8 GÜVENLİK DUVARI(Firewall)

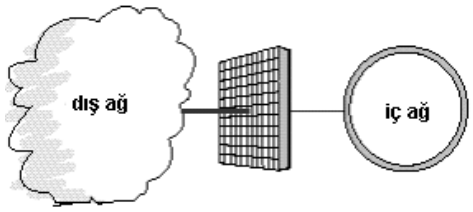
8.1 Giriş

İşletmelerin intranet ve extranet uygulamaları dolayısıyla dış dünyayla olan bağlantıları artmıştır. Böyle sistem yapılarının saldırılardan korunması daha zordur.

Terim olarak güvenlik duvarı (firewall) özel bir donanım ya da yazılım parçası değildir. Sadece iç ağı dışarıdan gelebilecek saldırılardan, davetsiz misafirlerden koruyabilmek için kullanılan donanım ve/veya yazılım çözümüdür.

Güvenlik duvarı (firewall), bir korumalı ağa giren ve çıkan haberleşme trafiğine, belirli (tanımlanmış) bir güvenlik politikası (security policy) uygulayan, donanım ve yazılım mekanizmalarından oluşan bir teknolojidir. Güvenlik politikası belli bir ağı korumak için geliştirilen bir plandır. Bir güvenlik duvarı, Şekil 8.1'de görüldüğü gibi, donanım, yazılım veya her ikisi ile beraber bir ağı korur ve izole eder.

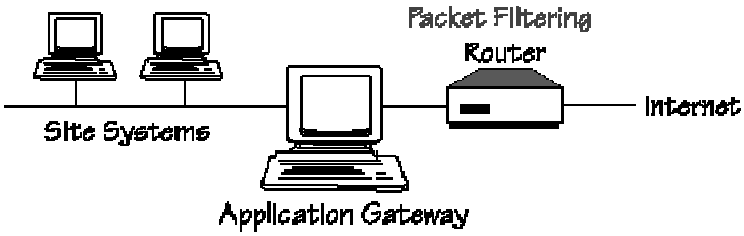
Bu araçların öncelikli görevi güvenilir ağ (iç ağ) ile güvenilmez ağ (internet) arasında bir güvenlik duvarı oluşturmaktır. Bir güvenlik duvarı bir iç ağı (*private,* örneğin bir intranet) bir dış ağdan (güvenilmeyen, örneğin internet) korur ve izole eder.



Şekil 8.1 Güvenlik duvarı

Güvenlik duvarları, günümüzde yaygın olarak TCP/IP tabanlı ağlarda (Internet ve özel Intranet ağlarında) kullanılmakla birlikte, temel kavramları diğer ağlar için de uygulanabilir. Bu teknoloji halen gelişen bir teknoloji olarak tanımlanmasına karşın, bir güvenlik politikası sağlayarak bir ağı güvenli kılan günümüzde mevcut en iyi yollardan biridir.

MS Windows NT ve Unix ortamları için en güvenli korunma uygulama geçidi (Application gateway) ve adaptif vekil (Adaptive Proxy) sayesinde geliştirilen durumsal paket filtrelenmesi yöntemidir. adaptif vekil (Adaptive Proxy) teknolojisi güvenlik duvarı teknolojilerinde önemli dönemeçlerden birisini temsil etmektedir. Çünkü kullanıcılara hem durumsal paket filtreleme denetimini hem de uygulama geçit güvenlik duvarı (Application gateway firewall) teknolojisini bir arada sunmaktadır. (Şekil 8.2.)
Daha önce bahsedilen güvenlik problemlerini bilinen ve mevcut olan teknikler ile artırabiliriz. Bunlardan biride güvenlik duvarlarıdır. Güvenlik duvarları önemli internet servislerine aynı zaman da izin vererek güvenliği artırabilir.



Şekil 8.2 Uygulama Geçitli Güvenlik Duvarı

8.2 Güvelik Duvarı Nedir?

Bir güvenlik duvarını'ı en iyi açıklayan ne olmadığıdır. Bir güvenlik duvarı ne bir yönlendirici ne bir host sistemi veya ne de ağ'ın güvenliğini sağlayan sistemlerin toplamıdır. Güvenlik duvarı bir güvenlik yaklaşımıdır. İzin verilecek servis ve erişimleri tanımlayan büyük bir güvenlik politikasının ve ağ, host sistemleri, yönlendiriciler ve diğer güvenlik tekniklerinin uygulandığı güvenlik ölçüm ayarlarındaki politikanın oluşturulmasına yardım eder.

Bir Güvenlik duvarı sisteminin esas amacı erişimleri kontrol etmek veya korumaktır. Güvenlik duvarı bağlantıların değerlendirilip ve gerekli değişikliğin yapıldığı bir host üzerinden geçmeğe zorlayarak ağ erişim politikasını oluşturur.

Güvenlik duvarı sistemi bir yönlendirici, bir kişisel bilgisayar, bir host veya hostların bir kümesi olabilir. Genellikle bir sitenin dış ağ'a olan bağlantıları için yüksek düzey gateway sağlar. Ayrıca küçük alt ağ bağlantıları arasında da düşük düzey gateway olarak kullanılabilir.

8.3 Niçin Güvenlik Duvarı

Güvenlik duvarı kullanılmasının arkasındaki sebep güvenli olmayan servisleri , ağ dışından gelen atakları engellemektir. Güvenlik duvarı olmayan bir ağ'da güvenlik, sadece hostun güvenliğine bağlıdır. Büyük bir alt ağ'da aynı düzeyde güvenliğe sahip hostların güvenliğini devam ettirebilmek çok zordur. Güvenlikte genelde bir çok hata yapılır ve ayarlardaki hata ve şifrelerin basitliğinden karmaşık ataklara gerek duyulmaz.Güvenlik duvarı yaklaşımı bütün host güvenliğini artıran bir çok avantajlar sağlar.

8.3.1 Zayıf servislerden koruma

Güvenlik duvarı güvenilir olmayan servisleri filtreleyerek ağ güvenliğini büyük oranda artırır ve riskleri azaltır. Sonuç olarak alt ağ daha az risk alır , çünkü sadece seçilen protokoller Güvenlik duvarı üzerinden geçer.

Güvenlik duvarı'lar ayrıca yönlendirme tabanlı ataklardan koruyabilir. Örneğin kaynak yönlendirme ve ICMP yönlendirmelerini kullanarak yönlendirme yolunu tekrar yönlendirmek gibi. Güvenlik duvarı bütün kaynak yönlendirme ve ICMP geri yönlendirmelerini engelleyebilir ve sistem yöneticilerine bilgi verebilirler.

8.3.2 Sisteme kontrollü girişler

Güvenlik duvarları ayrıca siteye erişim kontrolünü de sağlayabilir. Örneğin bazı hostlara dış ağ'dan erişim sağlanabilir, diğer hostlara ise istenmeyen erişimler yasaklanır. Bunlar e-posta sunumcular, bilgi sunumcuları gibi hostlar dışındaki dışarıdan gelen erişimleri önlemek gibi. Bu güçlendirilmiş ön erişim politikasını belirler.

8.3.3 Yoğunlaştırılmış güvenlik

Bütün veya bir çoğu değiştirilmiş yazılımlar ve ek güvenlik yazılımları bir çok konağa dağıtmak yerine sadece Güvenlik duvarı sisteminde kullanılabilir. Böylece Güvenlik duvarı kurum için daha

az maliyetli olabilir. Ek olarak one-time password sistemleri ve diğer doğrulama yazılımları da internete erişmek isteyen her sistem için koymak yerine Güvenlik duvarı içinde olabilir.

Ağ güvenliği için Kerberos gibi diğer bir çözüm her host için değişiklik gerektirir. Kerberos ve diğer tekniklerin avantajları düşünülürken bazı durumlarda Güvenlik duvarlarından daha iyi olabilir.

8.3.4 Mahremiyeti Artırmak

Bazı siteler içerdikleri hayati bilgiler nedeniyle saldırganlar tarafından sık sık rahatsız edilirler. Güvenlik duvarı kullanan bazı siteler finger, DNS gibi servisleri engellerler. Finger son giren kullanıcı, mailini okuyup okumadığı gibi ve diğer bilgileri gösterir. Bu saldırgan'a sistemin hangi sıklıkta kullanıldığı, aktif olan kullanıcılar gibi değerli bilgiler verir. DNS ise sistemdeki hostların isimleri ve IP'leri hakkında bilgiler verir.

8.3.5 Ağ Kullanımındaki Girişler ve İstatistikler

Bütün girişler ve çıkışlar bir Güvenlik duvarı üzerinden olursa, Güvenlik duvarları erişim bilgilerini tutabilirler ve ağ kullanımı hakkında değerli bilgiler sağlar. Şüpheli olan bir aktiviteyi Güvenlik duvarı'nın ve ağ'ın izlenip izlenmediği gibi detaylı bilgileri içeren alarm verebilir.

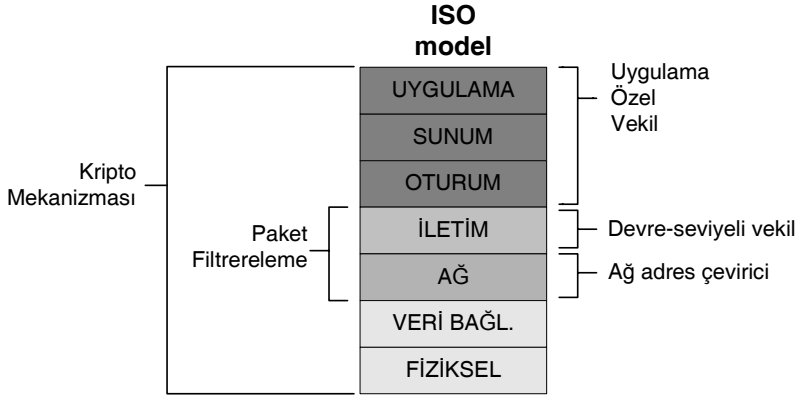
Ağ kullanım istatistiğini tutmak ve çeşitli araştırma ve saldırıların delillerini toplamak çok önemlidir. Çünkü en önemlisi, saldırılara karşı Güvenlik Duvarı'nın karşı koyup koymadığını ve Güvenlik duvarı kontrollerinin uygun olup olmadığını bilmektir.

8.3.6 Politikayı Güçlendirmek

Son olarak en önemlisi Güvenlik duvarı bir ağ erişim politikasının oluşturulması ve güçlendirilmesini sağlar. Etkili olarak kullanıcılara ve servislere erişim kontrolü sağlar. Böylece güvenliğin sadece kullanıcılara bağlı olmak yerine Güvenlik duvarı tarafından güçlendirilmiş bir ağ erişim politikası belirlenmiş olur.

8.4 Koruma Mekanizmaları

Bir güvenlik duvarının kullanacağı güvenlik mekanizmaları, Şekil 8.3'de görülen, OSI ağ modelinde kullanılacak katmanlara göre değişir. Örneğin, paket-filtreleme (packet-filtering) ve ulaştırma (transport) katmanlarında çalışmasına karşın, ağ adres çevirimi (network address translation) şebeke (network) katmanında çalışır. Uygulamaya bağlı çalışan vekil (proxy) koruyucular ise en üst üç katmanda çalışır. Şifreleme mekanizmaları yedi katmanda da uygulanabilir.



Şekil 8.3 OSI Güvenlik Duvarı Çözümleri

8.4.1 Güvenlik Duvarı Karakteristikleri

Bir güvenlik duvarı tasarımında aşağıdaki amaçlar hedeflenir.

- İçeriden dışarı veya dışarıdan içeriye bütün trafik güvenlik duvarı üzerinden geçmelidir. Bu yerel ağdaki bütün dış bağlantıların güvenlik duvarı üzerinden olmayanların kapatılmasıyla sağlanır. Bunun için değişik konfigürasyonlar olabilir.
- Yerel güvenlik politikasıyla belirlenen sadece yetkilendirilmiş trafiğin geçişine izin verilecektir. Farklı güvenlik politikası tanımlanan değişik güvenlik duvarı tipleri kullanılabilir.
- Güvenlik duvarının kendisi sızmaya karşı korunmalıdır. Bu emniyetli bir işletim sistemiyle birlikte güvenilir bir sistem ile sağlanır.

Güvenlik duvarları sitenin güvenlik politikasının uygulanması ve erişim denetimi amacıyla dört genel teknik kullanır. Bunlar

- **Servis Kontrol** : Dışarıya giden ve içeri giren İnternet servislerinin hangilerine erişileceğini belirler.Güvenlik duvarı ya basitçe IP ve port numarasına göre trafiği filtreler veya vekil sunumcu olarak servis isteklerin alır bunları yorumlar ve karşılar, veya kendisi web /mail sunumcu olarak isteği karşılar.
- **Yön denetimi:** Güvenlik duvarında hangi servis isteğinin hangi yönde olacağını belirler.
- **Kullanıcı Denetimi:** Kullanıcının servis erişimlerini denetler. Bu özellik yerel kullanıcılar(Güvenlik duvarının altındaki) için uygulanır. Aynı zamanda dış kullanıcılardan içeri giren trafiğe de uygulanabilir. IPSec gibi güvenli yetkilendirme tekniği de uygulanabilir.
- **Davranış Denetimi:** Kısmı servislerin nasıl kullanılacağını denetler. Örneğin güvenlik duvarı Spam'ı önlemek için e-postaları filtreler veya dış erişimlerin yerel Web sunumcunun sadece bir kısmına yapılmasını denetler.

8.4.2 Güvenlik Duvarından beklentiler.

Güvenlik duvarının uygulanmasında sağlanacak ve sağlanmayacak fonksiyonlar aşağıda belirtilmiştir.

Sağlanacak yararlar.

1. Güvenlik duvarı, yetkisiz kullanıcıların korunan ağın dışına çıkmasını önleyen, potansiyel güvenlik zayıflıkları olan servislerin ağ'a girmesini ve çıkmasını önleyen, ve değişik IP aldatması veya yönlendirme saldırılarını kısıtlayan tek bir tıkama noktası oluşturur. Tek bir tıkama noktasının kullanılması güvenlik yönetimini kolaylaştırır.
2. Bir Güvenlik duvarı, güvenlikle ilgili olayların görüntülenmesi için bir yer oluşturur. Denetim ve alarmlar güvenlik duvarı üzerinde ayarlanabilir.
3. Bir güvenlik duvarı güvenlik ile alakalı olmayan Internet fonksiyonları için uygun bir platformdur. Bunlar Ağ adres dönüşümü ve İnternet kullanımındaki denetim ve loglar dan sağlanan yönetimdir.
4. Bir güvenlik duvarı IPSec için bir platform görevi yapabilir.Tünel modunda çalışma kapasitesi nedeniyle, Sanal Özel Ağ gerçeklenmesi kullanılabilir.

Güvenlik duvarının sınırlamaları aşağıda belirtilmiştir.

1. Güvenlik duvarı kendisine uğramadan geçen saldırılara karşı koruma yapamaz. İç sistem bir ISP'ye bağlantı için çevirmeli hat kullanabilir veya modem havuzu bulunabilir. Bu tür bağlantılar güvenlik duvarını devre dışı bırakabilir.
2. Güvenlik duvarı dış saldırgan ile işbirliği yapan iç tehditlere karşı koruma sağlayamaz..
3. Güvenlik duvarı virüs bulaşmış olan dosya ve programların iletilmesine karşı koruma sağlayamaz. Değişik işletim sistemi ve desteklenen yazılım çeşitliliği nedeniyle bütün dosyaların virüs testine tabi tutulması pratik değil hatta imkansızdır.

8.5 Erişim Denetim Politikasının Belirlenmesi

Basit olarak bir organizasyonun erişim denetim politikası, ağ elemanları üzerinden ne tür erişimlere izin verileceğinin belirlenmesidir. Örneğin iç kullanıcılar Internet üzerinde http, ftp ve SMTP protokollerini kullanabilecekler, fakat Internet üzerinden sadece SMTP'ne izin verilmesi bir erişim politikasıdır. Bu politikaya göre erişim kontrol listeleri ayarlanır. Erişim kontrol politikasının belirlenmesinde ortak tanımlar gereklidir. Bunlar Tablo 8.1'de verilmiştir.

Tanım	Açıklama
Yön(Direction)	Kabul edilecek olan trafiğin akış yönüdür
Servis(Service)	Kullanılacak olan sunumcu uygulamaları(http,Smtp, vs)
Belirli Host(Spesific Host)	Erişimi belirlenmiş bir Host
Kişisel Kullanıcılar	Erişim hakkı belirlenmiş olan özel kullanıcılar
Günün Saati	Erişim için belirlenen zaman aralığı
Halka açık veya kapalı ağ	Verinin gideceği ağ türüne göre şifreli gönderilmesi gereken ağ
Servis Kalitesi(QoS)	Erişim için gerekli olan minimum bant genişliği

Tablo 8.1.Erişim politikası tanım bileşenleri

8.5.1 Güvenlik duvarı Tipleri

Güvenlik duvarı standart bazı araçlardan oluşur. Bu araçlar mimariye göre farklı yerlere konabilir. Bunlar;

1. Onaylama Sunucusu (authentication server)
2. Denetlemeli Yönlendirici (screening router)
3. Korumalı konak (bastion host)
4. Vekil sunucular (Application proxy servers)

Bir çok ticari üründe sunulan çözümlerde yukarıdaki araçların bir kısmı ya da karışımı tek bir ürün olarak sunulmaktadır

Koruma için kullanılan ürünlerde aşağıdaki teknolojiler kullanılmaktadır.

1. Paket Filtreleme(Statik ve Dinamik Paket filtreleyici Güvenlik Duvarları)
2. Uygulama-Seviyesi Ağ Geçitleri
3. Devre-Seviyesi Ağ Geçidi

Her güvenlik duvarı teknolojisinin kendisine göre avantaj ve dezavantajları vardır. Bunlar aşağıda özetlenmiştir.

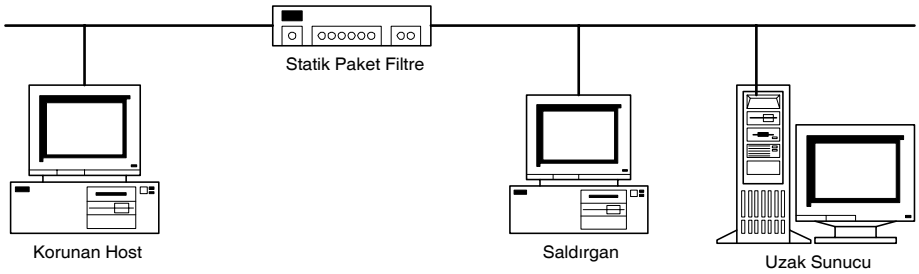
8.5.1.1 Paket Filtreleme

Statik ve Dinamik Paket filtreleyiciler olarak iki kısımda incelenebilirler.

Statik Paket filtreleme: Ağ trafiğini paket başlıklarındaki(Header) bilgiye göre denetler. Alınan paketin başlığındaki bilgiler önceden tanımlanmış olan erişim kontrol listesi(ACL) ile karşılaştırılarak trafik iletilir veya iletilmez. Statik filtre, trafik akışını denetlerken aşağıdaki bilgileri kullanır.

- Varış Adresi veya Alt-Ağ
- Kaynak Adresi veya Alt Ağ
- Varış Servis Portu
- Kaynak Servis Portu
- Bayrak(Sadece TCP de)

Blok Şeması Şekil 8.4'de gösterilen bu teknikte Güvenlik duvarı akıllı değildir. Gelişmiş saldırılara karşı zayıf bir koruma sağlar. Ağ trafiğini denetlemek için çok az bir bilgi kullanır. Çoğu yönlendirici bu türde filtreleme yapar.

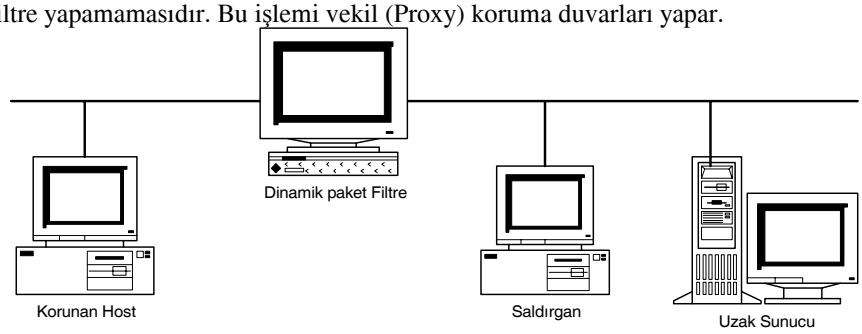


Şekli 8.4 Statik Paket Filtreleyen Güvenlik Duvarı

Dinamik paket Filtreleyici:
Dinamik paket filtreleyici, bağlantıların durum tablosunu tutarak statik filtreyi akıllı hale getirir. Bütün bağlantıları durum tablosu denilen bir tablo ile denetler. Bu özelliği ile ağa sızmaya yönelik gelişmiş saldırıları önler. Herhangi bir vekil sunucu ya da uygulama ağ geçidi güvenlik duvarlarına göre daha kapsamlı ve gelişmiş filtreleme özelliklerine sahiptir. Erişim kontrol listeleri(ACL) çok daha gelişmiştir. Örneğin aşağıdaki şekilde erişim kontrol listesi tanımlanabilir.

Uzak sunumcu ile korunan host arasındaki bir servis oturumunu gerçekle
Kurulmuş olan bir oturumun geçişine izin ver
Diğer trafiği engelle

Şekil 8.5'de blok diyagramı gösterilmiş olan Dinamik paket filtreleyici güvenlik duvarları, statik olanın eksikliklerinin giderilmesi ile gelişmiş yapıdadır. Trafik denetimini hem paket bilgilerine hem de durum tablolarına bakarak yaparlar. Durum tabloları , koruma duvarının bağlantı ile ilgili eski bilgileri hatırlamasını sağlar ve bu bilgilere göre denetim yapar.En büyük eksikliği veriye göre filtre yapamamasıdır. Bu işlemi vekil (Proxy) koruma duvarları yapar.



Şekil 8.5. Dinamik Paket Filtreleyici Koruma Duvarı

Paket Filtreleyici örneği
Paket filtrelemede ana rol oynayan bir yönlendirici (router) belli kuralları sağlamayan ağ trafiğine izin vermez. Örneğin, TPC/IP paket filtreleme güvenlik duvarında, yönlendirici datagram paketlerinin başlıklarındaki kaynak ve hedef adresler ile port numarasına bakar.

İki tür paket filtreleme yöntemi vardır;

1. Statik Paket Filtreleme: Eğer filtreleme işlemindeki kurallar, daha önceki veri paketlerinin durumlarından bağımsız olarak uygulanıyorsa, bu yönteme durumsuz paket filtreleme (stateless packet filtering) denir.

2. Dinamik paket filtreleme : Aynı bağlantıya ait paketlerin durum bilgileri saklanıp bir mesajın içeriğine göre filtreleme kararı veriliyorsa dinamik paket filtreleme yapılıyor demektir. Paket filtreleme, bir güvenlik duvarından geçen veri paketlerini incelemede ve kontrolde kullanılabilecek bir yöntem olmasına karşın tek başına güvenlik politikaları uygulamak için yeterli değildir.

Örnek Uygulama(Paket Filtreleme Örneği :)

C sınıfından 195.55.55.0 adresine sahip bir şirket olduğu varsayılsın. Bu şirket bir ISS (internet servis sağlayıcı) aracılığı ile Internete bağlanmıştır. Şirketin politikası herkesin giden paketlerine izin vermek fakat bütün gelen bağlantıları "mail host" a yönlendirilmesidir. Gelecek olan servisler sadece Mail ve DNS olacaktır.

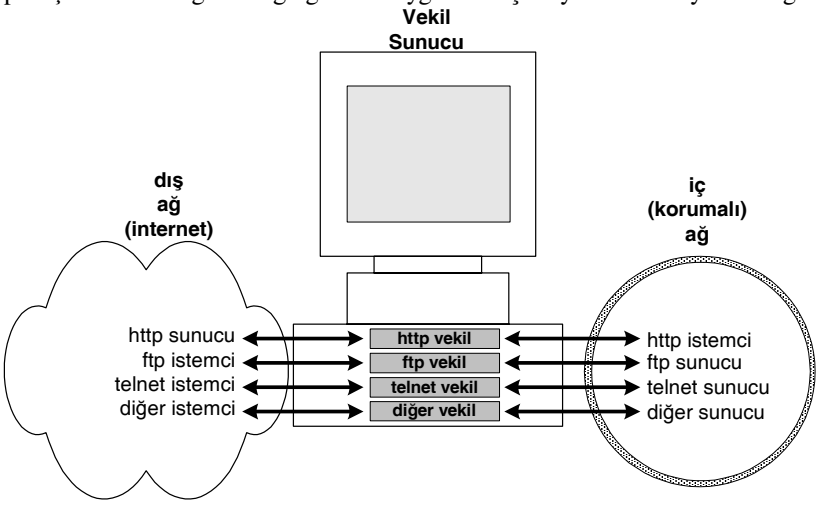
- İzin , Çıkan bütün TCP bağlantıları
- İzin, Gelen SMTP ve DNS isteklerini mailhost makinasına
- TCP portu 1024 ten büyük olan , gelecek FTP veri bağlantılarına izin ver
- Yüksek port numaraları ile çalışan servisleri korumaya çalış

Bu konfigürasyona göre sadece internet üzerinden gelen paketler kontrol edilecektir. Kurallar, uygunluk bulunduğu zaman durdurulur ya da yönlendirilir. Erişim listesinin (Access List) sonunda kesin bir kural vardır ki kabul şartlarına uymayan bütün paketler kesinlikle reddedilecektir. Aşağıdaki örnekte IP erişim listesi Cisco IOS v.10.3 ve sonrası için geçerlidir.

```
1  no ip source-route
2  !
3  interface ethernet 0
4  ip address 195.55.55.1
5  !
6  interface serial 0
7  ip access-group 101 in
8  !
9  access-list 101 deny ip 195.55.55.0 0.0.0.255
10 access-list 101 permit tcp any any established
11 !
12 access-list 101 permit tcp any host 195.55.55.10 eq smtp
13 access-list 101 permit tcp any host 195.55.55.10 eq dns
14 access-list 101 permit udp any host 192.55.55.10 eq dns
15 !
16 access-list l01 deny tcp any any range 6000 6003
17 access-list 101 deny tcp any any range 2000 2003
18 access-list 101 deny tcp any any eq 2049
19 access-list 101 deny udp any any eq 204
20 !
21 access-list 101 permit tcp any 20 any gt 1024
22 !
23
24 access-list 101 permit icmp any any
25 !
26 snmp-server community FOOBAR RO 2
27 line vty 0 4
28 access-class 2 in
29 access-list 2 permit 195.55.55.0 255.255.255.0
```

8.5.1.2 Uygulama Seviyesi Ağ Geçidi(Vekil(Proxy) Sunucu)

Uygulama Seviyesindeki Güvenlik Duvarıdır. Her uygulama için özel bir vekil (proxy) aracı programı ile ağ haberleşmesi sağlanır. Bu vekil program belirlenen güvenlik politikasına göre kontrol yapar. Şekil 8.6'da görüldüğü gibi her uygulama için ayrı bir vekil yazılımı gerekir.



Şekil 8.6 Uygulama seviyesi güvenlik duvarı.

Vekil sunucular genelde çift ara yüzlü konaklar üzerinde çalışırlar(dual-homed). Bu konaklar çift ağ ara yüzüne sahip olup sunucu bilgisayarlardır. Her ağ ara yüzü ayrı bir IP numarasına sahiptir. Bu ağ adaptörlerinden biriyle iç ağa diğeriyle de internete bağlanır. Konak üzerinde çalışan vekil sunucu yazılımı bir ağdan gelen trafiği diğer ağa geçirir ya da iptal eder.

