



T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLER ENSTİTÜSÜ

GÜVENLİK DUVARLARINDA TEST
YÖNTEMİ GELİŞTİRİLMESİ: TASARIM &
UYGULAMA

121300

Serkan KURT

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

**T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ**

TEZ DANIŞMANI
Yrd.Doç.Dr. Oya ERDİL

GEBZE

2002

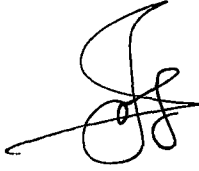
121300

Serkan KURT'un tez çalışması, G.Y.T.E Mühendislik ve Fen Bilimler Enstitüsü Yönetim Kurulu'nun 30.01.2002 tarih 2002/14 sayılı kararıyla oluşturulan jüri tarafında Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

:



(Tez Danışmanı)

Y.Doç.Dr. İbrahim SOĞUKPINAR

ÜYE

:



Doç.Dr. Osman Nuri UÇAN

ÜYE

:



Y.Doç.Dr. Mehmet GÖKTÜRK



G.Y.T.E Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 12.06.2002 tarih ve 2002/14 sayılı kararı.

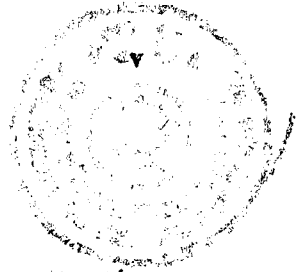
İmza / Mühür

ÖZET

Güvenlik Duvarları ağ güvenliğinde kullanılan ve en yaygın olan yazılım veya donanımdır. Piyasada bilinen Güvenlik Duvarı tipleri oldukça fazladır. Bu Güvenlik Duvarları tasarım açısından birbirlerinden farklılıklar göstermekte ve uygulama alanlarına göre tercih nedeni olmaktadır. Bazı Güvenlik Duvarları içerdikleri fonksiyonellik bakımından diğerlerinden üstün gözükselerde zayıflıkları olabilir. Dolayısıyla bir test yönetimi geliştirilip gerçekten de görüldüğü kadar güvenli olup olmadığı araştırılmalıdır. Test yöntemi geliştirilirken, performans, işletim sistemi, donanımsal yapı, yazılım, sistemin yapısı, vs. gibi belirli hususlar dikkate alınmalıdır. Ayrıca test yönteminin kullanıcıyı bilgilendirmesi ve yönlendirmesi de önemlidir.

Kurumlar için en önemli konulardan birisi de saygınlıktır. Bunun için de güvenlik ilk başta gelir. Bankacılığın bile internet üzerinde yapılır olması konunun hassasiyetini ortaya koymaktadır.

SUMMARY



Firewalls are hardware and software systems that protect a corporate network from attacks coming from the outside internet. There are several firewalls available in the market. Although some firewalls are stronger than others with respect to some security or functionality aspects, they may be weaker in others. Therefore it becomes necessary to find testing methodology that will ease the process of firewall comparison. Performance, operating system, hardware and software building, etc., properties are important to develop testing methodology. Testing methodology must be useful and give information to system administrator about configuration errors.

Prestige is very important for corporations. Because of this security is the first to take into consideration. Internet banking is used today, too.

TEŞEKKÜR



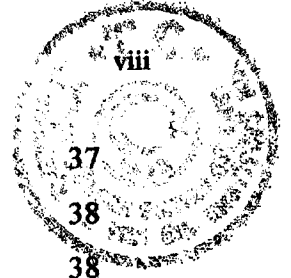
Çalışma esnasında bana değerli görüşleriyle yön veren danışman hocam Yrd.Doç.Dr. İbrahim SOĞUKPINAR'a, çalışmam esnasında maddi ve manevi desteğini esirgemeyen aileme ve isimlerini burada sayamadığım bütün arkadaşlarıma teşekkürü bir borç bilirim.



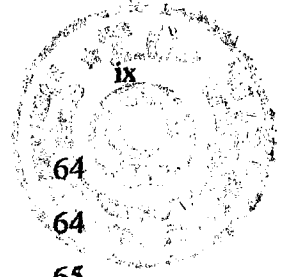


İÇİNDEKİLER DİZİNİ

ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER DİZİNİ	vii
SİMGELER VE KISALTMALAR DİZİNİ	x
ŞEKİLLER DİZİNİ	xi
TABLolar DİZİNİ	xii
1. GİRİŞ	1
1.1. Güvenlik Kavramı ve Güvenlik Duvarı	2
1.2. Kurumsal Güvenlik	2
1.3. Performans Kavramı	3
1.4. Performansın Kurumsal Ağ İçerisinde Ki Yeri Ve Önemi	3
1.5. Test Kavramının İncelenmesi Ve Güvenlik Duvarlarında Testin Gerekliliği	3
1.6. Güvenlik Duvarları Testi Konulu Yapılan Bazı Akademik Çalışmalar	4
2. GÜVENLİK DUVARI MİMARİLERİ VE TEST YÖNTEMLERİ	5
2.1. Ağ Kavramı	5
2.2. OSI ve TCP/ IP	5
2.3. Standartlar	32
2.4. Bazı İnternet Kaynakları	32
2.4.1. Haberler	32
2.4.2. Elektronik Posta	33
2.4.3. Gerçek Zaman Uygulamaları (Real Time Applications)	34
2.4.4. İnternet'e Erişim Yöntemleri	34
2.4.5. Terminal Erişimi	35
2.4.6. Ağ Erişimi	35
2.5. Güncel İnternet Konuları ve Güvenlik Kavramının Ele Alınması	36
2.6. Bilişim Sisteminizi Tehdit Eden Bazı Tehlikeler Ve Önlemler	36
2.6.1. Pasif Dinleme	37



2.6.2. Aktif Dinleme	37
2.6.3. Ana Bilgisayara Sızma	38
2.6.4. Kriptografi	38
2.6.5. Truva Atları	40
2.6.6. İnternet Bağlantıları	40
2.7. Saldırı Türleri	40
2.8. Güvenlik Duvarı Tanımı	42
2.9. Paket Filtreleme (Veri Paketleri Filtresi)	44
2.10. Vekil Sunucu (Proxy Server)	45
2.11. Güvenlik Duvarı Örnekleri	46
2.11.1. Paket Filtreleme Güvenlik Duvarı	46
2.11.2. Çift Taraflı Geçit (Dual-Homed Gateway)	47
2.11.3. Perdelenmiş Kullanıcı Tipindeki Güvenlik Duvarı -- Screened Host Firewall	49
2.12. Güvenlik Duvarı Tipleri	50
2.12.1. Yönlendirici Tabanlı Filtreleme	50
2.12.2. Devre Düzeyli Ağgeçitleri	51
2.12.3. Uygulama Düzeyi Firewalllar	51
2.13. Güvenlik Duvarı Yapıları	52
2.14. Test Kavramının İncelenmesi Ve Güvenlik Duvarlarında Testin Gerekliliği	53
2.15. Güvenlik Duvarları Testi Konulu Yapılan Çalışmalar	53
3. KURT TEST YÖNTEMİ	58
3.1. Güvenlik Duvarlarında Test Yöntemi Ve Güvenlik Duvarı Testleri	58
3.2. Güvenlik Duvarı Testleri	59
3.2.1. Donanımsal (Yapısal) Test	60
3.2.2. Yazılım Testi	60
3.2.3. Güvenlik Testi	60
3.2.4. Performans Testi	60
3.2.5. Yönetimsel Test	60
3.2.6. Kullanışlılık Testi	61
3.2.6.1. AltaVista Güvenlik Duvarı	97
3.2.6.2. Checkpoint Güvenlik Duvarı	62



3.3.Test PC	64
3.4.Test Yöntemi	64
3.5.Test Programın Yapısı	65
4.TEST YÖNTEMİNİN UYGULANMASI	66
4.1.Kurt Test Yönteminin Uygulanması	66
4.2.Yerel Ağın Tanınması	68
4.3.Port Tarama Sonuçları	68
4.4.Güvenlik Duvarlarında Tanımlanan Kuralların Testi	70
4.5.Mevcut Ağın Meşgul Edilmesi Ve Performansın Değerlendirilmesi	70
4.6.Analiz Sonuçlarının İncelenmesi	71
5. SONUÇ	73
KAYNAKLAR	75
ÖZGEÇMİŞ	76



SİMGELER VE KISALTMALAR DİZİNİ

TIS	Trusted Information Systems
LAN	Local Area Network (Yerel Ağ)
WAN	Wide area Network (Geniş Alan Ağ)
NAT	Network address Translation (Ağ adres Çevrimi)
ISO	International Standarts Organization (Uluslar arası Standartlar Organizasyonu)
TCP	Transmission Control Protocol (İletim Kontrol Protokolü)
IP	Internet Protocol (İnternet Protokolü)
RTP	Real-Time Transport Protokol (Eş Zamanlı Taşıma Protokolü)
DNS	Domain Name Service
FTP	File Transfer Protocol (Dosya İletim Protokolü)
SMTP	Simple Mail Transfer Protocol
ARP	Adress Resolution Protocol (Adres Çözümleme Protokolü)
UDP	User Datagram Protocol (Kullanıcı Datagram Prokokolü)
MAC	Media Access Control (Ortama Erişim Adresi)
OSI	Open System Interconnection
PDU	Protocol Data Unit (Protokol Veri Ünitesi)
SDU	Service Data Unit (Servis Veri Ünitesi)
GYTE	Gebze Yüksek Teknoloji Enstitüsü

ŞEKİLLER DİZİNİ



Şekil

2.1. İki Farklı Ağ ve Adresleme	25
2.2. İki Ağ Arasına Yönlendirici Bağlanması	26
2.3. Adres Konfigürasyonu	27
2.4. MS-DOS Ortamında "Route Print" Komutu	28
2.5. Yeni Bir Yönlendiricinin Ağa Eklenmesi	29
2.6. TTL Zamanının İncelenmesi	31
2.7. Ağa Sızma	37
2.8. Telnet ve SMTP için Paket Filtreleme Yapısı Örneği	45
2.9. Paket Filtreleme Güvenlik Duvarı yapısı	47
2.10. Yönlendirici ile desteklenmiş bir Dual-Homed Güvenlik Duvarı genel yapısı.	48
4.1. Test Bilgisayarının Güvensiz Ağ Üzerinden Güvenilir Ağda ki Hedef PC'yi Güvenlik Duvarı Üzerinden Testi	66
4.2. Test Bilgisayarının Güvenilir Ağ-1 Üzerinden Güvenilir Ağ-2 de ki Hedef PC'yi Güvenlik Duvarı Üzerinden Testi	67
4.3. Bir Posta Sunucusunun Güvenilir Ağ Üzerinden Port Taraması Sonuçları	69
4.4. Bir Posta Sunucusuna Güvensiz Ağ Üzerinden Yapılan Port Taraması Sonuçları	69
4.5. Güvenlik Duvarına Yapılan Port Taraması Sonuçları	70



TABLÖLAR DİZİNİ

Tablo	Sayfa
2.1. Üst Katman	7
2.2. Alt Katmanlar	8
2.3. PDU	9
2.4. Konfigurasyon Ve Çalıştırma Kıyaslaması	55
2.5. SOCKS ve FWTK Kullanımı Kıyaslaması	56





1. GİRİŞ

Bilgisayar Ağları kavramı ortaya çıkmasıyla birlikte Ağ güvenliği konusunda beraberinde gelmiştir. Çünkü şu anda internet üzerinde bankacılık işlemlerinin yapılıyor olması bile güvenlik konusunun önemini bir kez daha belirtmektedir.

Güvenlik Duvarları ağ güvenliğinde kullanılan ve en yaygın olan yazılımlardır. Piyasada bilinen Güvenlik Duvar tipleri oldukça fazladır. Bu Güvenlik Duvarları tasarım açısından birbirlerinden farklılıklar göstermekte ve uygulama alanlarına göre tercih nedeni olmaktadır. Bazı Güvenlik Duvarları içerdikleri fonksiyonellik bakımından diğerlerinden üstün özelliklerde zayıflıkları olabilir. Dolayısıyla bir test yöntemi geliştirilip gerçekten görüldüğü kadar güvenli olup olmadığı araştırılmalıdır.

Bu doküman da İnternet Güvenlik Duvarları ile ilgili olarak test yönteminin geliştirilmesi ve yapılan testlerin amacı anlatılmıştır ve test yönteminin geliştirilmesi konusu anlatımı sırasında öncelikle konuyla ilişkili olan Güvenlik ve Güvenlik Duvarı kavramları ele alınmıştır. Anlatımda yer alan Güvenlik Duvarları günümüzde en çok tercih edilen Güvenlik Duvarlarıdır.

Daha önce de bu konuda yapılan yapılan bir araştırmada [4] farklı bir test yöntemi geliştirilmiştir ve elde edilen sonuçlar bir tabloda sunulmuştur. Konu daha ayrıntılı olarak sonraki bölümlerde ele alınmıştır.



1.1. Güvenlik Kavramı Ve Güvenlik Duvarı

Günümüz iş dünyası, bilgi paylaşımının hızlı ve aynı zamanda güvenilir olması gerekliliğinin farkındadır. Kurumlar, bu tür ihtiyaçlarını İnternet üzerinden gerçekleştirebilmekte ancak beraberinde güvenlik açıklarından dolayı bu konuda çekingen davranmaktadırlar. Kurum veritabanına erişen bir saldırgan bu bilgileri kullanarak kurumun piyasada ki prestij ve finansal geleceğini çok rahatlıkla tehdit edebilir.

Kurumlar bazı güvenlik yazılımları, şifreleme gibi önlemleri alarak bu gibi durumların oluşmasını engellemeye çalışmaktadır. Güvenlik Duvarı internet ağından yerel ağı korumanın çeşitli yollarından birisidir. Ancak hızla gelişen teknoloji ile birlikte mevcut güvenlik sistemi bir süre sonra güvensiz hale gelebilir. Bu yüzden kurumlar tarafından teknoloji takip edilmeli ve esnek bir sistemle desteklenmelidir. Her kurum kendisine uygun bir güvenlik politikası oluşturmalı ve yapı mutlaka belirli testlerden sonra hayata geçirilmelidir. Bunun için ağ yapısı her yönüyle incelenmeli ve ihtiyaçlar doğrultusunda en uygun güvenlik politikası belirlenmekte, uygun tasarım yapıp, kuruluş gerçekleştirilmelidir. Gerekli test sonuçları incelenir ve sistem devreye alınır... [3,4,7]

1.2. Kurumsal Güvenlik

Kurumsal İnternet Bağlantıları'ndaki en önemli unsur şirketinizi dünyaya açtığınız zaman İnternet üzerinden gelebilecek olan saldırılar ve bunların sonucunda uğrayabileceğiniz maddi ve manevi hasarlardır.

Ağ güvenliğinde aşağıda belirtilen konuların incelenmesi gerekmektedir:

Şifreleme

Onaylama

Güvenlik Duvarı

Paket Filtreleme

NAT Sistemi

Vekil Sunucu (Proxy)

Virüs Koruma

Güvenlik Denetimi

Saldırı Tespiti



Diğer

İnternet ortamının çok hızlı gelişmesi sonucunda her geçen gün donanım ve yazılım bazında yeni güvenlik açıkları bulunmaktadır.

1.3. Performans Kavramı

Performans iş yapabilme kabiliyetidir. Bu birim zamanda yapabileceği iş miktarı gibi de tanımlanabilir. Performans denince akla ilk gelen kavramlardan bir tanesi de hız kavramıdır. Zira performans ve hız kavramları bir bütündür.

1.4. Performansın Kurumsal Ağ İçerisinde Ki Yeri Ve Önemi

Kurumsal ağ içerisinde ki veri alışverişinde ki hız, birim zamanda yapılabilecek iş miktarı ile doğru orantılıdır. Ayrıca birim zamanda gönderilebilecek veri miktarıda performans açısından önemlidir.

Örneğin bir bilgisayar üzerinde kullanıcı için gerekli olmayan servislerin kapatılması mevcut bilgisayarın performansını artıracaktır. Kurumsal bir ağda yapı incelenmeli ve gerekli testler ile performans artırımı sağlanmalıdır. Bu şekilde birim zamanda yapılan iş artacaktır.

1.5. Test Kavramının İncelenmesi Ve Güvenlik

Duvarlarında Testin Gerekliliği

Testin amacı; mevcut Güvenlik Duvarı Sisteminin amacına uygun bir şekilde çalışır olduğundan emin olmak ve tanımlanan kuralların (rule) istenilen şekil de olup olmadığından emin olmaktır. Ayrıca performans artırımı için yapılabilecekleri analiz etmektir. Burada bahsedilen Güvenlik Duvarı sistem testi, sadece Güvenlik Duvarını değil Güvenlik Duvarı ile birlikte çalışan sisteminde bir bütün olarak gözden geçirilmesidir.

