürekli

yenileyen, Internet kullanımının kamu sektöründe ve halk arasında daha yaygın hale gelmesiyle yeni ve entegre hizmetler veren, devlet tarafından verilen hizmetlerin özel girişim ve STK ortaklıkları ile başka kuruluşlar tarafından verildiği, bilginin araştırılması, seçilmesi, analizi ve paylaşımı için geliştirilecek teknolojilerin kamu görevlilerinin karar verme süreçlerini derinden etkilediği, bu teknolojilerin kullanımıyla birlikte, halk katılımı ve açık devlet kavramlarının mümkün kılındığı kamu sektöründe, elektronik arşivleme ve kayıt yönetiminin gündelik hayatın bir parçası haline geldiği, daha gelişmiş ve sürekli gelişmeleri takip eden bilgi teknolojileri yönetiminin varolduğu, araştırma kaynaklarının kullanılabilir bilgi sağladığı ve uygulanabilir yöntemler geliştirebildiği bir devlet yapısı ihtiyacı önümüzdeki yıllarda giderek artan bir biçimde hissedilecektir, günümüzde başta Amerika ve bazı batı Avrupa ülkeleri devlet kurumlarının kendi aralarında ve vatandaş ile olan ilişkilerinde yoğun şekilde bilgisayar teknolojisi kullanımına yönelmektedirler, bu eğilim e-devlet adı verilen yeni bir kavramı da ortaya çıkarmıştır. Devlet organlarının kendileri arasındaki iletişiminde bilgilerin diplomatik, stratejik, askeri vs. içeriğe sahip olması ihtimali bulunduğundan güvenlik bu kurumlarda dikkat edilmesi gereken en önemli husustur, vatandaş ve devlet arasındaki iletişim kanallarında ise yüksek hız önemli bir faktördür.

Ticari Kurumlar

Teknolojideki hızlı gelişmeler, başlangıçta sadece kurum içinde kullanılmak üzere düşünülmüş olan bilgi sistemlerini, tek bir iş yerinin fiziksel sınırlarının ötesine uzanabilecek özelliklerle donatılmış bir hale gelmeye zorlarken bir yandan da bu gelişimin itici gücü olmuştur. Yani bahsedilen bilgi sistemleri, işletmelerin birbiriyle etkileşime girmesine, veri paylaşabilmesine ve iş süreçlerinin tanımlanmasında diğer şirketlerle işbirliği yapabilmesine olanak tanımalıdır, kısaca kurumun dışarıya doğru genişletilebilmesine imkan vermelidir. Örneğin, müşteri hizmetleri uygulamaları sadece müşteri verilerini izlemekle kalmamalı, aynı zamanda müşterilerle etkileşime de olanak tanımalıdır. Coğrafi olarak farklı bölgelerde bulunan fabrika, tedarikçi firma ve dağıtım merkezlerinin eşgüdümlü olarak planlanması yüksek düzeyde bir bilgi entegrasyonu ve iletişimini gerektirmektedir. Hatta bu entegrasyonun yurt dışı bağlantılar nedeniyle küresel boyutlara taşınması gerekmektedir. Kurumların faaliyet gösterdikleri alanlara ve iletilen bilginin içeriğine göre ihtiyaç duyulacak güvenlik seviyesi belirlenmelidir ticari bilgiler, müşteri bilgileri vs söz konusu olduğu

durumlarda yüksek güvenlikli bir iletişim ortamına gerek duyulmaktadır ve böyle bir ortamı oluşturabilecek yazılım ve donanım ürünleri seçilmesi uygun olacaktır.

18.2.1. Avrupa Birliğinin Elektronik İletişim Konusundaki Önerileri

Internet gibi açık elektronik ağlarının elektronik ortamda iş konusunda gittikçe yaygınlaşması bilgi güvenliği konusunu gündeme getirmekte ve dünyada bir çok ciddi kurum bilgi güvenliğinde kullanılacak teknolojilerle ilgili geleceğe dönük araştırmalar yapıp öneriler sunmaktadır. Avrupa Birliği de bu kurumlardan birisidir ve burada Avrupa Komisyonu'nun konuyla ilgili görüşleri özetlenecektir. Bilgi güvenliğinde kullanılan teknolojilerin başında kriptografi bulunmaktadır. Sayısal imza ve şifreleme konularında kriptografi olmadan güvenliğin sağlanmasının mümkün olmadığı, bilgi güvenliğinin ancak kriptografik yöntemler kullanılarak sağlanabileceği Avrupa Komisyonu'nun çeşitli yayınlarında belirtilmiştir. Avrupa Komisyonu üye ülkelerde sayısal imza ve şifreleme konusundaki yasal düzenlemeleri takip etmekte ve üyelerini sayısal imzanın hayata geçirilmesi konusunda teşvik etmektedir. Sayısal şifreleme yasa dışı örgütlerin gizli haberleşmesinde yasal olmayan yollarla kullanılıp risk teşkil etme tehlikesini taşıdığından bununla ilgili yasal düzenlemeler yavaş ilerlemektedir. Oysa ki sayısal imzada veri zaten açık olduğundan bu konuyla ilgili yasaların çıkması daha kolay olmuştur. Üye ülkelerden Almanya ve İtalya çıkardığı sayısal imza yasalarını yürürlüğe koymuştur. Komisyon ve üye ülkeler OECD, Birleşmiş Milletler, Dünya Ticaret Örgütü gibi diğer uluslar arası kurumlarla da sayısal imzada teknik standartlar ve yasal düzenlemeler konusunda diyalog halindedir. Avrupa Parlementosu Eylül 1996'da bilgi güvenliği ve gizliliği, sayısal kimlik belirleme ve gizliliğin korunması konularında Komisyonu yasal hazırlıkların yapılmasına davet etmiştir. Kasım 1996'da Bakanlık Konseyi üye ülkelerden ve Komisyondan elektronik olarak transfer edilen verinin bütünlük ve doğruluğunun sağlanması için gereken ölçülerin hazırlanmasını istemiştir. Mart 1997'de OECD kriptografi politikaları konusunda dökümanlar hazırlamış, sayısal imza ve şifreleme konuları da dahil olmak üzere kriptografinin kullanımı konusunda ülkelerin kendi politikalarını belirlemelerinde yol gösterici olmuştur. Nisan 1997'de Komisyon şifreleme teknolojisinin ve ürünlerinin serbest kullanımı ve sayısal imza girişimi ile ilgili politikaların belirlenmesi için hazırlıkların yapılmasını duyurmuş ve bu politikaların tasarısı belirlenmiştir:

- Sayısal imza için Avrupa tasarısı saptamak.
- Kriptografiyle ilgili ürün ve servislerin iç piyasada kullanımını sağlamak ve bunu yaparken kamusal güvenliğe saygının ve Avrupa'da güvenlik alanının homojen bir şekilde yaygınlaştırılmasının garanti edilmesi.
- Avrupa endüstrisini kriptografik ürün ve servislerin kullanımı için teşvik etmek.
- Internet ve diğer elektronik ağlarda uluslararası platformu ilgilendiren sorularla ilgilenip, kriptografik servis ve ürünlerin önündeki ticari engellerin kaldırılması ve küresel ölçüde noktadan noktaya iletişimde güvenliğin mümkün olduğunca sağlanması.
- Avrupa ülkelerinin tasarıları içinde gizliliğin korunması, tüketici ihtiyaçları ve insan hakları gibi konularda kriptografinin entegrasyonu için temellerin atılması.
- Tüm ekonomik sektörlerdeki kullanıcıları küresel bilgi topluluğunun fırsatlarından faydalanmasını sağlamak ve teşvik etmek.

18.2.2. Kullanılacak Protokolun Belirlenmesi

Protokol seçimi konusunda faaliyet alanlarına göre belirlenecek farklı kriterlere uygunluk açısından değerlendirme yapılmalıdır. Bu kısımda çalışmada bahsedilen güvenlik, tünelleme, iletim protokolleri kullanım kolaylığı,yaygınlık güvenlik,hız,maliyet ve servis kalitesi kriterleri açısından 1-7 arasında değişen bir derecelendirmeye göre değerlendirilmiştir.

Kullanım kolaylığı: Yapılması gereken ayarların çokluğu, karmaşıklığı, gözetim ve bakım ihtiyacının miktarı, kullanım için gerekli bilgi seviyesi kullanım kolaylığını belirleyen faktörler olarak düşünülmüştür. En kolay 7, en zor 1 ile ifade edilmiştir.

Yaygınlık: Kullanılan donanıma olan bağımlılığı ifade eder donanımın yaygınlığı ile doğru orantılı bir değişim gösterir. En yaygın 7, en az yaygınlık ise 1 ile gösterilmiştir.

Güvenlik: İstenmeyen kimselerin iletişim sürecine müdahalelerine karşı olan direnci göstermektedir. En güvenli 7, en güvensiz 1 ile ifade edilmiştir.

Hız: En hızlı 7, en yavaş 1 ile gösterilmiştir.

Maliyet: Protokolun kullanılabilmesi için gerekli olan ek yazılım, cihazlar ve eğitim ihtiyacı maliyet unsurunu etkilemektedir. En düşük maliyet 7, en yüksek maliyet ise 1 ile gösterilmiştir.

Servis Kalitesi: Kullanım sürecinde önceden belirlenen beklentilere olan uygunluğu ifade eder. En yüksek servis kalitesi 7 ile gösterilmiştir.

Yukarıda bahsedilen kriterlerden yaygınlık, güvenlik gibi kriterler güvenlik ve tünelleme protokollerinde daha yüksek öneme sahiptirler, hız ve maliyet gibi kriterler ise güvenlik için kullanılan farklı protokollere göre birbirinden çok farklılık göstermeyen kriterlerdir. Veri iletimini sağlayan WAN protokolleri olarak bahsedilen protokollerde ise maliyet, hız ve servis kalitesi daha yüksek öneme sahiptir. Tablo 18.1.'de, kullanılan protokollerin yukarıda bahsedilen kriterlere göre değerlendirilmesi görülmektedir.