Çift ağ ara yüzüne sahip bulunan konak üzerinde çalışan vekil sunucu basit fonksiyonlu yönlendirici gibi çalışmaktadır. Farklı olarak daha akıllı ve zengin özelliklere sahiptir:

1. Gizliliği artırma ve bant genişliğini koruma : Uygulama seviyesi vekiller verileri depolayabilir (cache) ve kendi kayıtlarından hizmet verebilirler. Bu şekilde, hızlı verilmesi gereken cevaplara karşı disk alanı oluşturulmuş ve bant genişliği korunmuş olur.
2. Gelişmiş erişim kontrolü : Uygulama seviyesi vekil yazılımları doğrulamayı (authentatication) sağlamaktadırlar. Doğrulama bilgilerini erişim izni için kullanır.
3. Gelişmiş filtreleme : Uygulama seviyesi vekil yazılımlarının çok gelişmiş filtreleme özellikleri vardır. Protokollerin içeriğini anlayabilir ve sadece TCP/IP paketlerinin başlığıyla sınırlı kalmaz.
4. Kayıt tutma ve denetim : Vekil sunucu üzerinde olan işlemlerin kaydı tutulur. Bu şekilde web trafiğinin denetimi sağlanır.

Genelde yönlendirici ve vekil sunucular daha güvenli güvenlik duvarı çözümü sağladığı için birlikte kullanılır. Ayrıca vekil sunucular çift ağ ara yüzlü bilgisayarlar üzerinde çalıştırılmak zorunda değildir. Ağ seviyesindeki trafik kontrolü yönlendirici tarafından yapılır.

Aşağıdaki şekilde vekil sunucunun yönlendirici ile güvenlik duvarı konfigürasyonu görülmektedir. Yönlendirici internetten gelen, izin verilen port dışındaki (SMTP) bağlantı isteklerini iç ağa geçirmeyecektir. Buradaki yönlendiricinin tipik fonksiyonları şunlardır;

1. İç ağdan vekil sunucu bilgisayara olacak bağlantılara izin ver.

2. İç ağdan internete direk bağlantıları reddeder. Bu kural dış ağa çıkış için vekil sunucu kullanımına zorlar. Vekil sunucular böylece dış ağa çıkmak için tek bir noktayı kullanmak zorunda kalır. Bu şekilde internet ile iç ağ arasındaki olaylar ile ilgili kayıtlar sağlıklı olarak tutulmuş olur.
3. Vekil sunucudan internete olan bağlantılarda iyi bilinen port bağlantılarına izin verir (HTTPS,HTTP gibi).
4. Internetten vekil sunucuya olan bütün bağlantı isteklerini reddeder.

Daha güvenli bir güvenlik duvarı mimarisi aşağıdaki şekilde de görülmektedir. Vekil sunucu konağı (Güvenlik duvarı bastion ya da bastion host olarak da isimlendirilir.) iki tarafı da yönlendiriciler tarafından çevrilmiştir. Bu üç katmanlı güvenlik sağlar. Bu mimaride korumalı konak (bastion host) üzerinde çalışan vekil sunucunun görevleri şunlardır;

1. Web protokollerinin (HTTP, FTP,Gopher) dışarıya çıkışına izin ver.
2. SSL(Secure Socket Layer) protokolünün bilinen portlarla bağlantısına izin verir.(HHTPS için 443, SNEWS için 563).

Saydam Vekillik

Buradaki saydamlık iki farklı anlamda kullanılır. Genel anlamda kullanıcının direk sunucuya bağlanmakla, vekil sunucu üzerinden bağlanması arasında bir fark görmemesidir. Bu anlamda bütün vekil sunucular saydamdır.

Diğer anlamda saydam vekillik son zamanlarda bildirilmiştir: İstemci yazılım da vekil sunucunun farkında değildir. Genellikle bilinen, istemci yazılımın hangi vekil sunucuyla konuştuğunu bildiğidir. İstemci yazılımın direk ya da vekil sunucu üzerinden bağlantı kuracağını fark edebileceği bilinir.

Saydam vekillik uygulamasında, yönlendirici direk olarak vekil sunucudan istek alacak şekilde programlanır. Bütün HTTP bağlantıları kesilip vekil sunucu tarafından tekrar internete yönlendirilir. Bu bağlantılar saydam vekil sunucu tarafından kontrol edilir. Vekil sunucu tarafından filtreleme ve erişim kontrol kuralları uygulanır. Diğer istekler ya reddedilip başka vekil sunuculara gönderilir ya da vekil sunucu kayıtlarından (cache) hizmet verilir.

Saydam vekillikte, istemcinin kesinlikle arada bir vekil sunucu olduğundan haberi yoktur. Fakat, HHTP/1.1 protokolü arada bu tür bir vekil sunucu sağlamaz.

8.5.1.3 Devre seviyesi Ağ Geçidi (Circuit-Level Proxy Servers)

Devre seviyesi ağ geçidi, ya tek başına bir sistem veya belirli uygulamalar için uygulama seviyesi ağ geçidi olabilir. Devre seviyesi ağ geçidi uçtan uca TCP bağlantısı sağlamaz. Bunun yerine, birisi kendisi ile iç host üzerindeki TCP kullanıcısı, diğeri ise kendisi ile dış host üzerindeki TCP kullanıcısı arasında olmak üzere iki adet TCP bağlantısı sağlar. Bir kere bağlantı sağlandıktan sonra TCP segmentlerini içeriğine bakmadan iletir. Güvenlik fonksiyonu hangi bağlantıya izin verileceğini içerir. Uygulamaların bağlantılarını sağlar; ve uygulama seviyesi protokolüne bakmaksızın iki yönlü veri aktarımına başlar. Devre seviyeli vekil sunucular kavramsal olarak yönlendiriciler ile uygulama seviyesi vekil sunucular arasında yer alır. Yönlendirici paket seviyesinin üstünde ve uygulama seviyesi vekil sunucu protokol yapısı altında olduğundan bağlantı işlevini gerçekleştirir. Devre seviyeli vekil sunucu protokolü SOCKS olarak adlandırılmıştır.

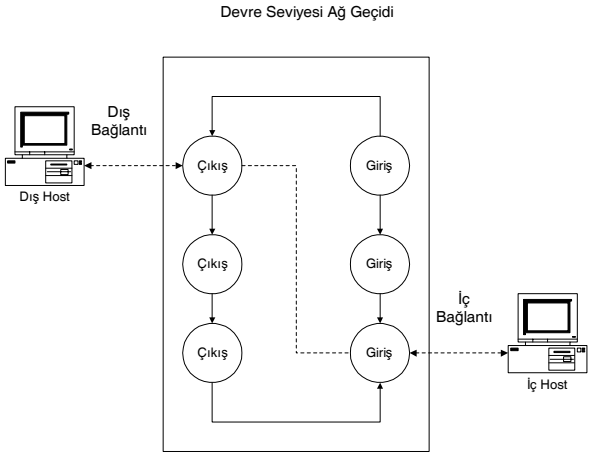
SOCKS aşağıdaki elemanları içerir.

UNIX tabanlı bir Güvenlik duvarı üzerinde çalışan SOCKS sunumcu.

Güvenlik duvarı tarafından korunan iç host üzerinde çalışan SOCKS sitemci kütüphanesi

FTP veya TELNET gibi istemci programlarının SOCKS ile bağlanmış versiyonları. SOKS protokollerinin kodlanması, TCP tabanlı istemci uygulamalarının SOCKS kütüphaneleri ile bağlantılı olarak yeniden derlenmesiyle elde edilirler.

Uygulama seviyesi Ağ geçitlerinin eksiklikleri vardır. Birkaç tanımlı protokol için sadece bir bağlantının kontrolüne imkan tanınır. Uygulama seviyesi vekil sunucu yazılımının sürümü güncellemeden, yeni ya da bilinmeyen protokoller çalışmaz. Devre seviyeli vekil sunucu bu noktada devreye girmektedir. Devre seviyeli vekil sunucular genellik oluşturabilmektedir. Böylece protokol bağlantıları bunlar üzerinden yapılabilir.



Şekil 8.7. Devre Seviyesi Ağ Geçidi Güvenlik Duvarı

Korumalı Konak(Bastion Host):
Bir Korumalı Konak Ağ güvenliğinde, kritik güçlü nokta olarak güvenlik yöneticisi tarafından belirlenen bir sistemdir. Tipik olarak bir Uygulama seviyesi veya devre seviyesi ağ geçidi olarak görev yapacak bir platformdur. Ortak özellikleri aşağıdadır.

- İşletim sistemini güvenli olarak çalıştıran böylece onu güvenilir yapan bir donanım platformudur.
- Sadece ağ yöneticisinin istediği servisler(DNS,SMTP,FTP vs.gibi vekil sunucu) kurulur.
- Kullanıcı vekil servislerine erişmek istediğinde her servis ilave yetkilendirme isteyebilir.
- Her bir vekil sadece standart uygulama komut kümesini içerecek şekilde ayarlanır.
- Her bir vekil sadece belirli konağa erişim sağlayacak şekilde konfigüre edilir.
- Her bir vekil, bütün trafik, bağlantı ve bağlantı süresince dahil olarak detaylı denetleme sağlar. Böylece saldırgan saldırıları önlenir.
- Her bir vekil modülü ağ güvenliğini sağlamak için olabildiğince küçük tasarlanmış yazılım modülüdür.
- Her bir vekil Korumalı Konaktaki diğer vekillerden bağımsızdır.Eğer bir vekil ile problem olursa diğerlerini etkilemeden kaldırılır.
- Bir vekil genellikle ilk ayarlarını okuduktan sonra disk erişimi yapmaz. Bu bir saldırganın Truva atı, koklayıcı veya diğer tehlikeli dosyaları host'un diskine yüklemesini zorlaştırır.
- Her bir vekil , Korumalı Konak üzerinde özel ve gizli bir katalog üzerinde ayrıcalıksız bir kullanıcı olarak çalışır.

8.5.2 Güvenlik Duvarı Yöntemlerinin Karşılaştırması

Yaygın olan ve yukarıda özetlen üç farklı güvenlik duvarının temel özellikleri Tablo 8.2'de özetlenmektedir.

Güvenlik Duvarı	**Avantajları**	**Dezavantajları**
Statik Paket Filtreleyici Güvenlik Duvarı	Ucuz Yüksek performans Kullanıcılara göre saydam	Sadece ağ protokollerini anlayabilirler. İçerideki ağ yapısını dışarıdan gizleyemezler. Daha yüksek katmanlardaki uygulamalara yönelik atakları engelleyemezler. Denetim kabiliyeti sınırlıdır. Kimlik onaylama, zamana ve saate göre kontrol, kayıt gibi özelliklere sahip değildir.
Dinamik Paket Filtreleyici Güvenlik Duvarı	Bütün OSI modeli kapsanır. Gelişmiş ataklar engellenir. Çok yüksek performans sağlanır. Kullanıcılara göre saydamdır. Bağlantısız protokollerin takibi için sanal oturum bilgisi oluşturulur.	Uygulama seviyesinde denetleme yapmak için veri akışı uygulama katmanına yükseltilmelidir. Gelişmiş kullanıcı kaydı yapmak zordur. İçerik güvenliği ve karmaşık uygulama filtrelemesini yapmak zordur.
Vekil Sunucu Güvenlik Duvarı	Uygulama katmanındaki protokolleri anlayabilirler. En sağlam güvenlik çözümü sağlarlar. Ayarlanması ve programlanması kolaydır. İçerideki ağ yapısını gizleyebilirler. Denetim ve kullanıcı kayıt araçlarına sahiptir. Kimlik onaylaması ile zaman ve saate göre kontrol gibi özelliklere sahiptirler.	Düşük performans. Kullanıcılara göre saydam değildir. Her protokol veya uygulama için yeni bir vekil geliştirilmesi gerekir. İşletim sistemini dış ataklara açarlar. OSI modelinin sadece 5 ile 7 arasındaki katmanları incelenir. UDP ve RPC gibi bağlantısız protokoller vekiller tarafından desteklenemez.

Tablo 8.2 Güvenlik duvarı mimarilerinin karşılaştırılması.

8.5.3 Güvenlik Duvarı Mimarileri

Çeşitli güvenlik duvarı mimarileri vardır bir kısmı burada incelenmiştir. Bunlar;
1.Çift ağ ara yüzlü güvenlik duvarı (dual-homed gateway)
2.Denetlenen konak güvenlik duvarı (screened host Güvenlik duvarı)
3.Denetlenen altağ güvenlik duvarı (screened subnet Güvenlik duvarı)
4.Karışık mimarili güvenlik duvarı çözümü

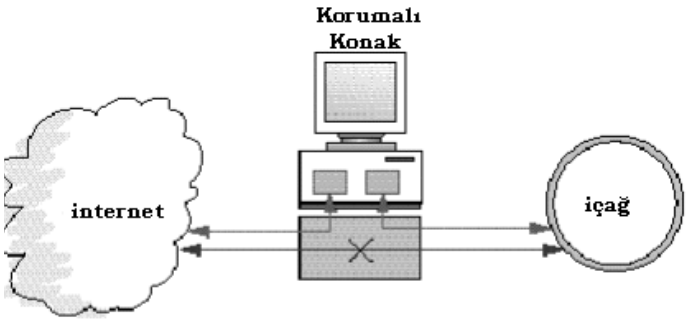
8.5.3.1 Çift Ağ Ara yüzlü Güvenlik Duvarı (dual homed gateway)

Çift ara yüzlü güvenlik duvarı mimarisi, en az iki ağa bağlantı sağlayan ara yüze sahip bir makine üzerine kurulmuştur. Şekil 8.8'den de görüldüğü gibi çift ağ ara yüzüne sahip bilgisayarın yönlendirici olarak da çalışması mümkündür. IP yönlendirme yeteneğine sahip olacak; fakat bir ağdan gelen paket diğerine doğrudan aktarılmayacaktır.

Bu mimaride yüksek seviyeli bir trafik kontrolü gerekmektedir. Böyle bir mimari kullanıldığında, belli bir servis için istek geldiğinde, bu isteğe ilişkin veri tiplerinin uygun olmamaları durumunda isteğin geri çevrilmesi mümkündür. Bu da çok büyük avantajları da beraberinde getirecektir. Servis isteklerinin, her servisin isteklerine ilişkin şartları yerine getirip getirmediğine bakılarak, bağlantıya kurması ya da reddetmesine olanak sağlayacaktır.

Çift ağ ara yüzlü güvenlik duvarı, iki şekilde hizmet sunarak iç ağ ile dış ağ arasındaki bağlantıları kurar.
1. Vekil sunucu (proxy server) ya da,
2. Kendisinden hizmet almak isteyen bütün kullanıcıların bir kullanıcı adı ve parolasıyla onaylanması suretiyle.

Kullanıcı adı ve şifresi kullanılarak gerçekleştirilecek bir bağlantı kontrolü işlemi, güvenlik açısından bazı sorunlar çıkartacaktır. Kullanıcı adı ve şifrelerinin öğrenilmesi sistemi güvensiz hale getirir. Bu durumda vekil sunucular kullanılarak servis verilmesi işlemi daha güvenlidir. Ancak burada da bazı zorluklar vardır. Verilmek istenen servislerin tamamı için vekil sunucu bulmak zordur.



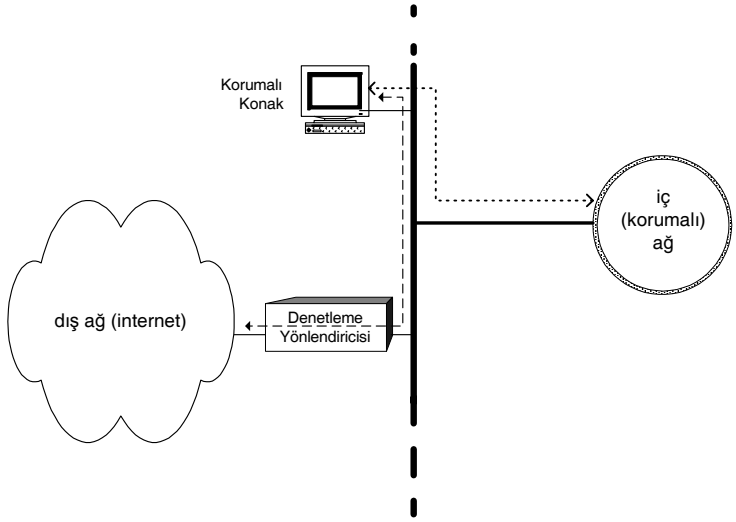
Şekil 8.8 Çift ağ ara yüzlü güvenlik duvarı

8.5.3.2 Denetlenen Konak Güvenlik Duvarı (screened host Güvenlik duvarı)

Paket filtreleme güvenlik duvarı tipine örnektir. Bir yönlendirici tek bir makineye erişimleri kontrol eder.

Denetlenen konak (screened-host) güvenlik duvarında, ağ katmanındaki bir yönlendirici, bütün korumalı ağ trafiğinin üzerinden geçmek zorunda olduğu ve korumalı konak (bastion host) olarak adlandırılan tek bir makineye erişimi kontrol eder. Korumalı ağa doğrudan erişim engellenir ve bastion host paketleri göndermez. Bu makine iyi korumalı ve bütün saldırılara karşı koyması beklenen güçlü bir noktadır.

Bu mimaride servisler sadece yerel ağa bir arayüzü bulunan bir konak(host) üzerinden verilir. Bu konak Şekil 8.9'da görüldüğü gibi bir yönlendiriciye bağlıdır ve bu yönlendirici üzerinden dış dünyaya açılmaktadır.



Şekil 8.9 Denetlenen Konak Güvenlik Duvarı Mimarisi

Bu mimaride güvenlik için paket filtreleme mekanizması önemlidir.

Korumalı konak yerel ağda yer alır. Yönlendirici üzerinde yer alan paket fitreleme kuralları, internette yer alan bilgisayarların yalnızca korumalı konak makinasına bağlantı sağlamaya izin verecek şekilde gerçeklenmiştir. Ayrıca sadece izin verilen servislere bağlanılabilmesine müsaade edecek şekilde düzenlenmiştir. Dış ağdan (internet) gelecek tüm servis istekleri korumalı konağa yönlendirileceğinden, bu konağın üst düzeyde güvenliğinin sağlanması gerekir. Aynı zamanda korumalı konak, dış ağda yer alan sunuculara bağlanarak istekte bulunma işlemini de yerine getirir. Yönlendirici üzerinde çalışan paket filtreleme iki şekilde davranabilir.

1. Yerel ağda yer alan bilgisayarların, belirlenmiş servisler için dış ağa bağlanabilmelerine izin verir.
2. Yerel ağda bulunan bütün bilgisayarların dışarıya erişimlerini yasaklayarak, bu tür isteklerin tamamının korumalı konak üzerinde bulunan vekil sunucular (proxy servers) üzerinden yapılmasını sağlar.

Bu yöntemler ayrı ayrı kullanılabileceği gibi birlikte de kullanılabilir. Bazı servisler için, sadece paket filtreleme mekanizması kullanılarak doğrudan dışarıya ulaşıma izin verilirken bazıları içinse sadece vekil sunucu üzerinden dışarıya çıkmasına izin verilir.

Çift ağ ara yüzlü güvenlik duvarı mimarisinde dış ağdan gelen iptal edilecek paketler yerel ağa aktarılmamaktadır. Oysa bu mimaride geçebilmektedir. Dolayısıyla bu mimari güvenlik açısından daha riskli gözükmektedir. Buna karşılık çift ağ ara yüzlü güvenlik duvarı mimarisinde güvenlik duvarı olarak kullanılan bilgisayar üzerinde olabilecek bir sorun sonucu dışarıya olan bağlantı kesilecektir.

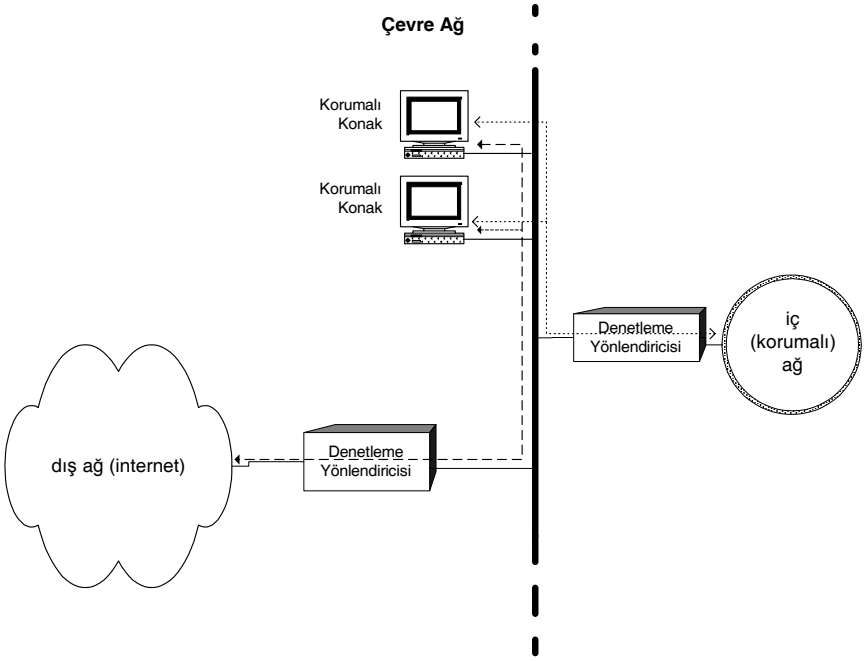
Bir yönlendiriciyi saldırılara karşı korumak, bir bilgisayarı korumaktan daha kolay olacaktır. Çünkü yönlendiricinin yapacağı işlemler sınırlıdır ve bunlarla ilgili olarak güvenliği sağlamak da, bir konağa ilişkin güvenliği sağlamaya göre daha kolay olacaktır. Bu yüzden bu mimarinin çift ağ ara yüzlü güvenlik duvarı mimarisine göre daha güvenli ve kullanışlı olacağı açıktır.

Bunlara karşın, bu mimarinin dezavantajları vardır. Saldırganın korumalı konağa (bastion host) ulaşması durumunda, ağdaki diğer makinalara ulaşmak için önünde bir engel kalmamış olacaktır. Denetleme yönlendiricisinde meydana gelecek herhangi bir sorun durumunda da saldırganın tüm ağa ulaşması için önünde bir engel kalmayacaktır.

8.5.3.3 Denetlenen alt ağ güvenlik duvarı (screened subnet Güvenlik duvarı)

Paket filtreleme güvenlik duvarları mimarisine örnektir. Yönlendirici çifti kullanılarak "DeMilitarized Zone — DMZ" olarak adlandırılan bir alanla ağ koruması yapılır.

Yapısı Şekil 8.9'da verilen güvenlik duvarı mimarisinde (screened-subnet), bir çift yönlendirici yardımıyla DMZ oluşturularak ağ koruması yapılır. Şekil 8.10.



Şekil 8.10 Denetlenen alt ağ güvenlik duvarı (Paket filtrelemeli).

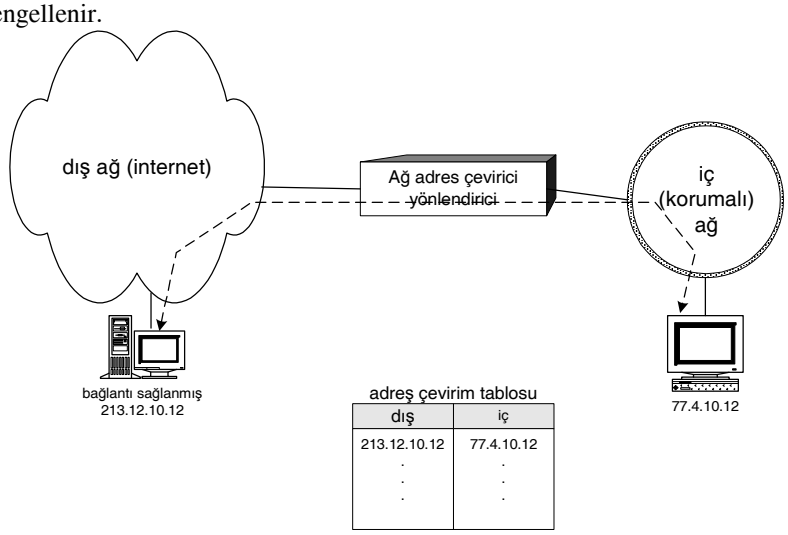
Böyle bir mimarinin geliştirilmiş olmasının en önemli sebebi *denetlenen konak güvenlik duvarı* mimarisindeki tehlikenin önüne geçmektir. Denetlenen Konak Mimarisinde korumalı konaklar açık birer hedef durumundadır. Saldırılar çoğunlukla buralara yapılacaktır; çünkü bunlar dış dünyaya açılan makinalardır. Saldırganların korumalı konağı aşması durumunda, iç ağa ulaşmaları için bir engel kalmamaktadır.Bu mimaride ise korumalı konağı aşan bir saldırganın, yerel ağda bulunan konaklara ulaşabilmesi için bir engeli daha aşması gerekmektedir.

En basit yapıdaki denetlenen alt ağ mimarisinde iki adet denetleme yönlendiricisi vardır. Bunların her ikisi de çevre ağa bağlanmıştır. Biri çevre ağ ile yerel ağ arasında yer alırken diğeri de çevre ağ ile dış ağ arasında yer alır. Yerel ağda yer alan konaklara saldırmak isteyen kişinin her iki denetleme yönlendiricisini de geçmesi gerekir.

Bazı güvenlik duvarı çözümlerin de bu mimariden yola çıkılarak birden fazla çevre ağ kullanmak suretiyle çok katmanlı bir güvenlik mekanizması kullanılmaktadır. Böylece saldırganların yerel

ağa ve burada yer alan sunuculara ulaşması zorlaştırılmaktadır. Yalnız böyle bir çalışmada dikkat edilmesi gereken bir nokta vardır. Her katmanın güvenlik özellikleri farklı olmalıdır. Aksi durumda, bir katmanın güvenlik mekanizmasını aşan bir saldırgan, aynı yöntemle diğer katmanları da aşacaktır.

Bir yönlendirici kullanılarak yapılan diğer bir güvenlik yöntemi Ağ Adres Çevirimidir (Network Address Translation—NAT). Bu yöntemde bir iç ağdaki adresler dış dünyadan saklanır (Şekil 8.11). Bir NAT yönlendiricisi iç ve dış adresleri tutan bir tablo içerir. Dışarıdan gelen mesajdaki adres NAT yönlendiricisi tarafından gizlenen iç adrese çevrilir. Dış erişimlerde de benzeri şekilde adres çevirimi yapılır. Bu tablonun bazen değişmesiyle iç adreslerin dışarıdan kolay bir şekilde bulunması engellenir.



Şekil 8.11 Ağ adres çevirimi.(NAT)

8.5.4 Karışık mimarili güvenlik duvarı çözümü

Güvenlik duvarı mimarilerinin en çok kullanıldıkları şekilleri ile girebilecekleri sınıflar yukarıda anlatılmıştır. Fakat bazı durumlarda, gerek güvenlik politikası, gerek bütçe, gerekse de ağın sahip olduğu mimari, bu mimarilerden sadece birinin, istenen güvenliği sağlamaması sonucunu doğurabilir. Böyle bir durumda, bu mimarilerin değişik özellik ve bileşenlerinin birlikte kullanıldığı yeni mimariler ve çözümler ortaya çıkacaktır.

8.5.4.1 Birden Fazla Korumalı Konaklı Mimariler

Denetlenen alt ağ mimarisinin birden fazla korumalı konak kullanılarak oluşturulmuş çözümü olarak düşünülebilir. Böyle bir çözüme sistemin sürekli çalışabilirliğinin (high availablity)sağlanması için gidilmiş olabilir. Ayrıca performansı da arttıracaktır. Hizmetler korumalı konaklar arsında paylaştırılarak performansta artış sağlanabilir ama bu yedekleme yapılmaması anlamı taşıyacağından risklidir.

8.5.4.2 Tek yönlendiricili Mimariler

Bu mimaride iç ve dış denetleme yönlendirici yerine tek yönlendirici kullanılır. Burada yönlendiricinin bu yapıya uygun olması ve konfigürasyonunun düzgün yapılması gerekir. İç ve dış yönlendiriciler, içerden dışarıya ve dışardan içeriye gerçekleştirilen bağlantıları denetlemektedir. Bunların yerine konan yönlendiricinin de bu yeteneklerinin olması gerekir.