Güvenlik Duvarı Sisteminin testi, sitem işleyişinin istenilen şekilde işleyip işlemediğini ve performansından emin olmaktır.



Hata mesajları anlaşılır ve çözüm getiren açıklamalar içermelidir. Donanımsal veya yazılımsal olarak her tipteki hata analiz edilebilir olmalıdır. Çünkü bir hata olduğunun sistem tarafından bildirilmesi hatanın kaynağının bildirilmemesi veya bilinmeyen bir hata mesajı alınması istenilen bir durum değildir. Testin bir amacında bilinmeyen yani öncesinde analiz edilmeyen bir hata durumunu araştırmak olmalıdır.

Güvenlik açığının en önemli nedeni mevcut sistem yapılandırmasının hatalı yapılandırılmasındandır. Bir Güvenlik Duvarı sistemi oluşturulduğunda mutlaka gerekli testlerden geçirilip yapıdan emin olunmalıdır.

1.6. Güvenlik Duvarları Testi Konulu Yapılan Bazı

Akademik Çalışmalar

İlk olarak bahsedeceğimiz makale çevirisi Khalid Al-Twai ve İbrahim A. Al-Kaltham tarafından yapılan ve konusu “Evaluation and Testin of Internet Firewalls” olan yani “İnternet Güvenlik Duvarlarının Değerlendirilmesi ve Testi” konulu bir araştırmadır. Araştırmanın amacı internet güvenlik duvarlarının değerlendirilmesi ve piyasada iyi bilinen iki güvenlik duvarınında ele alınarak test yöntemlerinin anlatımına yer verilmesidir, [4]

Anlatımda bazı mevcut güvenlik duvarı ürünleri açıklanmış. 1) Trusted Information Systems Inc. Tarafından geliştirilen TIS Güvenlik Duvarı aracı 2) D. Koblas tarafından geliştirilen socs kütüphaneleri. Bu çalışma bölüm 2 de daha ayrıntılı olarak ele alınmıştır.

Bir diğer akademik çalışma da H. Joseph Wen (School of Management, New Jersey Institute of Technology, Newark, USA) ve Jyh-Horng Micheal Tarn (Information Systems, Department of Business, Chowan College, Murfreesboro, USA) tarafından yapılan İnternet Güvenliği: Güvenlik Duvarı Seçimindeki Hususlar (A Case Study of Firewall Selection) konulu çalışmadır[2]. Bu çalışmada da yine Güvenlik Duvarı mimarileri incelenmiş ve güvenlik duvarı seçiminde dikkat edilmesi gereken hususlar anlatılmıştır. Genel olarak paket filtreleme, kullanıcı onaylama (User Authentication), Uyarı Denetimi gibi özellikler incelenmiştir.

2. GÜVENLİK DUVARI MİMARİLERİ VE TEST YÖNTEMLERİ

2.1. Ağ Kavramı

Bilgisayar ağı, bilgisayar ve benzeri sayısal sistemlerin belirli bir protokol altında iletişimde bulunmasını sağlayan sistemdir. Ağ üzerindeki bilgisayarlar, birbirlerinden çok uzakta olsalar bile aynı protokol sayesinde karşılıklı çalışabilirler. Karşılıklı çalışma, ağ üzerindeki iki sistemin uygulamaya dönük ortak işlemler yürütmesi olarak tanımlanabilir.

Bilgisayar ağı genel olarak geniş bir anlama sahiptir. Bir ofis içerisinde birkaç bilgisayar ve yazıcının bir HUB cihazı üzerinden bağlanıp belirli bir protokol altında haberleşmeleri de bir ağ oluşturur, internet te bir ağıdır. Ağın büyüklüğü ne olursa olsun, kapsamında , iletişimde bulunacak uç sistemler, ağı oluşturan HUB, switch, Yönlendirici gibi ağ cihazları, kablolu alt yapısı vardır. Bir ağ, LAN, WAN, kampüs ağı ve uzak bağlantılar olarak adlandırılan dört parçadan oluşur.

LAN (Yerel Ağ)

Kampüs Ağı

WAN

Uzak bağlantı

Herbir parçanın kendisine has teknolojisi ve standartları vardır.

2.2. OSI ve TCP/ IP

OSI (Open System Interconnection) Referans Modeli:

Modern bilgisayar ağları yapısal olarak tasarlanmıştır. Tasarım karmaşıklığını azaltmak için ağlar, herbiri diğeri üzerine inşa edilmiş bir katman şeklinde düzenlenmiştir.

OSI başvuru modeli ISO (International Standart Organization) tarafından sunulan bir model üzerine geliştirilmiştir. Bu model ISO- OSI (Open System

Interconnection) başvuru modeli olarak adlandırılır. Zira açık sistemlerin, yani diğer sistemlerle haberleşmeye açık sistemlerin bağlantısı ile ilgilidir. OSI modeli yedi katmandan oluşur. Bu katmanların oluşturulmasında uygulanan prensipler:

İletim işlemlerinde, her seviyenin altında değişik seçenekler oluşuyorsa yeni katman oluşturulmalıdır. Her katman iyi tanımlanmış bir işi yerine getirmelidir. Her katmanın işlevi standartlaştırılmış uluslararası protokoller açısından seçilmelidir. Katman sınırları arayüzler arası bilgi akışını en aza indirecek şekilde seçilmelidir.

Katmanların sayısı belirgin işlevlerin aynı katmanlar üzerinde taşma yapmayacak kadar fazla, mimariyi hantallaştırmayacak kadar az olmalıdır.

Bilgisayarın iletişime geçmesi için Uluslararası Standartlar Organizasyonu (ISO)-International Standart Organization tarafından geliştirilen ve OSI- Open System Interconnection denilen bir referans modeli geliştirilmiştir.

ISO, OSI' yi yedi katmana ayırmış ve birbiriyle iletişime geçecek iki bilgisayar arasında bağlantının nasıl kurulacağını modellemişlerdir. Bu model de kendi içinde ikiye ayrılmıştır. *Üst katman* ve *Alt katman* olmak üzere.

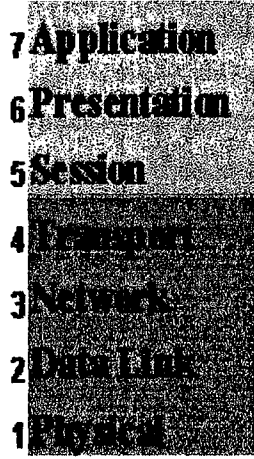
Üst katman içinde bulunan ilk üç, bu modelleme yapısında Uygulama-Application katmanı olarak gösterilir.

Her iki katmanda kendisine eş diğer katmanlarla iletişime geçer. Her katmandaki parçacık bir sonraki parçacığın çalışması için ortam ve servis sağlar.

Bu katmaların her ikisinde de *Protokol Veri Ünitesi-Protocol Data Unit* ve *Servis Veri Ünitesi-Service Data Unit* denilen yapılar bulunur.

PDU: Birebir bağlantılarda kullanılır.

SDU: Başlık bilgisi içeren alanlardan oluşur. Bu da her katmanda hangi parçacık olduğunu tanımlar. Bir üst katmanda neyin olduğunu gösterir.



Application

Uygulama
(Application)

Data Transport

Veri İletişim-Data Link

Katmanlanmış bir model bize şöyle avantajlar sağlar:

Modüler bir mühendislik tasarımı

Karmaşıklığı ortadan kaldırma

Gelişmeyi hızlandırma

Arayüzleri standartlaştırma

Ortak çalışabilir teknolojiler elde etme

Öğrenmeyi kolaylaştırma.

Üst Katmanlar:

Üst katman OSI iletişim modellemeye, iletişimin son aşamasına odaklanmıştır. Aşağıda her katman için bir örnek verilmiştir. Şimdi üst katman ile ilgili tablo.2.1.'i inceleyelim:

Tablo.2.1. Üst Katman

KATMAN	Fonksiyonu	PDU	İşaretleyici
Uygulama e-mail ve dosya transferi	İletişimde kullanılacak arayüzü sağlar	Pasif	Pasif
Sunum ASCII, EBCDIC JPEG, GIF, Resim MIDI, MPEG	Uygulama katmanındaki verilerin sıkıştırma,şifreleme ve bir sonraki katmanın kullanması için uygun hale getirme.	Pasif	Pasif
Oturum SQL, RPC, NFS	Uygulamalar arasında sonlandırma, yeniden başlatma, bağlantı kurma ve iletişim senkronizasyonu sağlar.	Pasif	Pasif

Alt Katmanlar:

Alt katmanlar ağ iletişimine odaklanmışlardır, bilgisayarlar arasındaki iletişim bu katmanlar ile sağlanır. PDU' lar alt katmanın her aşamasında kullanılır. Bu katman Data Link Katmanı olarak adlandırılır. Ek olarak bu katmanda verinin hata kontrolü yapılır.

Transport PDU= Segment

Network PDU=Paket

Data Link PDU= frame (Çerçeve)

Physical(Fiziksel) PDU=bit' ler.

Tablo.2.2. Alt Katmanlar

KATMAN	Fonksiyonu	PDU	İşaretleyici
İletim TCP/ UDP SPX	Pencereler kullanarak daha güvenli veri iletişimi sağlarlar. Hata denetimi için gelen verinin sırası izlenir.	Segmentler	Port
Ağ IP IPx rarp arp	Hiyerarjik, lojik adresleme kullanarak yol belirlenmesi işlemini yapar. İletişime geçeceği bilgisayarı bilir.	Paketler	Protocol
Veri Bağı ETHERNET_II 802.3/ 802.2 SNAP Frame- Relay	Fiziksel adres ve hata denetmi ile ulaşmak istenen yere gitmeyi sağlar. İki alt katmanı vardır: LLC- Servis Adres noktaları ve taşıma kontrolü yapar. Protokol erişimlerinin ağ katmanlarına ulaşmasını sağlar. MAC- Cihazı tanımlayan ona ait tek adrese ulaşmayı sağlar.	Frame'ler	SAP
Fiziksel EIA/TIA-232 V.35	Elektriksel ve mekaniksel fonksiyonlar ve prosedürel arayüzler kullanarak sinyalleme ve zamanlama işlemini yaparlar.	Bit' ler	



Bire Bir (Peer to Peer) :

Bir segment başlığı, İletim katmanı-Transport SDU, 1 adet port alanı içerir.

Port bir yön belirleyicidir. Verinin hangi uygulamalar için olduğunu belirtir,

Bir paket başlığı, Ağ katmanı-Ağ SDU, bir protokol alıcısı içerecek. Protokol bir yön belirteçidir. İletim-Transport katmanı için veriyi hazırlar.

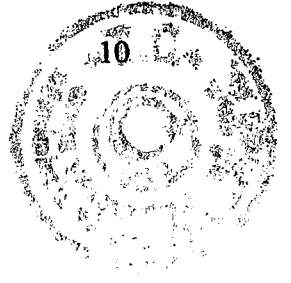
Bir çerçeve, veri Link-DataLink katmanı SDU, Servis Erişim noktaları ve tip alanları içerir. Bu alanlar yön belirtir. Ağ katman protokolünün kullanılması için veri hazırlanır.

İki katman arasında bilgi geçişi için, her katman direct olarak diğer cihazlar ile iletişime geçebilir. PDU' lar bütün katmanlar arasında bilgi taşırlar. Alt katmandaki SDU' lar üst katmanlardaki PDU' lar için servis sağlarlar.

Tablo.2.3. PDU

	Bire-Bir	
Uygulama	Uygulama PDU	Uygulama
	Bire-Bir	
Sunum	Sunum PDU	Sunum
	Bire-Bir	
Oturum	Oturum PDU	Oturum
	Bire-Bir	
İletim	İletim PDU	İletim
	Bire-Bir	
Ağ	Ağ- PDU	Ağ
	Bire-Bir	
Veri Bağı	Veri-hat PDU	Veri Bağı
	Bire-Bir	
Fiziksel	Fiziksel PDU	Fiziksel





Yedi Katmanlı Model

Tanımlanan yedi katman:

- 7) Uygulama: Uygulamalara değişik hizmetler sunar.
- 6) Sunum: Bilgi şeklinin çevrimini sağlar.
- 5) Oturum: Haberleşme ile ilgili olmayan problemlerle ilgilenir.
- 4) İletim: Uçtan uca haberleşme denetimi sağlar.
- 3) Ağ: Ağ üzerindeki bilgiyi yönlendirir.
- 2) Veri Bağı: Bağlı uçlar arasında hata denetimini sağlar.
- 1) Fiziksel: İletim ortamına bağlantıyı sağlar.

Fiziksel Katman:

Fiziksel katman ham bitleri bir haberleşme kanalı üzerinden iletmekle yükümlüdür. Tasarımın amacı, bir uçtan "1" biti gönderildiğinde, karşı tarafta da "0" değil "1" bitinin alınmasını sağlamaktır. Tipik sorunlar, "1" veya "0" bitini temsil etmek için kaç volt kullanılmalıdır, bir bit kaç mikrosaniye tutulmalıdır, aynı anda iletimin iki yönlü olup olmayacağı, ilk bağlantının nasıl kurulacağı ve iki taraf iletimi bitirdiğinde bağlantının nasıl sonuçlandırılacağı vs.. Tasarım konuları fiziksel katman altında yer alan mekanik, elektirksel ve fiziksel iletim ortamıdır. Fiziksel katmanın tasarımı elektrik mühendisliği kapsamında ele alınabilir.

Veri Bağı Katmanı:

Veri Bağı katmanın ana görevi, ham iletişim işini alıp, ağ katmanında hatasız olarak görünen bir hatta çevirmektir. Bu görevi gönderenin verisini, veri çerçevelerine (Data Frame, genellikle birkaç yüz byte'lık) bölüp, sıralı olarak gönderip, alıcının geri döndürdüğü onay pencerelerini işleyerek yerine getirir. Fiziksel katman bitlerin yapısı ile ilgilenmeden iletildiğinden çerçeve sınırlarını oluşturmak ve algılamak veri bağı katmanına bağlıdır. Bu, her pencerenin başına ve sonuna özel bit desenleri eklenmesi ile gerçekleştirilir. Eğer eklenen desenlerin veri bölümü içinde yer alma olasılığı varsa, karışıklığı engellemek için dikkat edilmelidir. Veri bağı katmanı ayrıca bağlı noktalar arası hata denetimini sağlamalıdır.

Veri bağı katmanında karşılaşılan diğer bir problem ise (Ayrıca diğer katmanlarda olacağı gibi) gönderen tarafı boğmadan yavaş bir alıcının veriyi sağlıklı nasıl alacağıdır. Bunun için ileten tarafın belirli bir anda alan tarafta ne kadar



miktarda tampon bellek boşluğunu bilmesini sağlayacak, trafik akışını denetleyecek bir mekanizmanın kurulması gereklidir.

Eğer hat iki yönlü iletim için kullanılabiliriyorsa bu, veri başı katmanı tarafından çözülmesi gereken başka bir problemi ortaya çıkarır. Problem A ucundan B ucuna doğru olan trafikte, B' den A' ya onay çerçevelerinin A' dan B' ye veri çerçeveleri ile çakışmasıdır.

Ağ Katmanı:

Ağ katmanı, alt ağda yapılan işlerin denetimi ile ilgilidir. Tasarımında anıtar konu veri paketlerinin gönderenden alıcıya nasıl yönlendirileceğidir. Yönlendirmeler sabit tablolara dayalı ve sıkça değişmeyecek şekilde ağ ile birlikte tanımlanmış olabilir. Bu yönlendirmeler ayrıca bir uç birim oturumunda olduğu gibi, her oturum için ayrıca belirlenebilir. Son olarak anlık ağ yüküne bağlı olarak her bir yeni paket için yeniden belirlenecek şekilde dinamik olabilir.

Aynı anda birbirinin rotasında çakışan paket ağa sunulursa performans sıkıntıları oluşabilir. Bu tür çakışmaların önlenmesini sağlamak ağ katmanının sorumluluğundadır. Ağ operatörleri hizmeti paralı olarak sunmak istediklerinde ayrıca bir ağ katmanı üzerinde raporlama özellikleride eklenebilir. Sonuç olarak, bir yazılım aracılığı ile her müşterinin ilettiği veya aldığı paket veya karakter sayısı faturalama bilgisinin oluşturulabilmesi için sayılır. Raporlama, değişik ücretlendirme oranlarının uygulandığı sınırları geçildiğinde daha karmaşık bir hal alabilir.