Tablo 18.1. Protokollerin değerlendirilmesi

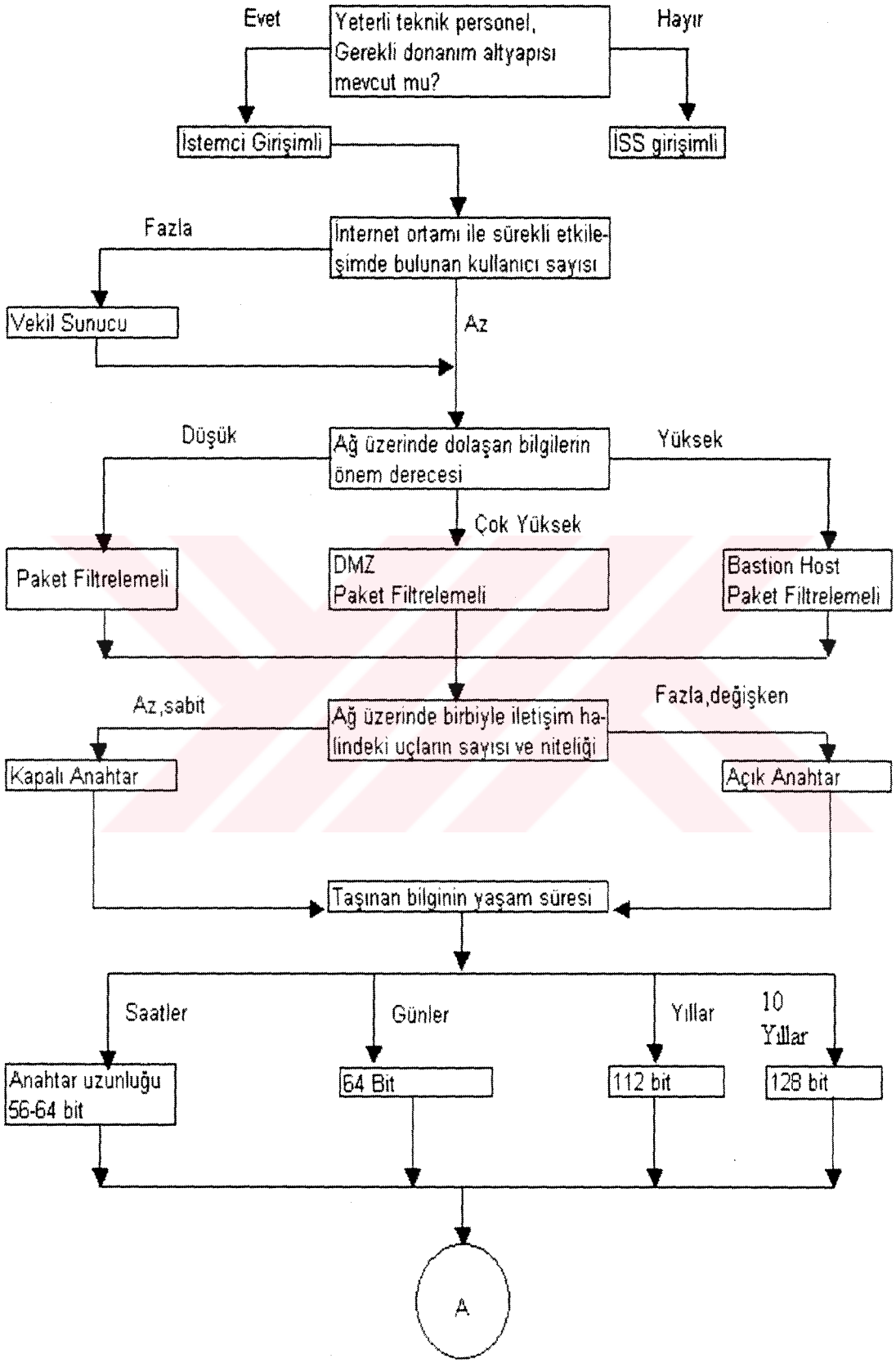
		Kullanım Kolaylığı	Yaygınlık	Güvenlik	Hız	Maliyet	Servis Kalitesi
Güvenlik	DES	5	4	5	5	5	5
	RSA	5	7	6	5	6	6
	Hash	5	6	5	5	6	5
	Diffie-Hellman	4	6	7	5	4	7
	PAP	6	6	3	6	7	4
	CHAP	6	5	5	6	7	4
VPN Protokolleri	IPSec	5	7	6	6	5	6
	LDAP	4	5	5	5	4	5
	RADIUS	6	7	6	6	4	6
	TACACS	5	5	5	5	6	5
Tünelleme	PPTP	6	6	5	6	5	6
	L2TP	5	7	6	6	6	7
	L2F	4	4	5	5	4	5
WAN Protokolleri	SDLC	4	3	4	4	4	4
	HDLC	5	7	6	6	5	6
	LAP-B	4	4	4	4	4	4
	PPP	6	6	5	5	5	5
	ATM	4	5	6	7	2	6
	X.25	4	4	4	4	4	3
	Frame Relay	5	6	6	6	6	6
	ISDN	6	5	5	5	5	6

Tablo 18.2.'de ise daha önce bahsedilen farklı faaliyet alanlarına sahip kurumlar için, kullanılabilecek protokoller ve kurumlar arasında kullanım amacına uygunluğa göre yapılan eşleştirmeler görülmektedir.