Böyle bir mimari, güvenlik ve paket filtreleme konusunda yetenekli yönlendirici kullanılması durumunda iyi bir çözümdür. Bu yönlendiricinin korumalı konağa, iç ağa ve dış ağa açılan üç ağ ara yüzüne sahip olması gerekir.

8.5.4.3 Korumalı Konak ile Dış Yönlendiricinin Birleştirildiği Mimariler

Çift ağ ara yüzüne sahip bir korumalı konak makinasına yönlendirici fonksiyonlarının da eklenip kullanıldığı çözümlerdir. Çift ağ ara yüzlü konağın aynı zamanda bir yönlendirici olarak çalışması performans açısından sistemi olumsuz olarak etkileyecektir. Ayrıca korumalı konağın direk olarak internete bağlantısının yapılmış olması güvenliğini daha da önemli hale getirir.

8.5.4.4 Korumalı Konak ile İç Yönlendiricinin Birleştirildiği Mimariler

Korumalı konak ile dış yönlendiricinin birleştirildiği mimaride çok fazla güvenlik problemi olmamasına karşı bu çözümde vardır. Güvenlik açısından tehlikeli bir çözümdür. Çünkü iç yönlendiriciler hem korumalı konak hem de dış yönlendirici için güvenlik katmanı olarak çalışmaktadır.

8.5.4.5 Çoklu İç Yönlendiricili Mimariler

Çevre ağı yerel ağa değişik noktalardan bağlamak üzere kullanılabilecek birden fazla yönlendirici ile sağlanan bir çözümdür. Güvenlik açısından bir takım problemler oluşturacağından tavsiye edilen bir mimari değildir. Performansın arttırılması için kullanılması zorunlu hale gelen birden fazla iç yönlendiricili mimarilerde güvenliğin arttırılması için ayrıca çalışılması gerekir. Aslında iç yönlendirici performans problemi oluşturmaz. Eğer iç yönlendirici dış yönlendiriciye göre çok hızlıysa ve trafik genelde iç ağ ile internet arasında akıyorsa, çoklu iç yönlendiricili mimariye geçilebilir. Bu sorun güçlü bir yönlendirici alınarak da çözülebilir.

Ayrıca organizasyondan kaynaklanan sebeplerden dolayı da böyle bir çözüme gidilmiş olabilir. Bu durumda da uygulanabilecek çözümler vardır. İç yönlendiricinin ağ arayüzü arttırılarak bu çözüm sağlanabilir.

8.5.5 Güvenlik Duvarı Jurnali

Güvenlik duvarları ağdaki trafik denetleme işlemlerini bir jurnale kaydetmelidir. Böylece daha önce olup biten olayların bilgilerinden analizler yapmak mümkün olabilecektir. Güvenlik duvarının tutması gereken bu bilgiler hakkında aşağıdaki özellikler göz önüne alınmalıdır.

- Jurnal bilgileri bütün olayları açık ve kolay okunur formatta tutmalıdır.
- Bütün olaylar tekbir dosyada tutularak trafik şekilleri daha iyi analiz edilebilmelidir.
- Jurnal(log),hangi trafiğin engellenip hangisinin iletildiğini açık olarak tutmalıdır.
- Jurnaldeki bilgiler filtreleme ve sıralama ile düzenlenebilmelidir.
- Jurnal dosya büyüklüğünün kısıtlanması nedeniyle kedi üzerine yazmamalıdır.
- Jurnali güvenli bir şekilde uzaktan gözlemek mümkün olmalıdır.
- Jurnal yazılımı bu bilgileri ASCII gibi genel bir formatta dışarı almaya imkan vermelidir.

9 NÜFUZ TESBİT SİSTEMLERİ (INTRUSION DETECTION SYSTEMS)

'Saldırı nedir?' Sorusuna cevap vermek için ilk olarak *saldırı, saldırgan ve nüfuz* terimlerini tanımlamak gerekir.

Bir ağ ortamında, ağ kaynaklarına izinsiz erişim yapan veya yapmaya çalışan, sistemi kötüye kullanan kişiler saldırgan kelimesinin kapsamındadır. Bunlara cracker, bazen de saldırgan(hacker) da denilmektedir.Saldırısını sonuçlandırarak sisteme girmeyi başaran saldırgan ise nüfuz eden(intruder) olarak tanımlanır. Bu özellik nedeniyle nüfuz tespit sistemleri güvenlik duvarının arkasında, yani ağ içerisinde çalışırlar.

9.1 Saldırganlar

Gerçeği Gizleyen(Masquerader): Bilgisayarı kullanmaya yetkisi olmayan ve bir başkasının hesabını kullanarak sisteme sızan kişi.
Hatalı Kullanım(Misfeasor): Veri, program veya diğer sistem kaynaklarına erişebilen legal kullanıcı, fakat bu erişimi yetkisizce ve yanlış olarak kullanan kişi.
Gizli Kullanıcı(Clandestine user): Sistemin yönetim haklarını ele geçiren ve bu kontrolü denetimden kaçmak için kullanan veya denetimi etkisizleştiren kişi.

Gerçekte problem kontrol altına alınamamıştır. Bir örnek olarak, Bell lab'da bir grubun yaptığı ve internet üzerinden bilgisayarlarına yapılan saldırılara ilişkin raporda aşağıdaki tecrübelere yer verilmiştir.

- Her gün artan bir hızda password dosyasını kopyalamaya yönelik teşebbüsler.
- Haftada bir kere şüpheli uzak altyordam çağrımı(Remote Procedure Call).
- En az iki haftada bir olmayan yem bilgisayarlara bağlanma girişimleri.

Bundan başka saldırganlardan gelen bir dizi atak gerçek ve büyüyen bir problemdir. Bu trendin büyümesinin nedenleri aşağıda belirtilmiştir.

- *Globalleşme:* Uluslararası rekabet baskısı bir dizi endüstri casusluğu vakasını üretmiştir. Bu da bazı bilgisayar korsanlarının becerilerini pazarlamalarına yol açmaktadır.
- *İstemci/Sunucu mimarisine yönelme.*: Firmalar verilerini ya özel güvenlik yazılımı ile korunan mainframelerde yada genellikle uzaktan erişilemeyen PC'lerde saklamışlardır. Ancak İstemci /Sunucu mimarisinin cazip hale gelmesiyle bu baraj ortadan kaldırılmaktadır.
- *Bilgisayar korsanlarının hızlı öğrenmesi:* Bilgisayar korsanları bilgi paylaşmayı çok severler. Bu yüzden yer altı BBS'leri aracılığı ile sistemlerin açıklarını ve korsanlık tekniklerini birbirlerine aktarırlar

9.2 Saldırı Teknikleri:

Saldırganın ana amacı sisteme erişimi kazanmak veya, sistemdeki erişilebilirliğini artırmaktır. Çoğu durumda bu bilgi kullanıcı şifresidir. Bazı diğer kullanıcı şifrelerini kullanan bir saldırgan, sisteme login olur ve legal kullanıcıya ait bütün hakları kullanır. Şifre dosyası iki şeklide korunur.

- Tek Yönlü Şifreleme: Sistem kullanıcı şifrelerini sadece kriptolanmış şekilde saklar. Bir kullanıcı şifre girdiği zaman sistem bunu şifreleyerek saklanmış olanı ile karşılaştırır.
- Erişim Kontrolü : Şifre dosyasına erişim bir veya birkaç hesap ile sınırlanır.

9.3 Teknik Olmayan saldırılara karşı Savunma Yöntemleri

- Bütün Çalışanların teknik olmayan saldırılar hakkında sürekli olarak eğitilmeleri, bilgi saklamanın nasıl yapılacağına ilişkin bilgilendirme yapılması. Çalışanlara ayrıca elektronik posta, ses postası ve Fax'ın açıkları hakkında bilgi verilmelidir. Saldırıları anlamak için sıkı ve periyodik denetimler yapılmalıdır.
- Bütün çalışanlar ve bağlantılı kimseler şirket politikası ve prosedürler altında sorumluluklarını anlatan bir anlaşma imzalanmalıdır.

9.3.1 Şifre Koruma

Saldırganlara karşı ön koruma, şifre sistemidir. Sanal olarak bütün çok kullanıcılı sistemler sadece kullanıcı adı değil aynı zamanda güvenliği aşağıdaki şeklide sağlayan bir şifre bulundurur.

- Kullanıcı adı, kullanıcının sisteme erişim hakkını kazanmasını yetkilendirir.
- Kullanıcı adı kullanıcının önceliklerini belirler. Süper kullanıcı veya, yönetici hakkına sahip olan kullanıcılar, işletim sistemi tarafından kısıtlanana bazı işlemleri yapabilirler
- Kullanıcı adı, ihtiyari erişim kontrolü vermek için kullanılabilir. Örneğin, diğer kullanıcıların listesinde , bazı kullanıcılara diğerlerinin kendi dosyalarını okuma hakkı verdiği görülebilir.

Kullanıcı parolalarının şifrelenerek saklandığı UNIX sistemini düşünelim. Her kullanıcının 8 karakter uzunluğunda bir parolası vardır. Bu kriptolama işlemi için 56 bitlik anahtara dönüştürülür. Kriptolama rutini DES tabanlı dır kript(3) olarak bilinir. DES algoritması 12 bit salt değeri kullanılarak değiştirilir. Bu değer kullanıcıya parola verilme zamanına bağlıdır. Değiştirilmiş DES algoritması, 64 bitlik sıfır bloğu içeren veri girişi ile uygulanır. Algoritmanın çıkışı, ikinci kriptolama için giriş olarak kullanılır. Bu süreç toplam olarak 25 kriptolama için Sonuçtaki 64 bitlik çıkış 11 karaktere dönüştürülür. Şifreli parola, uygun kullanıcı adı ile birlikte düz metin şeklinde saklanır.

- Salt şifre dosyasında çift parola oluşumunu engeller.
- Salt, kullanıcının hatırlamasına gerek olmaksızın, parola uzunluğunu artırır.
- Salt DES'in donanım kodlamasını önler.

9.4 Nüfuz Tespit Nedir?

Burada nüfuz terimi sistemde yetkisiz kullanım, kaynaklara izinsiz erişim, bilgi çalınması olabileceği gibi sadece sistemi meşgul ederek servis dışı bırakmayı da kapsamaktadır.

Ağ Nüfuz Tespit Sistemleri (Intrusion Detection Systems: IDS) temel olarak network üzerindeki paketleri yakalayarak bunları çeşitli kriterlere göre değerlendirip ağ trafiği üzerinde yorumlar yapan yapılardır. Örneğin dış ağ'dan içeriye doğru bir port'a yoğun bir şekilde gelen SYN paketleri, sistem sunucularına karşı yapılmaya çalışılan bir SYN FLOOD saldırısının belirtileri olabilir. Yada çeşitli portlara gelen SYN paketleri birilerinin ağımız üzerinde port taraması yapmakta olduğunu ve muhtemelen ardından gelecek bir saldırı için bilgi toplandığını gösterebilir.

IDS tüm ağı promiscous mod'da dinleyen belirli bir makine olabilecekleri gibi, sadece kendi trafiğini dinleyen bir uç birim de bir yazılım da olabilir (host based intrusion detection).

9.5 Ağ Üzerinden Gelebilecek Tehditlerin Kaynakları

- Yazılım Hataları
- Yanlış Sistem Ayarları
- Şifre Kırma
- Güvensiz Trafiğin Dinlenmesi
- Truva Atları, Virusler, Arka Kapılar

Tüm bu sebepler sistemde 'güvenlik açıklıkları' oluşturmaktadır. Bunları kullanarak sisteme saldırmak isteyen kişi normal ağ trafiğini kullanarak (fiziksel olarak sisteme erişimi olmadığı kabul edilmektedir) saldırıyı gerçekleştirecektir. Normal trafiği saldırı trafiğinden ayırabilme IDS'in yeteneğine bağlıdır.

Bir saldırı senaryosu, ilk olarak saldırgan'ın sistem hakkında bilgi toplamasıyla başlar. Sistemde kullanılan güvenlik sistemleri, sunucular, ağ yapısı ve yetkilendirme mekanizmaları ilk dikkatini çekecek yapılar olacaktır. Ardından kullanabileceği açıklıkları tarayacaktır. Yine ağ üzerinden gerçekleştireceği bu taramalarda belirli bir sunucu, işletim sistemi, script, bir şekilde ağa bulaşmış olabilecek bir arka kapı aranmaktadır. Bu noktaya kadar saldırgan ağ üzerinden sisteme erişmekte ve görünürde herhangi bir zarar verilmemektedir. Yine de bu tür taramaların hemen ardından asıl saldırı geleceğinden IDS'in bunları tanımlamadaki yeteneği nüfuz gerçekleşmeden tespit edilmesi açısından oldukça önemlidir.

Üçüncü adımda, bulunan bir zayıflık üzerinden nüfuz gerçekleştirilecektir. Yanlış çalışan bir CGI scripti, şifre kırmaya müsait bir servis yada bir arka kapıdan sisteme girilir. Artık sistemde olan saldırgan izlerini silmeye çalışacaktır. Bu noktada hedef genelde log dosyalarıdır. Erişim kayıtlarının, IDS kayıtları, hatta Güvenlik duvarlarındaki kayıt bilgileri bir saldırı hakkında oldukça bilgi verebileceğinden izlerin silinmesi için ilk hedeflerdir. Son adım olarak saldırgan amacını gerçekleştirecektir. Bu sisteme yeni bir arka kapı yerleştirmek, gizli bir bilgiyi ele geçirmek, yada sistem kaynaklarını kendi amaçları için kullanmak olabilir.

9.6 Saldırı İmzaları

IDS ağ üzerinden topladığı paketleri, bilinen saldırı imzalarıyla karşılaştırır. Bu imzaların en basit hali belirli bir saldırıyı tanımlayacak kadar genel paket maskeleridir. Örneğin dış networkten iç networke gelen ve 12345 portunu kullanan bağlantı istekleri bize sistemimizde bulunan Netbus adıyla bilinen bir arka kapı yazılımının dışardan tarandığını veya kullanıldığını gösterecektir ve IDS bu durumu derhal haber vermelidir.

Bir diğer saldırı imzası sistemde bulunan servislerin zayıflıklarının kullanıldığını belirleyecek yapılardır. Bu imzalar, saldırının tek bir port veya paketin incelenmesiyle çıkartılamayacak veya normal trafikten ayırt edilemeyeceği durumlarda kullanılır. Bunlar paketlerin içeriğine bakarak, (gerekirse birden çok paketi birleştirerek) belirli komutları karakterlerin aranmasını sağlarlar. Örneğin bilinen bir CGI zafiyetini kullanmak için 80. porta yollanan bir isteğin tespitinde bu tür bir içerik analizi gerekmektedir.

Üçüncü ve son saldırı imzası servis dışı saldırılarını belirlemekte kullanılır. Burada saldırgan normal bağlantılar açıyor gibi gözükmektedir. Ancak açılan bağlantı sayısı ve hızı sistemin normal işleyişini aksatacak ölçüde yoğundur. Bu tür saldırılarda network genişliği, işlemci gücü, yada disk kapasitesi saldırgan tarafından tüketilir ve sistem servis dışı bırakılır. Bunların tespitinde kullanılan imzalar belirli bir zaman süresince belirli bir adresten gelen isteklerin sayısını belirtirler ve limiti aşması halinde bunun bir servis dışı bırakma saldırısı olabileceğini gösterirler.

9.7 Taban Değer yanılgısı(Base Rate Fallacy)

Bir nüfuz tespit sisteminin taşıması gereken en önemli özelliklerden biri de sistemin etkili omasıdır. Etkililik ise sistemin yanlış alarm oranına ve nüfuz tespit oranına bağlıdır. Etkili bir nüfuz tespit sisteminde yanlış alarm oranının düşük, buna karşın tespit edilen saldırıların oranının yüksek olması beklenir. Etkililiğin ölçümünde ise (yanlış alarm oranının hesaplanmasında) taban değeri yanılgısı (Base-Rate Fallacy) kullanılmaktadır. Taban değeri yanılgısı, bir şartlı olasılık ve onun tersi arasındaki ilişkiyi belirten Bayes istatistiğinin temel aldığı bir kavramdır.

Olasılığa dayalı yorumlamada populasyon karakteristiği hakkında geniş tabanlı ve genel bilgiler ve gerçekleşen olaya ait önceki olasılıklar hesaba katılmalıdır. Bu bilgilerin ihmal edilmesi nedeniyle ortaya çıkan yanılgıya taban değer yanılgısı adı verilmektedir. Örneğin hasta veya sağlıklı insanlar populasyonu üzerinde uygulandığında %99 doğru sonuç veren bir test olsun. Tüm populasyon içerisinde ise hasta insanların oranı 1/10000 olsun. Bu durumda test sonucu pozitif çıkan bir insanın hasta olma olasılığı nedir?

Bunun için hasta olduğu bilinen insanlar S, sağlıklı insanlar ¬S, R pozitif test sonucu, ¬R ise negatif test sonucunu temsil etsin. Yukarıda verilen bilgiler ($P(R \mid S) = 0{,}99$, $P(\neg R \mid \neg S = 0{,}99)$, $P(S) = 0{,}0001$) ışığında bulmaya çalıştığımız P(S|R)'dir ve şu şekilde hesaplanmaktadır :

$$P(S \mid R) = \frac{P(S).P(R \mid S)}{P(R)} \qquad (9.1)$$

Eşitlik (9.1)'de P(R) bilinmemektedir ve *n* adet değişik S sonucu için şu şekilde hesaplanmaktadır:

$$P(R) = \sum_{i=1}^{n} P(S_i).P(R \mid S_i) \qquad (9.2)$$

Eşitlik (9.1), eşitlik (9.2) 'ye göre düzenlendiğinde Bayes istatistiğinin temel formülü olan eşitlik (3) elde edilmektedir.

$$P(S \mid R) = \frac{P(S).P(R \mid S)}{\sum_{i=1}^{n} P(S_i).P(R \mid S_i)} \qquad (9.3)$$

Taban değer yanılgısının nüfuz tespitine uygulanabilmesi için bazı olasılıkların bilinmesi veya bu olasılıklar hakkında varsayımlar yapılabilmesi gerekmektedir. Örneğin bir kaç düzine iş istasyonu, bir kaç sunucu ve bir kaç düzine kullanıcılı bir sistem için günde 1.000.000 izleme kaydının üretildiği, günde bir veya iki saldırı girişimi ile karşılaşıldığı ve bir saldırının ortalama 10 izleme kaydını etkilediği varsayımları yapılırsa ;

Alarma karşı Nüfuz(Intrusion) olma olaslığı (9.5) ile hesaplanır.

$$P(I \mid A) = \frac{P(I).P(A \mid I)}{P(I).P(A \mid I) + P(\neg I).P(A \mid \neg I)} \qquad (9.5)$$

$$P(I) = \frac{2.10}{1.10^6} = 2.10^{-5} \quad , \quad P(\neg I) = 1 - P(I) = 0{,}99998 \qquad (9.6)$$

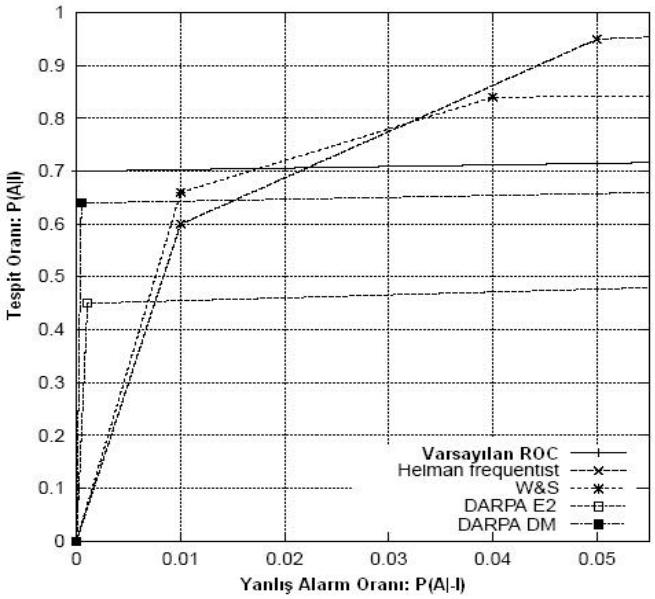
değerleri elde edilir. Bu değerler eşitlik (9.5)'te kullanıldığında

$$P(I \mid A) = \frac{2.10^{-5}.P(A \mid I)}{2.10^{-5}.P(A \mid I) + 0{,}99998.P(A \mid \neg I)} \qquad (9.7)$$

eşitliği elde edilir(Burada I: Intrusion, A: Alarm. Bu eşitliğe göre yanlış alarm hesabında belirleyici faktör ¬I (0,99998) 'dır.

Nüfuz tespit oranı, yanlış alarm oranının bir fonksiyonu olarak çizildiğinde elde edilen eğriye ROC (Receiver Operating Characteristic) eğrisi adı verilmektedir. ROC eğrisi nüfuz tespit oranının (0,0) ve (1,1) noktaları arasında, yanlış alarm oranına göre değişimini göstermektedir. (1,1) noktasında tüm olaylar saldırı olarak nitelendirilmektedir. Böylece nüfuz tespit oranı 1 değerine ulaşmaktadır. Ancak aynı şekilde yanlış alarm oranı da 1 olmaktadır ve bu kabul edilebilir bir oran değildir. (0,0) noktası ise tüm olayları normal olarak nitelendirmekte ve böylelikle yanlış alarm oranını 0'a indirmektedir. Bu durumda da nüfuz tespit oranı 0'a inmektedir ve yine kabul edilebilir bir oran değildir.

ROC eğrisi herhangi iki nokta arasında çukur içermemelidir. Bu durum hata yapıldığının bir göstergesidir. Ayrıca ROC eğrisi (0,0) noktasından sonra çok hızlı bir şekilde yükselmektedir. Çünkü en kısa zamanda 0 nüfuz tespit oranında kabul edilebilir bir orana ulaşılması gerekmektedir ve bu yapılırken de yanlış alarm oranı kontrol altında tutulmalıdır.



Şekil 9.1: Farklı nüfuz tespit sistemleri için ROC eğrileri.

Şekil 9.1'de farklı nüfuz tespit sistemleri için ROC eğrileri gösterilmektedir. Eğrilerin devamı çok yavaş yükseldiğinden diyagramın anlamlı kısmının görünürlüğünü artırmak amacıyla bu diyagramda (1,1) noktası bulunmamaktadır.

Bir nüfuz tespit sistemi için zaman içerisinde elde edilen yeni ROC eğrileri her zaman önceden elde edilen eğrilerin üzerinde olmalıdır. Aksi takdirde gelişmeden söz etmek mümkün değildir.

9.8 Nüfuz Tespit Teknikleri

Mevcut nüfuzlar iki kategoride toplanabilirler. Bunlar

- Suistimal Nüfuzları: Sistem üzerindeki bilinen zayıf noktaya tanımlanmış patern ile yapılan nüfuzlar.
- Anormallik Nüfuzları : Normal kullanım şeklinden sapmalar ile karakterize edilirler.

Suistimal Tesbiti:

Nüfuz Tespit Sistemlerinin büyük çoğunluğu bilinen saldırı imzalarını yakaladıkları ağ trafiğiyle karşılaştırarak çalışırlar. Yöntemin esası iz tanıma yöntemine dayanır.

İmza tanıma yönteminde sistemin saldırıların gelebileceği noktalarına yerleştirilmiş IDS'ler yakaladıkları paketlerin içerisinde tanıdıkları imzaları ararlar. Bu yöntemde sadece önceden tanımlanmış ve imzaları bilinen nüfuz tipleri yakalanabilir. Örneğin tüm paketlerin içerisinde "/cgi-bin/phf?" dizisini arayarak bilinen bir CGI açıklığının kullanıldığını anlayabiliriz. Bu tür diziler yüzlerce hatta binlerce olabilir. IDS bulduğu yakaladığı her paketi bu database içerisindeki imzalarla karşılaştıracaktır.

Temel teknikler aşağıda belirtilmiştir.

- Uzman Sistemler : Saldırı bilgileri karar kuralları yardımıyla değerlendirilerek saldırı anlaşılır.
- Model tabanlı Mantıksal karar sistemleri :Bu sistem de bir saldırı senaryosu veritabanı aracılığı ile nüfuz tespiti yapılır.
- Durum Geçiş Analizi: Saldırıları, gözlenen sistemdeki durum geçiş sekansları olarak gösterir.
- Tuş basmalarını gözleme: Özel kullanıcıya ait tuş basmalarının uyuşturulmasıyla nüfuz açığa çıkartılabilir.

9.8.1 Anormallik Tespiti:

Anormallik tespitinde sistemin çalışma mantığı toplanan istatistik bilgilerine belirli bir alt sınır koyarak bunun aşıldığı durumları anormal saymak ve saldırı alarmı vermektir. Bu sistem bilgilerini işlemci kullanımı, ağ kullanımı, disk aktivitesi, kullanıcı girişleri, dosya erişimleri oluşturur.

Örneğin uç birimlerin trafik kullanımını gözlemleyen bir IDS yapımız var. Burada saat 2:00AM tarihinde bir birimden ağ trafiği çıktığını ve bunun o sistem için daha önceden toplanan istatistiklere uymadığını görüyoruz. Bu durum muhtemelen bir saldırıya işaret etmektedir ve sistem uyarılmalıdır.

Anormallik Tespitinde avantaj saldırı detayları, imzası ve yapısı bilinmeden de saldırının tespit edilebilmesidir.

Bu anormallikleri sıralarsak:

- Normal logon zamanı veya terminalinden olan sapmalar, kaynakların kullanımı, icra edilen komutların tipleri(Kendini gizleyen başarılı saldırı).
- Yetkili kullanıcıların normal kullanımlarından olan sapmalar.
- CPU veya I/O kaynaklarının kullanımındaki sapmalar(Muhtemel Truva atı)
- Çalıştıracak programların bellek gereksinimlerinin artması veya olağan dışı program çalışması(Virüs)
- Tek bir kullanıcının anormal şeklide fazla kaynak kullanımı ve diğer kullanıcıları çok düşük kullanım oranı
- Parola girişlerindeki başarısızlıkların çok artması

9.8.2 İyi Bir Nüfuz tespit Sistemini Özellikleri

Saldırı tespit sisteminin hangisi olursa olsun aşağıdaki özellikleri taşımalıdır.

- Sürekli bir insan denetlemeden çalışabilmelidir.
- Hata toleransı olmalıdır.
- Yıkıma karşı dayanıklılığı olmalıdır.
- Minimum sistem yüklemesi yapmalıdır.
- Normal davranışlardan sapmaları gözlemelidir.

- Host sistemin değişikliklerine adapte edilebilmelidir.
- Yeni bir uygulama eklediğinde olan sistem değişikliklerinin üstesinden gelebilmelidir.
- Aldatılması zor olmalıdır.

9.9 Dağıtık Nüfuz Tespit Sistemi

Saldırı tespit sistemlerinin performanslarının artırılması amacıyla ağ üzerinde farklı noktalarda nüfuz tespit sistemi motorları çalışabilir. Böyle bir mimarinin özellikleri aşağıda belirtilmiştir.

- Dağıtık bir Nüfuz tespit sistemi, farklı denetim kayıt formatlarıyla çalışabilmelidir.
- Ağdaki bir veya daha fazla düğüm, ağ üzerinde iletilen datanın toplanması ve analizi için görev yapabilmelidir.
- Merkezi veya merkezi olmayan yapı kullanılabilir. Merkezi mimaride bütün denetlenecek datanın toplanıp analiz edildiği tek bir merkezi kontrol noktası vardır. Bu, gelen raporların ilişkilerinin düzenlenmesini kolaylaştırır. Ancak tek nokta bozulması zafiyeti bir darboğazdır.

9.10 Aktif Güvenlik

IDS tanımlayabildiği bir saldırıyla karşılaştığında buna değişik yöntemlerle karşılık verebilir. Bu işlemler arasında şunları sayabiliriz:

*Güvenlik duvarı ayarlarını değiştirmek:*IDS ağın trafiğini kontrol eden Güvenlik duvarı ile uyumlu çalışabiliyorsa, onu yeniden ayarlayarak saldırının yapıldığı kaynaktan gelen trafiğin belirli bir süre için durdurulmasını sağlayabilir.