Bir paket hedefine ulaşmak için bir ağdan diğer ağa geçmek zorunda kaldığında başka problemlerde baş gösterebilir. Adresleme, ağlar arında farklı olabildiği gibi bir ağ diğerinden çok geniş olduğu için paketi kabul etmeyebilir veya protokoller farklı olabilir. Heterojen ağların ara bağlantılarının sağlıklı bir şekilde yapılıp bu problemlerin üstesinden gelme ağ katmanının sorumluluğundadır.

İletim Katmanı:

Aktarım katmanının temel işlevi oturm katmanından veriyi alıp, ihtiyaç duyulduğunda küçük bileşenlere ayırıp ağ katmanına geçirerek, diğer uca bu parçaların doğru bir şekilde ulaştığına emin olmaktır. Ayrıca bu işlev oturum



katmanının donanım teknolojisindeki kaçınılmaz gelişmelere karşı izole edilerek verimli olarak yerine getirilmelidir.

Normal şartlar altında, aktarım katmanı, oturum katmanı tarafından ihtiyaç duyulan her taşıma bağlantısı için bir sanal ağ bağlantısı oluşturur. Eğer taşıma bağlantısı yüksek bir kapasite isterse, aktarım katmanı birçok ağ bağlantısı oluşturup, kapasiteyi arttırmak için veriyi bu bağlantılara paylaştırır. Öte yandan, farklı ağ bağlantılarının oluşturulması maliyeti artırdığı durumlarda aktarım katmanı çeşitli taşıma bağlantılarını bir ağ bağlantısı üzerinde maliyeti azaltmak için de birleştirebilir. Tüm durumlarda aktarım katmanının birleştirme işinin oturum katmanına yansımaması gereklidir.

Aktarım katmanı ayrıca oturum katmanına – sonuç olarak ağ kullanıcılarına – ne tür hizmetler sunulacağına karar verir. Taşıma bağlantısının en uygun türü veriyi gönderildiği sıra ile hatasız uçtan- uca ulaştıran kanallardır. Ancak, diğer tür taşıma, hizmet ve taşıma bilgisine ayrılmış mesajları değişik noktalara ileten ve hedefine ulaştırma konusunda herhangi bir garanti vermeyenidir. Hizmet tipi bağlantı sağlandığında belirlenir. Aktarım katmanı, gerçek bir gönderenden alıcıya veya uçtan uca katmandır. Başka bir deyişle, kaynak sistemde çalışan bir program, mesaj başlıkları ve denetim mesajlarını kullanarak hedef sistemdeki benzeri bir programla konuşabilir.

Birçok bilgisayar üzerinde birden fazla program çalıştırır, yani sisteme giren ve çıkan birçok bağlantı vardır. Bu yüzden hangi mesajın hangi bağlantıya ait olduğunun belirlenmesi için bir yöntem ihtiyacı duyulur. Aktarım başlığı bu tür bilgilerin konuşlandırılabilceği bir yerdir. Değişik mesajları bir kanal içinde birleştirmenin yanında, aktarım katmanı ağ boyunca bağlantıların kurulması ve çözülmesini de takip etmelidir. Bu, bir bilgisayar üzerinde kiminle konuştuğunu tarif edecek bir tür isimlendirme mekanizması gerekliliğini doğurur. Ayrıca hızlı bir bilgisayarın yavaş bir bilgisayarı tıkaşması için bilgi akışını düzenleyecek bir mekanizma da gereklidir. Her ne kadar ikisine de aynı prensipler uygulansa da uçlar arasındaki akış denetimi anahtarlar arası akış denetiminden ayrıdır.



Oturum Katmanı:

Oturum katmanı, değişik makinelerdeki kullanıcıların birbirleri arasında oturum açmasını sağlar. Bir oturum taşıma katmanının yaptığı gibi sıradan veri taşıma işini gerçekleştirdiği gibi, bazı uygulamalarda çok yararlı gelişmiş hizmetlerde sunar. Bir oturum bir kullanıcının uzaktaki zaman paylaşımli bir sisteme bağlanmasını (Log-on, Log-in) veya iki makina arasında dosya iletimi yapmasını sağlar.

Oturum katmanının sunduğu hizmetlerden biri de sistemlerin karşılıklı iletimlerinin yönetimidir. Oturumlar aynı anda tek yönlü veya aynı anda çift yönlü veri akışına izin verebilirler. Eğer oturum tek yönlü ise oturum katmanı iletim sırasının kimde olduğu konusunda yardımcı olur.

İlgili diğer bir oturum hizmeti jeton (Token) yönetimidir. Bazı protokoller için, her iki tarafın aynı anda aynı işlevi yerine getirmeye çalışmaması çok önemlidir. Bu aktiviteleri yönetmek için oturum katmanı taraflar arasında değiştirilebilecek jetonlar sağlar. Jetone sahip taraf kritik uygulamayı çalıştırma hakkına sahip olur.

Sunum Katmanı:

Sunum katmanı, kullanıcıların problemlerine kendi başlarına çözüm bulmaları yerine onlara yeterli bir genel çözüm sunar. Kısaca, diğer katmanların aksine, bitleri bir uçtan diğerine güvenli bir şekilde iletilmeleri yerine sunum katmanı iletilen bilginin söz dizimi ile ilgilenir.

Sunum hizmetlerine tipik bir örnek, standart, üzerinde anlaşılan bir şekilde veriyi kodlamaktır. Birçok kullanıcı programları rastgele bit dizilerinin kendi aralarında alış verişini gerçekleştirmez; şahıs adları, tarih, para gibi şeylerin alış verişini yaparlar. Bunlar başlıklar, karakter dizileri, tamsayılar, kayan nokta numaraları gibi daha basit veri yapıları olarak ifade edilirler. Değişik bilgisayarlar karakter dizileri ve tamsayıları ifade etmek için değişik kodlar kullanırlar. Bu bilgisayarlar arasında veri alış verişini standartlara uygun olarak yerine getirmek sunum katmanının işidir.

Uygulama Katmanı:

Uygulama katmanı sıkça ihtiyaç duyulan bir çok protokolü içerir. Örneğin dünyada birbirine uyumsuz yüzlerce uç birim türü vardır. Herbirinin farklı ekran düzenleri, metin silme ve düzenleme için farklı kaçış (Escape) dizileri, imleç konumlandırması vs. kullanan değişik uç birimlerle çalışan bir takım ekran metin editörünü ele alalım.

Bu problemi çözmenin yolu editörlerin ve diğer programların yazabildiği sanal bir ağ uç birimi oluşturmaktır. Her uç birim türünü karşılamak için, sanal uç birim işlevlerinin gerçek uç birim üzerine eşleşmesini sağlamak için bir yazılım yazılmalıdır. Örneğin bu yazılım, editor sanal uç biriminin imlecini sol üst köşeye konumlandığında, yazılım gerçek uç birimde imlecin asıl konumuna yerleşimi için düzgün komut dizisini işlemelidir. Tüm sanal uç birim yazılımları uygulama katmanındadır.

Uygulama katmanının bir diğer işlevi de dosya iletimidir. Değişik dosya sistemleri, değişik dosya isimlendirme tanımlamalarına, metin bilgisinin temsili için değişik yöntemlere sahiptirler. Değişik dosya isimlerinden dosya iletimi işlemleri bu uyumsuzlukları ortadan kaldırmasını gerektirir. Bu iş, yine, elektronik posta, dizin taraması, diğer özel ve genel amaçlı işlevlerde gerçekleştirildiği gibi uygulama katmanına aittir.

TCP/ IP :

TCP/IP nin kökleri 1960' ların sonları ve 1970 lerin başlarında Amerika Savunma Bakanlığı'na bağlı Advance Research Projects Agency (ARPA) paket anahtarlamalı ağ deneylerine kadar uzanır. TCP/IP nin yaratılmasını sağlayan proje, ABD' deki bilgisayarların bir felaket anında da ayakta kalabilmesini, birbirleri ile iletişime devam edebilmesini amaçlıyordu. Şimdi bakıldığında zaman projenin bir hayli amacına ulaştığını anlıyoruz.

TCP/IP' nin tarihi aynı zamanda internet tarihidir. İnternet ile TCP/IP ayrılmaz iki kardeş gibidir. TCP/IP internetin temelidir.

İnternetin sahibi yoktur, herkes internetin sahibidir. Ancak bu internet tamamiyle başı boş demek değildir. İnterneti, internet protokolü TCP/IP' yi düzenleyen gönüllü kuruluşlar vardır. Bunları şöyle sıralayabiliriz;

ISOC (İnternet Society: İnternet Derneği) 1992 yılında oluşturulmuştur. İnternetin kullandığı teknolojileri, uygulamaları, kuralları belirler. Her ülkede yerel Internet Society' ler bulunur.

IAB (Internet Architecture Board: İnternet Mimarisi Kurulu) ISOC içinde teknik kuralları öneren kuruldur. Bu kurulun altında üç kurul bulunur. İnternet'i düzenleyenlerde aslında bunlardır. Bu kurullarıda kısaca anlatırsak;

Internet Engineering Task Force: İnternet Mühendislik Görev Gücü; İnternet standartlarını oluşturur, teknik sorunlara çözüm üretir.

İnternet Assigned Number Authority: İnternet Numara Atama Merkezi: İnternet' te kullanılan protokolleri belirler ve gelecek için planlama yapar.

Internet Research Task Force: İnternet Araştırma Görev Gücü: TCP/IP ile ilgili araştırma projelerinden sorumludur.

TCP/IP : İNTERNET PROTOKOLÜ

TCP/IP, Transmission Control Protocol/Internet Protocol ifadesinin kısaltılmasıdır. Türkçe ye çevirirsek “ İletim Kontrol Protokolü/ İnternet Protokolü” oluyor. Protokol belli bir işi düzenleyen kurallar kümesi demektir. Ağ protoklleri de bilgisayarlar arası bağlantıyı , iletişimi düzenliyor.

TCP/IP, tek bir protokol diye düşünülmemelidir. TCP/IP bir protokoller kümesidir. Her biri değişik işleri yapan bir yığın protokolden oluşuyor.

TCP/IP ile kurulan bir bilgisayar ağında, bilgisayarın üç parametre ile tanımlarız. Bu parametreler şunlardır;

Bilgisayarın ismi

IP adresi

MAC (Media Access Control: Ortama Erişim Adresi)

TCP/IP protokller kümesi bu üç parametreyi kullanarak bilgisayarları birbirine bağlar.

Bilgisayar adı kullanıcı tarafından işletim sistemi yüklenirken bilgisayara verilen addır.

IP adresi: 212.35.45.233 gibi dört bölümden oluşan bir adrestir. Nokta ile birbirlerinden ayrılan her bölüm 0 ile 255 arasındadır.

MAC adresi, bilgisayarların ağ kartlarının ya da buna benzer ağ cihazlarının içine değiştirilmez bir şekilde yerleştirilmiş bulunan bir adrestir. 0020AFF8E771 örneğinde olduğu gibi onaltılı düzende (hexadecimal) rakamlardan oluşur. MAC adresi yerine donanım adresi ya da fiziksel adres de denilebilir.

Ağ üzerindeki iletişim aslında yalnızca MAC edresleri ile gerçekleşir, çünkü IP adresleri TCP/IP protokolüne özeldir. Başka bir protokolda örneğin: Novell' in kullandığı IPX/SPX protokolünde IP adresi diye birşey yoktur. Bütün protokollerde değişmeden kalan tek şey MAC adresidir.

Her protokol kendine göre bir adresleşme şeması kullanır ama bu şemalarda yer alan adreslerin dönüp dolaşıp en allta Mac adreslerin çevrilmesi gerekir.

Bir bilgisayar, bir başka bilgisayarın IP adresine sahipse ama MAC adresine sahip değilse Adres Çözümleme Protokolü (Adress Resolution Protocol- ARP) adı verilen bir protokol kullanılarak IP adresini MAC adresine çevirir. 'TCP/IP' nin bir protokol kümesi olduğunu biliyoruz, işte ARP bu kümenin bir üyesidir.

İletişime geçeceği bilgisayarın IP adresini bilen bilgisayar ARP protokolü ile "Bu IP adresine sahip bilgisayar bana MAC adresini bildirsin" şeklinde bir mesaj oluşturur. Bu mesajın Broadcast (Yayım) yapar. Yani ağdaki tüm bilgisayarlara gönderilir. Ağda ki bilgisayarların tümü bu mesajı alırlar. Eğer söz konusu IP adresi kendilerine ait değilse mesajı çöpe atarlar. Mesajdaki IP adresinin sahibi olan bilgisayar ise kendi IP adresini tanır ve hemen "Bu IP adresi bana ait, benim MAC adresim budur" şeklinde bir mesaj gönderir. İlk bilgisayar artık diğer bilgisayarın MAC adresini bildiği için asıl mesajını doğrudan Broadcast yapmadan gönderebilir.



Bir bilgisayara IP adresi iki yolla verilebilir. Birincisi manuel olarak elle girilebilir, ikinci yol ise sadece IP dağıtımını takip edecek özel bir bilgisayar ile yapılır. İlk yöntemle yapılan işlemin takibi ve hata yapma olasılığı yüksektir. Ayrıca sahip olunana IP adreslerinin gereksiz kullanımına yol açabilir. Diğer yöntemde ise belli bir aralık belirtilerek ağ dahil edilecek bilgisayarların bu IP havuzundan IP adresi alması sağlanarak daha güvenli bir ağ adresleme tekniği kullanılmış olur.

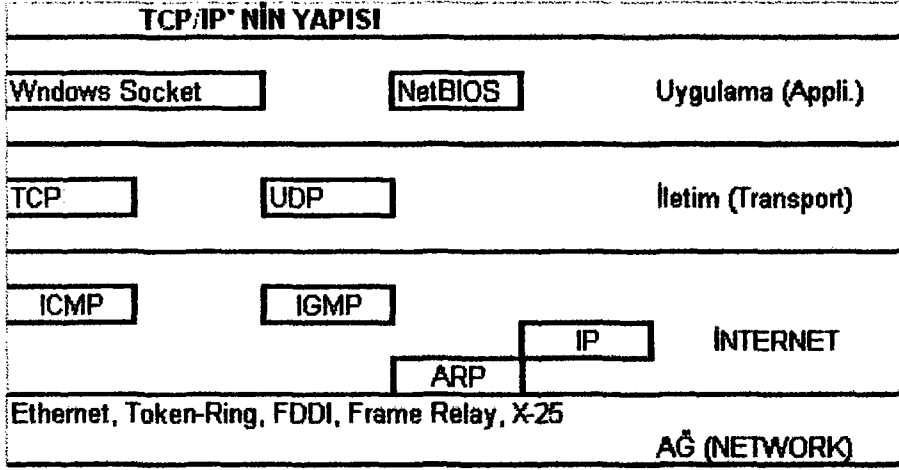
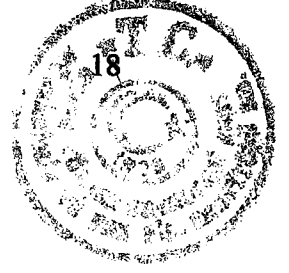
IP adreslerini otomatik olarak dağıtmanın bir yolu vardır ve bu yolun adı Dinamik Bilgisayar Konfigürasyonu Protokolü (Dynamic Host Configuration Protocol- DHCP). Bu protokol ile bir bilgisayar DHCP sunucu (server) olarak tanımlanır ve IP adres dağıtımı bu sunucu üzerinden yapılır.

Bilgisayarlar kendi aralarında MAC adresler üzerinden haberleşir demiştik. Peki bilgisayar kullanıcıları başka bir bilgisayar ile bağlantı kurmak istediği zaman bu MAC adreslerini akıllarında tutmak zorundadır? Elbetteki bu adresleri ezberlemek mümkün ama hatırlaması kolay olmayan heksadecimal rakamlardır. Bu işi de kolaylaştırmak için yine TCP/IP üzerinde yer alan protokoller mevcuttur.

Bilgisayar ismini kullanmak, kolayımıza geliyor ama ağ üzerinde bir iletişim gerçekte MAC adresler üzerinden gerçekleşiyor. O zaman bilgisayar ismini önce IP adresine çeviren sonrada MAC adresine çeviren mekanizmalar, protokoller olmalıdır. IP adresini MAC adresine çeviren protokol ARP protokolüdür. Ağ üzerindeki bilgisayar adreslerinin adını tutan diğer mekanizmalar ise DNS ve WINS yine TCP/IP protokolü içinde yer alan alt protokollerlerdir.

TCP/IP' NİN YAPISI:

TCP/IP anlatılırken dört katmanlı bir yapı düşünüyoruz.



Ağ (Network) Katmanı; bilgisayarda bulunan ağ kartına kabloları ve bunun gibi şeyleri gösteriyor. Veri paketlerinin ağa iletilmesinden ve ağdan çekilmesinden bu katman sorumludur.