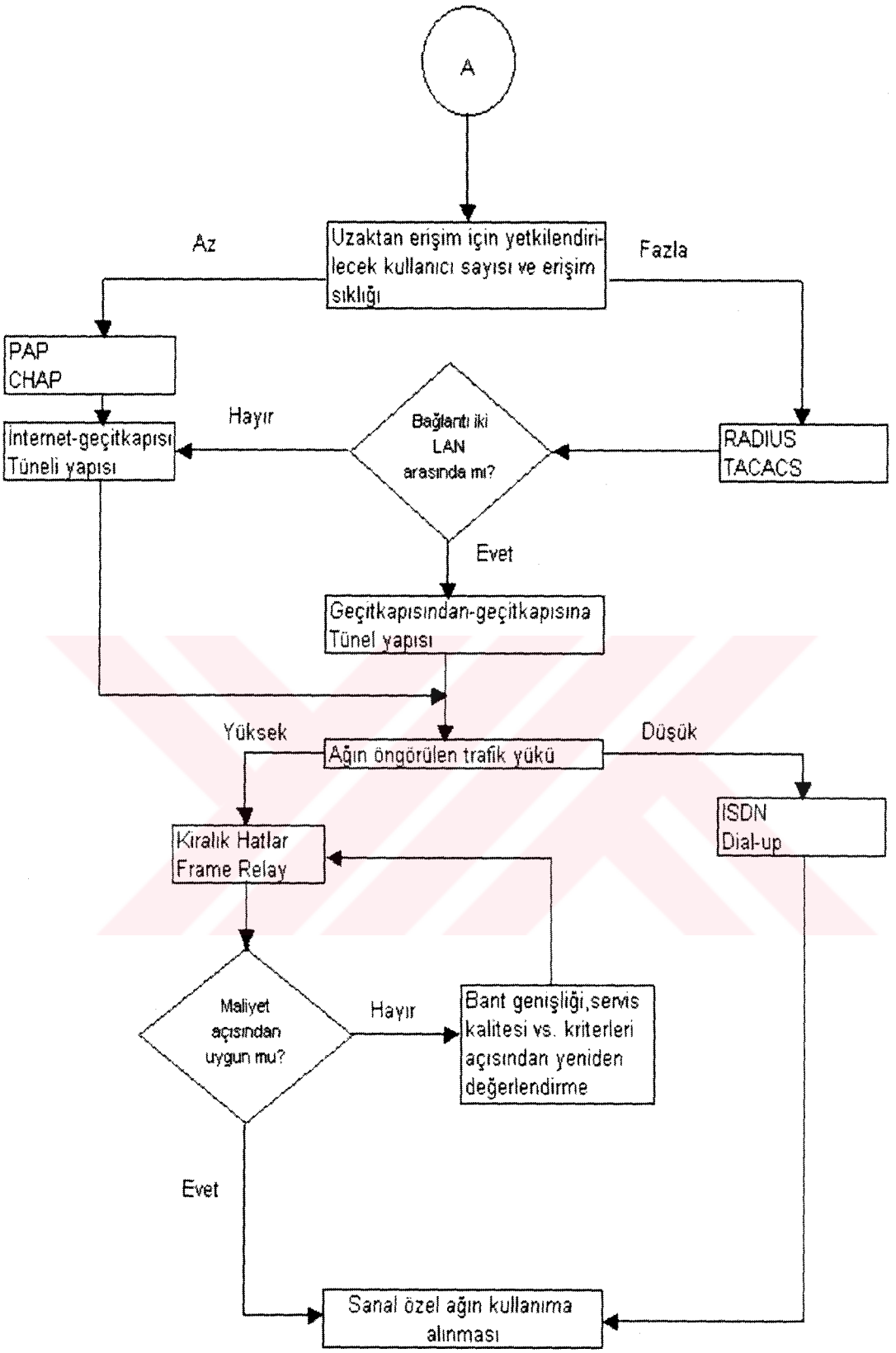
Tablo 18.2. Protokol uygunluk tablosu

		Eğitim K.	Devlet K.	Banka/Finans K.	Ticari K.
VPN Tipi	İstemci Girişimli	X	X	X	
	İSS Girişimli				X
Güvenlik Duvarları	Paket Filtrelemeli	X			X
	Vekil Sunucu	X	X	X	X
	Bastion Host				
	DMZ		X	X	
Kriptolama	DES	X			
	RSA		X	X	X
	Hash				
	Diffie-Hellman				
	Anahtar Uzunluğu	56-64(bit)	128(bit)	112(bit)	64(bit)
VPN Protokolleri	IPSec	X	X	X	X
	LDAP				
	RADIUS		X	X	
	TACACS				
	PAP				
	CHAP				
Tünelleme	PPTP	X			X
	L2TP		X	X	
	L2F				
İletim	SDLC				
	HDLC		X	X	
	LAP-B				
	PPP				
	ATM		X		
	X.25				
	Frame Relay	X	X	X	X
	ISDN				X

Şekil 18.1. ve 18.2. deki akış şeması ile bir sanal özel ağın kurulması sürecinin başlagıcından ağın kullanıma alınmasına kadar geçilmesi gereken aşamalar gösterilmiştir.



Şekil 18.1. Sanal özel ağ kurulum aşamaları



Şekil 18.2. Sanal özel ağ kurulum aşamaları

19. VPN'nin GELECEĞİ

VPN için(özellikle Internet tabanlı VPN için) her ne kadar güvenlik bir sorun ve hatta bazı eleştirmenlere göre en büyük sorun olarak görülse de, aslında VPN için şu anda en önemli olan Internet'tir. Internet üzerinde hızla artan trafik var olan mevcut alt yapıyı zorlarken, bunun üstünden elverişli ve etkin biçimde veri aktarma gerçekten önemli bir sorun oluşturmaktadır. Bu yapının aşılabilmesi için, Internet alt yapısına en basit çözüm olarak daha çok yönlendirici ve anahtar yerleştirilmesi düşünülmektedir. Bu akla gelen ilk çözüm olsa da, asla günü kurtarmadan ileriye gidemez. Bunun için daha esaslı yöntemler düşünülmektedir. Bu ileri sürülen yöntemlerden en belirgin olanı IP anahtarlama olarak göze çarpmaktadır. Başka şekilde olacak çözümler var olan karışık yapıyı daha da karıştırmaktan öteye gitmeyecektir.