*Sesli uyarı:*Sistem başında bulunan operatöre sesli veya görsel bir uyarı verilebilir.

*SNMP mesajı:*Ağ yönetim cihazlarına mesaj yollanabilir.

Sistem Mesajı: NT veya Unix sistem kayıtlarına saldırı hakkında mesajlar eklenebilir.

*E-posta:*Bir diğer uyarı ve raporlama yolu olarak saldırı hakkında belirli kişilere bilgi vermek amacıyla elektronik posta atılabilir.

*Raporlama:*Yazıcı gibi sistemlerle hardcopy bir kayıt tutulabilir. Özellikle IDS saldırılara maruz kalabilecekse bu tür bir raporlama bilgi kayıplarını önleyecektir.

Saldırıyı Log'lama: Saldırı hakkında zaman, kaynak, varış adresleri, protokol ve port bilgileri gibi kayıtlar tutulabilir.

Kanıt toplama: Saldırı ile ilgili daha fazla bilgi edinilmeye çalışılabilir. Saldırının kaynağına traceroute yapılabilir. Saldırıya ait işlenmemiş paketler tutulabilir.

Yardımcı Program Çağırma: IDS sistemini daha fazla meşgul etmemek için saldırıya ait bilgileri toplamak ve diğer işlemler için ayrı bir process çağrılabilir.

Bağlantıyı kapatma: Açılan TCP bağlantısına FIN paketleri yollanarak bağlantının kopması sağlanabilir.

9.11 IDS, Güvenlik Duvarı ve Diğerleri

Güvenlik duvarı: Genelde ağ güvenliğinin ilk ve (bazen tek) yapı taşı olarak güvenlik duvarları görülür. Oysa ağda bulunan güvenlik duvarı'nın nasıl geçilebileceği bulunduktan sonra sadece güvenlik duvarı bulunan bir ağ oldukça kolay bir hedef olacaktır. Bu konuda en iyi yaklaşım sistemlerin düzgün konfigüre edildiği, IDS'lerin ve diğer güvenlik sistemlerinin tam çalıştığı bir yapıda en son güvenlik duvarı'na güvenmektir. Böylece tüm sistemlerin gözden kaçırdığı bir durumda güvenlik duvarı bize temel güvenlik sınırını oluşturacaktır.

Aynı zamanda saldırıların %80'nin içeriden kaynaklandığı düşünüldüğünde sadece bir güvenlik duvarına güvenmenin yetersizliği anlaşılmaktadır.

Zayıflık Tarayıcıları: Sistemde bulunabilecek zayıflıkları taramak bunların ilerde olası bir saldırıda kullanılmadan önce düzeltilmelerini sağlaması açısından oldukça önemlidir. Bu tür taramalar otomatik araçlarla yapılabildiği gibi daha detaylı analizler de gerekli olabilir.

VPN: Ağ Trafiğini ek güvenlik mekanizmalarıyla koruyan VPN yapıları dışardan gelebilecek saldırılardan network'ü bir ölçüde yalıtacaktır. IPsec gibi şifreleme ve kimlik doğrulama sağlayan VPN çözümleri ağa uzaktan erişimlerde güvenlik sağlayacaktır.

Şifreleme: Önemli dokümanların uç birimlerde bile şifreli olarak tutulması, emaillerin şifreli olarak kullanılması gibi alışkanlıklar sistem kaynaklarının ele geçirilmesi durumunda bile saldırganların önemli bilgilere erişimini engelleyecektir.

Honeypot: Saldırganların tespitinde sık olarak kullanılan honeypot'lar çeşitli sistem servislerini çalıştırdıkları izlenimi vererek saldırganları üzerlerine çeken yapılardır. Bunlar saldırganların tekniklerini, kaynakları ve amaçlarını öğrenmekte oldukça etkili yapılardır**.**

9.12 Ticari Nüfuz Tespit Sistemleri iyi ve kötü yönleri

Real Secure – Internet Security Systems (ISS)

Güvenli ve dağıtık bir mimarisi vardır. Saldırı tespiti çoklu tespit motorları ile yapılır. Herbir motor, farklı ağlara dağıtılabilir. Ve merkezi bir yönetim konsolundan gözlenebilir.

İyi Yönleri

- Doğru saldırı tespiti
- Esnek güvenli dağıtık yönetim.
- Kullanışlı bir GUI
- İlginç oturum kayır tool'u ile kaliteli raporlama.

Kötü Yönü

- Kullanıcı saldırı tanımlayamaz.

NFR – Network Flight Recorder

Kolayca anlaşılarak kullanılabilen iyi bir saldırı tespit sistemidir. NFR, N-kodu denilen bir skript dili ile konfigüre edilen ve kontrol edilebilen bir saldırı tesbit ssitemidir.

İyi Yönleri

- N-kodu trafik analizini yapmaya imkan verir.
- Yüzde yüz tanıma için güçlü dil
- Grafik destekli zengin özellikli raporlama.
- Java tabanlı GUI ile herhangi bir yerde çalıştırılabilir.

Kötü Yönleri

- N-kodunun öğrenilmesi
- Dağıtık yönetim yok
- SNMP ve reaktif fonksiyonlar kullanılmaz.

SALDIRI ANALİZLERİ

A. Port Scan

16:20:56.592924 193.140.144.68.4084 > 193.140.72.10.44767: udp 1

16:20:56.970312 193.140.144.68.4116 > 193.140.72.42.44767: udp 1

16:20:57.113190 193.140.144.68.4126 > 193.140.72.52.44767: udp 1

16:20:57.141546 193.140.144.68.4128 > 193.140.72.54.44767: udp 1

16:20:57.382976 193.140.144.68.4151 > 193.140.72.77.44767: udp 1

16:20:57.483436 193.140.144.68.4158 > 193.140.72.84.44767: udp 1

16:20:57.492848 193.140.144.68.4161 > 193.140.72.87.44767: udp 1

16:20:58.097130 193.140.144.68.4200 > 193.140.72.126.44767: udp 1

16:20:58.144901 193.140.144.68.4202 > 193.140.72.128.44767: udp 1

16:21:00.932829 193.140.144.68.4320 > 193.140.72.246.44767: udp 1

16:21:00.991974 193.140.144.68.4326 > 193.140.72.252.44767: udp 1

16:21:01.023088 193.140.144.68.4328 > 193.140.72.254.44767: udp 1

1-İz Kaynağı: Dış Network

2-Tanım: Kaynak IP hedef network üzerinde pek çok makineyi taramaktadır. Muhtemelen taradığı port üzerinde çalışan bir arka kapı aramaktadır**.**

B. TraceRoute

10:01:05.215067 3.4.5.6.35232 > 139.179.11.11.33435: udp 12 [ttl 1]

10:01:05.233197 3.4.5.6.35232 > 139.179.11.11.33436: udp 12 [ttl 1]

10:01:05.236577 3.4.5.6.35232 > 139.179.11.11.33437: udp 12 [ttl 1]

10:01:17.993377 3.4.5.6.35232 > 139.179.11.11.33453: udp 12

10:01:18.025531 139.179.11.11 > 3.4.5.6: icmp: 139.179.11.11 udp port 33453 unreachable [tos 0xc0]

10:01:18.028065 3.4.5.6.35232 > 139.179.11.11.33454: udp 12

10:01:18.077717 139.179.11.11 > 3.4.5.6: icmp: 139.179.11.11 udp port 33454 unreachable [tos 0xc0]

10:01:18.087372 3.4.5.6.35232 > 139.179.11.11.33455: udp 12

10:01:18.127293 139.179.11.11 > 3.4.5.6: icmp: 139.179.11.11 udp port 33455 unreachable [tos 0xc0]

1-İz Kaynağı: İç Network

2-Tanım: Kaynak IP dışarıdaki bir makineye traceroute yapmaktadır. Bu bir saldırı değildir. Ancak bağlantı yolu hakkında bilgi alınmaya çalışılıyor olabilir ve yinede kaydedilmesi güvenlik açısından önem taşıyabilir**.**

C. SYN FLOOD

23:31:33.894939 10.30.10.1.2346 > 192.168.4.99.telnet: S

23:31:33.894987 10.30.10.1.2346 > 192.168.4.99.telnet: S

23:31:33.895055 10.30.10.1.2346 > 192.168.4.99.telnet: S

23:31:33.895124 10.30.10.1.2346 > 192.168.4.99.telnet: S

23:31:33.895193 10.30.10.1.2346 > 192.168.4.99.telnet: S

23:31:33.895258 10.30.10.1.2346 > 192.168.4.99.telnet: S

1-İz Kaynağı: Test Network

2-Tanım: Tipik bir SYN flood. Saldırılan makinanın telnet servisine servis dışı saldırısı yapılıyor.

D. SMURF

14:41:39.627866 43.12.87.118 > 43.12.86.122: icmp: echo reply

14:41:39.627977 43.12.87.117 > 43.12.86.122: icmp: echo reply

14:41:39.628273 43.12.87.186 > 43.12.86.122: icmp: echo reply (DF)

14:41:39.629431 43.12.87.6 > 43.12.86.122: icmp: echo reply

14:41:39.629528 43.12.87.79 > 43.12.86.122: icmp: echo reply

14:41:39.632340 43.12.87.118 > 43.12.86.122: icmp: echo reply

14:41:39.632762 43.12.87.117 > 43.12.86.122: icmp: echo reply

14:41:39.633106 43.12.87.10 > 43.12.86.122: icmp: echo reply

14:41:39.633235 43.12.87.11 > 43.12.86.122: icmp: echo reply

14:41:39.633363 43.12.87.186 > 43.12.86.122: icmp: echo reply (DF)

14:41:39.634608 43.12.87.221 > 43.12.86.122: icmp: echo reply

1-İz Kaynağı: Test Network

2-Tanım:	Farklı kaynaklardan aynı makineye ping reply'ları geliyor. Dağıtık bir saldırı olan SMURF olabilir. Saldırgan, saldırılan makinadan geliyormuş gibi bazı networklere ping request'leri yollar ve bu networklerin yolladığı cevaplar hedef makineyi servis dışı bırakabilecek yoğunlukta olabilir.

E. NMAP

14:18:44.086517 192.168.4.99.3842 > 192.168.4.17.netview-aix-5: S

14:18:44.086523 192.168.4.99.3843 > 192.168.4.17.qmtp: S

14:18:44.086528 192.168.4.99.3844 > 192.168.4.17.948: S

14:18:44.086532 192.168.4.99.3845 > 192.168.4.17.tcpnethaspsrv: S

14:18:44.086537 192.168.4.99.3846 > 192.168.4.17.dbbrowse: S

14:18:44.086542 192.168.4.99.3847 > 192.168.4.17.nsc-ccs: S

14:18:44.086547 192.168.4.99.3848 > 192.168.4.17.857: S

14:18:44.086552 192.168.4.99.3849 > 192.168.4.17.dsp3270: S

14:18:44.086556 192.168.4.99.3850 > 192.168.4.17.26: S

14:18:44.086561 192.168.4.99.3851 > 192.168.4.17.dixie: S

14:18:44.088619 192.168.4.99.3852 > 192.168.4.17.tns-cml: S

14:18:44.088623 192.168.4.99.3853 > 192.168.4.17.hdap: S

1-İz Kaynağı: Test Network

2-Tanım:	Kaynak adresi saldırılan makine üzerinde port taraması yapmaktadır. Aslında bu çıktı karşı sistem hakkında imza çıkartmaya yarayan unix komutu "nmap" komutuyla alınmıştır. Saldırıdan önce karşı sistem hakkında bilgi alma yöntemlerinden biri olan port taraması IDS tarafından mutlaka tespit edilebilmeli ve sistem uyarılmalıdır.

10 BİYOMETRİK GÜVENLİK SİSTEMLERİ(Biometric Security Systems)

Biyometrik tanıma, datayı kodlama veya şifreleme /deşifreleme için vücut özelliklerini kullanan bir süreçtir. Parmak izi, retina ve iris, avuç içi izi,yüz yapısı ve ses tanıma günümüzde sıkça araştırılan biyometrik tanıma teknikleridir. Bu özellikler her şahsa özel olduğu için biyometrik yöntemler hırsızlık ve dolandırıcılığa kısmen de internet üzerinde ticarete cevap olabilecektir.Bu yeni teknolojinin özelliği parola veya PIN numarası yerine çalınamayan kaybolmayan veya yeniden oluşturulamayan biyometrik özelliğin kullanılmasıdır. Bir endüstri uzmanına göre, Kullanıcının erişim haklarına sahip olabilmek için onun parmağını kesmedikçe, biyometrik tanıma erişim kontrolü için mükemmel bir yöntemdir.

Tablo 8.1 'de ifade edildiği üzere biyometrik yöntemleri kullanmak için oldukça fazla seçenek bulunmaktadır.Tablo 10.1 'de verilmiş olan biyometrik yöntemler bugüne kadar kararlılığı test ve kabul edilmiş olan yöntemlerdir.Bunlar için daha doğru bir ifade kullanılması gerekirse bu yöntemler bilinen biyometrik yöntemlerdir.Bu yöntemlerin ötesinde halihazırda araştırma aşamasında olan bir çok biyometrik yöntemde bulunmaktadır.Bunlar arasında en dikkat çekici olanlarından birisi insanların kulak yapılarını algılayıp tanıyan sistemlerdir.Bu da göstermektedir ki insanların kendilerine has olan bütün uzuvları biyometrik tanımlayıcı olarak kullanılabilir. Bu da biyometrik sistemlerin ana amacını oluşturmaktadır.

Biyometrik Yöntem	Hata Oranı
Retina Tarama(ışığı ileten damarlar)	1:10.000.000
İris Tarama(göz rengini veren bölge)	1:131.000
Parmak İzi Tarama	1:500
El Geometrisi Tarama	1:500
İmza(Yazı Yazma) Tarama	1:50
Ses Tarama	1:50
Yüz Tarama	Veri Yok
Vascular Patterns	Veri Yok

Tablo 10.1. Biyometrik Yöntemlerin hata oranları

10.1 Biyometriğin Tarihçesi

Bugünün biyometrik tanıma süreçleri geçmişteki bazı yaygın biyometrik tekniklerinden türetilmiştir. Doğal olarak en yaygın olan ve suçluların tespitinde, çalışanların lisanslarında kullanılan parmak izidir. Bu süreç, yazılı kopya üzerinden manuel olarak haftalarca süren bir inceleme sonucunda bazen de yanlış sonuçlar vererek gerçeklenirdi. Bilgisayar teknolojisinin gelişmesiyle, bazı kuruluşlar, arşivlerini elektronik olarak tutmaya ve parmak izi eşleştirme sürecini daha hızlı ve doğru olarak yapmaya başladılar. Parmak izi tanıma sürecinin sonraki adımı sadece kişileri tanımak değil aynı zamanda belirli yerlere erişimlerini denetlemektir. Bu teknik ile birlikte biyometrik tanıma koddaki bilginin çözümlenmesiyle, kişilerin belirli yerlere girişlerini sağlayacak biyometrik parola olarak kullanılmaya başlamıştır.

10.2 Biyometrik Tanıma Nasıl Çalışır?

Tanıma, iletilen veya bir veritabanında saklanan bilginin anlaşılmasına yardım eden bir matematiksel süreçtir, ve bir kripto sistemini belirleyen üç ana faktör vardır, matematiksel süreç

veya algoritmanın karmaşıklığı, mesajı anlamakta kullanılan tanıma özelliğinin uzunluğu, anahtar yönetimi olarak bilinen anahtarın emniyetli saklanması.
Algoritmanın karmaşıklığı, ters işlem ile doğrudan bağıntısı olması nedeniyle önemlidir. Bazıları tanımanın bu alanının kolayca kırılabileceğini düşünür, bununla birlikte kripto sistemleri saldırılara karşı zafiyet olan en az bu üç faktörü içerecek şekilde iyi tasarlanır.

Mesajı anlamakta kullanılan tanıma anahtarının uzunluğu, tanıma sürecinin ikinci en önemli parçasıdır. Daha kısa olan anahtarlar brute force saldırılarına karşı daha zayıftır. Bunun anlamı bir kişinin hesaba girebilmek için bütün mümkün parola kombinasyonlarını denemesi demektir. Parola veya PIN numarası gibi biyometrik olmayan tanıma süreçlerinde, anahtarın uzunluğuna bağlı olarak enformasyon yetkisiz kişilerce erişilmeye karşı güvensizdir.Örneğin üç karakterlik bir şifre, mümkün olan permutasyonlar bakımından on karakter uzunluğundaki bir şifreye göre daha zayıftır. Mevcut bilgisayar gücü ile, 64 karakter uzunluğundaki bir anahtarın bulunabilmesi için gerekli permutasyonlarının hesabı dört yüz yıl alabilecektir Biyometrik tanıma, personel tanımlayıcısı ile normal anahtar karakterlerinin yerlerini değiştiren bir standart karakter uyuşturma yapar. Bu biyometrik anahtar olmadan veriye erişilemez.

Anahtarların emniyetli olarak saklanması tanıma sürecinin en zayıf yönüdür. En kolay olarak gözüken saklama süreci en zor işlemdir çünkü parola veya PIN numarası kaybolabilir veya çalınabilir. İyi tanıma özelliği çok uzun olan ve hatırlanamayan parolaların, kağıtta akıllı kartlarda, veya disketlerde saklanarak yetkisiz kişilerin erişimi önlenebilir. Biyometrik tanıma sistemleri anahtarın kaybetme veya çalınma olmadan taşınmasını mümkün kılar.

Bütün biyometrik teknolojiler, bilgi elde etme, özellik çıkartma, karşılaştırma ve uyuşma/uyuşmama olmak üzere dört adım olarak benzer şekilde çalışırlar. Bilgi elde etme aşamasında, sistem uygun teknik ile bir görüntü veya bilgi elde eder. Bilgi veya görüntü elde edildikten sonra, işleme amacıyla, yerelleştirilmelidir. Yerelleştirme, özellik çıkartma aşamasında olur. Özellik çıkartma aşamasında, konu ilgisi olmayan enformasyon atılır ve konu ile ilgili olan enformasyon, alınarak bir biyometrik şablon şeklinde saklanır. Bir tanıma işleminde, bir yeni bilgi/görüntü alınarak saklanan biyometrik şablon ile karşılaştırılır. Bu karşılaştırmanın sonucu, eğer yeni alınan bilgi şablon ile aynı ise uyuşma var, değil ise uyuşma yoktur sonucuna varılır.

Bu dört biyometrik işlem iki farklı moddaki biyometrik tanımaya eşit olarak uygulanır., tanıma ve doğrulama. Bu iki yaklaşım arasındaki çok önemli fark, sistemin yapması gereken karşılaştırmalardır. Tanıma, bire –çok yaklaşımı ile, bir bilgi çoklu şablon ile karşılaştırılır, oysa doğrulamanın amacı, kişinin erişim hakkının olup olmadığının anlaşılmasıdır. Doğrulama, saklanan şablon ile yeni bilgi karşılaştırılarak, bire-bir yaklaşımını kullanır. Genellikle, doğrulama modu , bire-bir karşılaştırma olması nedeniyle daha hızlıdır.

Biyometriğin gerçeklenmesi sırasında, seçilecek dört farklı karar planı vardır. (a) Tek biyometrik plan, avuç içi gibi tek biyometrik görüntüden,şahsı tanımlama veya doğrulama yapar. (b) Çoklu biyometrik plan, kişinin çoklu testten geçirilmesi nedeniyle daha güvenlidir.(retina taramasından sonra ses denetimi gibi) Daha fazla biyometrik testten geçilmesi gerektiği için, yanlışlıkla kabul etmeme olasılığı daha fazla olacaktır. (c) Ağırlıklı bir biyometrik plan,farklı biyometrikleri, çoklu biyometrik plandakine benzer şeklide birleştirir. Bununla birlikte, ağırlıklı biyometrik plan, biyometrik ağırlıkları kullanıcıların,yanlış kabul veya ret edilme olasılığını optimize etmek için uygular. (d) Katmanlı biyometrik plan ise, çoklu biyometrik ve ağırlıklı biyometrik plana benzeyen en güvenli plandır. Bununla birlikte, katmanlı biyometrik planda, birkaç teknoloji birbirleriyle iletişim kuracak şekilde birleştirilir. Eğer bir biyometrik parça değişirse, sonraki biyometrik üzerine daha katı doğrulama uygulanacaktır.

Biyometrik tanıma tekniklerinin temelinde örüntü tanıma yöntemleri vardır. Bu nedenle bölüm 8.3'de örüntü tanıma teknikleri açıklanacaktır.

10.3 Örüntü Tanıma Teknikleri

10.3.1 Giriş

Örüntü Tanıma, gereksiz detaylardan arındırılmış olan giriş datasından çıkartılan anlamlı özellikler yardımıyla teşhis sınıflarına ayrılan verinin sınıflandırılmasıdır.

Görüntü, geçici mantıksal gibi değişik örüntü sınıfları mevcuttur. Geniş bir yorumlama ile örüntü tanımayı birçok akıllı faaliyette kullanabiliriz. Tek bir teorisi olmayan örüntü tanıma geniş çaptaki problemin çözümünde kullanılabilir. Bununla birlikte birkaç standart model aşağıda özetlenmiştir.

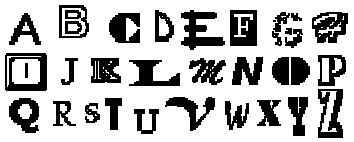
- İstatistiksel veya bulanık örüntü tanıma
- Sentetik veya yapısal örüntü tanıma
- Bilgi tabanlı örüntü tanıma(Yapay sinir ağları, Uzman sistemler)

Burada istatistiksel yaklaşım ile kendimizi sınırlandıracağız. Örüntü tanımayı, bir girişi bir sınıfa atayan sınıflandırma olarak göreceğiz.. Problemi böyle sınırlamakla ihtiyaçlarımızı gören bazı yararlı teknikleri geliştirecek ve aşağıdaki temel kavramlar üzerinde yoğunlaşacağız:

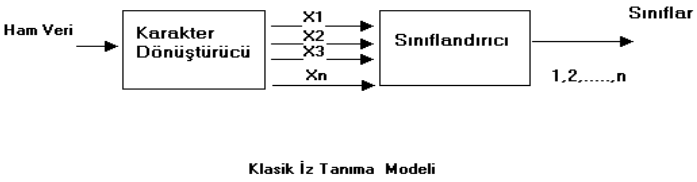
- Sınıflandırma
- Özellikler
- Özellik vektörleri
- Standart sınıflandırma modelleri

10.3.2 Sınıflandırma Modeli

Görsel örüntü ile çalıştığımızı ve Roman alfabesinin 26 harfini temsil eden örüntüyü bildiğimizi kabul edelim. Buradan örüntü tanıma problemini, giriş verisini 26 sınıftan birisine atama olarak ifade edebiliriz.(Şekil 10.1) Genelde girişin sınıf 1 veya Sınıf 2 veya .. veya …Sınıf c 'ye ait olduğu şeklinde kendimizi sınırlayacağız..



Sekil 10.1. Harflerden olusan Görsel örüntü



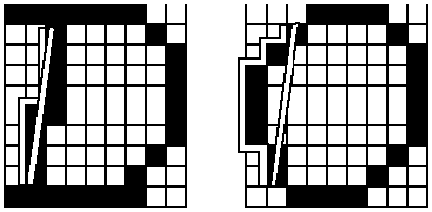
Şekil 10.2. Örüntü(iz) tanıma modeli

Daha ileriye giderek, görsel girişi sayısal hale getirmek için bir kamera kullandığımızı ve bir karakteri parlaklık değerlerinin dizisi olarak ayrıştırdığımızı kabul edelim. Bilgisayar bu veriyi nasıl sınıflandıracaktır. Belli bir yaklaşım, girişi, her bir sınıf için standart bir örüntü ile karşılaştırmak ve en iyi uyuşan sınıfı seçmektir. Bu yaklaşımdaki açık problem neyin karşılaştırılacağı ve uyuşmanın mertebesini ölçmenin söylenmeyeceğidir.(Şekil 10.2.)
Aynı sınıfa ait olan girişlerin, farklı sınıflardaki örüntüler arasındaki farklılığa göre değişkenliği örüntü tanıma problemlerini böyle karmaşıklaştırır. Bu problemin üstesinden gelmenin bir yolu karakteristik özelliklerin araştırılmasıdır.

10.3.3 Özellikler

Bir nesne veya bir olayı sınıflandırmanın tek yolu onun karakteristik özelliklerinin veya belirleyici niteliklerinin ölçülmesidir. Örneğin yazılı bir harfi sınıflandırmak için onun alan ve çevresini bilmek faydalı olacaktır. Onun alanının çevresinin karesine oranı ile onun sıkılığını ölçebilirdik.Onun yatay eksene göre üst ve altta kalan kısımlarının alanlarını karşılaştırarak simetrikliğini ölçebiliriz.(En iyi ölçmenin simetriklik olduğu düşünülebilir.)

Bazı özellikler önemli küçük farklara duyarlı olabilir. Örneğin Şekil 10.3'te gösterilen "D" harfini "O"'dan ayırt etmek için sol tarafın düzlüğü ölçülebilir, belki de düz çizgi farkının yay uzunluğuna oranı ölçülebilir Açıkçası, çözülmesi gereken önemli bir özellik olan belirleyici niteliklerin tasarımı bir bilimden çok sanattır.



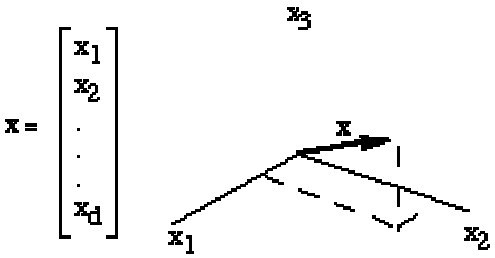
Şekil 10.3: D ve O harflerine ait görsel veri

10.3.4 Belirleyici Özellik Vektörleri

Herhangi bir nesne veya olayı sınıflandırmak için sıkça belirleyici özelliklerin sabit bir kümesi elde edilir. Örneğin her zaman,.

x_1 = alan
x_2 = çevre
...
x_d = yay uzunluğu / Düz çizgi uzaklığı
her zaman ölçülebilir.

Bu durumda, belirleyici özellik kümesini, x belirleyici özellik vektörü olarak düşünebiliriz, burada x, d boyutlu bir sütun vektörüdür. Şekil 10.4 de gösterilmiştir.



Şekil 10.4: Özellik vektörü

Benzer olarak, x'i d boyutlu belirleyici özellik uzayında bir nokta olarak düşünebiliriz.

10.4 Standart sınıflandırma modelleri.

10.4.1 Klasik Model

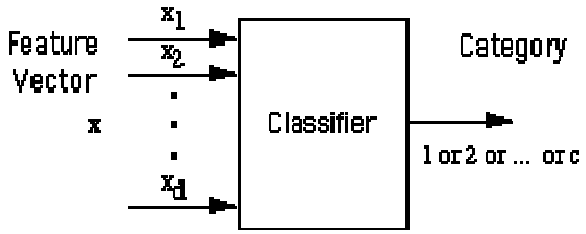
Aşağıdaki klasik model örüntü tanıma için önde gelir.

Belirleyici özellik çıkartıcı olarak adlandırılan bir sistem veya program, bir özellik vektörü olan x'in elemanlarına karşılık gelen belirleyici özellikleri x_1, x_2, ..., x_d olan d sayısal kümesini belirlemek için ham veriyi işler. Sınıflandırıcı denilen bir sistem veya program, x'i alır ve Sınıf 1 sınıf 2 , , sınıf c 'den birine atar.

Belirleyici özellik çıkartıcının tasarımı çoğunlukla probleme bağlıdır. İdeal belirleyici özellik çıkartıcı aynı sınıftaki bütün örüntüler için aynı x özellik vektörünü, farklı sınıftaki örüntüler için ise farklı özellik vektörünü üretmelidir. Pratikte, farklı girişler, belirleyici özellik çıkartıcı tarafından farklı özellik vektörü üretilmesin sağlar, fakat sınıf içindeki değişkenliğin sınıf arasındakine göre küçük olmasını bekleriz.