IP katmanında IP 'ye göre düzenlenmiş veri paketlerini görüyoruz. İletim katmanından gelen veriler burada internet paketleri haline geliyor. Paketlerin yönlendirilmesi ile ilgili işler burada yapılıyor. Bu katmanda dört adet protokol bulunuyor:

ARP: IP adreslerini Mac adreslerine çeviriyor.

ICMP: Kontrol mesajları gönderip karşılığında gitti-gitmedi bilgisi sağlar. Ping komutu bu protokolü kullanarak karşı bilgisayarın TCP/IP konfigürasyonu bakımından ayakta olup olmadığını anlar.

IGMP: Multicast gruplarını belirtmek için kullanılır. Bir ağda mesajlar üç şekilde gönderilebilir: mesaj ya bütün makinalara (Broadcast mesaj), ya bir gruba (multicast), ya da doğrudan bir makinaya (directed) gönderilebilir.

IP: Paketlerin adresleme ve yönlendirme işlemlerini yapar.

İletim (Transport) katmanında bilgisayar arası iletişim için oturumlar düzenlenir. Burada iki seçenek söz konusudur;

TCP: Bağlantılı (connection- oriented) ve güvenilir bir bağlantı sağlar. Buradaki bağlantı mantıksal bir bağlantıdır. TCP ye uygun olarak gönderilen paketler



için bir onay mesajı beklenir. Belli bir süre içinde cevap gelmezse paket tekrar gönderilir. Bu da iletimin güvenli olması anlamına gelir.

UDP: Bağlantısız ve güvenilir olmayan bir bağlantı sunar. Güvenilir olmayandan kasıt; iletim için karşı tarafla iletişim kurularının anlaşma gerekmediği ve giden mesajın yerine ulaşp ulaşmadığı kontrol edilmediği için bu protokol daha hızlı bir veri iletişimi sağlar. Verinin çok hızlı bir şekilde karşı tarafa ulaşmasının gerektiği yerlerde bu protokol kullanılır.

Uygulama katmanı ağ üzerinden iş yapacak uygulamaların bulunduğu katmandır. FTP, DNS, WINS gibi uygulamalar bu katmanda bulunur.

TCP (Transmission Control Protocol- İletim Kontrol Protokolü):

TCP/IP protokol kümesine adını veren TCP, bağlantılı ve güvenilir bir iletişim sağlar. Bilgisayarlar iletişime geçmeden önce aralarında bir oturum açarlar. Oturumun açılması sırasında bilgisayarlar kendi iletişim parametrelerini birbirlerine iletiyorlar. İletişim sırasında bu parametrelere göre hareket ediyorlar.

TCP kullanmanın avantajı; bir bilgi gönderdiğimizde karşı tarafa gönderdiğimizden emin oluyoruz. Bu da gönderdiğimiz bilginin alındığına ilişkin bir onay mesajının (acknowledge, ACK) bize gelmesi ile karşı tarafın eline geçmiş oluyor. Yok eğer belli bir süre içinde bu bilgiyi alamaz isek gönderilen bilginin karşıya ulaşmadığını anlıyoruz.

TCP/IP kümesi içinde kritik işler yapan protokoller ve servisler verilerini TCP ile gönderirler. Örnek olarak 21 nolu portu FTP kullanır, 23 nolu portu Telnet, 53 nolu portu DNS kullanır.

İletişiminde iletilmek istenen veriler segmentlere ayrılır, her segmente bir sıra numarası verilir. Gönderici bilgisayar, segmentleri, yani çerçeveleri teker teker gönderip bunların herbiri için teker teker onay beklemez. Bunun yerine çerçeveleri belli bir sayıda topluca gönderir. Örneğin; onar onar. Alıcı bilgisayar da çerçeveleri kendisine ulaştıkça, kendi tampon belleğine yerleştirir. İki ardışık çerçeve, tampon belleğe yerleştirilince alıcı bilgisayar aldığı en son çerçeve için bir onay mesajını göndericinin bilgisayarına yollar.

Bir TCP segmenti iki kısımdan oluşur: Başlık (Header) ve Veri (Data) kısmı. Başlık kısmı şu alanlardan oluşur:

Kaynak Portu (source port): Gönderen bilgisayarın kullandığı TCP portu

Hedef Portu (destination port): Alıcı bilgisayarın TCP portu.

Sıra numarası (Sequence number): Segmentlere verilen numara.

Onay numarası (Acknowledgement number):

Veri Uzunluğu (Data lenght): TCP segmentinin uzunluğu.

Rezerve (Reserved): Gelecekte kullanılmak üzere reserve edilmiş.

Bayraklar (Flags): Segmentin içeriğine dair bilgi.

Pencere (Window): TCP penceresinde ne kadar yer kaldığını gösterir.

Kontrol Toplamı (Checksum): Başlık kısmının bozulup bozulmadığını gösteren kontrol kısmı.

Acil veri göstergesi (Urgent Pointer): Bayrak kısmında belirtilen acil bir verinin iletilmek istendiğini gösterir.

UDP (User Datagram Protocol: Kullanıcı Datagram Protokolü):

UDP, TCP' nin tersine hem bağlantısız hem güvensiz bir protokoldür. UDP' ye uygun bir veri iletimi gerçekleştirdiğimizde verimizi hazırlıyoruz, yolağan kısmına kendi adresimizi, alıcı kısmına hedef bilgisayarı yazıyoruz, yolluyoruz. Bu verinin yerine gidip gitmediğini bilemiyoruz.

UDP, güvenilir değildir diyoruz peki o zaman neden güvensiz bir protokol kullanıyoruz şeklinde ki bi soruya cevap olarak "hız" diyebiliriz. UDP kaşı tarafa gönderilen mesajın alıcıya gidip gitmediği ile ilgilenmez dolayısı ile de karşı taraftan herhangi bir cevap beklemez, sadece mesaj gönderilir. Bu özellik UDP ye belirgin bir hız kazandırır. UDP' ye örnek olarak 161. portu kullanan SNMP servisini (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü) verebiliriz.

Şimdi ibraz UDP' yi inceleyelim;

Kaynak Portu (Source Port): Gönderen bilgisayarın kullandığı UDP portu.

Hedef Portu (Destination Port): Karşı tarafın kullnadığı UDP portu

Mesaj Uzunluğu (Message Lenght): UDP mesajının büyüklüğü

Kontrol Toplamı(Checksum): Başlık bilgisinin bozulup bozulmadığını gösteren kısım.

ARP (Adres Resolution Protocol- Adres Çözümleme Protokolü)

ARP, IP adresi bilinen bir makinanın MAC adresini bulmak için kullanılır. Daha öncede belirttiğimiz gibi bilgisayarlar arası iletişim yalnızca MAC adresleri üzerinden gerçekleşir.

İletişime geçmek istediğimiz makinanın MAC adresini bulmak için ARP kullanılır. ARP MAC adresini öğreneceği bilgisayarı bulmak için ağ ortamına şöyle bir broadcast gönderir “ IP adresi şu olan makine bana MAC adresini bildirsin”. Bu mesaja karşılık gelise bu MAC adresleri üzerinden iletme geçilir. Tekrar aynı bilgisayarla iletme geçmek istendiğinde artık tekrar broadcast yapılmaz, ARP kendi belleğinde bu MAC adresi saklar ve buradan MAC adresini çağırır. ARP belleğinde iki türlü kayıt bulunur: Statik ve Dinamik. Dinamik kayıtlar broadcast ile bulunan adreslerdir. Dinamik kayıtlar bellekte sonsuz kadar kalmazlar. Belleğe yazılan dinamik kayıtlara saat bilgisi eklenir. Eğer belleğe eklenen kayıt iki dakika içinde kullanılmaz ise silinir. Eğer iki dakika içinde kullanılırsa bu sefer 10 dakika sonra silinir. Eğer bu iki ve on dakikalık süreler içinde kayıt için tutulan alan dolarsa eski kayıtlar silinir ve yeni kayıtlara yer açılır. Bu kayıt süreleri Registry ile oynayarak değiştirilebilir.

IP Adresleme:

IP adresi herhangi bir bilgisayarı gösteren 32 bitlik bir numardır. TCP/IP protokolü kullanan bir bilgisayar ağında her bilgisayarın bir IP adresi olmalıdır. IP adresleri ev adreslerine benzer. IP adresi bilgisayarın ait olduğu ağı, hem de bilgisayarın o ağ içindeki adresini belirler. Elimizde adresleme için kullanacağımız 32 bit varsa toplam $2^{32}=4$ milyar tane bilgisayarı adresleyebiliriz.

IP adresini oluşturan 32 bit, kolayca okunabilmesini sağlamak için sekiz bitlik dört gruba ayrılmıştır. Bu grupların herbirine oktet denir. Örnek bir IP adresi şu şekilde olabilir:

10000011 01101011 00000001 00001100

Bu adresi okunaklı kılmak için herbir oktetin onlu düzene çevirip oktetlerin arasın nokta koyuyoruz. Örneğin yukardaki adresin onluk düzendeki karşılığı 131.107.1.12 şeklinde yazılıyor.

IP adres sınıfları A,B,C,D ve E şeklinde sıralanır.

A Sınıfı adreslerde ağ adresi ilk oktet ile belirlenir. Geri kalan üç oktet ise o ağdaki bir bilgisayar gösterir.

B sınıfı adreslerde ağ adresi ilk iki oktet ile belirlenir. Geri kalan iki oktet o ağdaki bir bilgisayar gösterir.

C sınıfı adreslerde ağ adresi ilk üç oktet ile belirlenir. Geri kalan tek oktet o ağdaki bilgisayarları gösterir.

D ve E sınıfı adresleri ise özel test adresleridir. Bizim tarafımızdan kullanılmazlar.

126 arasında A sınıfı adres.

128- 191 arasında B sınıfı adres.

192- 223 arasında C sınıfı adres.

Burada bazı adresler kayıp gibi görünmekte.Örneğin 127 ile başlayan adresler özel adreslerdir ve herhangi bir bilgisayara verilmezler. Örneğin 127.0.0.1 adresi kendi adresimizi gösterir(loopback adres). 127 ile başlayan diğer adreslerin de özel anlamları vardır. 223' ün yukarısı ise D ve E sınıfı adreslere girer. Onlarda bizim tarafımızdan verilmezler.

Peki IP adresleri sınıflara atılınca ne oluyor ya da bu ne işimize yarıyor? Bu sınıflar neyi gösteriyor?

Bu sınıflar herhangi bir ağ adresine kaç adet bilgisayar tanımlayabileceğimizi gösteriyor. Örneğin A sınıfı adresi ele alalım. Bu adreslemede ağımızın adresini ilk oktet belirliyordu. Ağ adresi için bir oktet kullandığımıza göre yaklaşık 256 farklı A sınıfı adres kullanabiliriz gibi geliyor. Ama A sınıfı adresleri belirtmek için bu adreslerin en soldaki bitleri 0 yapılıyor. Bu yüzden ağ adresi için 7 bit kullanabiliyoruz. Bu da 126 farklı A sınıfı adrese karşılık geliyor.

A sınıfı bir adres ele alalım. Örneğin, ilk oktetimiz 10 olsun. Geri kalan üç oktet ise 10 adresine sahip ağdaki bilgisayarları tanımlamak için kullanılabilir. Elimizde üç oktet bulunduğuna göre adresleme için $3 \times 8 = 24$ bit var. $2^{24} =$ yaklaşık 16 milyon yaptığına göre bu ağda 16 milyon bilgisayar bulunabilir.

B sınıfı adreste ağ adresini ilk 2 oktet belirliyor. Ama B sınıfı adreslerin ilk oktet 128 ile 191 arasında değer alabilir. İkinci oktet de ise 256 değişik seçenek vardır. Dolayısı ile tanımlana bilecek B sınıfı adresleri sayısı yaklaşık 16.000 dir (tam rakam 16384). Geri kalan 2 oktetle de her bir B sınıfı, ağdaki bilgisayarları tanımlayabiliyoruz. 2 oktetden 16 bit geliyor 2^{16} yaklaşık 65 bin olduğu için bir B sınıfı adresimiz varsa 65 bin bilgisayarı tanımlayabiliriz.

C sınıfından bir adreste ağımız ilk üç oktetle tanımlanıyor. İlk oktetin 192 ile 223 arasında olması gerektiğini öğrenmiştik. Hesap yaparsak 2.097.152 adet C sınıfı adres tanımlayabiliriz. Bu durumda bize bir bilgisayarı tanımlamak için tek bir oktet kalıyor yani, yalnızca 8 bit kalıyor. 8 bit ile biz tamı tamına 254 bilgisayar tanımlayabiliriz.

Alt Ağ Maskesi (Subnet Mask):

Bir bilgisayar yalnızca kendisi ile aynı ağda bulunan bilgisayarlarla doğrudan iletişime geçebilirler. Bir bilgisayar iletişime geçeceği bilgisayarın, kendisi ile aynı ağda olup olmadığını nereden anlar sorusuna cevap Alt Ağ Mask olacaktır.

Ağı tanıyabilmek için elbette ki IP adreslerini kullanacaktır. IP adresinin bir bölümü ağ bir bölümü ise bilgisayarın o ağ içindeki adresini tanımlar.

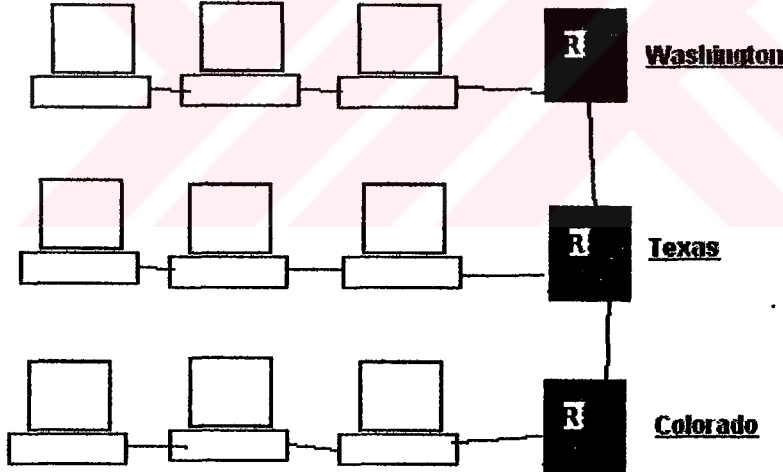
Bir bilgisayar, IP adresinin hangi bölümünün ağı tanımladığını, hangi bölümünün ise bilgisayarı tanımladığını bilmek zorundadır. Bunun için Subnet maskesini kullanır. Subnet maskesi dört bölümden oluşur ve ağ adresinin hangi bölüme kadar geldiğini göstermek için kullanılır.

Subnet Mask, ağ adreslerini bulurken bildiğimiz temel mantık (lojik) işlemlerini (AND, OR gibi) kullanır. Kendi IP adresimiz ile subnet maskesinin değerini çarparsak bulunduğumuz ağı tanımlarız. Gideceğimiz bilgisayarın IP adresi ile de gene bizim Subnet değerimizi çarparak sonuçların aynı olması durumunda hangi ağda olduğumuzu anlamış oluruz.

Alt Ağlara Ayırma (Subnetting) :

Alt ağlara ayırma (subnetting), verilen bir adres aralığını bölümlemek demektir. Neden böyle birşeye gerek duyarız. İnternet ' e erişim için yetkili bir kurumdan bir ağ adresi alırız. Örneğin aldığımız ağ adresimiz 195.67.78.0 olsun. Bu adresin ilk oktedi 195 olduğu için bir C sınıfı adres olduğunu anlıyoruz. C sınıfı adresler için de subnet mask 255.255.255.0 şeklindeydi. Bu durumda adresi vereceğimiz yere maksimum 254 adet bilgisayar tanımlarız. Ama adresi vereceğimiz yerler fiziksel olarak birbirinden farklı yerdeserse ne olacak? Diyelim ki bir yer Washington diğeri Texas ve Colarado olsun. O zaman ihtiyaç duyacağımız şey üç ayrı ağ adresi ve bu ağ adreslerini görüştüreceğ yönlendiriciler.

Şimdi ihtiyacımız olan üç ayrı segmentli adresler. Bunu nasıl yapacağız elimizde tek bir adres aralığımız var?



Yönlendiriciler ile birbirine bağlanan ağların herbiri için ayrı bir ağ tanımlayıcısı (network ID) gerekli. Ek olarak yönlendiriciler arasında kalan kısımlar da ayrı bir ağ sayılır. Bu na göre toplam 5 adet ağ bölümü (segment) ihtiyacımız var.