VPN için bir diğer önemli husus, özellikle gelecek açısından, VPN oluşturmada kullanılacak yöntemin belirlenmesinde yaşanacak gibi gözükmektedir. VPN için geçerli ve gerekli olan adres dönüşümlerinin sağlanması hem yasal olmalı çünkü resmi güvenliğin sağlanması yasal olan IP'lerle mümkündür hem de isteği karşılamalıdır. Bunun yanında maliyet de en önemli engeldir. Maliyet, dönüşüm için gereken yazılımsal ve donanımsal yükler açısından bir zorlama oluşturmaktadır. Ancak bunun için şu anda iki geçerli görüş mevcuttur. Bunlardan ilki, yine akla gelen ilk çözüm olan, kısa vadede kar sağlayan ama uzun vadede pek de parlak gözükmeyen donanım değişikliğidir. Bir diğer görüş ise bekle ve gör düşüncesine ilişkin olan yaklaşımdır. Elbette kısa vadede kar sağlamayacak olan ama uzun vadede IP sürüm 6'nın etkin olmasını bekleyen düşünce ile bakıldığından gerçekten önemli ve diğerine göre mali açıdan iyimser olanıdır denebilir. Ancak belirtilmesi gereken en önemli nokta yeni nesil IP'nin beklentileri vadedildiği gibi karşılayıp karşılamayacağıdır. Üstüne oturduğu platform her ne kadar inanılmaz vaadlerde de bulunsa, teknolojik açıdan bakıldığında ikinci yaklaşımın yani bekle ve gör düşüncesinin hakim olması gerektiği de ortadadır.

Gelecek ile ilgili olarak, donanımsal konuda da bir takım görüşler ileri sürülmektedir. Bu konuda şu anki omurganın temelini oluşturan POP'ların yetenekleri ve elbette Internet ortamının şu anki yapısı, yeterli gözüken POP ölçeğinin mutlaka artması yönünde eğilim göstereceğini bildirmektedir. Bu açıdan yeni nesil MegaPOP olarak adlandırılan yeni bir teknoloji ileri sürülmektedir. Bu yeni teknoloji analog modemler için, ISDN için, Frame Relay için ve DSL için yüksek sığalı uzak erişimi sağlayan IP anahtarlamayı çözüm olarak bir arada sunmaktadır, ancak gerçekleme tamamlandığında ortaya çıkabilecek olası mühendislik sorunlarından henüz bahsedilmemektedir.

Pazar payı olarak bakıldığında, uzmanların, VPN'nin DSL destekli tasarımının Internet'in gelecekteki omurgasını oluşturacağı hususunda birleştiği görüşü ortaya çıkmaktadır. Hatta bu şekildeki yaklaşımın belki en uç noktası WAN kavramının ortadan kalkacağıdır. Ütopik olarak nitelenecek dahi olsa, VPN'nin aslında ne kadar etkin bir teknoloji olduğu kesinlikle dile getirilmiş olur, bir bakıma bu ütopya doğru sayılır. Biraz maliyet tabanlı düşünce ile, yeni kurulmuş büyük ölçekli kuruluşların, ilk olarak iletişimlerini (kar seviyesi istenen konumda değilken) pahalıya getirmesi anlamsızdır. Bu yüzden VPN, maliyetinin getirisi ile bir adım önde olacaktır. Bu sayıyı arttırdığımızda ise VPN'nin WAN için büyük tehlike olduğu görülebilir.

VPN için hizmet kalitesi aslında DSL destekli olan için, geleneksel özel veri ağlarından fark gözetmeksizin çalışır. Ancak tamamen VPN tercih edilmeyedebilir. Bunun da nedeni Hizmet Seviyesi İttifakı olarak bilinen kavramdaki temel eksikliğidir. Özellikle ilk olarak gerçeklemede T1 seviyesinin indirgenmiş hali bu kuruluşlar için uygun olan mimariyi desteklemektedir. Bu da madalyonun diğer yüzüdür. Hizmet niteliği bir ağda uçtan uca sağlanan başarımın belirgin bir seviyede olması anlamında kullanılmaktadır. Daha teknik biçimde ise temin edilmiş bir bant genişliği veya hesaplanan gecikmelerin ötesine geçmeyen bekleme süresi konularını tek tek ya da her ikisini birden kapsar. Internet'in şu anki durumuna bakarsak kelimenin tam anlamını yansıtmadığını görmekteyiz. Çok üreticili çözümler adına da söylenebilecek birkaç şey vardır. Bunlardan en önemlisi, zaten olayın mali açıdan değerlendirilmesinin bir sonucu olan tercih sebebidir. Elbetteki tercih, rekabet ve dolayındaki fiyat indirgenmesi sebebiyle çoklu üretici tarafına olacaktır. Ancak ilerisi için düşünülen Ipsec standardının bu çokluluk yüzünden tam oturmadığını söylemek de gerçekçi olmak adına gereken bir düşüncedir. Bu çoklu üreticiler fikri

düşünce tabanında gerçeklenebilir olsa dahi, gerçek zamanda oldukça zor, zorluğu aşılsa bile belli sorunlarla birlikte gelecektir.