Bu noktada, belirleyici özellik çıkartıcının tasarımcısının yapabileceğinin en iyisi ile işini tamamladığını kabul ederiz, ve özellik vektörü örüntüleri ayırt etmek için gerekli olan bilgiyi içerir. Verilen belirleyici özellik kümesinden sınıflandırıcıyı tasarlamak bizim işimizdir.

10.4.2 Basit Sınıflandırıcılar.



Şekil 10.5: Basit sınıflandırıcı

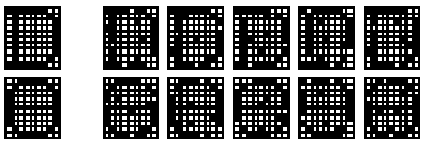
Bir sınıflandırıcı tasarlama yaklaşımı için en az iki yol vardır:

- Makul bir çözümün varsayımı ve onu probleme uydurulması
- Problemin matematik modelinin çıkartılması ve en iyi sınıflandırıcının üretimi

Daha çok sezgisel olan ilk yöntem pratikte daha çok kullanılır, ve bizim ele alacağımız yaklaşımdır. Basit bir çözüm ile başlayacağız, karakteristiklerinin analizi, zayıf yönlerin belirlenmesi, ve sadece gerektiği şekilde karmaşıklaştırma.. Bu bölümde aşağıdaki kavramlar üzerinde duracağız:

- Şablon Uyuşturma(Template matching)
- En az mesafe sınıflandırıcılar(Minimum-distance classifiers)
- Metrikler(Metrics)
- İç Çarpımlar(Inner products)
- Doğrusal farklılıkların anlaşılması(Linear discriminants)
- Karar sınırları(Decision boundaries)

10.4.2.1 Şablon Uyuşturma(Template Matching)



Şekil 10.6: Şablon Uyuşturma

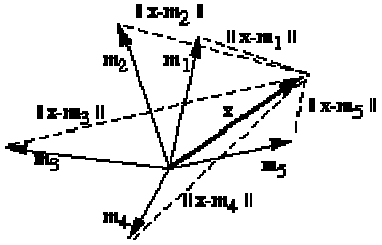
Şablon uyuşturma örüntü sınıflandırma için doğal bir yaklaşımdır. Örneğin Şekil 10.6'da gösterilen gürültülü "D" ve "O" yu düşünelim. Gürültüsüz versiyon şablon olarak sol tarafta gösterilmiştir. Gürültülü örneklerin birisini sınıflandırmak için, onu iki şablon ile karşılaştırmak gerekir. Bu işlem aşağıdaki yöntemlerden birisi ile yapılabilir:

- Uyuşmaların miktarını say(uyuşan siyahlar siyah, uyuşan beyazlar ise beyaz). En fazla sayıda uyuşan sınıfları ayıkla. Bu en fazla karşılıklı ilişki yaklaşımıdır.
- Uyuşmayanların miktarını say (Siyah yerde beyaz, beyaz yerde siyah olmalı). En az sayıda uyuşmayanların olduğu sınıfları ayıkla. Bu en az hata yaklaşımıdır.

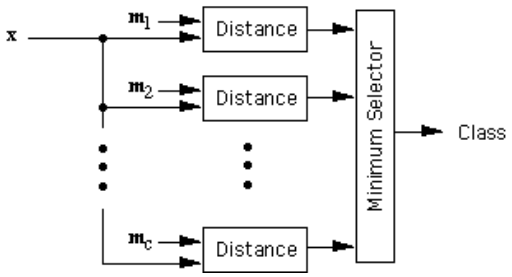
Şablon uyuşturma , eğer farklılıklar sınıf içinde kalırsa iyi çalışır. Açıkça, bu örnekte karakterlerde öteleme, dönme, kırpma, çarpıklık, genişleme veya, büzülme gibi başka bozukluk olmadığı için yöntem çalışır. Yöntem bütün problemlerde çalışmayacaktır fakat uygun olduğu zaman çok verimlidir. Aynı zamanda kullanışlı şekilde genelleştirilebilir.

10.4.2.2 En küçük Mesafe Sınıflandırıcılar(Minimum-Distance Classifiers)

Şablon uyuşturma matematiksel olarak kolaylıkla ifade edilebilir. **x,** bilinmeyen giriş için ayırt edici özellik vektörü olsun ve $\mathbf{m}_1$, $\mathbf{m}_2$, ..., $\mathbf{m}_c$ c sınıfları için şablonlar olsun.(i.e., mükemmel gürültü de ayrılmış özellik vektörleri).Buradan **x** 'in $\mathbf{m}_k$ Ya göre uyuşma hatası;
$\| \mathbf{x} - \mathbf{m}_k \|$. ile verilir.
Burada $\| \mathbf{u} \|$ 'ya **u** vektörünün **norm** 'u denir.Bir en küçük hata sınıflandırıcısı $\| \mathbf{x} - \mathbf{m}_k \|$ 'yı k = 1 den c ye kadar hesaplar ve bu en küçük hataya göre sınıfı seçer. $\| \mathbf{x} - \mathbf{m}_k \|$ aynı zamanda **x** 'den $\mathbf{m}_k$'ya kadar uzaklık olduğu için, buna en küçük mesafe sınıflandırıcısı denir. Açıkça bir şablon uyuşturma bir en küçük mesafe sınıflandırıcısıdır Şekil 10.7 ve Şekil 10.8.



Şekil 10.7: En Küçük mesafe sınıflandırıcısı vektörsel gösterilim



Şekil 10.8 :En küçük mesafe sınıflandırıcısı blok diyagram

10.4.2.3 Metrikler(Metrics)

$\| \mathbf{u} \|$ normunu tanımlamak için birden çok yol vardır ve bunlar mesafe ölçümü için farklı yollara dolayısıyla farklı metriklere karşılık gelir. Çok bilinen ik tanesi aşağıda verilmiştir.

Öklid(Euclidean) metriği: $\| \mathbf{u} \| = \text{sqrt}(u_1^2 + u_2^2 + ... + u_d^2)$

Manhattan (or taxicab) metriği: $\| \mathbf{u} \| = |u_1| + |u_2| + ... + |u_d|$

Uyuşmazlıkların sayılarak karakterlerin sınıflandırıldığı şablon uyuşturma örneğimizde, kapalı olarak Manhattan metriğini kullanıyorduk. Bu notların devamında ya Euclidean mesafe veya bazen de Mahalanobis mesafesi denilen ve Şekil 10.9'da gösterilen metriği kullanacağız..

- Sabit Euclidean mesafelerinin sınırları dairelerdir. (veya küreler)
- Sabit Manhattan mesafelerinin sınırları karelerdir. (veya kutular)
- Sabit Mahalanobis mesafelerinin sınırları elipslerdir. (veya elipsoidler)

Şekil 10.9 :Değişik metriklerin gösterilimi

10.4.2.4 İç Çarpımlar(Inner Products)

En küçük mesafe sınıflandırıcılarını küçük bir doğrusal cebir kullanarak kolaylıkla analiz edebiliriz.. $x_1, x_2, ... , x_d$ 'den oluşan d sütun vektörünü temsil etmek için **x** sembolünü kullandık. **transpose operatörünü** ' kullanarak **x** sütun vektörünü **x**' satır vektörü şekline dönüştürdük.

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ x_d \end{bmatrix} \qquad \mathbf{x}' = [x_1 \; x_2 \; ... \; x_d]$$

iki sütun vektörü **x** ve **y** 'nin iç çarpımı ;

$$\mathbf{x}'\mathbf{y} = x_1 y_1 + x_2 y_2 + ... + x_d y_d = \sum_{k=1}^{d} x_k y_k$$

ile tanımlanır. Böylece **x** 'in normu (Euclidean metriği kullanılarak) aşağıdaki şekilde verilir.

$\| \mathbf{x} \| = \text{sqrt}(\mathbf{x}' \mathbf{x})$.

İç çarpımların bazı ilave önemli özellikleri aşağıdadır.

$\mathbf{x}' \mathbf{y} = \mathbf{y}' \mathbf{x} = \| x \| \| y \| \cos(\ \mathbf{x}$ ve $\mathbf{y}$ **arasındaki açı** $)$

$\mathbf{x}' (\mathbf{y} + \mathbf{z}) = \mathbf{x}' \mathbf{y} + \mathbf{x}' \mathbf{z}$.

x ve y nin iç çarpımı aralarındaki açı sıfır olduğu zaman en büyüktür. Bazen $\mathbf{x}' \mathbf{y}$ nin $\mathbf{x}$ ve $\mathbf{y}$ arasındaki korelasyon olduğunu söyleriz, ve $\mathbf{x}$ ve $\mathbf{y}$ noktaları aynı yönde ise korelasyon en büyüktür.Eğer $\mathbf{x}' \mathbf{y} = 0$ ise, $\mathbf{x}$ ve $\mathbf{y}$ vektörlerinin ortogonal veya korelasyonsuz olduğu söylenir

10.4.2.5 Doğrusal farklılıkların anlaşılması(Linear Discriminants)

Bir özellik vektörü olan $\mathbf{x}$'i sınıflandırmak için minimum mesafe sınıflandırıcısını kullandığımız zaman, $\mathbf{x}$ 'ten $\mathbf{m}_1$, $\mathbf{m}_2$, ..., $\mathbf{m}_c$ şablonlarına olan mesafeyi ölçtüğümüzü hatırlayalım ve , **x'i** en yakın şablon sınıfına atayalım. $\mathbf{x}$ ten $\mathbf{m}_k$ 'ya olan Euclidean mesafesini açıklamak için iç çarpımı kullanarak,

$$\| \mathbf{x} - \mathbf{m}_k \|^2 = (\mathbf{x} - \mathbf{m}_k)' (\mathbf{x} - \mathbf{m}_k)$$

$$= \mathbf{x}'\mathbf{x} - \mathbf{m}_k'\mathbf{x} - \mathbf{x}'\mathbf{m}_k + \mathbf{m}_k'\mathbf{m}_k$$

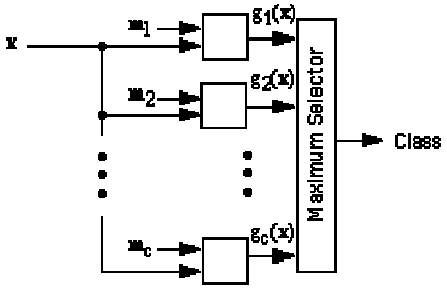
$$= -2 [\mathbf{m}_k'\mathbf{x} - 0.5\, \mathbf{m}_k'\mathbf{m}_k] + \mathbf{x}'\mathbf{x}$$

yazabiliriz.

Her sınıf dolayısı ile her k için $\mathbf{x}'\mathbf{x}$ terimi aynıdır. $\| \mathbf{x} - \mathbf{m}_k \|$,yı minimize eden $\mathbf{m}_k$ şablonunu bulmak için, $\mathbf{m}_k'\ \mathbf{x} - 0.5\ \mathbf{m}_k'\ \mathbf{m}_k$ ifadesini en büyük yapan $\mathbf{m}_k$ 'yı bulmak yeterlidir. Doğrusal farklılıkları ayrıştırma fonksiyonu g(x) 'i aşağıdaki şekilde tanımlayalım.

$g(x) = \mathbf{m}'\ \mathbf{x} - 0.5 \| \mathbf{m} \|^2$.

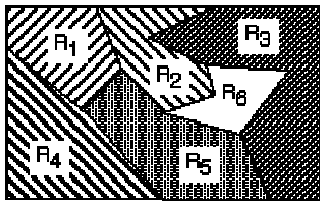
Sonra, bir minimum-Euclidean-mesafe sınıflandırıcısının $g_1(\mathbf{x})$, $g_2(\mathbf{x})$, ... , $g_c(\mathbf{x})$, c doğrusal ayrıştırma fonksiyonunu hesaplayarak bir giriş özellik vektörü $\mathbf{x}$'i sınıflandırdığını ve $\mathbf{x}$'i en büyük ayrıştırma fonksiyonuna uygun bir sınıfa atadığını söyleyebiliriz. Aynı zamanda, doğrusal ayrıştırma fonksiyonlarını, $\mathbf{x}$ ve $\mathbf{m}_k$ arasındaki korelasyonun, $\| \mathbf{m}_k \|^2$ ile temsil edilen "şablon enerji" için bir düzeltme ile birlikte hesaplanması olarak düşünebiliriz. İçerdiği bu düzeltme ile birlikte, bir minimum-Euclidean-mesafe sınıflandırıcısı, bir maksimum-korelasyon sınıflandırıcısına eşittir.Şekil 10.10.



Şekil 10.10 : Euclidean Mesafe sınıflandırıcısı

10.4.2.6 Karar Sınırları(Decision Boundaries)

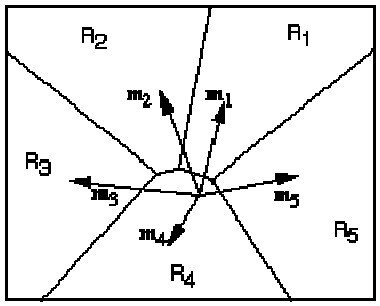
Genel olarak, bir örüntü sınıflandırıcı, bir belirleyici özellik uzayını karar bölgeleri denilen bölümlere ayrıştırır(veya parçalar). Karar bölgesindeki bütün belirleyici özellik vektörleri, aynı kategoriye atanır. Karar bölgeleri çoğunlukla basit şekilde bağlıdır, fakat; onlar iki veya daha fazla değmeyen bölgeyi içerecek şekilde çoğaltılarak bağlanabilir. Şekil 10.11.



Şekil 10.11: Karar sınırları

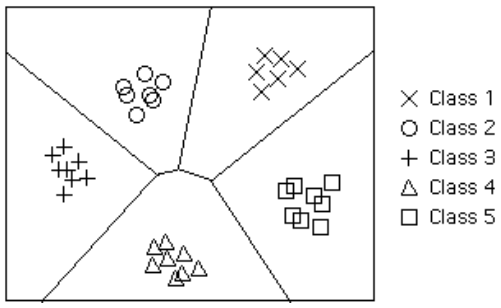
Karar bölgeleri, **karar sınırları** denilen yüzeyler tarafından ayrılırlar. Bu ayırma yüzeyleri, iki veya daha fazla kategoriyi bağlayan noktaları temsil ederler.

Bir minimum mesafe sınıflandırıcı için karar sınırları, iki veya daha fazla şablondan eşit uzaklıktaki noktalardır. Bir Euclidean metriği ile, i bölgesi ile j bölgesi arasındaki karar sınırı, $\mathbf{m}_i$ den $\mathbf{m}_j$ ye olan dikey bölmeleme çizgisinin oluşturduğu çizgi veya düzlemdir. Analitik olarak, bu doğrusal sınırlar,ayrıştırma fonksiyonlarının doğrusal olmasının bir sonucudur. (Mahalanobis metriği ile, karar sınırları elipsoid, paraboloid veya hiperboloid gibi kuadratik yüzeylerdir.)



Şekil 10.12: En yakın bölge karar sınırları

Şablona benzeyen sınıflandırılacak giriş örüntüsünün ne kadar yakın olduğuna bağlı olarak sınıflandırıcı nasıl iyi çalışır. Şekil 10.12'de çizilen örnekte, uyuşma çok yakın ve mükemmel performans beklenir. Bununla birlikte,pratikte işler böyle iyi değildir, basit sınıflandırıcıların sınırlamaları olduğu bilinmelidir.

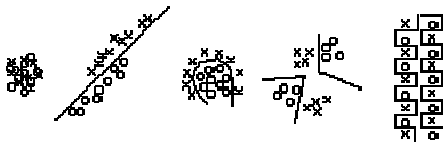


Şekil 10.13

10.4.3 Sınırlamalar(Limitations)

Eğer bir basit minimum-mesafe sınıflandırıcısı yeterli ise, daha karmaşık olan bir diğerini kullanmak için bir sebep yoktur. Bununla birlikte,böyle bir sınıflandırıcıda çok fazla hata meydana gelir. Bunu muhtemel bir kaç nedeni vardır.: Şekil 10.14.

- Ayırıcı özellik vektörleri farklı sınıfları ayırt etmek için yeterli olmayabilir.
- Ayırıcı özellikler yüksekçe ortak özellikli olabilir.
- Karar sınırları daire şeklinde olabilir.
- Veride farklı alt sınıflar bulunabilir.
- Belirleyici özellik uzayı gerçekten çok karmaşık olabilir.



Şekil 10.14

10.4.4 Mahalanobis Sınıflandırıcıları(Mahalanobis Classifiers)

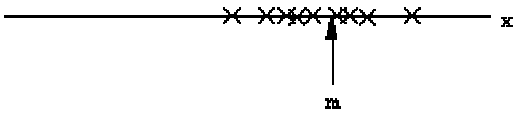
Minimum-Euclidean mesafe sınıflandırıcısının bazı basit sınırlamaları, Mahalonobis metriği kullanılarak giderilebilir. Bu, zayıf ölçekli ve/veya birbirine çok bağımlı özelliklerden kaynaklanan problemleri çözebilir.

Euclidean Metriği için uygun olan data üzerinde ölçekleme ve doğrusal transformasyonları düşünerek dolaylı şekilde Mahalonobis metriğini geliştireceğiz. Aşağıdaki konuları içerir.

- Ortalama değer ve varyans
- Ölçekleme
- Doğrusal Transformasyonlar
- Kovaryans
- Kovaryans Matrisi
- Mahalanobis metriği

10.4.4.1 Ortalama değer ve varyans

Bir x ayırt edici özelliği düşünelim. Tamamı aynı sınıfa ait n adet örüntü örneğini düşünelim. Ayırt edici özellik olan x'in x(1), x(2), ..., x(n) için farklı değerlerde olduğunu varsayalım.



Şekil 10.15: Ort. Değer.

Bu örnekleri karakterize etmek için kullanabileceğimiz m ortalama değer ve varyans v. Ortalama değer(**mean**) aritmetik ortalama veya kütle merkezidir:

$$m = [x(1) + x(2) + ... + x(n)] / n .$$

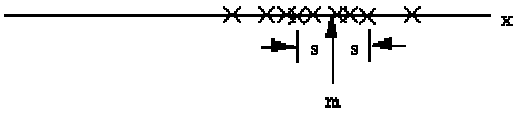
Genel olarak, eğer veri bir grubun içine düşerse, ortalama değerin az veya çok grubun içinde olmasını bekleriz. Bu ortalama değerin tipik bir büyüklüğü olduğunu gösterir. Sapma(**variance)** grubun genişliğinin tipik değerden ne kadar ayrıldığını gösteren bir ölçümüdür. Ortalama değerden

sapmaların karelerinin aritmetik ortalaması olarak tanımlanır.Tam doğru olan geleneksel tanımlama;

$v = [(x(1) - m)^2 + (x(2) - m)^2 + ... + (x(n) - m)^2] / (n - 1)$. dır.

Açıkça, m, x ile aynı boyutludur, fakat v kareli boyuta sahiptir. Varyansın karekökü RMS değeri veya standart sapma s'dir, ve x ile aynı boyutludur. Şekil 10.16

$s = sqrt(v)$.



Şekil 10.16: Ort. değer ve Standart Sapma.

Burada, ortalama değer, grubun merkezinin konumunu ölçer, standart sapma ise onun yarıçapını ölçer. Bu dağılım eğer bir normal (Gaussian) dağılımsa m ortalamasının +s ve –s civarındaki salınımlarda, yani ortalamanın +1 ve –1 standart sapması içindeki izlerin %68.26'sı belirtilen aralıkta kalmaktadır. Aynı şekilde aralığı +2s ve –2s olarak ölçeklersek izlerin %95.4'ü belirtilen aralıkta yer alacaktır.

10.4.4.2 Ölçekleme(Scaling)

Genel olarak, ayırıcı özellik için sayısal değer kullanılan birime(veya ölçeğe) bağlıdır. Eğer x bir a ölçek faktörü ile çarpılırsa ortalama değer ve standart sapma da a ile çarpılmış olur.(varyans a^2 ile çarpılır.)

Bazen verinin ölçeklenmesi arzu edilebilir, böylece sonuçtaki standart sapma birim değer alır. Bu x'i s standart sapmaya bölerek kolaylıkla yapılır. Benzer şekilde, x'ten m'ye olan mesafenin ölçümünde, sıkı olarak standart sapmaya göre anlam kazanır. x'ten m'ye Standart mesafe aşağıdaki ifade ile verilir.

$$r = \left| \frac{x - m}{s} \right|$$

r, dönüşüm ve ölçeklemeyle değişmez. Bu minimum-Euclidean- mesafe sınıflandırıcısının önemli bir genelleştirilmesini gösterir. x(i) yi I özelliği için bir değer olarak kabul edelim, m(i,j) , j sınıfı için I özellik değerinin ortalama değeri ve s(i,j) , j sınıfı için i özelliğinin standart sapmasıdır. j sınıfı için x özellik vektörü ve $\mathbf{m}_j$ ortalama vektörü arasındaki mesafenin ölçülmesinde standart mesafeyi kullandığımızı kabul edelim.

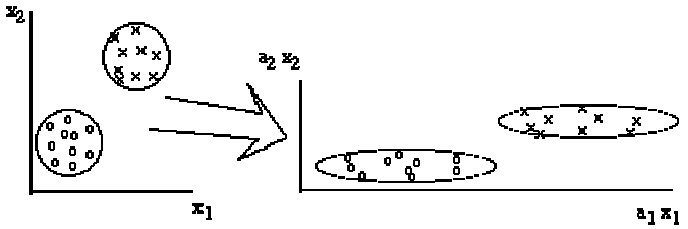
$$r(x, m_j)^2 = \left[\frac{x(1) - m(1,j)}{s(1,j)}\right]^2 + \left[\frac{x(2) - m(2,j)}{s(2,j)}\right]^2 + ... + \left[\frac{x(d) - m(d,j)}{s(d,j)}\right]^2 .$$

Bu mesafenin, ölçeklemeden bağımsız önemli bir özelliği vardır. Eğer bu yol ile mesafe ölçersek, değişik özellikler için kullandığımız birimlerin sonuçtaki mesafelere bir etkisi olmayacak ve böylece sonuç sınıflandırma üzerinde etkisi olmayacaktır. Mahalanobis mesafesi bu standart mesafenin bir genelleştirilmesidir.

10.4.4.3 Doğrusal Transformasyonlar (Linear Transformations)

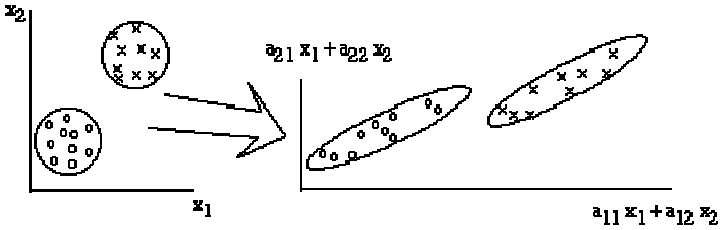
Ölçekleme bir doğrusal transformasyonun kısmi bir örneğidir. Geometrik olarak, ölçekleme, özellik uzayındaki eksenlerin genişletilmesi veya büzülmesidir. Orijinal olarak küresel olan veri

grupları elipsoidlere çekilir, burada elipsoidlerin başlıca eksenleri koordinat eksenleri ile düzene sokulur.



Şekil 10.17: Doğrusal Transformasyon

Daha genel bir transformasyon, koordinatları çektiği kadar döndürür. Orijinali küresel olan veri noktalarının grupları, eksenleri koordinat eksenlerine göre döndürülen elipsoidlere dönüştürülür. Bu ayırıcı özellik vektörünün elemanları arasındaki bir kovaryansı açıklar.



Şekil 10.18: Diğer bir doğrusal Transformasyon

Hangi amaçla küresel grupları elipsoidal gruplara dönüştürmek istediğimizi hayal etmek güçtür. Bununla birlikte, elipsoidal grupları küresel gruplara dönüştürmeyi isteyebiliriz. Bunu yapmak için kovaryansı daha iyi anlamak gerekir.

10.4.4.4 Kovaryans(Covariance)

İki ayırıcı özelliğin kovaryansı, onların birlikte değişim veya ortak değişme eğilimlerini ölçer. Burada, varyans bir ayırıcı özelliğin , ortalamasından olan sapmanın karelerinin ortalamasıdır, kovaryans ise ayırıcı özellik değerlerinin ortalamalarından olan sapmaların çarpımının ortalamasıdır.

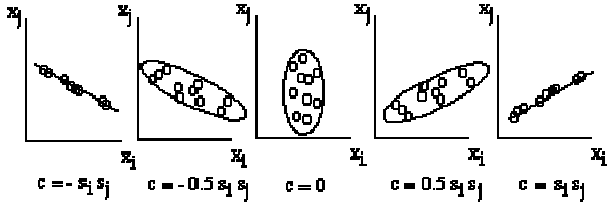
Daha emin olmak için, i ayırıcı özellik ile j ayırıcı özelliği düşünelim. i ayırıcı özelliğin n örneğinin kümesi { x(1,i), x(2,i), ... , x(n,i) } olsun ve j ayırıcı özelliğin n örneğinin kümesi { x(1,j), x(2,j), ... , x(n,j) } olsun. (Bu , x(k,i) ve x(k,j) aynı k örüntüsünün ayırıcı özeliliğidir.) Benzer şekilde,m(i) ayırıcı özellik i'nin ortalama değeri, ve m(j) de ayırıcı özellik j'nin ortalama değeri olsun. Buradan, i ve j ayırıcı özelliklerinin kovaryansı aşağıdaki ifade ile tanımlanır.

$$c(i,j) = \{ [x(1,i) - m(i)] [x(1,j) - m(j)] + ... + [x(n,i) - m(i)] [x(n,j) - m(j)] \} / (n - 1) .$$

Kovaryansın birkaç önemli özelliği vardır:

- Eğer özellik i ve özellik j birlikte artma eğiliminde ise, $c(i,j) > 0$ dır.
- Eğer özellik i ve özellik j birlikte azalma eğiliminde ise, $c(i,j) < 0$ dır
- Eğer özellik i ve özellik j bağımsız ise $c(i,j) = 0$ *
- $c(i,j) | <= s(i)\, s(j)$, burada s(i) i ayırıcı özelliğinin standart sapmasıdır.
- $c(i,i) = s(i)^2 = v(i)$

Böylece, kovaryans c(i,j) özellik i ile özellik j arasındaki bağlılığ ölçen -s(i)s(j) ve +s(i)s(j) arasındaki bir sayıdır, eğer hiç bağlılık yok ise c(i,j) = 0 dır. Kovaryans ile veri grubunun arasındaki benzerlik Şekil 10.19'de gösterilmiştir.



Şekil 10.19: Veri grubu ile kovaryans arasınaki benzerlik.

10.4.4.5 Kovaryans Matrisi(Covariance Matrix)

c(i,j) kovaryanslarının tamamı bir C kovaryans matrisinde birleştirilebilir:

$$C = \begin{bmatrix} c(1,1) & c(1,2) & \cdots & c(1,d) \\ c(2,1) & c(2,2) & \cdots & c(2,d) \\ \vdots & \vdots & & \vdots \\ c(d,1) & c(d,2) & \cdots & c(d,d) \end{bmatrix}$$

Bu matris, verinin doğrusal transformasyonlarda değişmeyen mesafe ölçümü için bir yol sağlar. Ortalama değer vektörü $\mathbf{m}_x$ ve kovaryans matrisi C_x olan d boyutlu bir x ayırıcı özellik vektörü ile başladığımızı kabul edelim. Eğer ,x'i y 'ye , dxd boyutlu bir A^{dxd} matrisi kullanarak aşağıdaki ifade ile dönüştürürsek;

$\mathbf{y} = A\mathbf{x}$,

y için ortalama vektörü aşağıdaki ifade ile verilen ifadede göstermek güç değildir.

$\mathbf{m}_y = A\,\mathbf{m}_x$,

ve y için kovaryans matrisi aşağıdaki ifade ile verilir.