Elimizde tek ve C sınıfı bir adres var, o zaman C sınıfı adresde sadece son oktet ile ilgili ayarlamaları biz yapabiliyorduk, dolayısı ile segmentlere ayırma işlemini sadece bu son oktet ile yapabiliriz.

Bunun için bu son oktetin birkaç bitini kullanalım.

Biz beş adet alt ağ kurmak istiyoruz çünkü ihtiyacımız olan bu, o zaman son 8 bitin en az kaç adetini alt ağa bölmek için kullanmalıyım sorusuna cevap olarak 3 diyebiliriz. Neden $2^3 - 2 = 6$ adet ağ oluşturmak zorundayız.

Son oktette üç biti ağ tanımı için ayırıyoruz, geriye kalanları herbir ağdaki bilgisayarlar için kullanacağız. Geriyede kalan beş bitti. Yani $2^5 - 2 = 30$ adet olur. Yani herbir ağda 30 adet bilgisayar tanımlayabiliriz.

IP Yönlendirme:

Bir bilgisayar yalnızca kendisi ile aynı ağda bulunan bilgisayarlarla doğrudan görüşebilir. Başka ağlarda ki bilgisayarlarla ise dolaylı yollarla görüşebilir.

Şekil.2.1. inceleyelim;

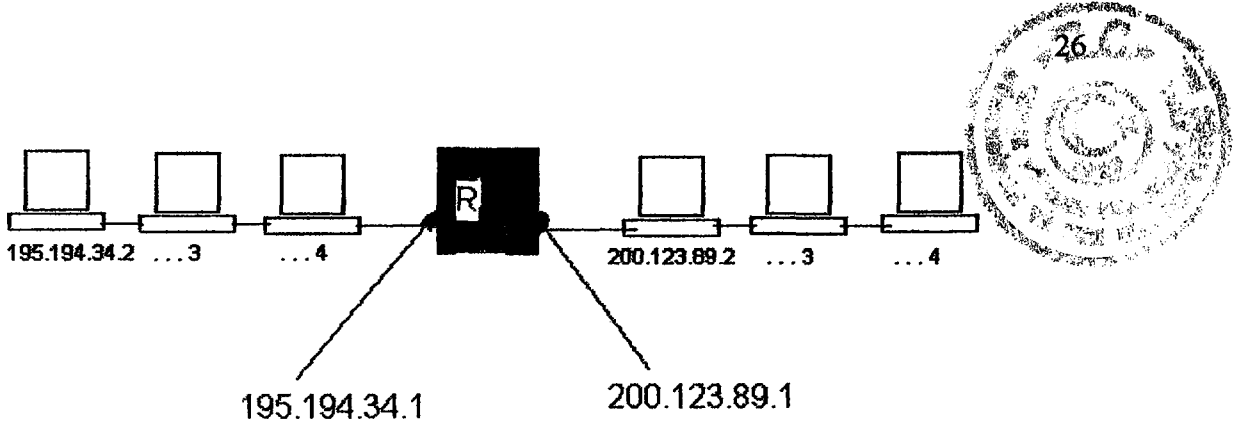


Şekil.2.1. İki farklı Ağ ve Adresleme

Bu şekilde iki ayrı ağ görüyoruz. Soldaki ağda bulunan bilgisayarlar birbirleri ile iletişime geçebilirler. Ama sağdakiler, solda ki bilgisayarlarla iletişime geçemezler.

Ağ maskesi ile bulunduğumuz ağı tesbit edebildiğimize göre, artık sağdaki ve soldaki ağ ifadelerini kullanmamıza gerek kalmaz. Sağdaki ağ 200.123.89.0, soldaki ağ 195.194.34.0 ağıdır. Şimdi bu bilgisayarların farklı ağlarda olduğunu anladık. Peki bu bilgisayarların haberleşmesi için ne yapmalıyız.

Farklı bilgisayar ağlarının birbirine bağlanması için yönlendiriciler (router) kullanılır. Yönlendiricinin görevi ortada bir yerde durup bir ağdan diğerine gidecek olan veri paketlerini alıp hedef ağa ulaştırmaktır; yani adı üstünde, yönlendirmek.



Şekil.2.2. İki Ağ Arasına Yönlendirici Bağlanması

İki ağı birleştirmek için ortaya bir yönlendirici koyduk. Yönlendiricinin iki bacağı var. TCP/IP protokolü ağda ki her ucun ayrı bir IP adresinin olmasını şart koşuyor. Bu yüzden yönlendiricinin bacaklarına da birer IP adresi veriyoruz. Yönlendiricinin bacaklarına IP verirken o bacak hangi ağa bağlı ise o ağa uygun bir adres vermemiz gerekir. Bu zorunludur; çünkü ağ üzerindeki uçlar (bilgisayar ya da yönlendiriciler vb.) yalnızca kendi ağlarındaki makineler ile doğrudan görüşebilirler.

Dikkat etmemiz gereken diğer bir konu ise yönlendiricinin bacaklarına IP adresi verirken, o ağa ait ilk adresi vermeliyiz. Bu ağ mimarisi açısından ve bir problem durumunda ağın kolay analiz edilmesini kolaylaştırır.

Yönlendiricileri kurduk ama her iki ağda da bilgisayarların bundan haberi yok. Onları haberdar etmek için TCP/IP konfigürasyonu kısmına “default gateway” parametersini kullanabiliriz. Bu parametre varsayılan çıkış kapısı anlamına geliyor ve eğer kendi ağında olmayan bir adrese ulaşmamız gerekirse ilişki kuracağımız yönlendiriciyi gösteriyor.

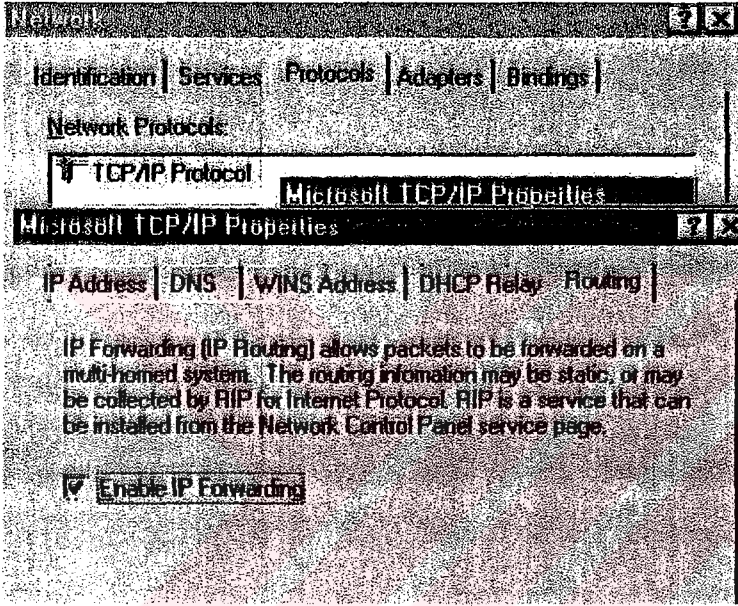
195.194.34.0 ağında bulunuyorsak bilgisayarların hepsinde default gateway olarak 195.194.34.1 adresini veriyoruz (bu yönlendiricinin bizim ağımıza bağlı olan bacağıdır). 200.123.89.0 ağında bulunuyorsak bu sefer default gateway olarak 200.123.89.1 adresini tanımlıyoruz.

Eğer 195.194.34.2 adresinden 200.123.89.3 adresine, örneğin bir ping çekersek hedef bilgisayarın bizimle aynı adreste olup olmadığını anlarız. Ping komutu, mesajları yönlendiriciye yolluyor. Yönlendirici mesajın içindeki hedef adres kısmına bakıyor, mesajı 200.123.89.3 adresine yolluyor.



Yönlendirici adı altında satılan cihazlar kullanılabileceği gibi bir NT bilgisayarı (Server veya çalışma istasyonu) da yönlendirici olarak kullanılabilir. Bunu şöyle yapabiliriz; bir NT bilgisayara iki adet ethernet (ağ kartı) takarız, herbirini bir ağa bağlarız, sonra da bir yönlendirici olarak çalışacağını söyleriz.

Bir NT bilgisayarı yönlendirici olarak çalıştırmak için TCP/IP özelliklerinden IP Routing sayfasına gidip *Enable IP Routing* kutusunu işaretleriz.



Şekil.2.3. Adres Konfigürasyonu

TCP/IP protokolünün kurulduğu her bilgisayarda bir yönlendirme tablosu tutulur. Bilgisayarlar bu yönlendirme tablosuna bakarak hangi veri paketini nereye göndereceklerine karar verirler.

Bir NT bilgisayarda bu tablonun içeriğine bir göz atalım: Bunun için ROUTE komutunu kullanacağız. Route komutu bilgisayarımızda bulunan yönlendirme tablosunu görmemizi ve bu tabloda değişiklikler yapabilmemizi sağlar.

Tabloyu görmek için vermemiz gereken komut ROUTE PRINT komutudur. Bu Komuta karşılık Şekil.2.4.'de ki ekranı alırız:

```

Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>route print

=====
Interface List
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 80 ad 76 7d 47 ..... CMEI PRO200VL PCI Fast Ethernet Adapter
=====

Active Routes:
=====
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.16.7.1       172.16.7.126     1
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
172.16.7.0                 255.255.255.0    172.16.7.126     172.16.7.126     1
172.16.7.126              255.255.255.255  127.0.0.1        127.0.0.1        1
172.16.255.255            255.255.255.255  172.16.7.126     172.16.7.126     1
224.0.0.0                 224.0.0.0        172.16.7.126     172.16.7.126     1
255.255.255.255          255.255.255.255  172.16.7.126     172.16.7.126     1
Default Gateway:          172.16.7.1
=====
Persistent Routes:
None
=====
C:\>

```

Şekil.2.4. MS-DOS Ortamında “Route Print” Komutu

Şimdi bu satırları teker teker inceleyelim.

Network Adresi: Ağ adresi.

Netmask: Bu ağda kullanılan ağ maskesi.

Gateway adres: Çıkış kapısı. Bu ağdaki bilgisayarlara erişmek için gitmem gereken çıkış kapısı adresi. Yani o ağa bakan yönlendiricinin adresi.

Interface: Arabirim. Bu ağa ulaşmak için bilgisayarımızda kullanılan IP adresi. Bilgisayarımızda birden fazla ağ kartı bulunabileceğini, her birine birer IP adresi verebileceğimizi biliyoruz. Tek bir ağ kartına birden fazla IP adresi de verilebilir.

Metric: Bu ağa ulaşmak için kat edilmesi gereken yönlendirici sayısı. Yukarda ki örnekte metric değeri 1 yani sadece 1 yönlendirici geçmiştik.

İlk satırda varsayılan çıkış kapısı ile ilgili bilgiler görüyoruz. Eğer elimizde ki adres kendi ağımıza ait değilse , bu adresle ilgili daha ayrıntılı bir yönlendirme bilgisi de yoksa bu adrese ulaşmak için varsayılan çıkış kapısına gidilir. Burada ilk alanda ağ adresi olarak 0.0.0.0 ifadesini görüyoruz. Bu kendi ağ adresimizin dışındaki hertürlü adres demektir.

İkinci satırda loopback adresi bilginizi görüyoruz. Loopback adresimiz bizim kendi adresimize karşılık geliyor ve test amaçlarıyla kullanılıyor. Bu satırlar TCP/IP yüklendiğinde otomatik olarak oluşturulur.

Üçüncü satırda ağ adresimizi görürüz. 172.16.7.0. Yanında kendi ağ maskemiz vardır 255.255.255.0 bu adres için çıkış kapısı kendi adresimiz olacak.

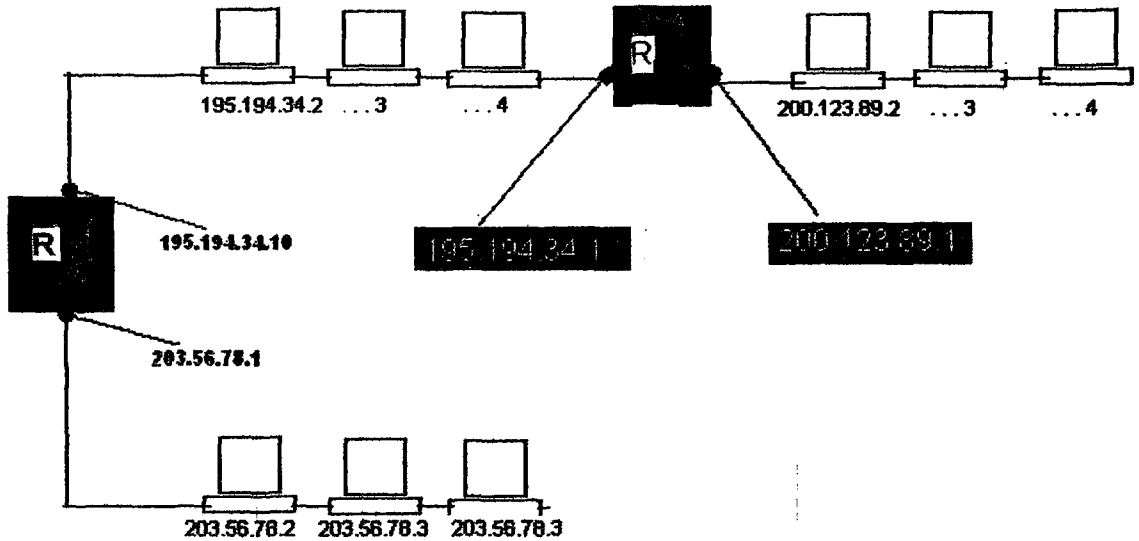
Dördüncü sırada; ağ adresi olarak 172.16.7.126'yı görüyoruz. Bu satır eğer 172.16.7.126 adresine birşey göndereceksen onu loopback adresine gönder anlamına gelir.

Beşinci satırda; kendi ağımızdaki broadcast adresimizi görüyoruz. 172.16.255.255

Altıncı satırda; Multicast adres grubuna karşılık gelen 224.0.0.0 geliyor. Bir TCP/IP ağında mesajlar üç şekilde gönderilir. Noktadan-noktaya, herkese-broadcast ya da sadece bir gruba- Multicast, 224 ile başlayan adresler multicast adreslerdir.

Yedinci satırda 255.255.255.255 ağ adresini görüyoruz. Bu da broadcast adresi oluyor.

Bu tabloya bir eklenti yapmak istersek bu sefer ROUTE ADD komutunu kullanacağız. Şimdi şekli inceleyelim;



Şekil.2.5. Yeni Bir Yönlendiricinin Ağa Eklenmesi

Şekil.2.5.'de görüldüğü gibi ağda bir değişiklik olmuş ve ağımıza yeni bir segment eklenmiş. Segmentteki ağ adresini yine bu segmentte kullanılan ağ maskesi

ile VE işleminden geçirip ağ adresini buluyoruz. Bu ağda 195.194.34.3 adresinden 203.56.78.2 adresine ulaşmak istersek;

195.194.34.3 adresli bilgisayar elindeki adresin kendi ağında olmadığını anlayacaktır. O zaman ne yapacak kendisinde var sayılan çıkış kapısına gidecektir. Ama ona giderse yanlış yönlendiriciye gitmiş olacak, çünkü o yönlendirici kendisini yalnızca 200.123.89.0 ağına bağlayabilir. Kendisini doğru ağa bağlayabilecek bir ağ var ancak bilgisayarın bu yönlendiriciden haberi yok.