VPN gerçekten düşünce olarak birçok beklentiye yanıt verecek konumdadır. Ancak bu beklentileri karşılayabilmek adına yukarıda bahsedilen hususların en başta gerçeklenmesi gerekir. Bu, VPN'yi tek başına etkin kılması için, yazılım ve donanımın doğrudan ve etkin biçimde bir arada gerçeklenmesi demektir. Örnek olması açısından, beklentileri karşılayacağına inanılan VPN için ateş duvarı desteği mevcut iken, IPsec standardının oturmuş olması vb. gibi bir çok maddenin arka arkaya sıralanması ile mümkündür. Bunun göz önünde bulundurulması şarttır. Bu şekilde düşünüldüğünde, beklentilerin karşılanması (ya da tersi durum) hali için düzeneği oluşturduktan sonra çok iyi bir çözümleme yapılmalıdır. Bunun daha da açık ifadesi, VPN aslında biraz da deneyim işidir. Bir sonraki adımdan emin olmak için, bir önceki adımda yapılmış olası hataları düzeltmek gerekir. Infonetics Research tarfından yapılan bir araştırmaya göre VPN ürünlerinin ve servislerinin dünyadaki pazarı 2003'te 32 milyar dolara yükselmesi beklenmektedir. Araştırmaya göre müşterilerin VPN'lere karşı ilgisinin arttığı da ortaya çıkmıştır. Bu araştırmaya katılan şirketlerin %85'i uzaktan erişim VPN, %78'i site-to-site VPN kurmayı düşünmektedir, %58'lik bir kesim ise bu yıl içinde ekstranet VPN planlamaktadır.

20. DEĞERLENDİRME ve SONUÇ

Özel sanal ağ teknolojisi, dünyanın neresinde bulunulduğundan bağımsız olarak Internet üzerinden, kurumların yerel ağlarına oldukça ekonomik bir şekilde bağlantı kurabilmesini sağlar. Herkesin ulaşabildiği Internet gibi paylaşılmış bir ağda yaşanacak problemler güvenlik çözümleridir. Güvenlik sorunları Internet üzerinden şifreleme teknikleri kullanılarak güvenli yollar oluşturularak çözülebilir. Bu konuda ağ donanım üreticileri her geçen gün daha gelişmiş ürünlelerini piyasaya sürmektedirler. Aşağıda VPN kavramı ile birlikte düşünülmesi gereken bazı temel değerlendirme kriterleri açıklanmaya çalışılmıştır;

Performans:Ağ performansını etkileyen en önemli etkenler paket kaybı ve ortaya çıkabilecek gecikmelerdir. Sadece düz yazı tabanlı ve grafiklerin iletildiği bir çözümde, paket kaybı ve gecikme çok fazla sorun çıkarmayacaktır ve kullanıcının işlemi yerine getirmek için bekleme süresini arttıracaktır. Fakat çoklu ortam ve video konferans gibi zaman kritik uygulamalarda, verinin gecikmeye uğramadan iletilmesi gerekir. Günümüzde Internet servis sağlayıcılar, 10 abone için sadece 1 adet modem donanımı yatırımı yapmaktadır. Kurumsal uzak erişim çözümlerinde bu oranın 5-1 hatta her bir kullanıcı için bir modem atanması gerekebilir.Internet servis sağlayıcı bağımsız modelde, tünel sonlandırıcı donanımların, şifreleme ve sıkıştırma işlemleri için ayrı işlemciler. Bu tür çözümlerde ana işlemci tünelleme ve yönlendirme işlemlerini yerine getirirken, veri şıkıştırma ve şifreleme işlemleri performansın düşmesine yol açmaz. Internet servis sağlayıcılar üzerinden yapılan VPN bağlantılarında ise İSS'nin yaptığı altyapı yatırımlarının yeterliliğine bağlı olarak performans konusunda sıkıntılar yaşanabilir.

Güvenlik: Güvenlik sistemlerinde sağlanan gelişmeler neticesinde günümüzde VPN ler için güvenliğin büyük ölçüde sorun olmaktan çıktığını söylemek mümkündür. Güvenlik politikaları, tutulan kayıtlar ve izinsiz erişim istekleri durumlarında gönderilen uyarı mesajları sayesinde, istemciler izinsiz erişimlerden ve potansiyel saldırılardan korunurlar. Belirli kullanıcı gruplarına, ihtiyaca yönelik, kapsamlı ve

ölçeklenebilir bağlantı kurallarının tanımlanabilmesi mevcut güvenlik düzeyini daha üst seviyelere çıkaran bir uygulamadır ayrıca güvenlik konfigürasyonu doğrulama sistemleri ile istemci tarafında sistemin güvenli bir şekilde oluşturulup oluşturulmadığı kontrol edilebilir.