$C_y = A\,C_x\,A'$.

x ten $\mathbf{m}_x$, e veya **y** den $\mathbf{m}_y$ ye olan mesafeyi ölçmek istediğimizi kabul edelim. Elbette Euclidian normunun kullanabilirdik, fakat eğer, **x** ten $\mathbf{m}_x$ ye olan Euclidian mesafesi **y** den $\mathbf{m}_y$ ye olan ile aynı olursa çok kullanışsız olacaktır.(Geometrik olarak, A ancak çok ilginç olmayan döndürme ve yansıtmaya karşılık gelir.) mesafeyi normalize etmek için ne yapmak istiyoruz, tek bir ayırıcı özellik için standart hale getirilen mesafeyi tanımladığımızda bunu yaparız. Soru şudur: Skaler ifadenin matris genelleştirilmesi nedir.

$$r^2 = \left[\frac{x-m}{s}\right]^2 = (x-m)\frac{1}{s^2}(x-m)$$

Cevap aşağıdaki şekilde ortaya çıkar.

$$r^2 = (\mathbf{x}-\mathbf{m}_x)'\,C_x^{-1}(\mathbf{x}-\mathbf{m}_x)$$

Eğer biraz doğrusal cebir biliyorsanız, bu ifadenin herhangi bir tekil olmayan doğrusal transformasyonda değişmediğini ispatlayabilirsiniz. Bu, eğer **y** = A **x** yer değiştirir ve yukarıdaki $\mathbf{m}_y$ ve C_y formüllerini kullanırsanız, A sorun olmadan r için çok benzer aynı ifadeyi bulacaksınız.

Şimdi, grupların küresel olduğu bir ayırıcı özellik uzayının olduğunu ve **y** den $\mathbf{m}_y$ ye olan mesafe ölçümünde Euclidean metriğinin doğru yolu sağladığını varsayalım.Bu uzayda, kovaryans matrisi özdeşlik matrisidir ve **r**, **y** den $\mathbf{m}_y$ ye tam olarak Euclidean mesafesidir.

10.4.4.6 Mahalanobis Metriği(Mahalanobis Metric)

$r^2 = (\mathbf{x}-\mathbf{m}_x)' C_x^{-1} (\mathbf{x}-\mathbf{m}_x)$ ifadesindeki r miktarına, **x** ayırıcı özellik vektöründen $\mathbf{m}_x$ ortalama değer vektörüne olan **Mahalanobis mesafesi** denir. burada, C_x ,x için kovaryans matrisidir.

Sabit r deki yüzeylerin $\mathbf{m}_x$ etrafında merkezli elipsoidler olduğu gösterilebilir. Ayırıcı özelliklerin korelasyonsuz ve varyansların bütün yönlerde aynı olduğu özel durumda, bu yüzeyler küreseldir ve Mahalonobis mesafesi Euclidian mesafesine eşit olur.

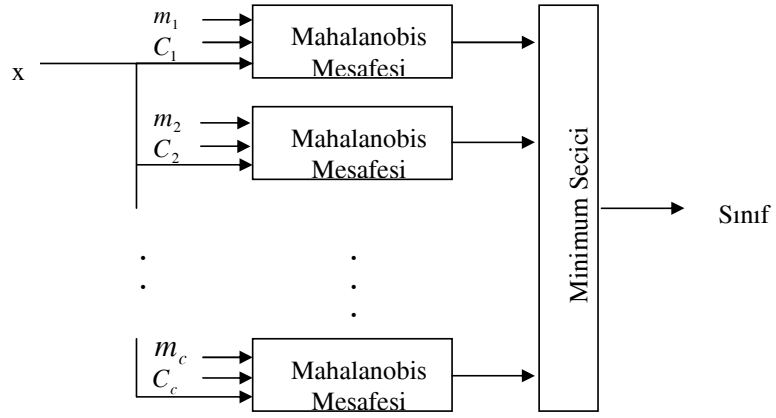
Mahalonobis mesafesi minimum mesafe sınıflandırıcısı şeklinde aşağıdaki gibi. $\mathbf{m}_1$, $\mathbf{m}_2$, ... , $\mathbf{m}_c$, c sınıfları için ortalama değerler (şablonlar) olsun, ve C_1, C_2, ... , C_c ise buna karşılık gelen kovaryans matrisleri olsun. **x**'ten ortalamanın herbirine olan Mahalonobis mesafesini ölçerek bir x ayırıcı özellik vektörü sınıflandırılır, ve **x'i** Mahalonibis mesafesinin minimum olduğu sınıfa atanır.

Mahalanobis metriğinin kullanılması,Euclidean metriğinin kullanılmasındaki bazı sınırlamaları ortadan kaldırır.

- Koordinat eksenlerinin ölçeklenmesini otomatik olarak hesaplar.
- Farklı ayırıcı özellikler arasındaki korelasyonları düzeltir.
- Doğrusal karar sınırları olduğu kadar eğrisel sınırlarda sağlayabilir.

Bununla birlikte, bu avantajların ödenmesi gereken bir bedeli vardır. Kovaryans matrislerinin doğru olarak belirlenmesi zordur, belirleyici özelliklerin doğrusal artmasıyla bellek ve zaman gereksinimi üstel olarak büyür.Sadece birkaç ayırıcı özellik gerektiğinde bu problemler önemsiz olabilir, fakat ayırıcı özelliklerin büyümesiyle, çok önemli hale gelebilirler.

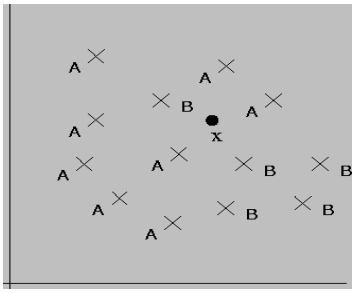
Silinmiş: <sp>



Şekil 10.20: Mahalonobis Sınıflandırması

10.4.4.7 K En Yakın Komşu (KNN) Sınıflandırması

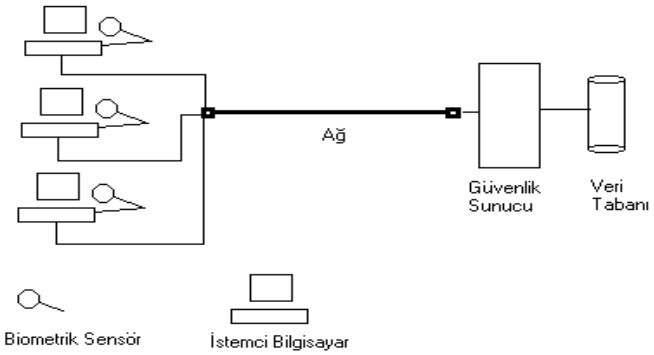
Biyometrik izleri sınıflandırmada kullanılabilecek yöntemlerden birisi de K en yakın komşu sınıflandırması olarak adlandırılabilecek olan yöntemdir. Bu yöntem teorisi oldukça karmaşık sayılabilecek bir yöntemdir. Konunun pratikte anlaşılabilmesi açısından Şekil 10.21.'deki örnek değerlerin A ve B değerleri olduğunu varsayalım. Herhangi bir zamanda elde edilmiş olan X değeri, kendisine en yakın K adet komşu örnek değere bakılarak sınıflandırma yapılır. Şekil 10.20.'de örneğin K = 1 olarak belirlendiğinde sınıflandırma B'dan yana , K = 3 olarak belirlendiğinde ise sınıflandırma A'dan yana olabilir. Örnek değerler içerisinde kendisine en benzer olan değere eşitlenir. Böylece bir sınıflandırma yapılmış olur. Bu yöntem daha çok olasılığa dayanır. Bir izi tanımlamak için çevresindeki izler hesaplamaya konulur ve bir olasılık bulunmaya çalışılır.



Şekil 10.21: En yakın K Komşu Sınıflandırması Örnek Dağılımı

10.5 Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

Şimdiye kadar ki bölümlerde biyometrik yöntemlerin genel çalışma prensiplerinden öte bu tür sistemlerin çalışabilmeleri için nasıl bir fazladan donanıma ihtiyaç duyduklarını anlatıldı.Örneğin bir parmakizi tanıma sisteminde her istemci için bir CCD kamera içeren sensöre ihtiyaç vardı. Bahsedilen sensörlerin içeriklerinin farklı olmasına rağmen yaptıkları iş aynıdır. Bütün biyometrik sistemlerin kurulumu için istemci başına bir sensör gerekmektedir.Daha sonra buradan okutulan bilgiler tasarlanan sistemin mimarisine bağlı olarak işletilirler. Şekil 10.22'de bir biyometrik sisteme ait kuramsal çizim yer almaktadır.



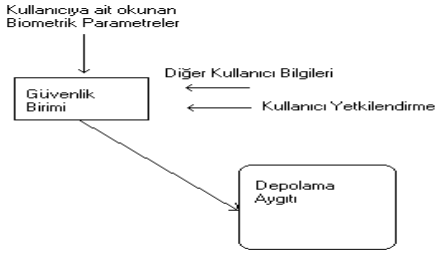
Şekil 10.22-Biyometrik Sistemlerin genel yapısı

Biyometrik sistemlerin tasarımı için uygulanan iki model vardır.

- On-line Model
- Off-line Model

10.5.1 On-line Model

On-line model yapısında, kullanıcı okunması gereken biyometrik parametresini sisteme okutturur. Sistem almış olduğu biyometrik parametreleri eğer gerekliyse şifreleyerek ağ üzerinden güvenlik parametrelerinin tutulduğu sunucuya gönderir. Sunucu bu parametreleri veritabanı içerisindeki bilgilerle karşılaştırır. Eğer kullanıcı sisteme kayıtlı biriyse sisteme giriş izni gönderir. Kullanıcı tanımlanamadıysa sistem giriş izni vermez. Günümüzde on-line sistemler kullanılmaktadır. On-

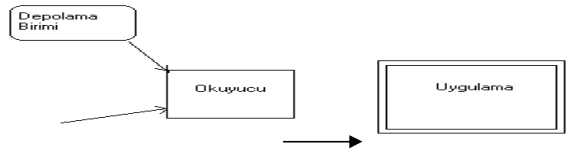


Şekil 8-23:On-line Model

line bir sistemde önemli olan nokta biyometrik bilgileri okuyan sensörlerin sunucuya çok güvenli bir şekilde bağlanmaları gerekmektedir. Bunun için ya sensörler ve sunucu arasında güvenli bir yol tayin edilmelidir yada bilgiler yukarıda bahsedildiği üzere çok iyi şifrelenmiş olarak gönderilmelidir.Bilgilerin herhangi bir nedenden dolayı yetkisiz insanların eline geçmesi sistemin büyük bir zaafa uğramasına sebep olabilir. Öyleyse parametreler öyle bir şekilde şifrelenmeli ki bu parametreler bir şekilde elde edilse bile kullanılamamalılar.

10.5.2 Off-line Model

Off-line sistemlerde ,On-line sistemlerde olduğu gibi gerçek zaman bir doğrulama işlemi yapılmaz. Bunun için gerekli olan bir manyetik kart gibi aparatlar kullanmaktır. Kullanıcıya ait olan bilgiler bu kart üzerinde tutulurlar. Kullanıcı sisteme girmek istediği zaman bu kartı kullanır. Bu tür sistemlerde güvenlik tamamen kullanıcının inisiyatifindedir. Kendisine verilmiş olan depolama aygıtını çok iyi korumak zorundadır. Tersi bir durumda sistemin güvenilirliğinden söz etmek gerçekçi olmayacaktır.



Şekil 10.24:Off-Line Model

Bu sebeplerden dolayı off-line bir sistem tasarlanırken güvenlik açısından üzerinde çok daha fazla düşünülmesi gereklidir.

10.6 Biyometrik tanıma Teknikleri

Bu gün birçok biyometrik tanıma uygulaması vardır. Aşağıda bunların türleri verilmiştir.

- Parmak izi tanıma
- Optik Tanıma
- Yüz Yapısı Tanıma
- Ses Tanıma

- İmza Tanıma
- Yazma Ritmi Tanıma
- Toplardamar İzi Tanıma
- Avuç içi izi
- Kulak Şeklinden tanıma

10.6.1 Parmak izi Tanıma

İnsanları ayırt etmede kullanılan ve en çok bilinen yöntem parmak izidir. İnsanlar çok uzun bir süreden beri parmak izlerinin ayırt edici özelliğinin farkındadır. Bu bağlamda parmak izi tanıma sistemlerinin tarihi bilgisayarın tarihinden çok öncelere kadar uzanır. İlk parmak izi yöntemini Çin'de yazarların yazmış oldukları metinleri işaretlemek için kullandıkları söylenir. Fakat teknik manada ilk parmak izi kullanımını İngiltere'nin Hindistan'da görevli polis kuvvetlerince tutukluları ayırt etmek için 1800'lü yılların başlarında kullanıldığı bilinmektedir. Bu sistem Henry Sistemi olarak adlandırılmıştır.Yöntem elde edilen parmak izinin küçük parçalara bölünerek bu parçaların karşılaştırılmasını öngörür. Bu sebeple parmak izlerinin ayırt ediciliğini bilgisayar sistemlerinin güvenliğini sağlamak için kullanmak parlak bir fikirdir. Nihayet,günümüzde en çok kullanılan güvenlik sistemlerinden birisi parmak izi tabanlı güvenlik sistemleridir. Bu sistem için kullanılması gereken Parmak İzi Okuyucu, Retina /İris okuyucuya benzer bir çalışma prensibine sahiptir.Kullanıcı parmağını cam bir tabaka üzerine bastırır.camın arka tarafında yer alan bir CCD kamera görüntüyü yakalayarak sisteme iletir. Sistem bu bilgiyi kullanarak kullanıcıyı tanımaya çalışır.

Bu tür bir sistemin Retina/İris Tanıma sistemine göre dezavantajı hassasiyetinin çok düşük olmasıdır.Donanım maliyeti ise Retina/İris Tanıma sistemlerine göre daha makul bir seviyededir.

10.6.2 Optik Tanıma

Retina tanıma sistemleri, isminden de anlaşılacağı üzere insanların göz yapılarını algılayarak ayırt etme prensibine dayanır. Sisteme girmek isteyen bir kullanıcı cam veya diğer bir saydam malzemeden yapılmış olan ekrana gelerek gözünü ekrana yaklaştırır.Gözünü camın arkasında yer alan bir hedef üzerinde yoğunlaştırır.Retina tarama sensörü kullanıcının gözüne bir ışın demeti gönderir ve kullanıcının retinasına ait olan özellikleri algılar. Bu bir nevi kullanıcının retina haritasını çıkartmaktır. Burada kullanılan ışın infared(Kızıl ötesi) dalga boyunda olan bir ışındır. Retina okuyucu tarafından elde edilen görüntü sistem tarafından kullanılarak kullanıcı hakkında karar verilir. Tablo 10.1'de görüldüğü üzere retina tanıma sistemleri hassasiyeti en yüksek biyometrik tanıma sistemidir. Tek dezavantajı ise hassasiyetinin yüksekliğiyle doğru orantılı olarak maliyetinin yüksekliğidir.

İris taramada da benzer yöntem kullanılır fakat İris tarama yönteminin Retinal taramaya göre hassasiyeti daha düşüktür. Bunun sebebi insanlarda retina tabakasının iris tabakasına göre daha ayırt edici bir özellik olmasıyla açıklanabilir.

10.6.3 Yüz Tanıma

Yüz tanıma sistemi aslında en doğal biyometrik ayırt edici yöntemdir. İnsanlar birbirlerini ayırt etmede yüzlerinden faydalanırlar. Bu sebeple bu yöntem neredeyse insanlık tarihiyle yaşıt bir biyometrik ayırt etme yöntemidir. Buna rağmen bu yöntemin bilimsel olarak incelenerek bir ayırt edici özellik olarak bilgisayarlarda kullanılması oldukça yeni sayılabilecek bir konudur. Örneğin bir suçluyu tanımlamada polis tarafından kullanılan yöntem. Suçluyu anlatan insana suçlu hakkında sorular sorup yüz şeklinin belirlenmesine çalışmaktır. Bu konuda polis ressamlarının standart olarak daha önce çizdikleri bazı yüz parçaları vardır.Verilen tarife göre bu parçalar bir araya getirilerek suçlunun yüz şekline yakın bir yüz şekli bulunmaya çalışılır.Bilgisayarların hayatın içerisindeki hızlı kullanımı yüz tanıma yöntemleri konusunda da oldukça ilerlemeler

sağlanmasına neden olmuştur. Günümüzde yüz tanımlama konusunda kullanılan iki yöntem vardır.Bunlar,

Yüz Metriği Yöntemi
Eigenfaces Yöntemi(Yüz Parçaları).

Yüz Metriği Yönteminde yüz üzerinde yerleşik olan organlar arasındaki mesafeler ölçülerek bunlardan bir matematik ifade çıkarılmaya çalışılır.Örneğin gözler arasındaki mesafe ağız ve burun arasında ki mesafe vb….

Eigenfaces Yönteminde ise polis ressamının yaptığına benzer bir yöntem uygulanır. Yüz 150 parçaya bölünür.Bu 150 parçadan 40 tanesinin belirleyiciliği diğer parçalardan daha fazladır.İlk etapta bu 40 parçadan başlayarak yüz tanımlama işlemine geçilir.Böylece yüz tanımlanmaya çalışılır.Bu yöntem Yüz Metriği Yöntemine göre yeni bir yöntemdir ve hala test aşamasındadır.Araştırmacılar tarafından geliştirilmektedir.

Bu tür ürünün en önemli özelliği maliyetidir. Tipik fiyatı 150$dan azdır.

10.6.4 Ses Tanıma

Ses tanıma sistemleri oldukça yaygın kullanılan maliyeti düşük ve günümüz teknolojisinde fazladan hiçbir donanım gerektirmeyen güvenlik sistemlerinden biridir. Ses Tanıma Sistemleri genel olarak iki ana gruba ayrılır.

Ses Tanıma Sistemleri
Konuşma Tanıma Sistemleri

Ses tanıma sistemlerinde kullanıcı sisteme parola olarak belirlediği bir kelimeyi bazı heceleri vurgulu olacak şekilde söyler sistem parolanın kendisiyle beraber vurguların zamanlamasına ve şiddetine bakarak kullanıcıyı ayırt eder.

Konuşma Tanıma Sistemleri,Ses Tanıma Sistemlerinden teknik manada daha gelişmiştir.Burada vurgu tamamen ortadan kalkar. Yani kullanıcı özellikle bir vurgu yapmaz.Sistemle normal olarak konuşur.Sistem kullanıcıyı konuşma modundan anlamaya çalışır. Ses tanıma sistemleri hassasiyet olarak en düşük biyometrik sistemlerden birisidir. Avantajı ise sahip olma maliyetinin düşüklüğüdür.

Burada en büyük dezavantaj sesin bilgisayar ortamına aktarılırken geçirdiği büyük değişim ve formatındaki bozukluktur. Bu sebeplerden dolayı Ses Tanıma Sistemleri vurgu içermeleri açısından Konuşma Tanıma Sistemlerine göre daha güvenilirdir. Ses Tanıma Sistemleri de diğer araştırma ve geliştirme aşamasında olan sistemler gibi hala üzerinde çalışılan biyometrik sistemlerden biridir. Fakat burada en önemli kriter ses işleme aşamasını daha doğru hale getirebilecek olan donanım parçalarının geliştirilmesidir. Günümüzde standart PC'lerde kullanılan mikrofonlar ve hoparlörler bilgisayarda ses işlenmesi için iyi bir alternatif sunmamaktadır. Buna rağmen yüksek hassasiyete gerek olmayan uygulamalarda standart ses Girdi/Çıktı aygıtlarını kullanarak bir güvenlik sistemi tasarlamak maliyetler göz önüne alındığında iyi bir seçenek olarak gözükmektedir.

Ses işleme yöntemiyle kurulacak bir sistemin en büyük dezavantajı kullanıcıları tanımlamak için veritabanında tutulan kayıtların büyük yerler işgal etmesidir. Tasarlanan güvenlik sistemi ağ üzerine çok fazla yük getirmemelidir.

10.6.5 İmza Tanıma

Her insanın gerçek hayatta kullandığı ,el yazması metinlerde insanları ayırt edici bir özellik olan imzaları bulunmaktadır.Eskiden beri insanlar kendilerini veya kendi ailelerini betimleyen imza, arma yada özel işaretler kullana gelmişlerdir.Gerçekten dikkat edilirse imzalarımızı devamlı aynı şekilde,aynı hızda birbirleriyle oldukça benzer biçimde atarız. İmza Tanıma Sistemleri'nin temelinde de bu mantık vardır.Eğer herkes imzalarını her zaman aynı biçimde atıyorlarsa bu imzalar elektronik ortama aktarılarak ayırt edici bir güvenlik sistemi olarak kullanılabilir.Bunun için yazıyı elektronik ortama aktaran cihazlar uzun zamandır kullanımdadır. Bu aletler uygun şekilde kalibre edilerek bu tür bir güvenlik sistemi kurmak oldukça kolaydır. Güvenilirlik seviyesi Parmak izi ve El Geometrisi Sistemlerine göre oldukça düşüktür. Bu tip sistemler iris tarayıcılar kadar pahalı değildirler.

10.6.6 Tuş basma ritmi Tanıma

Diğer biyometrik sistemlerin en büyük dezavantajlarından birinin bütün terminallerde kullanılmak üzere ekstra donanım gereksinimi olmalarının yanı sıra, yazma ritmi sistemlerini diğer biyometrik sistemlerden ayıran en temel özellik kendisine has özel bir donanıma ihtiyaç duymamasıdır.Bir Yazma Ritmi sistemi tasarlamak için ihtiyaç duyulan tek girdi aygıtı sadece klavyedir.

Böyle bir avantaja sahip bir biyometrik sistemin gerçek hayatta kullanılmaması için hiç bir sebep yoktur. Özellikle üniversiteler gibi pek çok yerde bu tür bir sistem hem bilimsel hemde teknik manada rahatlıkla kullanılabilir.Çünkü insanların el yazıları gibi klavye yazış şekilleri arasında büyük bir benzerlik vardır. Gerçektende bir insan klavye üzerinde bir şeyler yazmaya başladığında bu klavye ve doğal olarak bilgisayar üzerinde bir iz bırakır.Yani kullanıcının klavyede karakterler üzerinde gezinmesi aslında onun gayet düzenli olarak yapmış olduğu bir yazma ritmi hareketine tekabül eder.

Diyelim ki klavyeyi kullanarak bilgisayarda bir editöre bir kelime yazmak istiyorsunuz. Teorik olarak kelime içerisinde yer alan harfleri yazarken geçen süre birbirine eşittir.

Bir kullanıcıdan soyadı yazılması istenmiş ve yazılma aşamasında geçen süreler tespit edilmiştir;**Stephenson** Kelimesi için geçen süreler ölçülmüş ve bu sürelere ait grafik Şekil –8-25 'te gösterilmiştir.

Şekil 10.25:Stephenson kelimesinin yazılış ritmine ait gösterim

Şekil 10.25 kullanıcının Yazma Ritmi sistemine ait bulgular vermektedir.Kullanıcı, t ve e karakterleri arasında oldukça zaman kaybederken n ve s yada s ve o karakterleri arasında geçişi oldukça hızlı yapabilmektedir.Klavyeden girilen iki karakter arasında geçen zamanı ölçerek kullanıcıların yazma ritimlerini tespit etmeye çalışılmaktadır. Aslında yazma ritmi'yle ilgili olarak bir çok çalışmada ölçülen ve değerlendirilmeye çalışılan değer budur.

Yazma ritmi sistemlerinin en önemli dezavantajlarından birisi karar vermek için gerekli olan verilerin ancak tek bir parametreden yani iki tuş arasındaki gecikme süresinden elde edilmesinden kaynaklanmaktadır. Sadece tuş aralıklarını değil tuşlara basılırken geçen süreninde tespiti yazma ritmi çalışmalarında güvenilirlik oranını arttıracaktır.

10.6.7 Toplardamar Şekli

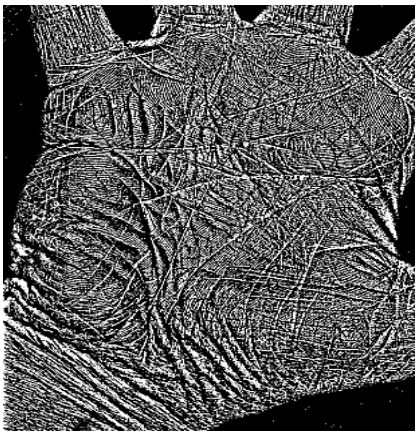
Toplardamar biyometrik sistemler kullanıcıların tek ve özel tanımlaması için deri altındaki toplar damarların yapısı infrared olarak kaydedilir. Toplar damar teknolojisi, kişiler için damarsal bar kod okuyucu olarak benzetilebilir.

Toplardamar biyometriğindeki temel düşünce, insanın damar yapısındaki birbirine benzemeyen yapıdır. Araştırmalar herkesin farklı damar yapısına sahip olduğunu göstermiştir.Toplardamar tekniği diğer biyometrik sistemlere göre üstünlüğe sahiptir. Teknoloji retinal tarama gibi içeriye nüfuz eden bir teknik değildir. Ek olarak teknik elin kirliliğinden etkilenmez ve değişik sıcaklıklarda çalışabilir. Sonuç olarak,.insan damar sistemi , yetişkin bir insanda değişmeyeceği için sıkça güncelleme gerektirmez. Damar şeklinin sahteciliği son derece güçtür. Şekil 10.26 infrared damar görüntüsünün yapısını göstermektedir.

Şekil 10.26: Damarlara ait görüntüler

Toplardamar şekli biyometriğinin uygulamaları, işyerlerine giriş/çıkıştan bankalardaki kasalara erişimde olabilir. Teknoloji yenidir ve gelişmeye devam etmektedir. Genellikle, toplardamar şekli biyometriği, hemen her ortamda çalışmaya uygun olması ve cihaz ile temas gerektirmemesi nedeniyle elverişli ve güvenli bir yöntem olarak tercih edilecektir.

10.6.8 Avuç içi izi



Sekil 10.27:Avuc ici izinin yapısı

Avuç içi biyometriği, güvenilirlik açısından parmak izi biyometriğine benzedir. Ana farklılık, avuç içi okuyucu parmak izi okuyucudan daha fazla yer gerektirir. Parmak izi ve avuç izi tanıma kullanıldığı zaman, kullanıcı tarayıcı ile doğrudan temas eder, hiçbir cihaz direkt temas olmadan avuç içini okuyamaz. Tarayıcı, sonra şahsın avucundaki, daire ve olukları okur. Çünkü, parmak izi ve avuç içi izi tarayıcıları karmaşık daire ve çizgileri ölçer. Onlar yüz tanıma sisteminden karmaşıktır. Aynı zamanda bu tarayıcılar, kesintileride barındırır.

Parmak izi tanıma, kişilerin tanınmasında geniş olarak kullanılırken, avuç içinin parmak izine benzemesi nedeniyle diğer biyometrik tekniklere göre geniş olarak kullanılır. Parmakizi ve avuç içi izi tanımanın dezavantajları, a) Temas tarayıcı üzerinde yağ ve kirlilik bırakabileceğinde bu teknikler birçok ortam için uygun değildir. b.) Halk yaşayan ve ölü parmak izi veya avuç içi izinin çalınmasından

korkabilir. Bununla birlikte bir tanıma cihazının önemli görevi canlı ve ölü izleri ayırt edebilmesidir.

El Geometrisi Tanıma Sistemleri, her insanın el yapısının ve şeklinin farklı olduğu kabulüne dayanır.Gerçektende belli bir yaştan sonra insanların el yapıları değişiklik göstermezler. Bu yöntem kullanılarak tasarlanan bir güvenlik sisteminde sistem kullanıcıların parmak uzunluklarından avuç içlerinde yer alan çizgilere kadar bir çok parametreyi algılayarak karar verir. Avuç içini algılamada kullanılan yöntem parmak izi tayininde kullanılan yöntemin aynısıdır. El Geometrisi sistemi kullanılarak tasarlanan bir sistemin hassasiyeti parmak izi sistemleri kadardır. Bu açıdan bakıldığında güvenilirlik ve sahip olma maliyeti açısından özdeş sistemlerdir denilebilirler.