O zaman bilgisayarın yönlendirme tablosunu değiştirmek gerekecek. Yönlendirme tablosuna yeni ağ ile ilgili bilgileri yazmamız gerekiyor. Burada *Route Add* komutunu kullanmamız gerekiyor. Bu komutun yazılışına bakalım;

Ruote ADD ağ-adresi MASKağ-maskesi çıkış kapısı adresi Metric

Yukardaki 193.194.34.3 nolu bilgisayara şöyle bir komut vereceğiz:

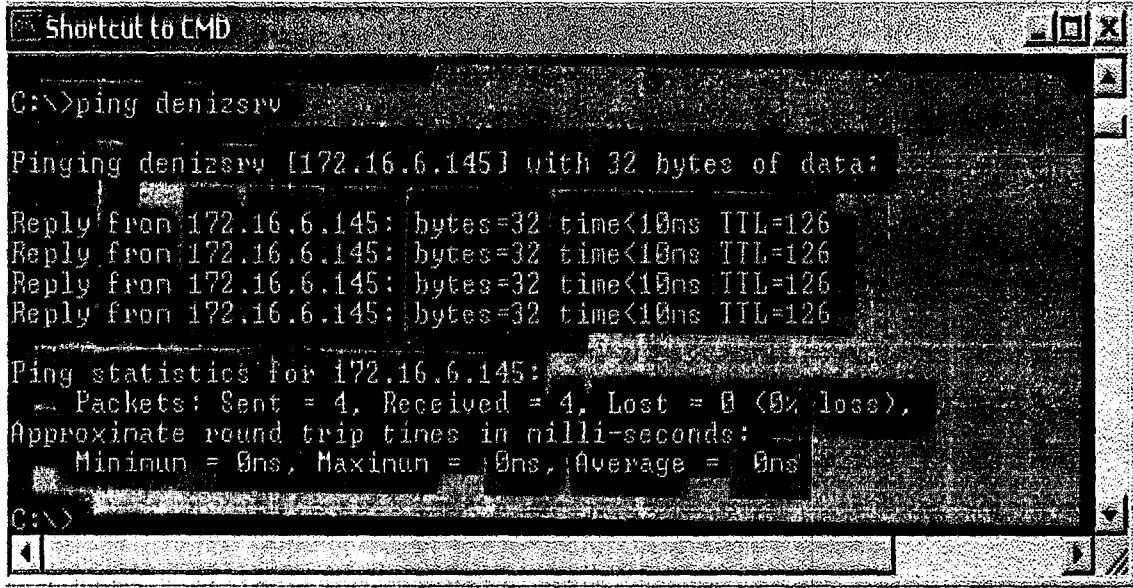
Route add 203.56.78.0 mask 255.255.255.0 195.194.34.10 metric 2

Bu komut verildikten sonra artık 193.194.34.3 bilgisayarından 203.56.78.2 bilgisayarına da, o segmentte bulunan diğer bilgisayarlara da erişilebilir.

Metric değerinin 2 seçilmesinin sebebi: Metric değeri geçilmesi gereken yönlendirici + 1' e eşittir.

Yönlendiriciler nereye ait olduğunu bilmedikleri paketleri sonsuza kadar gönderecekler mi peki? Bununda çaresi düşünülmüş paketlere bir TTL (Time to Live- Yaşam Süresi) zamanı verilmiş. Örneğin bir NT makinadan çıkan paketin TTL süresi 128' dir. Her paketin bir yönlendiriciye ulaşması ile değeri 1 azaltılır. Eğer bu değer 0 olursa bu paket yeterince dolaşmış, artık silinmeli anlamına gelir.