Ağ Yönetimi ve Erişim Kontrol:Ağ yönetim yazılımları, bilgi işlem yöneticilerine tek bir merkezden, ağları üzerinde bulunan farklı donanımlarını gözlemlemelerini ve gerektiğinde bunların konfigürasyonlarını, kullanıcıların isteğine uygun olarak değiştirebilmelerini sağlar. Internet servis sağlayıcı bağımlı modelde, bilgi işlem yöneticileri VPN donanımlarını yönetme şansına sahip değillerdir ve konfigürasyon değişikliği gerektiğinde hizmet aldıkları servis sağlayıcıya başvurmaları gerekir. Servis sağlayıcı bağımsız modelde ise bilgi işlem yöneticisi, farklı ağ yönetim araçları ve uygulamaları kullanarak, konfigürasyonlarına anında müdahale etme şansı vardır.

Maliyet:VPN çözümleri, şehirlerarası ve milletlerarası telefon bağlantılarına son verdireceğinden, VPN'ye yapılacak olan yatırımın geri dönüş süresi kısa olacaktır. Toplam sahip olma maliyeti düşecektir. Bunun yanında ücretlendirme konusunda hizmet alınan İSS'nin sahip olduğu donanımlar ve bunların bakım maliyetlerine göre farklılıklar olabilmektedir buna karşılık diğer WAN bağlantı yöntemlerine göre bağlantı ücretleri açısından önemli maliyet kazançları getirmektedir.

Esneklik ve optimizasyon:Kullanıcıların taşınabilir veya ev PC'leri ile kurumsal yerel ağ arasında iletişimin sağlıklı bir şekilde kurulabilmesi için, VPN yazılım ve donanımlarının birlikte çalışabilmeleri için uyarlanmaları gerekir. Bazı servis sağlayıcılar ile bağlantıda, mevcut ağ yapısı üzerinde bir değişiklik gerekmezken, bazılarında ise yönlendiricilerinde yazılım güncellemeleri veya tamemen yeni WAN arabirimine geçiş yapılmasını gerektirir. Ağ yönetimi ve gözlemlemesi için özel yazılımlar kurulabilir. Kurumların ağları, işlerinin değişmesi yeni yatırımlar, farklı sektörlere atılmaları gibi nedenlerle, ihtiyaçları cevap verebilmek amacıyla zamanla değişir. İş gereksinimleri değişikliğe uğradıkça mevcut uzak erişim çözümleri buna ayak uydurabilmelidir. Servis sağlayıcılar çözümden çok ürün önerebilir ve bu ürünlerin kurumun gelişimine ayak uydurabilmeleri ve esnek olmalarına dikkat edilmelidir.

Ölçeklenebilirlik ve terfiler :Servis sağlayıcılar, kullanıcılarına sorunsuz ve ölçeklenebilir hizmet verebilmeliler. Hizmet alınacak servis sağlayıcı seçilirken sahip olduğu altyapı itibariyle kurumun isteklerine cevap verip veremeyeceği önemli bir karar kriteri olmalıdır.

1960'lı yıllara kadar uzanan tarihçesi içerisinde ERP kavramı tek tek işletmelerde malzeme ihtiyacının planlanması işi için kullanılmaya başlanıp ilerleyen yıllar içerisinde başta artan müşteri taleplerinin yarattığı rekabet ortamının gereği ve bunun bir anlamda sonucu olan öncelikle bilgisayar teknolojisi olmak üzere gelişen teknoloji sayesinde bugün ERP II yada genişletilmiş ERP adlarıyla bilinen ve tedarikçiden müşteriye kadar olan tüm sürecin son derece etkin, hızlı ve kolay bir şekilde yönetilebilmesini sağlayan bir yapıya kavuşmuştur. E-ticaret, CRM, SCM, BI Internet üzerinden tedarik, APS gibi kavramlar geleneksel ERP kavramının dışında kalan ve bugün ulaşılan teknolojik düzeyin sağladığı imkanlarla ortaya çıkmış kavramlardır. Tüm dünyanın tek bir pazar haline gelmeye başladığı günümüzde şirketlerin faliyetlerini tek bir şehir, bölge yada ülke ile sınırlamaları bu şirketlerin gelecekte faaliyetlerini sürdürebilmeleri açısından önemli bir dezavantaj oluşturabilmektedir, son yıllardaki eğilimler (şirket evlilikleri ve birleşmeleri gibi) şirketlerin bu gerçeğin farkında olup buna göre yatırım stratejilerini belirlediklerinin bir göstergesidir. Bu kaçınılmaz gelişmeler şirketlere daha geniş pazarlara ulaşma imkanları sağlamasının yanında coğrafi olarak geniş alanlara yayılmış olmanın beraberinde getirdiği zorluklar da bulunmaktadır şöyle ki; farklı ülkelerde hatta farklı kıtalarda faaliyet gösteren şirketlere ait fabrika, depo, satış noktaları vs. gibi birimlerin birbirleriyle sürekli irtibat halinde bulunmaları müşteri taleplerine doğru ve zamanında cevap verebilmeleri, malzeme tedariğinin zamanında ve doğru şekilde yapılabilmesi yeni üretim planlarının doğru bir şekilde yapılabilmesi açısından bir zorunluluktur, bu noktada coğrafi olarak çok uzak noktalarda bulunan uçların birbiriyle iletişiminin nasıl sağlanacağı sorunu ortaya çıkmaktadır. Günümüz teknolojisinin nimetlerinin belki de en faydalısı olan Internet bu soruna bulunanabilecek en uygun çözüm olarak görünmektedir. Internet'in çok uzaklara erişim olanağı tanıması ve kesintisiz doğası, onun hızla bir uygulama platformu haline gelmesine yol açmıştır. Birden fazla yerleşkeye dağılmış çalışanlar, kolay bir şekilde Internet üzerinde çalışan uygulamaları kullanabilirler. Bu tür uygulamalar aynı zamanda mobil çalışanlara da yarar sağlar. Çünkü, dizüstü bilgisayarlarına