10.6.9 Kulaklar

Kulak biyometrisi, en az kullanılan ve bilgiyi elde etme bakımından en zor olanıdır. Kulak biyometrisi, dış kulağın şekli, kulak memesi, ve kemik yapısına dayanır. Polis pencere ve kapı dinlenirken kulak şeklinin kopyalanmasıyla kulak biyometrisini kullanır. Hollanda da polis bu teknolojiyi suçlu bulmada kullanır.
Kulak biyometrisi, yüzün tanıma için yüz tanıma ilke birlikte geliştirilmeye devam etmektedir. Ancak geniş uygulama için yeni bir tekniktir.

10.7 Biyometrinin örnek uygulamaları

- Zaman ve katılım raporlaması
- Bina giriş denetimi
- ATM işlem gerçekleme
- Bilgisayar veritabanı ve ağ erişimi
- Araç erişimi ve ateşleme güvenliği
- Yerleşim yeri girişi ve güvenlik alarmı kontrolü
- Kubbe ve emniyet erişimi
- İmza doğrulama
- Parola ve ev girişi gözetleme
- Personelize yangın alarm emniyeti
- Satış noktası kimlik doğrulama
- "Gözetim zinciri doğrulama
- Güvenlik devriye turu izleme
- Hapishane kimlik doğrulaması
- Mülteci ve doğrulama
- Taşınabilir kanun uygulamaları
- Güvenli kablo TV uygulamaları
- Süreç kontrol güvenliği
- Hücresel telefon güvenliği

10.8 Biyometrik Sistemlerin Veri Kayıt Analizleri

Biyometrik sistemlerin seçiminde kullanılan önemli parametrelerden biriside kayıtların veri boyutlarının büyüklüğüdür. Hangi biyometrik sistem kullanılırsa kullanılsın veriler mutlaka bir veritabanı üzerinde tutulup yönetilmek zorundadır.Böyle bir durumda ortaya çıkan soru sisteme kayıt edilecek kullanıcılara ait biyometrik özelliklerin kayıt uzunlukları ne kadar olacaktır? Tablo 10.2 bir kayıt için gerekli olan miktarları byte olarak göstermektedir.

Biyometrik Yöntem	Data Büyüklükleri(bytes)
Retina Tarama	35
İris Tarama	256
Parmak izi Tarama	512 – 1000
El Geometrisi Tarama	9

Tablo 10.2: Biyometrik Data Büyüklükleri (Birim Kayıt için)

Tablo 8.2'den anlaşıldığı gibi biyometrik yöntemlerin sistem üzerinde kaplamış olduğu alan miktarı birbirlerine nazaran oldukça farklıdır. Örneğin retinal tarama sistemleri iris tarama sistemlerine nazaran yaklaşık 10 kat daha güvenli oldukları halde kullanıcı tanımlamak için ihtiyaç duydukları kayıt alanı;

Ampirik bir hesaplamayla 256 / 35 = 7.31

Yaklaşık 7 kat daha az yere ihtiyaç duymaktadır. Aynı şekilde bir kullanıcının parmak izini tutmak için gerekli olan alan 512-1000 byte arasında değişmektedir. Parmak izi tanıma sistemlerinin iris ve retina tanıma sistemleri gibi kendisinden kıyaslanamayacak kadar güvenli sistemlerin ihtiyacı olan alandan çok daha fazla bir disk alanına ihtiyaç duyması çok büyük bir dezavantajdır.Veri uzunluğu açısından bakıldığında en uygun biyometrik güvenlik sistemi El Geometrisi tanıma sistemleridir.Tablo 8.2'den açıkça görüldüğü üzere ihtiyacı olan alan sadece 9 Byte 'dır.

Tablo 10.2'de verilen değerleri en küçük veri depolama ihtiyacı duyan El Geometrisi Tanıma Sistemine göre normlarsak Tablo 10.3'deki gibi bir sonuç elde ederiz.

Biyometrik Yöntem	**Norm**
Retina Tarama	4
Iris Tarama	28
Parmak izi Tarama	57 – 111
El Geometrisi Tarama	1

Tablo 10.3: Biyometrik Veri Kıyaslaması (El Geo.Sist.göre normlanmış)

Tablo 8.3'den açıkça görüldüğü üzere bir Parmak İzi Tarama sisteminde tutulan 1 kayıt El Geometrisi Tarama yöntemine göre tasarlanmış bir sisteme göre yaklaşık 100 kat daha fazla yer kaplamaktadır. Bu da açıkça göstermektedir ki bu tür sistemlerin kurulmasında biyometrik sistemin güvenlik oranı,maliyeti gibi parametrelerin yanında veri büyüklüklerinin de tasarımcılar tarafından göz önüne alınarak karar verilmesi gerekmektedir.Çünkü veri uzunluğunun fazla olması ilave donanım ihtiyacı yada ağ trafiğini gereksiz yükleme gibi bir çok dezavantajı yanında getirecektir.

11 SANAL ÖZEL AĞLAR (Virtual Private Networking)

11.1 Giriş

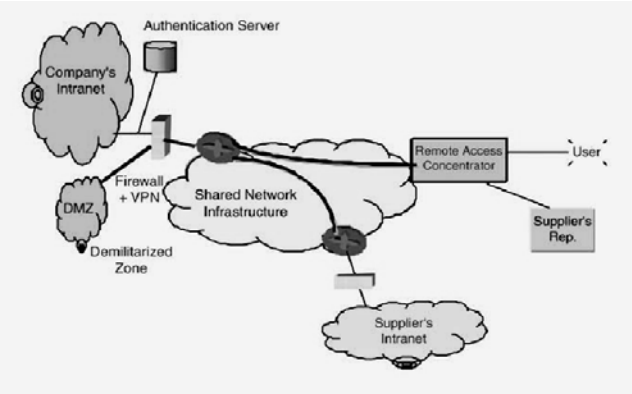
Günümüzde, pekçok büyük ve küçük çaplı organizasyon için bilgisayar ağları organizasyonun genel altyapısı içerisinde büyük önem kazanmış durumdadır. Bilgisayar ağlarının öneminin yüksek olduğu bu organizasyonlarda spesifik ve önemli bir konu da bu ağların uzak yerlere ve kullanıcılarına nasıl bağlanacağıdır.

Geleneksel olarak, uzak yerler birbirilerine kiralık hatlar (leased lines) veya Frame-Relay sayesinde bağlanıyordu. Uzak kullanıcılara hizmet onlara iç telefon numaralarını kullanarak dial-in ağ imkanları sağlanarak veriliyordu. Fakat bu yaklaşımlar zamanla pahalılık ve esneklik problemleri göstermeye başlamıştır. Kiralık hatların ve iç telefon imkanlarının temel birim bedelinin azalmaya yüztutmasına rağmen bant-genişliği ihtiyacının artmasıyla organizasyonun toplam masrafı da artmaktadır. Ayrıca bu artışla beraber oluşan karmaşık altyapının yönetilebilirliği problemi de artmaktadır.

VPN teknolojisi, bağlanma problemine güvenli, ölçeklenebilir, ve fiyat yönünden uygun bir çözüm sağlamaktadır. VPN bir organizasyonun uzak birimlerine merkez birimden herhangi bir sahibi olmayan ortak ağlar (mesela Internet) üzerinden güvenli bir şekilde bağlanabilme imkanı sağlar. Ayrıca uzaktaki kullanıcılara da yine bu tip ağların sahip olduğu iletişim alyapısını kullanarak ortak organizasyon ağına bağlanabilme imkanı sağlar. Her iki durum için de bağlantı Interneti omurga olarak alır fakat bağlantılar, kullanıcılar ve birimler için özel (private) bir ağ kullanılıyormuş görüntüsündedir.

11.2 Sanal Özel Ağ(VPN) nedir

VPN bir ağı veya tek bir bilgisayarı aracı bir ağ üzerinden (tipik olarak internet) başka bilgisayarlara bağlar. Şekil 11.1'de görüldüğü üzere iki türlü VPN senaryosu bulunmaktadır. İlki uzakta bulunan bir kullanıcının (genellikle tek bir bilgisayar) kollektif ağa bağlanması (mesela şirket ağı), ikincisi de uzaktaki bir ağın kolektif ağa bağlanması şeklindedir. Uzaktaki bir kullanıcının ortak ağa bağlanabilmesi için öncelikle dial-up bağlantısının kullanarak bir ISP (Internet Service Provider-Internet Servis Sağlayıcısı) üzerinden Internete bağlanması ve daha sonra da kendi bilgisayarı ile ortak VPN özellikli (VPN-enabled) yönlendirici arasında ikinci bir VPN bağlantısı kurması gerekmektedir. Uzaktaki bir ağı da VPN kullanarak ortak ağa bağlama durumunda benzer bir işlem gerçekleştirilmesi gerekmektedir. Bu senaryoda uzak ofisin VPN özellikli yönlendiricisi yerel ağ'daki istemciler adına VPN bağlantısını başlatır. Ayrıca uzak yönlendirici ile ISP arasndaki bağlantı tipi IP trafiğini taşıyabildiği müddetçe önem taşımamaktadır.



Şekil.11.1

11.3 VPN istemci ve sunucuları

Bir VPN'de VPN bağlantısını başlatan bilgisayar VPN *istemcisi* olarak isimlendirilir. VPN istemcisi bu durumda uzaktaki bilgisayarla (VPN *sunucusu*) bir VPN bağlantısı oluşturur. Uzak kullanıcı senaryosunda uzak bilgisayar da VPN sunucuya bağlantı oluşturan VPN istemcisidir. Bu yüzden bu uzak bilgisayar birisi VPN bir diğeri de ISP bağlantısı olmak üzere aynı anda iki bağlantıyı birden aktif halde tutmak zorundadır. Uzak ofis senaryosunda uzak ofisin yönlendiricisi VPN istemcisi konumundadır. Her iki senaryo için de VPN sunucusu, VPN bağlantısındaki bitiş noktası olarak görev yapan ortak ofisteki bir sunucudur. Sonuç olarak iki tür VPN'ler inşa edilebilir:

- **Uzak kullanıcı VPN:** Uzak bir kullanıcı ortak intranete erişir ve VPN istemcisi olarak davranır.
- **Uzak ağ VPN:** İstemci uzak bir yönlendiricidir ve VPN son kullanıcılara tamamen saydamdır.

11.4 VPN'in sağladıkları

1. Güvenli ağa erişimi artırır: VPN sayesinde güvenli ortak ağa uzakta bulunan ve fiziksel atanmış hat kullanımına sahip olmayan kullanıcı ve ağlar Internet üzerinden güvenli ağa erişirler.
2. Uzaktan erişim sağlar: Daha önce de belirtildiği üzere VPN sayesinde fiziksel sınırlamalar kalkar ve erişim konusunda uzaklık problemi çözülmüş olur.
3. Diğer kurumlara güvenli iletişim: VPN kullanıldığında 3. kurumlar ve şahıslar çok kolay bir şekilde ortak ağa girebilirler. Ayrıca bunların ağdaki erişebilecekleri yerler de istenilen şekilde sınırlandırılabilir.
4. Ucuz maliyet: Leased line'ların (özel atanmış hat) pahalı olması sebebiyle VPN teknolojisi maliyeti düşürmektedir. Maliyeti oluşturanlar sadece bazı VPN cihazlarına verilen paradır ki bunların maliyeti ayrıca özel bir ağ kurmak yanında kıyaslanamayacak seviyede ucuzdur.
5. İstenilen anda güvenli iletişim: VPN teknolojileri güvenlik konusunda yeterli seviyededir. Ayrıca Internet kullanıldığı için yönlendirme alternatifleri bulunduğundan istenilen anda kullanılabilirliği daha yüksektir.
6. Ölçeklenebilir yapı: VPN'ler ölçeklenme konusunda gayet başarılıdır. İstenilen anda istenilen yere ekler yapılabilir, VPN büyütülebilir. Kullanılan VPN cihazlarının sınırlamalar dışında sınırlama yoktur. VPN'e yeni bir ağ eklenmek istendiğinde yapılması gereken sadece yeni ağın önüne gerekli cihazları koymak ve bütün VPN cihazlarında gerekli konfigürasyon değişikliklerini gerçekleştirmekten ibarettir.
7. Gizlilik, bütünlük, kimlik doğrulama, erişim kontrolü: VPN teknolojileri bu güvenlik seviyelerini gerçekleştirir.

11.5 Güvenlik Servisleri

VPN teknolojileri güvensiz ağı omurga olarak kullandıkları için bilgi güvenliği için belli başlı bazı güvenlik servislerini desteklemek zorundadır. Bu servisler hakkında aşağıda bilgi verilmiştir:
1. Gizlilik: VPN teknolojileri gizliliği sağlamak için bilgiyi şifrelerler. Bilginin şifrelenmesi için simetrik veya asimetrik algoritmalar kullanılabilir. Sıkça kullanılan şifreleme algoritmaları simetrikte DES ve TripleDES, asimetrikte RSA'dir. Şifrelemede genellikle gidip gelen paketler şifrelenir. Gönderen paketi anahtarı ile şifreler alıcı da yine algoritmanın türüne göre anahtar kullanarak şifreyi çözer. Bağlantının türüne göre transport mod ve tunel mod olmak üzere iki ayrı seviyede şifreleme yapılır.
2. Kimlik Doğrulama: VPN teknolojilerinde şifreleme tek başına kimlik doğrulamayı gerçekleştirmiş olsa bile ayrıca kullanılan teknikler vardır. Burada özet algoritmaları ve anahtar kullanılarak bilginin özeti çıkarılır ve alıcı ortak anahtarı kullanarak aynı şekilde özet çıkarıp karşılaştırır. Eğer özetler aynı ise kimlik doğrulanmış olur aksi halde paket atılır. Genellikle kullanılan özet algoritmaları MD5 ve SHA'dır.

3. Bütünlük: Bilginin bütünlüğü de yine şifreleme ve özetleme teknikleri ile sağlanmış olur.
4. Erişim kontrolü: VPN cihazları kimlik doğrulama yaptıktan sonra karşısındaki kullanıcıyı tesbit eder ve o kullanıcının erişim iznine göre gerekli yerlere erişmesine izin verir.

11.6 VPN Protokolleri

Bir VPN istemci ile sunucu arasındaki bağlantı üç değişik protokol ile gerçekleştirilebilir.

11.6.1 PPTP (Point to Point Tunelling Protocol)

PPTP IP internetworklerin üzerindeIP datagramlardaki PPPframeleri enkapsüle eden bir katman 2 protokolüdür. PPTP Microsoft tarafından geliştirilmiştir ve eskidir.

11.6.2 . L2TP (Layer 2 Tunelling Protocol)

PPTP'ye göre daha yeni bir protokoldür. Cisco'nun L2F protokolü ve Microsoft'un PPTP protokolünü taban olarak almıştır. Çoklu protokoller ile çalışır. IP, X.25, Frame Relay ve Asyncronous Transfer Mode (ATM) üzerinden gönderilen PPP framelerini enkapsüle eder.

11.6.3 IPSec (IP Security)

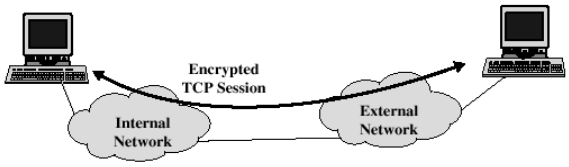
Diğer iki protokol 2. katmanda çalışmaktadır. IPSec ise IP katmanında (3. katman) çalışır. Temel mantığı IP paketlerinin gönderilmesi sırasında şifrelenmesi, özetlenmesi gibi ve böylece gerekli güvenlik seviyelerinin gerçekleştirilmesidir. İki protokol güvenliğin sağlanmasında kullanılır: AH (Authentication Header) başlığı kullanan bir kimlik doğrulama protokolü ve şifreleme-kimlik doğrulama yapan ESP (Encyription Security Payload) protokolü. IPSec tarafından sağlanan servisler şunlardır:

- Erişim kontrolü
- Bağlantısız bütünlük
- Veri kaynağı kimliği doğrulanması
- Tekrar yollanan paketlerin reddedilmesi
- Gizlilik
- Sınırlı trafik akış gizliliği

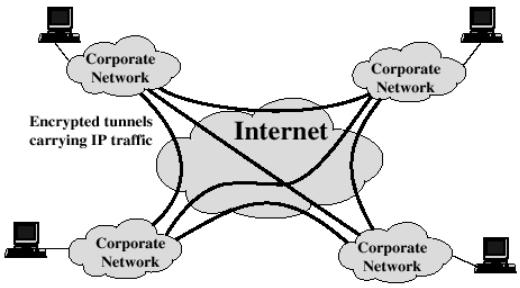
IPSec'de enkapsülasyon seviyesi açısından iki ayrı mod bulunmaktadır: Tunel mod ve transport mod. Bu modların genel sistemi Şekil 11.2 'de gösterilmiştir.

Tunel mod:
Genelde VPN Gateway'lerde kullanılır. Bu gateway'ler ağların önüne konulur ve ağların birbirine bağlanması durumunda kullanılır. Bu modda IP paketleri tamamen ele alınır. ESP bütün IP paketini şifreler ve şifrelenen paketin önüne bir ESP başlığı bir de yeni gateway'in Internete bağlı arayüzünün adresini içeren IP başlığı eklenir. Böylece IP paketi tamamen kapatılmış olur. Ayrıca bu sayede güvenli ağdaki IP adresleri de gizlenmiş olur. Kimlik doğrulama başlığı (AH) da paketin tamamı özetlendikten sonra paketin başına eklenir. Şekil.11.3'de de bunlar ayrıntılı olarak gösterilmiştir.

Transport mod:
Bu mod genellikle bilgisayarlar arası iletişimde kullanılır. Burada tunel moddaki gibi IP paketinin tamamı değil Transport katmanınından gelen kısım şifrelenir ve bu şifrelenmis kısmın önüne de başlığı eklenir. Burada IP başlığı değişmediği için orjinal IP adresi aynen kalır. Kimlik doğrulama da aynen tüm IP paketine değil de geri kalan kısma uygulanıp paketin başına başlığı eklenir. Şekil 11.3'de de bunlar ayrıntılı olarak gösterilmiştir.



(a) Transport-level security



(b) A virtual private network via Tunnel Mode

Sekil.11.2 Tünel ve Transport mode VPN

11.7 VPN'in Dezavantajları

VPN teknolojileri pekçok avantaja sahip olduğu gibi dezavantajları da bulunmaktadır. Öncelikle VPN halen gelişmekte olan bir teknoloji olduğu için hala tam olgun hale gelmemiştir. Internetin genelde güvensiz olması sebebiyle ciddi güvenlik tedbirleri uygulanmaktadır ve bu da belirli bir seviyede performans kaybına sebep olmaktadır. Bir diğer önemli husus da Internet kullanıldığı için performans kontrolü zordur ve ağın trafiğine bağlı olarak belirli performans düşüşleri kaçınılmazdır.

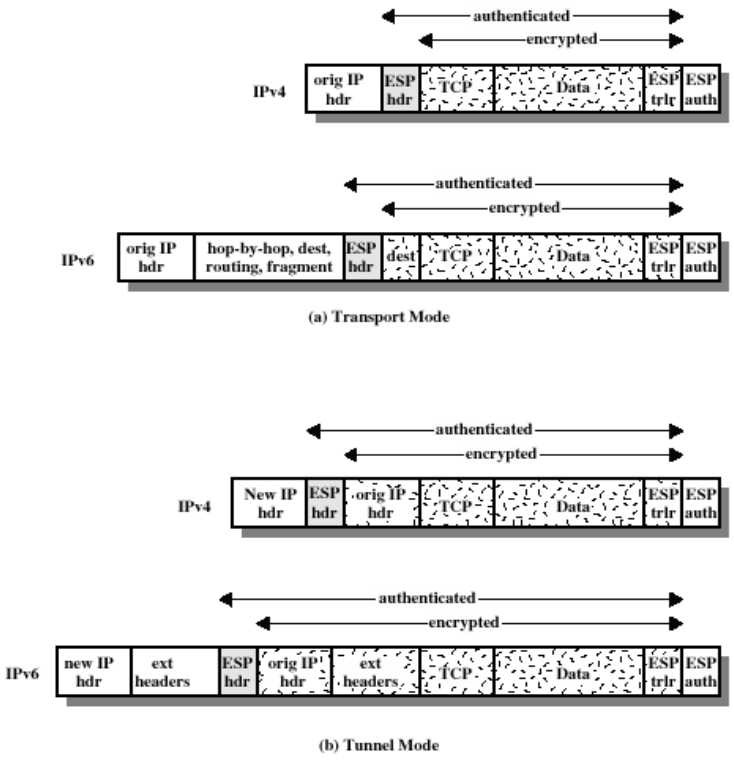
Güvenlik duvarının VPN Özelliği

Birçok güvenlik duvarı, bir çeşit VPN özelliği ile kriptolu güvenlik duvarı yapısındadır. Güvenlik duvarları arasındaki bütün trafik kriptolanarak IP paketleri ile birlikte Internet üzerinden iletilir. Uzak sitede, şifreli veri IP paketi içinden çıkartılarak gideceği son noktaya yönendirilir.

11.7.1 Güvenlik duvarından uzak sisteme

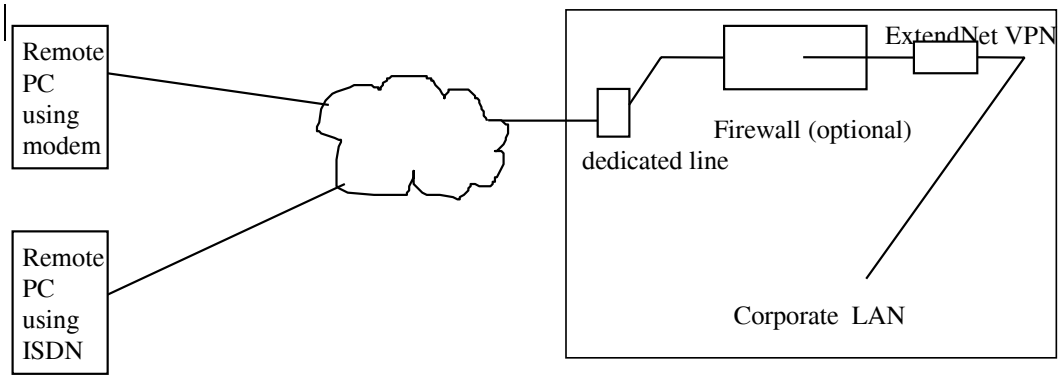
VPN teknolojisi güvenlik duvarı ile tek bir site arasında olabilir. Bu sık sık, gezgin kullanıcıların firma sistemine özel bağlantısı amacıyla kullanılır. Güvenlik duvarları arasındaki VPN'de olduğu gibi, bu erişim açık veya kontrollü olarak yapılabilir. Kontrollü erişim istemciler için uygundur ve ortaklar, belirli saatlerde belirli servislere erişebilirler Açık erişim, yoldaki çalışanların paylaşılmış dosyalar, yazıcılar vs. ye ağ güvenliği içinde erişmeleri için uygundur. Bir VPN ile, bu işleri güvenli şekilde yapabilirler.

.



Scope of ESP Encryption and Authentication

Şekil.11. 3



Şekil .11.4. Güvenlik duvarları arasında VPN

11.8 IPSEC

IEFT'nin IP Güvenliği çalışma grubu IPv4 ve IPv6 için,IP katmanı güvenlik mekanizması standardını geliştirdiler.IPSEC mimarisi, yetkilendirme ve kriptolamayı içerir. Bu mekanizmalar birlikte veya ayrı ayrı kullanılabilir.

11.8.1 Doğrulama Başlığı

IP doğrulama başlığı, IP data gramına,doğrulama bilgisini ekleyerek güvenliği sağlamayı araştırır. Bu doğrulama bilgisi, iletimde değişmeyen IP data gram alanları kullanarak hesaplanır. İletimde değişme gerektiren alanlar('hop sayacı', 'yaşama süresi' vs.) doğrulama bilgisinin hesabı için sıfır olarak düşünülür. Bu, mevcut Ipv4'ü daha güvenli hale getirir ve çoğu kullanıcının gereksinimini karşılar.

11.8.2 Güvenlik datasının bütünleştirilmesi(Encapsulating Security Payload, ESP)

ESP, IP data gramlarına bütünlük ve gizlilik sağlayan bir mekanizmadır. Bazı durumlarda, IP data gramlarına aynı zamanda doğrulama da sağlar. Mekanizma hem Ipv4 hem de Ipv6'da çalışır..

Doğrulama kullanılan algoritmaya göre sağlanabilir. IP doğrulama başlığı, doğrulamayı sağlamak için, ESP ile birleşmede kullanılabilir. Gizlilik olmadan bütünlük ve doğrulama isteyen kullanıcılar, ESP yerine IP doğrulama başlığı kullanmalıdırlar.

IPSEC'de ESP, bütün IP data gramını veya İletim katmanındaki bilgiyi şifrelemekte kullanılabilir(TCP,UDP.)

RFC'den alıntıya göre,Tünel mod ESP'de orijinal data gram, bütünleşik güvenlik datasının şifrelenmiş parçasına yerleştirilir ve bütün ESP frame'i şifresiz IP başlığı içeren data gramın içine yerleştirilir. Kriptosuz IP başlığı içindeki bilgi, güvenli data gramın başlangıçtan varışa kadar yönlendirilmesinde kullanılır. Kriptosuz IP yönlendirme başlığı, IP başlığı ve bütünleşik Güvenlik Datası arasında bulunabilir..

Transport moddaki ESP'de ESP başlığı, iletim katmanı protokol başlığına(TCP,UDP, veya ICMP). Bu modda Kriptolanmış IP başlıları veya OP opsiyonları olmadığı için, bant genişliği korunur.

11.9 PPTP:

PPTP, mikrosoft ile ortak çalışma sonucunda PPP(pointo Point Protokol) ün genişletilmesiyle geliştirilmiştir. . PPTP, IP,IPX, veya NetBEUI protokollerinin IP paketleri içerisinde tünellenmesi veya bütünleştirilmesidir. Mikrosoft ve NT sunucular tarafından desteklenmesi şirket ağına dışarıdan bir VPN ayarının yapılmasını mümkün kılar.

Kavramsal olarak, PPTP kullanılarak istemciden güvenlik duvarına olan haberleşme ile, IPSEC olanaklı IP yığınını kullanarak güvenlik duvarı ile haberleşen veya VPN teşkil edilmesi arasında fark yoktur. PPTP IP protokolü dışındaki protokolleri de destekler, bununla birlikte,

VPN 'in gerçeklenmesi dört farklı alanda anlaşmayı gerektirir.

Kriptolama mekanizması	swIPe , IPSEC , PPTP
Kriptolama algoritması	RC2, RC4, DES, 3DES, IDEA, CAST
Kriptolama ve anahtar değişimi anlaşması için mekanizma	ISAKMP, SKIP
Şifreleme anahtar değişim bilgisi için algoritma.	RSA , Diffie-Hellman

12 YIKIMDAN KORUMA VE GERİ KAZANMA(Disaster Prevention and Recovering)

12.1 Giriş

Günümüzde bilgi Teknolojisinde oldukça önemli gelişmeler yaşanmaktadır. Bu gelişmelerle beraber insanların Bilgi Teknolojilerinden beklentileri artmış ve yatırımların büyük bir bölümü bu alana yönlendirilmiştir. İnteraktif bankacılık, online alışverişler, fatura ödemeleri ve bunlar gibi daha birçok hizmet insanlara sunulmuştur.

Bilgi Teknolojilerinde bu tür gelişmelerin yaşanması beraberinde bazı zorlukları da getirmektedir. Aynı anda binlerce müşteriye hizmet vermesi düşünülerek planlanan servislerin ayakta kalabilmesi, müşteriyi memnun edecek hızda işlem yapabilmeleri oldukça kompleks modeller ortaya çıkarmaktadır. Öte yandan bu sistemlerin servis dışı kalmaları da milyonlarca dolar zarara mal olabilmektedir. Bu sebeple *acil durum planlaması* yapma ve problemleri teşhis önem verilmesi ve sistemle birlikte idame edilmesi gereken kavramlardan birisi konumuna gelmiştir.