Bir örnek ile açıklarsak, kendi ağımızın dışında bir ağı ping' leyelim, böylece TTL zamanında ki azalmayıda görelim;



```

C:\>ping denizsrv

Pinging denizsrv [172.16.6.145] with 32 bytes of data:

Reply from 172.16.6.145: bytes=32 time<10ms TTL=126
Reply from 172.16.6.145: bytes=32 time<10ms TTL=126
Reply from 172.16.6.145: bytes=32 time<10ms TTL=126
Reply from 172.16.6.145: bytes=32 time<10ms TTL=126

Ping statistics for 172.16.6.145:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

Şekil.2.6. TTL Zamanının İncelenmesi

Ping Komutu ile verilen IP adresine sahip bilgisayarın TCP/IP bakımından ayakta olup olmadığını öğreniriz. Ayakta ise ona ne kadar sürede ulaştığımızı görebiliriz.

DNS ve RTP:

Domain Name Service- Alan Adı Servisi çok önemli servislerden biridir. Sunucu bilgisayarların, örneğin bir FTP sunucusunun adresi <ftp.xyz.com> olsun. XYZ alan adına ait sunucunun bir ftp sunucusu olduğunu bilen ve bu sunucuya ait ve tek olan IP numarasını ve fiziksel adresini tutan bir servistir. Bu bize ne sağlar, bu bize aranan adresteki sunucu ile hızlı bir iletişim ve yol sağlar.

RTP:

Real- Time Transport Protokol- Eş Zamanlı Taşıma Protokolü, aynı zamanda iletişim için çok önemli bir protokoldür. Eş zamanlı iletişimin yapılması gereken yerlerde kullanılır. Örneğin ses ve video verileri gibi.

RTP' nin çıkış noktası, internetin yeni yaygınlaşmaya başladığı zamanlarda VAT- Visual Audio Tool Protokol' ün bir uzantısı şeklinde olmuştur. Zaman içinde bu protokol geliştirilerek bugün birçok yerde kullanılan RTP protokolüne temel teşkil etmiştir.

2.3. Standartlar

TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Bir çoğu, IP datagramlarının alt katman protokollerine nasıl taşınacağını gösterir. Setteki anahtar protokoller İletim Kontrol Protokolü (TCP), İnternet Protokolü (IP) ve Kullanıcı Datagram Protokolü'dür (UDP- User Datagram Protocol). Uygulama servisleri içinde uc temel protokol bulunmaktadır. Bunlar virtual terminal hizmeti veren TELNET protokolü, Dosya Aktarma Protokolü (FTP File Transfer Protocol) ve Basit Posta Aktarma Protokolü'dür (SMTP-Simple Mail Transfer Protocol). Ağ yönetimi ise Basit Ağ Yönetim Protokolü'nce (SNMP-Simple Network Management Protocol) sağlanmaktadır.

TCP/IP başından beri Yerel Ağ bağlantısı (LAN-Local Area Network), Yerel ve Geniş Bölge Ağları (LAN-WAN) bağlantısı, bilgisayar ağı yönetimi, ve bilgi servisi sağlanması gibi yeni ortaya çıkan konulara da hitap etmektedir. Protokol kümesi akla gelebilecek her tip bilgisayara destek vermektedir. TCP/IP'nin kaynak kodu genel ortamda bulunup, kullanımı teşvik edilmektedir. Ağ yönetimi açısından SNMP, İnternet'i oluşturan TCP/IP tabanlı ağların yönetiminde de-facto standart durumundadır. SNMP istemci/sunucu (client/server) mimarisini kullanarak çeşitli ağ aygıtlarını işletmekte ve denetlemektedir. 1988'de kullanılmaya başladığından beri SNMP öylesine basarili olmuştur ki bir çok ticari ağ işletmeni kendi özel İnternet'leri üzerindeki çeşitli Yerel Bölge Ağ elemanları için SNMP'yi kullanmaya başlamışlardır. Pek çok endüstri çözümleyicisi ise SNMP'nin yaygın kullanımını, OSI-tabanlı ağ yönetim sistemlerinin yavaş ilerleme nedeni olarak görmektedir.

2.4. Bazı İnternet Kaynakları

2.4.1. Haberler

İnternet üzerindeki en yararlı kaynaklardan biri, çok sayıda konu içeren ilan tahtası sistemlerinin (BBS-Bulletin Board Systems) bir toplamı olan ağ haberleri'dir (Netnews). Haber grupları, bir ağaçyapısında düzenlenmiştir. Bu yapıdaki her bir kok bilim, sanat gibi ana bir konuya ayrılmıştır. Kokler de, her biri bir konu alanı belirleyen dallardan oluşur. Ağ haberleri UNIX tabanlı sistemlerde ortaya çıkmıştır. Rn, nn, trn ve xrn gibi UNIX programları ağ haberlerini okumak için

kullanılmaktadır. UNIX kullanıcısı olmayanlar, ağ haberlerini IBM PC ve uyumlularıyla, Machintosh ve VAX/VMS sistemlerinde okuyabilecek yazılım paketlerini kullanmaktadırlar. Pek çok yerel ilan tahtası da ağ haberlerine erişimi sağlamaktadır.

2.4.2. Elektronik Posta

Internet dünyanın en büyük elektronik posta (e-mail) ağıdır. Bugün yaygın olarak kullanılan elektronik posta sistemleri arasında büyük farklar vardır. Buna rağmen, Internet, kullanıcılarına mesajları okuma, saklama, gönderme, sıraya sokma ve yanıtlama gibi çeşitli hizmetler vererek kullanıcılarının dünyanın dört bir tarafı ile haberleşmesini sağlamaktadır. Internet'in ani popülerliğinin nedeni aslında elektronik posta servislerinde sunduğu artan etkileşimli bağlantıdır. Internet'te kullanıcı kodu bulunan bir kişi diğer Internet kullanıcılarıyla olduğu gibi, Compuserve, BITNET, MCI, Applelink ve benzer posta sistemleri kullanıcılarıyla da elektronik posta iletişimi kurabilir. Benzer şekilde bu sistemlerin kullanıcıları da Internet'i kendi aralarında bir iletişim yolu olarak kullanabilirler.

Aynı zamanda, çeşitli yazılım kurumları kişisel bilgisayarlardan oluşmuş Yerel Ağlar ve UNIX ortamları arasında da mesaj değişimi için geçityolu (Gateway) sağlamaktadırlar. Örneğin, Bilgisayar Posta Servisleri kurumu (Computer Mail Services, CMS), S-bridge adında, mesaj servisi veren posta ofislerini, SMTP tabanlı elektronik posta sistemlerine bağlayan bir geçityolu ürünü sunmaktadır. Bu ürün, Mesaj Kontrol Servisleri'ni (Message Handling Service, MHS) destekleyen kişisel bilgisayar tabanlı elektronik posta programlarıyla, UNIX işletim sistemindeki SMTP tabanlı elektronik posta programı arasında mesaj değişimini sağlamaktadır. MHS, kişisel bilgisayarlardan oluşmuş 'Yerel Ağlar' da kurulu olan en popüler elektronik posta sistemlerinin kullandığı sakla-ve-ilet (Store-and-Forward) teknolojisini kullanmaktadır. CMS'in bir diğer geçityolu ürünü ise UNIX tabanlı makinalar için M-bridge'tir. Bu ürün MCI Mail'i faks ve teleks servisleri ile birlikte SMTP tabanlı elektronik posta sistemlerine bağlamaktadır.

2.4.3. Gerçek Zaman Uygulamaları (Real Time Applications)

Elektronik postaya ek olarak, Internet çeşitli gerçek zaman işlemlerini de desteklemektedir. Örneğin, Amerika'daki belli başlı üniversitelerdeki öğrenciler birbirleri ya da çevrim-ici programlarla 'etkileşimli oyunculuk benzetimleri' ve diğer etkinlikleri gerçekleştirmektedirler. Bu benzetimler gerçek ya da hayal ürünü olan politik veya tarihsel olaylardan oluşabilmektedir. Öğrencilerden varolan karakterlerden kendi rollerini seçmeleri istenir. Öğrenciler bu rolleri oynarken aynı zamanda derslerini de öğrenirler.

Karar verme benzetimlerinde, öğrenciler çevreye en az etkisi olan çeşitli çevre ve inşaat problemleriyle karşı karşıya bırakılırlar. Buna örnek olarak verilebilecek bir program, Michigan Üniversitesi Eğitim Okulu'nda Etkileşimli İletişim ve Benzetimler Projesi dahilinde dokuz yıldır çalışmaktadır. Bu zaman içerisinde yirmi ülkedeki dört yüz okuldan on iki binden fazla öğrenci programın çeşitli öğrenim benzetimlerine katılmıştır.

2.4.4. Internet'e Erişim Yöntemleri

Internet'e, modemi ve kişisel bilgisayarı olan biri çok az bir ücret karşılığında bağlanabilir. Bir çok durumda istenilen servisin türüne göre BBS üzerinden dahi bir bağlantı temin edilebilir. Aynı şekilde, E-mail olanaklarını kullanan bir geçit yolu sayesinde de Internet'e bağlanılabilir. Örneğin, MCI Mail ve AT&T's Easy Link kullanıcıları elektronik posta mesajlarını Internet üzerindeki herhangi bir adrese gönderebilirler. Fakat, bu dolaylı bağlantı yöntemleri, Internet'in gerçek zaman uygulamalarını desteklemez.

Kullanıcılar, Internet'e çeşitli yollarla bağlanabilirler. Bağlantı şeklini, kullanıcının Internet'e ne kadar sıklıkla bağlanacağı belirler. Internet'e arada sırada bağlanan kullanıcılar dial-up hat kullanabilirler, ancak bu tip bağlantı sıklıkla bağlananlar için verimli değildir. Bu kullanıcılar, Internet'e kiralık hatlar yada paket anahtarlama ağıyla bağlanmalıdırlar.

Bağlantıların nasıl yapılabileceğine ilişkin ayrıntılı teknik bilgi ilerideki bölümlerde verilecektir.



2.4.5. Terminal Erişimi

Terminal erişimi, kullanıcının istediğinde Internet'e dial-up tipi bağlantı yapmasını sağlar. ABD'de herkese açık, NetCom (SanFrancisco), World (Brooklyn, MA) gibi kamu bilgisayarlarına, modem yoluyla dial-up terminal bağlantısı yapılabilir. Bütün Internet servisleri ve kaynakları, bu bilgisayarlar vasıtasıyla kullanıcı ve erişim kısıtlamaları dahilinde, kullanıcıya açıktır. Bazı servislere erişmek için ise özel şifreler gerekmektedir.

2.4.6. Ağ Erişimi

TCP/IP'nin çalıştığı bir bilgisayar veya LAN server'la Internet'in tüm fonksiyonlarına ulaşabilecek bir bağlantı gerçekleştirilebilir. Internet'le bir ağ katmanı bağlantısı kurarak, bir bilgisayar veya server Internet üzerindeki diğer bilgisayar ve sunucularla iletişim kurabilir. TCP/IP yazılımı, çoğu UNIX tabanlı bilgisayarlarda işletim sistemi ile birlikte gelmektedir. MS-DOS tabanlı diğer sistemler için ise bu yazılımı paylaşılabılır ve ücretsiz yazılım olarak elde etmek mümkündür.

Bilgisayarlarında TCP/IP çalıştıran kullanıcılar TELNET, FTP, IRC (Internet Relay Chat) ve diğer IP uygulamalarını doğrudan kullanabilirler. Böylelikle Internet'le, bir terminal olarak dial-up bağlantı kurmak zorunda kalmazlar. Bu yöntem kullanıcılara tam bir IP bağlantısı sağladığı için, bir çok uygulamayı aynı anda çalıştırmak mümkündür. Örneğin, ayrı ayrı pencerelerde, iki FTP, iki TELNET ve bir IRC aynı anda çalıştırılabilir.

Genel dial-up bağlantı hizmeti sunan bir servis sağlayıcı kuruluş aracılığı ile de IP bağlantısı kurmak mümkündür. Bilgisayar, TCP/IP'yi desteklemenin yanı sıra telefon hattı üzerinden haberleşmeyi sağlayacak geçerli bir protokolü de desteklemelidir. Çoğu durumda, TCP/IP yazılımı dial-up bağlantı biçiminde ya Point-to-Point Protokolü (PPP)'nu ya da Serial Line IP Protokolü (SLIP)'nu kullanır.



2.5. Güncel Internet Konuları ve Güvenlik Kavramının Ele Alınması

IAB pek çok konuyu gündeme getirmektedir. Bunlardan ağırlıkta olan ikisi güvenlik ve Internet adreslerinin yetersizliğidir.

Internet'teki güvenliğin olmaması SNMP standartları surecinin çabuk ve basit felsefesinin bir sonucudur. 1988'de ilk orijinal SNMP tanımlamaları geliştirildiğinde standartlar topluluğunda bunun nasıl güvenli yapılabileceği konusunda bir uzlaşma sağlanamadı ve SNMP, güvenlik özellikleri olmaksızın kullanıma sunuldu. IAB'ce göz önüne alınmakta olan tanımlamalar aşağıdaki güvenlik özelliklerini sağlamaktadır:

- * SNMP ve kullanıcının birbirine gönderdiği mesajlar için veri şifrelemesi : Bu bir SNMP istasyonunun hangi yönetim işlevlerine erişeceğini belirleyen veya istasyon içerisindeki yetki düzeyini tanımlayan anahtarların gönderilmesinde büyük fayda sağlar.

- * Köken doğrulama (origin authentication): Yetkili olmayan kullanıcıların bir SNMP iş istasyonunun erişim kodunu alarak yetkili bir kullanıcıymış gibi yanıltmalarını engeller.

- * Replay koruması (Replay protection): Kullanıcıların SNMP iletişimini geciktirmelerini engeller. Örneğin, bir komut bir iş istasyonunu çevrim dışı (off-line) bırakarak bir SNMP iletişiminin gecikmesine yol açabilir.

- * Mesaj bütünlüğü (Message Integrity): Yetkisiz kullanıcıların SNMP mesajlarının içeriğini değiştirmesini engeller.

alınarak yeniden düzenlenmelidir.

2.6. Bilişim Sisteminizi Tehdit Eden Bazı Tehlikeler Ve Önlemler

1-Pasif Dinleme

2:Aktif Dinleme

3-Ana Bilgisayara Sızma

4-Kullanıcı Bilgisayarlarına Sızma

5-Kriptografi

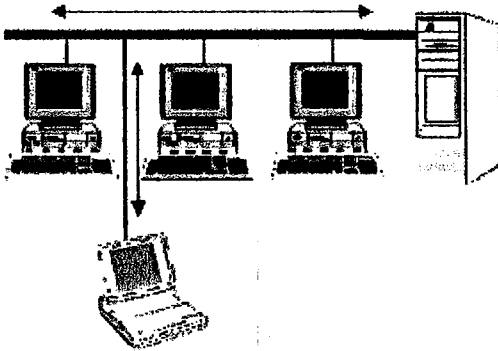
6-Truva Atları

2.6.1. Pasif Dinleme

Ağa gizlice bağlanan bir PC veya Laptop ağ üzerinde gidip, gelen data paketlerini izleyebilir, isterse bu bilgileri gizlice diskine kaydederek daha sonra analiz edebilir. Aynı tehdit firma içinde çalışmakta olan masum görünen bir eleman tarafından da kolaylıkla yapılabilir. Bu amaç için gereken bilgisayar programları kolaylıkla Internet üzerinde bulunan çeşitli sitelerden ücretsiz olarak temin edilebilir. Pasif Dinlemenin amacı firma içinde yapılan yazışma, haberleşme, mesajlar ve login password'lerini kolayca elde etmek içindir. Pasif dinlemenin tesbiti imkansızdır. Pasif dinleyici sadece dinler, aradığı bilgileri elde etmeye çalışır ancak hiç bir mesaj göndermez.

2.6.2. Aktif Dinleme

Aktif dinleme yapan bir PC ise sadece mesajları dinlemekle kalmaz, kendisi de sisteme mesajlar göndermeye başlar. Bu mesajları öyle oluşturur ki, sistemdeki diğer unsurlar bu makinayı legal bir makina gibi görürler. Bu sayede aktif dinleyici yanıltıcı mesajlar göndermeye başlayabilir. Örneğin sahte e-mail'ler, talimatlar, v.s. Eğer sistem TELNET gibi bir protokol ile login yapılarak çalışıyorsa, önce pasif dinleme ile hedeflediği kullanıcıların password'lerini elde eder. Daha sonra uygun bir zamanda bu kullanıcılar gibi login yaparak, örneğin muhasebe programına girerek, istediği işlemleri yapabilir. Bunun sonucu olarak suçlanabilecek tek kişi password'ünü çaldığı kullanıcı olacaktır.



Şekil.2.7. Ağa Sızma

2.6.3. Ana Bilgisayara Sızma

Ağa bir şekilde bağlanan bir saldırgan belirli bir süre pasif olarak dinleme yaptıktan sonra sisteminin zaafiyetleri kolaylıkla anlayabilir. Bu bağlamda klasik güvenlik delikleri vardır. Örneğin TELNET, NFS, POP3, SMTP, FTP, v.s. gibi servislerin çalıştırılmaları son derece tehlikelidir. Bu servislerden en tehlikelileri TELNET ve NFS'dir. Saldırgan bu sistemlerin şifrelerini çok kolaylıkla elde edebilir ve kolayca ana bilgisayara bağlanır. Ana bilgisayara bağlandıktan sonra veya önce ağı dinleyerek ROOT password şifresini sistem operatörlerinden birisinin makinası üzerinden kolaylıkla elde edebilir. Bu şifreyi kullanarak öncelikle sistemin gizli ve yarı gizli password dosyalarını alır. Bu dosyaları hızla analiz ederek, kısa bir süre içinde kullanıcı şifrelerin büyük bir bölümünü çözebilir. Bu yetkiye dayanarak sistemin loglarında oynayabilir, kendisine üstün yetkilere sahip yeni hesaplar açabilir, sistemde yeni servisler çalıştırarak, arka plana çekilir. Yeni servisler tamamen şifreli işlem yaparak ağ üzerinden anlaşılmadan hizmet verilmesine olanak sağlar. Ana bilgisayara hakim olan kullanıcının ORACLE, INFORMIX, v.s. gibi SQL serverlara hakim olması son derece basit bir işlemdir. (şifreler TELNET bağlantısı yapan kullanıcıların ağ üzerinden yaptığı iletişim dinlenerek elde edilebilir). SQL komutları verebilen bir kullanıcı da verileri istediği gibi değiştirebilir, istediği hesaba istediği kadar para ekleyebilir, v.s., v.s. Bundan da vahimi bu bilgisayardan başka bilgisayarlara internet üzerinden saldırı başlatabilir. Bu bağlamda karşı taraf saldırının sizin bilgisayarınızdan yapıldığı kanısına varacaktır ve bu nedenle yasal kovuşturmayaya uğrayabilirsiniz.

2.6.4. Kriptografi

Tehdit altında olan veri güvenliğine yardımcı olacak en güçlü araç kriptografi (şifreleme teknikleri) olacaktır. Kriptografi bilgilerin gizlenmesi için uygulanan teknikleri kullanan bilim dalıdır. Derin olarak matematik ile ilişkilidir. İlk kriptotekniklerini Sezar'ın kullandığı iddia edilir. Sezar, gizli bir mesaj göndermek için harfleri belirli bir sayıda ileri veya geri alarak mesajlarını gizlemeyi başarmıştır. Örneğin A yerine D, B yerine E gibi. Böylece EDED diye gördüğümüz mesaj aslında BABA anlamına gelir. Doğal olarak bu çok basit bir şifreleme tekniğidir. Yerine Koyma (substitution) yöntemi olarak bilinir.

Bu yöntemin biraz daha karışığı harfleri belirli bir kaydırma yerine karmaşık olarak eşleştirerek yapılır. Örneğin, A yerine X, B yerine G gibi, yani BABA kelimesi GXGX'e dönüşecektir. Önceki yöntemde bir harfi çözdüğümüzde tüm şifreyi çözerken, bu yöntem için biraz daha fazla uğraşmamız gerekecektir ama yine de çok kolay kırılır. Bu yönteme Tek Alfabe Yerine Koyma yöntemi denir (Mono alphabetic Substitution) Tekniklerimizi biraz daha geliştirdiğimizde Çoklu Alfabe Yerine Koyma yöntemine erişiriz. Bunu şöyle düşünebiliriz, yerine koyma listeleri birden çok olabilir, örneğin 10 tane diyelim. Harfin sırasına göre farklı listeyi seçeriz. Örneğin şöyle bir tablo yaparsak:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

1:NOPQRSDEXYZFGHIJKLMTABCUVW

2:DEXHIJKYZFTABCUVWGNOPQRSML

3:DEXYZNOPQRSFGTABCHIJKLUMVW

4: LVMUZNAIJWOPQBCHRSFGTDEXY

BABA mesajımız ODEL haline dönüşecektir, B ve A harfleri tekrar bile etse her seferinde farklı harflere karşılık gelecektir.

Görüldüğü gibi yöntemler bu şekilde gittikçe geliştirilebilir, şifrenin kırılması zorlaşır. Uyguladığımız yönteme şifreleme algoritması denir, yukarıda oluşturduğumuz tablolar ise şifre anahtarıdır. Bununla ötesinde kullanıcının kendi özel anahtarını vermesi sağlanabilir, örneğin 7349 diyelim. Bu durumda bu sayılar yukarıdaki tablolarda belirtilen sayıda bir kayma sağlayabilir. Örneğin klasik BABA mesajımız B harfinden birinci tablo da 7 harf kayarak X, A harfi ikide 2 harf kayarak H, üçüncü de 4 harf kayarak N, dördüncü de 9 harf kayarak K, yani XHNMK olacaktır. Karşı tarafın mesajı çözebilmesi için hem tablolara, hem de şifre sayısına gereksinimi olacaktır. Bu örnekler öğretici olması için verilmiştir, her ne kadar ilginç, güzel ve sağlam gibi gözükse de bu gibi şifrelerin kolaylıkla kırılabileceğini bilmeniz gerekir.