hantal büyük yazılımları yüklemelerine gerek kalmaz. Artık, cep telefonu ve avuçiçi bilgisayar gibi küçük mobil ve telsiz aygıtlardan çalıştırılabilecek uygulamalar geliştirmek mümkün olmaktadır. Internet'in herkese açık bir ortam olması bu altyapı üzerinde ticari faaliyetlerini sürdüren işletmeler için çekince yaratabilecek bir hususdur, sanal özel ağ teknolojisi daha önceki bölümlerde ayrıntılı olarak anlatılan kriptolama, ateş duvarı vs. gibi tekniklerle güvenliği bir sorun olmaktan çıkarmıştır bunun yanında en önemli karar kriterlerinden olan maliyet konusunda ise kendisine alternatif seçeneklere büyük üstünlük sağladığı yine önceki bölümlerde anlatılmıştı. Tüm bu hususlar göz önünde bulundurulduğunda her sistemin kendi çevresel koşulları içerisinde değerlendirilmesi gerektiği gerçeğini her zaman akılda tutarak ERP sistemleri için sanal özel ağ teknolojisinin iletişim için kulanılabilecek en uygun yöntemlerden biri olduğu söylenebilir.

KAYNAKLAR

Kobu, B., 1996. ÜRETİM YÖNETİMİ, Avcıol Basım Yayın

Tanyaş, M.,1995. Üretim ve Dağıtım Kaynaklarının Planlanması , Otomasyon Dergisi Mayıs 1995

Tanyaş, M., 1999. Üretim Kaynakları Planlaması Ders Notları , İ.T.Ü.

Akgeyik, T.,1998. Stratejik ÜretimYönetimi, Sistem Yayıncılık

Durmuşoğlu, B., 1998. Tam Zamanlı Üretim sistemleri Ders Notları, İ.T.Ü.

Loos, P., 2002. Advanced Information Technology Application in ERP Systems, Chemnitz University of Technology, Germany

Esteves, J. And Pastor, J., 2001. ERP Systems Research :An Annotated Bibliography, Departament de Lienguatges Sistemes Informatics Universitat Politecnica de Catalunya

Fui Hoon Nah, F and Lee Shang Lau, J. and Kuang, J., 2001. Critical factors for successful implementation of enterprise systems, University of Nebraska-Lincoln, Lincoln, Nebraska, USA and University of Nebraska-Lincoln, Lincoln, Nebraska, USA

Guichard, J. and Pepellnjak, I., 2000. MPLS and VPN Architectures, Ciscopress

Norris, M. and Pretty, S., 2000. Designing the Total Area Network: Intranets, VPNs and Enterprise Networks, John Wiley & Sons

Quiggle, A., 2001. Implementıng Cisco VPNs, McGraw-Hill Osborne Media

Carlton, D., 2001. IPSec:Securing VPNs, McGraw-Hill

Faulkner Information Services, 2001. Developing Site to Site VPNs, Faulkner Information Services

Scott, C., Wolfe, P., and Erwin, M.,1998.Virtual Private Networks, O'Reilly

Çölkesen, R.,1997. Bilgisayar Ağlarına Bir Bakış, Endüstri Otomasyon Dergisi

Manas, O.,2000.Sanal Özel Bilgisayar Ağları

Manas, O., 2001. Çok Protokollu Etiketleme

Güncan, M., Sönmez, C.,1999.Kimlik Tabanlı Kripto Sistemler ile Güvenli Veri Aktarımı

Maurer U., Yacobi Y., 1996, A Non-Interactive Public-Key Distribution System, Designs, Codes and Cryptography

Stallings, W.,2002, Cryptography and Network Security: Principles and Practice, Prentice Hall

Cheswick, W., Bellovin, S., and Rubin, A., 2002, Firewalls and Internet Security, Addison Wesley Professional

Pohlmann, N., and Crothers, T., 2003, Firewall Architecture for the Enterprise, John Wiley & Sons

Luoyonen, A.,1997,Web Proxy Servers, Prentice Hall

Black, D.,1999,PPP and L2TP:Remote Access Communications,Prentice Hall

http://www.oracle.com

http://www.sap.com

http://www.cisco.com

http://www.nortel.com

ÖZGEÇMİŞ

Mete Çavdar 1978 yılından Bursa'da doğdu. 1992 yılında girdiği Bursa Ali Osman Sönmez Fen Lisesinden 1995 yılında iyi dereceyle mezun oldu.

Lisans eğitimini 1995 yılında girdiği İstanbul Teknik Üniversitesi İşletme Fakültesi Endüstri Mühendisliği Bölümünde 2000 yılında tamamlayarak Endüstri Mühendisi ünvanı aldı.

Aynı yıl İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Endüstri Mühendisliği Ana Bilim Dalı Mühendislik Yönetimi Programında başladığı lisans üstü eğitimine halen devam etmektedir.

İngilizce bilmektedir.