12.2 Acil Durum Metodolojisi

Acil durum metodolojisi, belirli bir hizmeti veren servislerin, anormal davranışlar sergileyerek tümünün ya da bir kısmının işlevselliğini yitirmesi ve servis dışı kalması esnasında uygulanması gereken program olarak tanımlanır. Acil durum metodolojisinde problemlerin ve risklerin tanımlanması, bu risklerin azaltılma sı amacıyla neler yapılması gerektiğinin belirlenmesi ve bu riskler gerçekleştiği esnada nasıl bir planla iyileştirme sürecine girileceğinin saptanması önemlidir.

12.3 Risklerin Tanımlanması

Bu aşama maliyet etkinliği oldukça yüksek bir aktivite olmasına karşın bir çok sistemde ihmal edilmektedir. Risklerin saptanmadığı bir sistemde, sağlıklı bir şekilde problemlerden sakınma yollarının belirlenmesi ya da acil durum planlaması yapılması düşünülemez.

Akla uygun ve pahalı olmayan ölçülerle riskin saptanması, binlerce dolara mal olabilecek felaketleri, gelir, güven ve prestij kayıplarını önlenebilir. Bir organizasyonun işlevselliğini etkileyebilecek faktörlerden birkaçı şu şekilde sıralanabilir:

- Donanım problemleri
- Zararlı saldırılar (ağ atakları, virüs vs)
- Görevli personel faktörü
- İklim koşulları
- Yangın, sel baskını gibi doğal etkenler
- Güç kaynaklarındaki voltaj dalgalanmaları
- Elektrik kesintisi
- Teçhizatın çalınması vs.

Bu risklerin tanımlanması esnasında ilgili kuruluşun yetkili görevlileri bir araya gelmelidir. Sistemin sahip olduğu varlıklar (assets) belirlendikten sonra bu varlıkların hangi tehditlere karşı ne derecede zafiyetler içerdiği tartışılarak belirlenmelidir. Her sistemin kendine has özellikleri, koşulları olacağından risklerin belirlenmesinde izlenecek en sağlıklı yol budur. Daha sonra bu riskler birbiri ile kıyaslanarak maliyet etkin ve minimum tehdit dengesine göre hangi risklerin giderilmeye çalışılacağı belirlenmelidir.

12.4 Problemlerden Sakınma

Problemlerden sakınma yukarıda tanımlanan risklerin ışığında yapılan çalışmalardan ibarettir. Sistemlerin yedeklemesinin sıklığı ve doğruluğu, yedeklemenin yapılacağı medyanın tipi, donanım ve yazılım envanter listesi, kesintisiz güç kaynakları, virüs tarama yazılımı vs. Bu aşamaya başlamadan önce bazı noktalara dikkat edilmesi gerekmektedir:

- Bütün teçhizatın, özellikle bilgisayar ve haberleşme öğelerinin detaylı envanteri çıkarılmalıdır. Bu envanterler her zaman güncel tutulmalıdır. Envanterler bütün yazılımları, donanımları, haberleşme cihazlarını, yedekleme medyalarını ve güç kaynağı cihazlarını kapsamalıdır. Envanter şu bilgileri içermelidir:
  - Model ve Seri Numaraları
  - Miktar
  - Üretici firma ya da sağlayıcı
  - Alternatif üretici firma ya da sağlayıcı
  - Kullanılabilirliği
- Acil durumlarda ya da felaketlerin oluşma ihtimaline karşı aynı bölgede bulunan bir firma ile bakım ve onarım anlaşması imzalanmalı.
- Kullanılan araç, yazılım ya da verinin garanti kapsamlarını belirlenmeli.
- İlgili ortamda bulunan kritik ağ bileşenlerini, işlemleri, servisleri, uygulama sistemlerini belirleyen bir yönerge hazırlanmalı
- Bir sonraki başlıkta geçecek acil durum kotarma stratejileri belirlenmeli.

Felaketlerden sakınma acil durum kotarma ve iş devam planının anahtar elementi olmalıdır. Felaketlerden sakınma, riskleri minimize etme ya da eleme noktalarında yardımcı olur, firmanın acil durum ya da felaketlerde minimum seviyede etkilenmesini sağlar. Aşağıda genel bir acil durum sakınma planının genel başlıkları bulunmaktadır. Bu plan genel anlamda konuyu ele almakta olup eksiksiz bir plan olarak kabul edilmemelidir.

12.4.1 Çalışanların bilinci

Güvenlik ve emniyet bilinci acil durum sakınma programının kritik noktalarından biridir. Birçok problem eğitimli personelin felaketle sonuçlanabilecek durumları gözlemesiyle engellenebilir. Bu sebeple yönetimde bulunanlara sistemi gözetleyecek, potansiyel güvenliği ortaya çıkaracak, acil durumlara mahal verecek durum ya da koşulları bilecek personelin oluşturulmasına öncelik vermeleri gerektiği vurgulanmalıdır.

12.4.2 İmkanlar

İmkanlar ofisin genişliği, elektrik tesisatı dolabı, saklama alanı kapasitesi, elektrik ve mekanik işlere tahsis edilmiş dolapları ve çalışma kapsamında tahsis edilmiş diğer alanları kapsamaktadır.

12.4.3 Yangın Saptama ve Önleme

Her bir iş ünitesinde bulunan yangın saptama aletlerinin yeterli olduğu kesinleştirilmeli ve düzenli aralıklarla çalışıp çalışmadığı test edilmelidir.

12.4.4 İnsan Faktörü

Bu alan en az uğraşa mal olan alanlardan biri olmasına karşın genellikle ihmal edilmekte ya da problemleri giderme veya iş devam planlarını yapanlar tarafından hesaba katılmamaktadır. Fakat insan faktörünün nasıl göz önünde bulundurulduğu problemlerden sakınma ve giderme yolunda çok fazla öneme sahiptir.

12.4.5 Yerel Alan Ağı

Günümüzde YAŞ ortamları normalde her ne kadar Main Frame ortamları kadar kararlı olsalar da bu sistemlerin birçok kullanıcıya açık olması durumu düşünüldüğünde yeterince korunmadıkları görülmektedir. Bir çok iş ünitesinde bilgiyi işleme ve saklama işlemleri YAŞ üzerinden yapılmakta, ayrıca endüstriyel sistemlere de yine YAŞ üzerinden erişilmektedir. Bundan dolayı YAŞ ortamlarında belirli derecelerde güvenlik önlemleri alınmalı ve ortamın kararlı olması sağlanmalıdır.

12.4.6 Medya Kotarma ve bilgi Saklama

Manyetik medya insan, sıcaklık, manyetik alan, toz zerrecikleri gibi birçok faktöre karşı zayıflık göstermektedir. Bu zayıflıklar tespit edilip giderilmelidir.

12.4.7 Bakım ve Temizlik

Sistemlerin gerektirdiği periyodik bakım ve temizlikler yapılmalıdır.

12.4.8 Veri İletim Ağı

Veri iletim ağının sağlıklı ve kesintisiz çalışması hayati önem taşımaktadır. Bu nedenle veri iletim ağından beklenen sürekli çalışabilme ve istenen bant genişliğini sağlaması için gerekl iönlemler alınmalıdır.

12.4.9 Güç Kaynağı

Güç kaynağındaki ufak dalgalanmalar verinin kaybolmasına veya işlemlerin kesintiye uğramasına yol açtığı gibi kullanılabilirliğin de kaybolmasına sebep olur. Bu dalgalanmalar kaynağın kendisinden kaynaklanacağı gibi temizlik görevlileri gibi bilgisi az olan insanlar tarafından da sebep olunabilir.

12.4.10Mevsimsel Değişimler

Mevsimler arası meydana gelen sıcaklık değişimleri ve havanın yağışlı olması sebebiyle nem miktarındaki artış bazı servislerin kullanıcıya ulaşmasını etkileyebilir, yapılan işlemler üzerinde ters etkiler meydana getirebilir. Ayrıca yıldırım gibi etkenler elektrik kesintilerine sebep olabilir.

12.4.11Teçhizatın Çalınması

Bilgisayar ortamına sahip olanlar genelde bir cihazın çalınması ya da zarar görmesi durumunda sadece ilgili hasarın giderilmesini ya da yenisiyle değiştirilmesini düşünürler. Bu cihazlarda bulunan ve kaybolan veri genelde göz ardı edilir. Gerçekte çoğu zaman kaybolan veri cihazlara göre çok daha fazla zarara mal olur. Özellikle çalınan bilginin gizliliği ya da hassaslı fazlaysa zararın miktarı çok daha yüksek olabilir.

12.4.12Çok Önemli kayıtlar

Organizasyon için can alıcı olan kayıtlar belirlenmeli ve bu bilgilerin önemi nispetinde güvenlik seviyesi belirlenmelidir.

12.4.13İş İstasyonları

YAŞ ortamında çalışan organizasyonlarda işistasyonları Main Frameler'deki aptal terminallere çok daha fazla önem taşımaktadırlar. Bu sebeple iş istasyonlarından kaynaklanabilecek hatalar ölçülerek hesaba katılmalıdır.

12.5 Acil Durum Müdahale Planlaması

Problemlerden sakınma safhasını gerçekleştirdikten sonra, işleyen sistemlerde oluşabilecek diğer problemleri minimum kayıpla kotarabilecek *Acil Durum Planlaması* yapılmalıdır. Acil durum planlaması, acil durum öncesi, esnası ve sonrasında yapılabilecek faaliyetleri kapsamlı olarak ele alır. Acil durum planlaması belirli bir sürede bitecek bir proje olarak görülmemelidir. Etkili bir acil durum planı her zaman hayatta olan(live) plandır. Plan, operasyonların devamını ve acil durum esnasında kullanılacak kaynakların kullanılabilirliğini garantilemek için iyi dökümante ve test edilmelidir.

Acil durum planlamasının asıl hedefi bilgisayar servislerinin tamamının ya da bir kısmının kullanılamaz hale gelmesi durumunda organizasyonu korumaktır. Burada can alıcı nokta ön hazırlıkların yapılmasıdır. Ön hazırlık operasyonların kesintiye uğramasını minimize etmeli, belirli bir seviye kararlılığı ve acil durumdan sonra sistemli bir müdahaleyi garanti etmelidir. Acil durum planlamasının diğer hedefleri şunları içerir:

- Güvenlik kanısını vermelidir.
- Gecikmeleri minimize etmelidir.
- Yedek sistemlerin güvenliğini garanti etmelidir.
- Planın testi için standartları sağlamalıdır.
- Acil durum esnasında karar vermeyi (decision-making) minimize etmelidir.

Bu hedefler ışığında plan şu safhalardan oluşur:

- Plan öncesi aktiviteler
- Açıklık analizi ve gereksinimlerin genel tanımı
- İş Etki Yönergesi
- Gereksinimlerin detaylı analizi
- Plan geliştirme
- Programın testi
- Programın devamının sağlanması
- Planın başlangıç testi ve yerine getirilmesi

12.6 Programın Tanımlanması

Acil durum planlaması oldukça kompleks olduğu ve yoğun çalışma gerektirdiği için kaliteli personelin, bilgi işleyen kaynakların ve uygun bir bütçenin bu alana kaydırılmasını gerektirmektedir. Yetersiz kaynak ayırımından doğabilecek etkileri minimize etmek için acil durum planının uygulanması ve oluşturulması organizasyonun normal planlama aktiviteleri arasında yer almalı, arka plana itilmemelidir. Hedeflenen proje metodolojisi aşağıda tanımlanan sekiz safhayı içermektedir.

12.6.1 Safha1- Plan öncesi aktiviteler

Safha 1 organizasyonun varolan ve projelendirilen bilgisayar ortamını anlama amaçlıdır. Proje takımının projenin faaliyet alanını ve ilgili çalışma programını analiz etmesi, proje takvimi geliştirilmesi, projenin başarılması ve uygulanmasının ne gibi etkiler ortaya çıkaracağını saptaması adına bakış açısını belirler.

Bu safha esnasında Yönetim Kurulu kurulmalıdır. Bu kurul proje takımının yönlendirilmesi ve bu takıma rehber olabilme adına bütün sorumluluğu üstlenmelidir. Kurul ayrıca acil durum planlaması konusunda ne kadar çalışma yapılması gerektiği kararını vermelidir. Proje menajeri, detaylı iş planı çıkarılmasına ve güvenlik, iş etki analizi için gerekli olan görüşmelerin yapılma takviminin belirlenmesine kadar Yönetim Kurulu ile beraber çalışmalıdır.

Bu safhadaki iki kilit nokta müdahale programlarını destekleyecek politikaların geliştirilmesi ve bu projeye katılacak yöneticilerin ve kıdemli personelin bilinçlendirilmesidir.

12.6.2 Safha2- Açıklık analizi ve gereksinimlerin genel tanımı

Bir organizasyonda güvenlik ve kontrol, devamlılık arz eden bir kavramdır. Ekonomik ve iş stratejileri perspektifinden felaketlerin oluşumu riskinin azaltılması felaket oluşumunda ortaya çıkan etkileri azaltmaktan daha tercih edilebilirdir. Bu safha felaketlerin oluşma ihtimalini azaltmaya yöneliktir.

- Personelin pratiği, fiziksel güvenliği, işletimsel prosedürleri, yedekleme ve olasılık planlarını sistem geliştirme ve idamesini , veritabanı güvenliğini vs. içeren iletişim ve bilgisayar ortamının eksiksiz güvenlik yönergesinin oluşturulması
- Varolan acil durum ve felaket önleme planlarının geliştirilmesini ya da bu planların baştan oluşturulmasını sağlayacak güvenlik yönergesinin oluşturulması.
- Eldeki bulguların ve güvenlik yönergesindeki önerilerin yönetim kuruluna sunulması zamanlamanın da ayarlanmasıyla doru aksiyonların yerine getirilmesi.
- Planlama işgücünün sınırlarının tanımlanması.
- Planların geliştirilmesi destekleyecek ve idamesini sağlayacak yazılımların analizinin, teklifinin ve satın alımının yapılması.
- Plan iskeletinin oluşturulası
- Proje takımının kurulması ve bilinçlendirme seanslarının yönetilmesi

12.6.3 Safha3- İş etki Yönergesi

İş ortamının parçası olan ünitelerin iş etki yönergesi, kritik sistemlerin, fonksiyonların, işlemlerin tanımlanması, sistem servislerine erişimi engelleyecek kaza ve felaketlerin ekonomik etkilerinin saptanması, sistemlere, servislere erişilemeden iş ünitelerinin ne kadar ayakta kalabileceklerinin saptanmasını sağlar.

İş etki yönergesi raporu yönetim kuruluna sunulmalıdır. Bu rapor kritik servis fonksiyonlarını ve kesintiden sonra ne kadar süre içerisinde iyileştirilmesi gerektiğini tanımlar. Bu rapor daha sonra tanımlanan kritik sistemlere destek olacak sistemleri ve kaynakları tanımlamada temel olarak kullanılmalıdır.

12.6.4 Safha4- Gereksinimlerin detaylı analizi

Bu faz esnasında, müdahale gereksinimlerinin profili çıkarılır. Bu profil alternatif müdahale stratejilerinin analiz edilmesi için kullanılacaktır. Profil faz 3'de tanımlanan kritik fonksiyonlara destek verecek kaynakların tanımlanmasıyla geliştirilir. Bu profil donanımları, dokümanları, dış destekleri, imkanları ve her iş ünitesi için gerekli personeli içermelidir. Müdahale stratejileri kısa, orta ve uzun dönem aksamalar esas alınarak belirlenmelidir.

Bu fazdaki diğer kilit faaliyet ise plan kapsamının, hedeflerin ve varsayımların tanımlanmasıdır.

12.6.5 Safha5- Plan geliştirme

Bu fazda müdahale planı öğeleri tanımlanır ve planlar dokümante edilir. Ayrıca kullanıcı prosedürlerinde yapılan değişikliklerin uygulanması, müdahale stratejilerinin uygulanması için gerekli veri işleyen işletim prosedürlerinin güncellenmesi, alternatiflerin belirlenmesi, destek firmaları ile pazarlık çalışmaları, müdahale ekiplerinin tanımlanması, rolleri ve sorumluluklarının belirlenmesi gibi faaliyetler yapılır. Bunların yanında müdahale standartları bu fazda geliştirilir.

12.6.6 Safha6- Programın testi

Programın testi, tatbikatı bu fazda yapılır. Test/tatbikatın amaçları saptanır, alternatif test stratejileri belirlenir. Test stratejileri uygulanacak ortamlara göre adapte edilir.

12.6.7 Safha7- Programın devamının sağlanması

Planların idamesi gerçek müdahalenin başarısı açısından önemlidir. Planlar ilgili ortamın üzerinde yapılacak değişiklileri yansıtmalıdır. Sistemde herhangi bir değişiklik yapılırken müdahale planları da hesaba katılmalıdır. Eğer değişiklik yönetimi bulunmayan alanlar varsa bunlar tanımlanmalı ve uygulanmalıdır. Birçok müdahale yazılımı bu gereksinimi hesaba katmaktadır.

12.6.8 Safha8- Planın başlangıç testi ve yerine getirilmesi

Plan geliştirildikten sonra, planın ilk testleri yapılmalı ve plandaki gerekli modifikasyonlar bu testlere göre ele alınmalıdır. Bu fazdaki aktiviteler aşağıdadır:

- Testin amacının, bakış açısının saptanması
- Test gruplarının tanımlanması
- Testin kurulumu
- Testin yönetimi
- Test sonuçlarının analiz edilmesi
- Uygun bir şekilde plan değiştirilmesi

Planın testi sırasındaki bakış açısı büyük oranda müdahale stratejilerinin seçimine bağlıdır. Müdahale stratejileri belirlendiğinde belirli test prosedürleri yazılan planların kapsamlı ve doğru oluğunu garantilemek amacıyla oluşturulmalıdır.

Günümüzün durmadan değişen ortamında, insanlar daha az çabayla daha çok işler yapmanın yollarını ararken sistemleri ayakta tutmak daha fazla bir çaba gerektirmektedir. Planın doküman kısmı eksiksiz olarak hazır olsa da bu planların hızlı bir şekilde uygulanması, belirli problemlerle karşılaştığında hangi aksiyon listesinin yapılması gerektiğinin saptanması, ilgili uyarı prosedürlerinin bilinmesi, kritik sağlayıcı bilgilerinin hızlı bir şekilde elde edilmesi ciddi bir problemdir. Bu sebeple bu planlara önem verilmeli, gerekli personel istihdam edilmeli, eğer imkanı varsa acil durum müdahalesi yapabilen yazılımlar kullanılmalıdır.

13 AĞ KULLANIM POLİTİKALARI (Network Usage Policies)

Bir organizasyonun bilgi sistemi güvenlik yönetiminin başarılı olabilmesi için ağ kullanım politikası belirlemesi gereklidir. Bu bölümde verilecek olan ağ kullanım politikası modern bir kuruluşun güvenlik gereksinimlerine cevap verebilecek şeklidedir. Ancak buna uyulması zorunlu değildir. Daha basit veya daha karmaşık düzenlemeler seçilebilir. Bir güvenlik politikası yayınlandıktan sonra ağın dışında kalan kullanıcıların erişim hakkı alabilmesi sağlanmalıdır. Bazıları güvenlik politikasının aşağıdaki hususları içerebilecektir.

- Bir hizmetli rehberi
- Bir intranet WEB sunumcu sitesi veya sunumcuda paylaşılmış bir dosya
- Bütün sunumcu logon ekranları
- Bütün uzak logon bayrakları
- Ağ donanımı için bütün terminal ekranları

Ağ güvenlik politikasının belirlenmesi için ağdaki elemanların özetle aşağıdaki bileşenlerden meydana geldiği varsayılır.
Ses ve Elektronik bilgi taşımakta kullanılan bütün kablolar.
Ses ve Elektronik bilgi akışını denetleyen bütün elemanlar.
Kasa,Depolama birimleri,ağ arabirim kartları, bellekler, tuş takımları, ve kablolar gibi bütün bilgisayar parçaları.
Bütün Bilgisayar Yazılımı.
Yazıcı ve Faks makinası gibi bütün bilgisayar çıkış cihazları.

13.1 Ağ Yönetimi

Masaüstü bilgisayarların konfigürasyon değişimlerine kadar bütün ağın bakımı, operasyon personeli tarafından yapılır. Operasyon personeli haricindeki personelin konfigürasyon değişikliği yapmasına izin verilmez. Sistem konfigürasyonu için aşağıdaki aktivitelerin yapılması düşünülür.

- Yeni bir yere ağ eklenmesi
- Farklı bir işletim sistemi yüklenmesi için sistemin floppy sürücüsünün kullanılması
- Bir sistemin kapağının veya kasasının açılması
- Internetten çekilen bir yazılımın yüklenmesi

Donanım yönetimi için uyarılar ile birimlerin garanti dışı kalması önlenir. Yazılım lisanslarına uyulur. Yazılım desteği iç personel ile sağlanır.

13.2 Şifre Gereksinimleri

Sistemleri kullanabilmek için her bir çalışanın bir kullanıcı adı ve şifresi bulunmalıdır. Ağ kaynaklarına bu ikili ile erişebilmek mümkün olmalıdır.Her bir personel kendi şifresinin gizli kalmasını sağlamalıdır. Şifre korunması için aşağıdaki hususlara dikkat edilmelidir.

- Şifreler en az altı karakter olmalıdır.
- Şifreler çalışanın adı, firma adı gibi kolay bilinen türden olmamalıdır.
- Her kullanıcı şifresini en fazla 60 gün aralıkla değiştirmelidir. Şifresini değiştirmeyen kullanıcının hesabı kilitlenmelidir.
- Yetkilendirme sırasında üçten fazla yanlış şifre girilmesi durumunda hesap kapatılmalıdır. Hesabın açılması için şahıs, ağ işletim personeline başvurmalıdır.
- Her bir kurum bilgisayarında ekran koruyucu olmalı ve 15 dakikalık aktif olmama durumunda korumaya almalıdır. Kullanıcı yeniden kullanmak isterse yetkilendirme sürecini yerine getirmelidir.

- Ağa uzaktan bağlanmak için çevirmeli modem veya Sanal özel ağ kullanılması durumunda, her bir 60 saniyede şifre üreten bir güvenlik jetonu kullanmalıdır. Güvenlik jetonu tarafından üretilen şifreler kullanılmalıdır.
- Şifreler gizli olarak saklanmalıdır. Şifreler açık yerlere yazılmamalı, tanıdıklara verilmemelidir.
- Kurum dışındaki başka ağlara bağlanmak için farklı şifreler kullanılmalıdır. Bu sizin kritik şifre dizilerinin halka açık ağ üzerinden göndermenizi engeller.
- Kurum, kullanıcı şifresinden dolayı olabilecek hasarlardan kullanıcının sorumlu olması gerektiğini açıklamalıdır.

13.3 Virüs Koruma Politikası

Bütün Bilgisayarlar anti–virüs yazılımı ile korunmalıdır. Anti virüs yazılımlarının çalıştırılmasının kullanıcının kendi sorumluluğunda olduğu belirtilmelidir.Eğer bir virüs uyarısı alınırsa hemen ağ işletme personeli uyarılmalıdır.

Eğer ağ işletme personeli anti-virüs yazılımının güncellemesinden sorumlu olursa bu işlem otomatik olarak yapılmalıdır. Kendi virüs yazılımlarının 60 günlük sürede güncellemeyen kullanıcıları hesabı kapatılmalıdır.

13.4 İş İstasyonu Yedekleme politikası

Ağ işletim personeli haftalık bazda, her bir personelin iş istasyonundaki dokümanları yedekleme yapmalıdır. Personel haftanın belirlenen bir gününde bilgisayarının açık bırakarak yedekleme yapılmasına imkan vermelidir. Herkes dokümanlarının belli bir katalog da saklamalıdır. Örneğin C:\My Documents

13.5 Uzaktan Ağ Erişimi

Kurum, ağ kaynaklarına, ya modem havuzu yada Internet tabanlı VPN ler ile erişilmesine imkan sağlar. Uzaktan ağ erişimi ihtiyaç esaslı olarak sağlanır. Uzaktan ağa erişim ihtiyacı hisseden bir personel, kendi yöneticisinden geçen bir istek formunu ağ işletim bölümüne iletmelidir. Personele aşağıdaki bilgiler ve yazılımlar verilecektir.

- Ağ kaynaklarına erişmek için bir bilet,
- Modem havuzundaki telefon numaralarının listesi
- Internet üzerinde VPN oluşturmak için gerekli Yazılım.
- VPN Yazılımı kurulumu ile ilgili bilgiler
- Uzaktan ağa erişim için yönlendirmeler.

Ancak uzaktan erişim yapacak olan kullanıcının aşağıdaki birimlere ihtiyacı olacaktır.

- Bir Telefon hattı
- Bir modem
- Daha hızlı bir işlemci
- Ek Disk alanı

Ek olarak uzaktan ağ erişimi, ağ işletim personeli tarafından desteklenmelidir. Çalışan , bunun dışında kendi bağlantı problemlerini çözmekten sorumlu olacaktır. Aynı zamanda bu kişiler güvenlikten de sorumludurlar. Çünkü, şifrelerini, ve VPN yazılımlarını korumak zorundadırlar.

13.6 Genel Internet Erişim Politiakası

Kurumun Internet tabanlı sitelere erişimi iş esaslı olmalıdır. Bu politika, ağın verimli kullanılmasını , ve bütün personeli paylaşmasını sağlayacaktır. Yöneticiler, bu politika ve aşağıdaki hususlar çerçevesinde ağ kullanımını onaylamalıdırlar.

- Ağ kaynaklarının planlı olarak kullanımı en az olmalıdır.
- Ağ kaynaklarının planlı kullanımı çalışanın düzenli işini aksatmamalıdır.
- Ağ kaynaklarının planlı kullanımı, kurum amaçlarıyla uyuşmalıdır.
- Ağ kaynaklarının planlı kullanımı, eğitim amaçlı ve çalışanın iş fonksiyonunun içerisinde olmalıdır.
- Ağ kaynaklarının planlı kullanımı, herhangi bir site, eyalet veya ülke kanunlarının ihlal etmemelidir.
- Ağ kaynaklarının planlı kullanımı,ağı aşırı yüklemeyecektir.

13.6.1 Diğer Internet erişim Politikaları

Kullanılan web tarayıcılar uygun konfigürasyon ile kullanılmalıdır. Standart Netscape tarayıcının konfigürasyonu aşağıda verilmiştir..
Ek plug-in olmamalıdır.
Java ve JavaScriptler kapalıdır.
Otomatik Yükleme kapatılmış.
Cookies kapatılmış
E-posta ve Grup altındaki özdeşlik tabı siyahtır.

Bu konfigürasyonlar kullanıcının internette gezinirken, tehlikeli bir uygulamayı yüklemesini önleyecektir. Web tarayıcılar ağ işletim personeli tarafından yüklenmelidir. Yazılım lisanslarının korunması açısından kullanıcılar browser üzerinden yazılım yüklememelidirler.

Internet üzerinden gönderilen posta mesajlarının büyüklüğü 8 Mbyte'ı geçmemelidir. Fazla büyük olan dosyalar FTP ile transfer edilmelidirler.
Kurum ağ kaynakları kişisel Internet hesabı olarak kullanılmamalıdırlar. Bunlar,
Personel e-posta hesapları
Personel kabuk hesapları
Servis sağlayıcılardan verilen personel hesapları
Online sistemlerdeki personel servislerine şirket sistemlerinden erişilmemelidir.Bu Internet tabanlı sistemlerdeki şirket hesaplarını içermez.
Kurum ağa girişleri izlemelidir. Çalışanlar şifrelerini, dosyaları, ve/veya diğer gerekli kaynakları, korumalıdır.

KAYNAKÇA

1. Abrams,M.,and Podell,H. *Computer and Network Security***.**Los Alamitos,CA:IEEE Computer Society Press,1987.

2. Feistel H.,*Cryptography and Computer Privacy,*Scientific American,May 1973.

3. Konheim,A. ,*Cryptography: A Primer***.**New York :Wiley,1981.

4. Stallings W., *Network And Internetwork Security***,**New Jersey:IEEE PRESS,1995

5. W. Stallings,"Network Security Essentials" P.Hall 2000 ,ISBN0-13016-093-8

6. **W. Stallings**, "Cryptography and Network Security",P.Hall 1999 ,ISBN0-0-13-869017-0

7. Chris Brenton., "Mastering Network Security", ISBN: 0-7821-2343-0