Bu yöntemin biraz daha gelişmiş olan ENİGMA şifresi ikinci dünya savaşı sırasında Almanlar tarafından efektif olarak kullanılmıştır. Yerine koyma işlemleri, dişliler ve elektrik kontaktları ile yapılmış. Almanlar gemilerine, denizaltılarına ve birliklerine mesajları ENİGMA ile göndermişler. Savaşın sonuna doğru ENİGMA İngilizler tarafından çözülmüş ve bundan habersiz Almanlar büyük bir darbe yemiştir.

UNIX sistemlerinden birçoğunda hala ENİİGMA temel alınarak yapılmış CRYPT fonksiyonu ile kullanıcı şifreleri üretilmektedir. Bu şifreler kolaylıkla kırılabilir.

Zaman içinde bu tür yerine koyma ve karıştırma şifreleri gelişmiş ve bugün bile kullanılan standard şifre sistemlerinin temelini oluşturmuştur. DES böyle bir şifre sistemidir.

2.6.5. Truva Atları

PC disketleri, CD'leri, Internet ve diğer ağ bağlantıları yoluyla sisteminize bulaşan , görünüşte masum ve başka birşey yapan ama arka planda sinsice çalışarak hasarlı veya hasarsız başka işlem yapan programlara TRUVA ATI denilir. Bunlar tüm sisteminizi çökertebilir, diskleri silebilir veya rasgele değiştirebilir, rasgele mesajlar gönderebilir, sistemizden bilgi çalarak rakiplere gönderebilirler veya sisteminize güveni tamamen yok edecek bir duruma sokabilir. Truva atlarına karşı çok ciddi önlemler alınması ve sürekli monitoring şarttır. Truva atları mutsuz ve psikopat elemanlar tarafından da yerleştirilebilir. Bu tür kişiler bunu eğer bir şekilde işten çıkarılır iseler bankadan intikam almak için düşündükleri sabotaj projelerine alt yapı için planlayabilirler.

2.6.6. İnternet Bağlantıları

Direkt olarak Internet'e bağlı bir sistem büyük bir tehdit altındadır. Kesinlikle Internet'e bağlı bir ana sisteminiz veya yan bir sistem olup aynı anda hem Internet'e, hem de Banka sistemine bağlı sistemlerde olmamalıdır. Bu sisteme sızan bir saldırgan buradan ana sisteme geçebilir. Internet üzerinde hizmet verecek sistemler kesin sınırlarla izole, Güvenlik Duvarı sistemleri ile korunmalıdır. Güvenlik Duvarı sistemleri de her zaman iyi olmayabilir ve %100 güvenilmemelidir. Zaman zaman bu sistemlerinde açığı yakalanmaktadır.

2.7. Saldırı Türleri

Genellikle çok karşılaşılan saldırı türleri aşağıda özetlenmiştir.[10, 11. 13]

Probe,Scan,Scam: Bir sistemdeki açık ve kullanılan portların taranması ve bu portlardan hizmetlere yönelik saldırıları türüdür.



Prank: Kullanıcı hesaplarının yanlış oluşturulması sonucu oluşan açıklardan yapılan saldırı türleridir.

Email spoofing: Başka bir kullanıcı adına e-posta gönderilmesi...

Email bombardment: Bir e-posta adresine genelde farklı adresten çok sayıda e-posta gönderilmesi

Sendmail attack: Smtip portuna yönelik saldırılardır...

Break-in: Verilen hizmetlerin devre dışı bırakılmasına yönelik saldırı türüdür.

Intruder gained root access: Saldırganın normal kullanıcı olarak girdi i sistemde süper kullanıcı yetkisini kazanması.

Intruder installed trojan horse program: Saldırganın girdi i sisteme genelde daha sonra tekrar rahat girebilmesi ya da uzaktan yönetim için ajan program yerle tirimesi.

Intruder installed packed sniffer: Saldırgan tarafından hedef makinaya yönelik paket dinleyici yerle tirilerek yapılan saldırı türüdür. Bu şekilde bir yerel ağ korumasız bir konak üzerinden saldırılara açık hale gelebilir.

NIS attack: Ağ kullanıcı yönetim sistemine yönelik saldırı türüdür.

NFS attack: Ağ dosya yapısına yönelik saldırı türüdür. Genellikle ağ erişimini devre dışı bırakmada kullanılır.

Telnet attack: Uzaktan erişim protokolünün açıklarından faydalanılarak yapılan saldırı türüdür.

Rlogin or rsh attack: Uzaktan erişimde kullanılan servislerin açıklarına yönelik yapılan saldırı türüdür.

Cracked password: Kolay tahmin edilebilir parolaların tahmini ya da şifreli hallerine göre sözlük saldırısı yapma türüdür.

Anonymous FTP abuse: Anonim erişim izni verilen dosya aktarım sunucularına yönelik saldırılardır.

IP spoofing: IP adres yanıltmasıyla yapılan saldırı türüdür.

Configuration error: Çok kullanılan programdaki kullanıcılardan kaynaklanan konfigürasyon hatalarından doğan açıklıklardır.

Misuse of hosts resources: Konak kaynaklarının yanlış kullanımı sonucu ortaya çıkan açıklıklar.

Worm, Virus Konaklarda kullanıcılardan habersiz çalışan zararlı programlar[3]



2.8. Güvenlik Duvarı Tanımı

İnternette güvenlik ile ilgili konular arasında adı sık sık geçen Güvenlik Duvarı (Firewall) kavramı esas olarak yazılım ile oluşturulup, internet üzerinden bir sisteme girişleri kısıtlayan/yasaklayan ve genellikle bir internet gateway servisi (ana internet bağlantısını sağlayan servis - ağ geçidi) olarak çalışan bir bilgisayar üzerinde bulunan güvenlik sistemine verilen genel addır.

Güvenlik Duvarı (İnternet Güvenlik Sistemi), internet üzerinden bağlanan kişilerin, bir sisteme girişini kısıtlayan/yasaklayan ve genellikle bir internet gateway servisi (ana internet bağlantısını sağlayan servis) olarak çalışan bir bilgisayar ve üzerindeki yazılıma verilen genel addır.

Güvenlik Duvarı sistemleri, bu engelleme işini, sadece daha önceden kendisinde tanımlanmış bazı domainlere erişim yetkisi (telnet,ftp, http vb) vererek yaparlar. Günümüzde, İnternet Servisi veren makinalar oldukça sofistike Güvenlik Duvarı sistemleri ile donanmışlardır.

Güvenlik Duvarı internet ağından yerel ağı korumanın çeşitli yollarından birisidir. Genel olarak iki türlü Güvenlik Duvarı yapısından bahsedebiliriz; veri trafiği engelleyen türler ve veri trafiğine izin veren türler. Bazı Güvenlik Duvarı tiplerinde veri akışının engellenmesi esas iken bazılarında da veri trafiğini düzenlemek ve sınırlamak önem kazanır. Genellikle firewallar dışarıdan ağa yetkisiz erişimleri engellemek için düzenlenir. Ağdan dışarıya erişim serbest iken dışarıdan ağa erişim kısıtlanır. Bazı Güvenlik Duvarları sadece e-mail trafiğine izin verirken diğerleri farklı cinsden veri iletimine izin vermekle birlikte problem olabilecek servisleri (FTP, NFS, X-Windows gibi) ve bazı iletişim türlerini bloke ederler. Bu tür seçimler ve erişim izinleri tamamen kullanıcıların tercihlerine göre belirlenir.

Güvenlik Duvarının esas amacı ağa zarar vermek yada sızmak isteyenleri engellemektir. Genel olarak kurumlar ve veri merkezleri için Güvenlik Duvarı sıkça kullanılan bir güvenlik yöntemidir.

Güvenlik Duvarları güvenlik ve denetim için bir tür geçit noktası oluşturur. Ayrıca sisteme modem ile bağlantı kurulmak istendiğinde Güvenlik Duvarı bu bağlantıyı kontrol edip izleyebilme imkanına da sahiptir.

Güvenlik Duvarı ile birlikte çeşitli kullanıcı erişimi denetleme ve yetkilendirme mekanizmalarının kullanılmasında (one time password gibi) yerel ağın güvenliğini arttıran bir unsurdur. Güvenlik Duvarı bu türden, kullanıcı şifre ve yetkilerinin tanımlanıp kullanılması ve bu bilgilerin ağlar arasındaki trafiğinin gizlenmesi konusunda extra özellikler sunar.

Güvenlik Duvarının bazı dezavantajları ve kusurlarında eksik değildir tabii ki. Bu problemleri şöyle özetleyebiliriz:

Güvenlik Duvarı için en büyük dezavantaj kullanıcıların bazı çok kullanılan (telnet, ftp, x-windows, nfs gibi) servislere erişiminin kısıtlanmasıdır. Ancak, bu dezavantaj Güvenlik Duvarına özgü değildir. Güvenlik Duvarı ile ağ erişimi, yerel ağların güvenlik planına bağlı olarak, host (kullanıcı) düzeyinde çeşitli opsiyonlar ile kısıtlanılabilir. Kullanıcı ihtiyaçları ile güvenlik şartlarını dengeleyen iyi planlanmış güvenlik planı, bu tür kısıtlanmış erişim problemlerini çözebilir. Bazı durumlarda yerel ağ sistemleri Güvenlik Duvarına uygun olmayan topolojiye sahip olabilirler veya Güvenlik Duvarı kullanıldığında, sistemin yeniden yapılandırılmasının gerektiği NFS gibi servisleri kullanabilirler. Örneğin, bir yerel ağ, ağ geçitleri (gateway) arasında NFS ve NISA protokollerini kullanmak zorunda ise, Güvenlik Duvarını eklemenin bedeli, hack'lanabilirliklerin bedeli ile karşılaştırılmalı ve risk analizi yapılmalıdır. Bu durumlarda alternatif çözümler (Kerberos gibi) daha uygun olabilir.

Güvenlik Duvarı, trojan türü data içeren veri paketlerine karşı da ağı koruyamaz. İçinde bir hacker tarafından yerleştirilmiş programlar bulunan veri paketleri ile yapılan saldırılarda (backdoor oluşturan programlar) Güvenlik Duvarı için potansiyel bir tehlike mevcuttur. Bu yöntemle istemci, sunucudaki erişim kontrollerini değiştirip gizli dosyaları açabilecek programları bizzat sunucu yani server tarafında çalıştırabilir. Saldırıların bu türü sendmail'in çeşitli versiyonlarına karşı geçmişte çok defa yapılmıştı.

Eğer firewall tarafından korunan ağın içine sınırsız modem erişimi izini verilirse, saldıran kişiler Güvenlik Duvarı'ı rahatça geçebilir. Modem hızları , slip (serial line ip) ve ppp (point point protokol) için oldukça yüksektir. Güvenli sanılan



alt ağılar içindeki slip veya ppp bağlantıları, aslında diğer ağlara bağlantı kurulabilecek gedikler ve potansiyel backdoor'lardır.

Güvenlik Duvarı genellikle ağıın içerisinde gelen tehditlere karşı koruma sağlamaz. Multicast video ve ses içeren IP paketleri de Güvenlik Duvarı tarafından filtre edilmediğinden ayrı bir potansiyel tehlike kaynağıdır.

Güvenlik Duvarı konusunun daha açık anlaşılabilmesi için bazı Güvenlik Duvarı türlerinin yapısını incelemek faydalı olabilir. Ancak bu incelemeye geçmeden önce VEKİL SUNUCU ve paket filtreleme konularını kısaca açıklamakta fayda var. [1, 2, 4, 5, 15]

2.9. Paket Filtreleme (Veri Paketleri Filtresi)

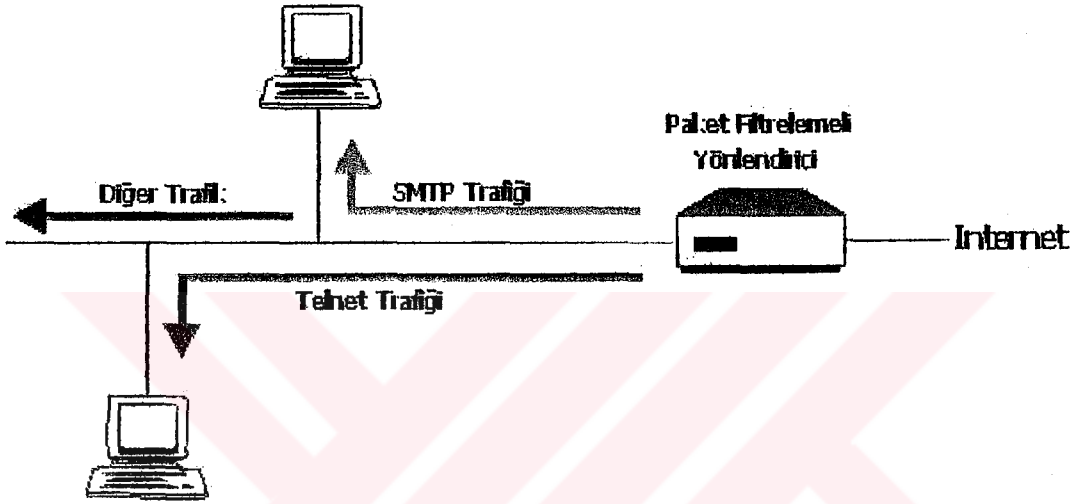
IP paketleri filtreleme işlemi, yönlendirici (Router) ara birimleri arasında geçen veri paketlerini süzmek için tasarlanmış bir yönlendirici (Router) kullanılarak yapılır. Paket Filtreleme yönlendiricisi (Packet Filtering Router), aşağıdaki kriterlerin hepsine veya bazısına göre IP paketlerinin trafiğini süzebilir.

Kaynak	(source)	IP	adresleri
Hedef	(destination)	IP	adresleri
Kaynak	TCP/UDP		portu
Hedef	TCP/UDP portu		

Tüm paket Filtreleme yönlendiricileri sadece kaynak TCP/UDP portlarını süzmekle kalmayıp, bazı yönlendiriciler, yönlendirici arabirimine bir veri paketi geldiğinde bu paketin nasıl kullanılacağını da incelerler. Filtreleme ağda ki veya ana makinadaki bağlantıları bloke etmek için kullanılan çeşitli yöntemlerden birisidir ve belirli portlar için bu portlardan yapılacak veri iletişimini bloke eder. Bir ağ, güvenilirmez olarak tanımladığı ana makina veya ağlardan (belirli adreslerden) bağlantı yapılmasını engellemek isteyebilir yada dışarıdan gelen tüm trafiği (e-mail, smtp gibi malum istisnalar dışında) bloke etmek isteyebilir.

IP adres Filtresine, TCP ve UDP port filtresi ekleyerek sistem daha esnek hale getirilebilir. Eğer bir Güvenlik Duvarı TCP veya UDP portlarının bağlantısını bloke edebiliyorsa belli makinalar için yapılan belirli bağlantı tiplerinide

yönlendirebilir. Örneğin bir ağ, Güvenlik Duvarı'na bağlı olanlar dışındaki makinalara giren bütün bağlantıları engelleyebilir. Ya da bir sistem için telnet veya ftp bağlantıları serbest iken bir diğeri için sadece smtp bağlantısı açık olabilir. TCP veya UDP portlarının süzülmesi yolu ile bu tür seçimlerin uygulanması, paket Filtreleme kapasitesine sahip host yoluyla veya paket Filtreleme yönlendiricisi tarafından yapılır.



Şekil.2.8. Telnet ve SMTP için Paket Filtreleme Yapısı Örneği

Bununla birlikte paket Filtreleme yöntemi herhangi bir veri içeriği kontrolü yapmadığından birtakım dezavantajlara sahiptir. Ayrıca portların veri transferi aşamasındaki yönlendirilmeleri ve yönetimleri ile de ilgili bazı problemler olduğu bilinmektedir.

2.10. Vekil Sunucu (Proxy Server)

Vekil Sunucu servisi, internet üzerindeki yerel bir ağ (ya da internete bağlı bir bilgisayar) ile, dış dünya arasındaki ilişkiyi sağlayan bir yardımcı geçit (gateway) sistemidir. Vekil Sunucular sık sık yönlendirici (router) makinaların yerine, benzeri bir işlev ile ağlar arası trafiği kontrol etmek amacıyla kullanılır. Aynı zamanda bir çok Vekil Sunucu, kullanıcı erişimleri için denetleme ve destek de sağlar. Vekil Sunucular kullanılan uygulama protokollerine hakim olmaları nedeniyle bazı özel güvenlik protokollerinde uygulayabilirler. Örneğin bir ftp Vekil Sunucuyu, ftp protokolü üstünden giriş yada çıkışları denetleyecek ve bloke edecek şekilde konfigüre edilebilir.



Vekil Sunucu özel bir uygulamadır. Vekil Sunucu yoluyla yeni bir protokolü desteklemek için, o protokole özel bir Vekil Sunucu yapısı geliştirilmelidir. (Soketler, bir Güvenlik Duvarı gibi çalışması için, istemci tarafındaki uygulamalar için oluşturulmuş Vekil Sunucu sistemleridir. Avantajı , kullanım kolaylığıdır. Ama Vekil Sunucular gibi erişim kontrolüne ve özel protokol kullanma olanağına sahip değildir.)

Bir Vekil Sunucu servisi (sunucusu), sizin adınıza (Vekil Sunucunun kelime anlamı vekil'dir) sizden aldığı "internet'ten bilgi alma" isteklerini yürütür ve sonucu yine size iletir. ancak, aynı anda, bu bilgilerin bir kopyası da (cache),bu Vekil Sunucu üzerinde tutulur ve bir dahaki erişimde kullanıcının istediği bilgiler doğrudan ilgili siteden değil de, Vekil Sunucu servisinden gelir; dolayısıyla, iletişim daha hızlı olur. İnternet'e erişim için mutlaka bir Vekil Sunucu servisine ihtiyaç yoktur, ancak, size en yakın bir servis noktasındaki Vekil Sunucu servisini kullanmanız, internet erişiminizi hızlandıracaktır.

2.11. Güvenlik Duvarı Örnekleri

Güvenlik Duvarının temel parçalarını incelenileyecek olursak bazı örnekleri konuyu daha iyi anlamak amacıyla irdelemekte fayda var. Bazı genel Güvenlik Duvarı tipleri:

Paket Filtreleme yapan Güvenlik Duvarı türü - Packet Filtering Firewall.

Çift taraflı Geçit tipindeki Güvenlik Duvarı türü - Dual-homed gateway firewall.

Perdelenmiş kullanıcı tipindeki Güvenlik Duvarı türü - Screened host firewall.

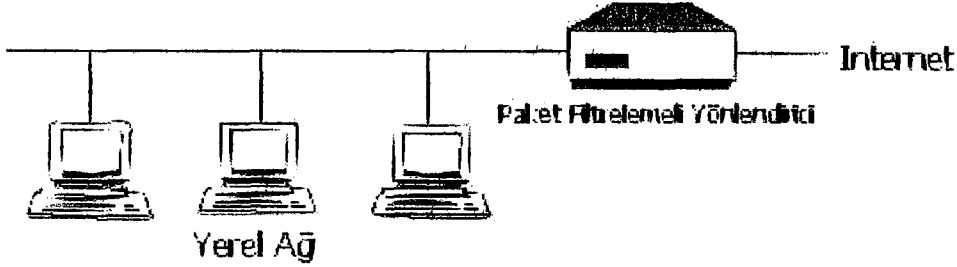
Perdelenmiş alt ağ tipindeki Güvenlik Duvarı - Screened subnet Güvenlik Duvarı.

Ek olarak Güvenlik Duvarı ile modem erişiminde bağlantıları entegre etmek için kullanılan yöntemleri de ayrı bir bölümde değerlendirilebilir.

2.11.1. Paket Filtreleme Güvenlik Duvarı

Paket Filtreleme, küçük ve basit siteler ve ağlar için en yaygın ve en kolay yöntemdir. ancak bir çok dezavantajlarından dolayı diğer Güvenlik Duvarı türlerine göre pek tercih edilmez. Basit olarak, bir internet ağ geçidinde (gateway), Paket

Filtreleme yönlendiricisi (router) kurulur ve sonra , protokollar ve adresleri engellemek veya süzmek için yönlendiricide gerekli ayarlar yapılır. İnternetden sisteme erişim engellenirken, sistemden internete erişim genellikle serbest bırakılır. Bununla beraber yönlendirici (router) güvenlik planına bağlı olarak sistemler ve servislere kısıtlı erişimlere izin verebilir. nıs nfs ve x-windows gibi tehlikeli olabilecek servisler için genellikle erişim ve trafik bloke edilir.



Şekil.2.9. Paket Filtreleme Güvenlik Duvarı yapısı

Paket Filtreleme Güvenlik Duvarı için de yönlendiricilerde ki dezavantajlar geçerlidir. Yerel ve korunması gereken ağların güvenlik ihtiyaçları daha karmaşık olduğundan sorun dahada büyüktür. Bu sorunlar:

Erişim denetleme yetenekleri sınırlıdır. ağ yöneticisi saldırıyı anında farkedemez. Paket Filtreleme kuralları, bilinmeyen türden saldırılara karşı ağı test edebilme yeteneğine sahip değildir.

Eğer karmaşık filtre kuralları ve düzenlemeleri istenirse sistemin idaresi zor olabilir.

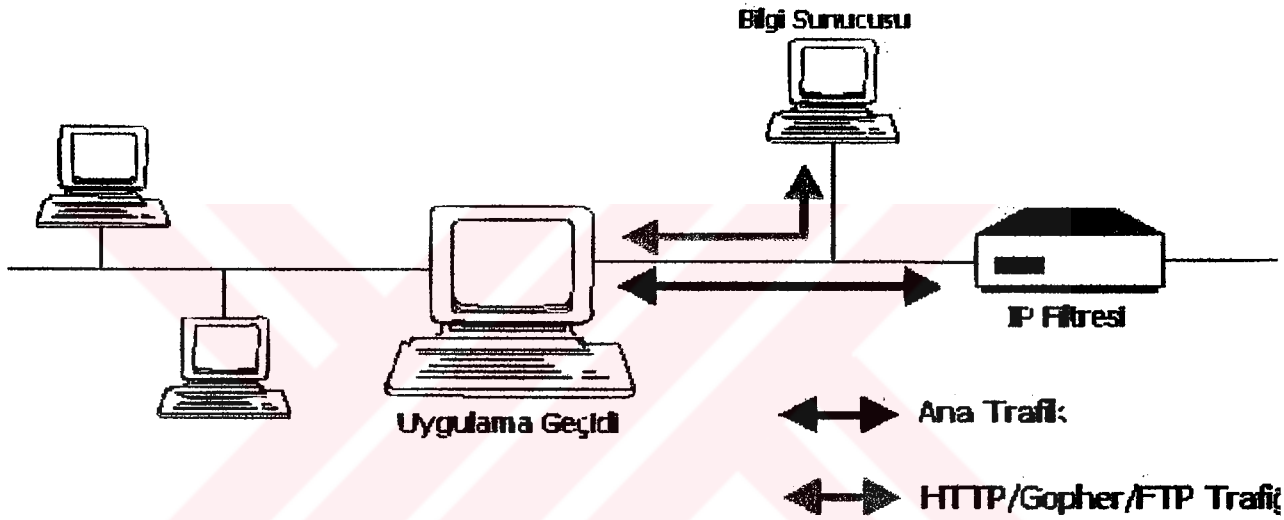
2.11.2. Çift Taraflı Geçit (Dual-Homed Gateway):

Bu tür, "paket Filtrelemeli Güvenlik Duvarına karşı iyi bir alternatiftir. İki ağ ara birimi ile IP iletişimi engellenen bir terminalden oluşur. Burada terminal artık veri paketlerini direk olarak iki ağ arasında iletmez. Ayrıca bu sistemde Paket Filtreleme yönlendiricisi internet bağlantısı üzerine, ek bir koruma sağlamak için yerleştirilebilir. Bu yönlendirici sayesinde bilgi sunucusu (information server) ve modem gibi sistemleri tanımlamak için kullanılabilen dahili ve perdelenmiş bir alt ağ yaratılır. "Paket filtrelemeli Güvenlik Duvarından farklı olarak, "çift taraflı geçit" mekanizması, internet ile ağ arasında IP trafiğini tamamen bloke eder (Vekil Sunucu tarafından kullanılan servisler hariç tabii). Servisler ve sistemlere erişim, bu geçitteki

(gateway'deki) Vekil Sunucu sunucusu tarafından sağlanır. Basit ve emniyetli bir Güvenlik Duvarı türüdür.

Alt ağ (subnet) sadece Güvenlik Duvarı tarafından bilinir ve algılanır. İnternet üzerinde bu ağa ait bir bilgi bulunmaz.

Bu sayede ağ içindeki isimler ve ip adresleri internet sistemlerinden saklanılır. Çünkü Güvenlik Duvarı DNS bilgisini geçirmez.



Şekil.2.10. Yönlendirici ile desteklenmiş bir Dual-Homed Güvenlik Duvarı genel yapısı.

"Çift taraflı geçit" sisteminin kurulumunda telnet, ftp, ve merkezi e-mail servisi için bir Vekil Sunucu düzenlenmelidir. Bu sistemde ek olarak Güvenlik Duvarı davetsiz misafirlerin faaliyetini ve sisteme erişim çabalarını izleyebilir.

"Çift taraflı geçit" tipindeki Güvenlik Duvarı, ağa gelen ve giden veriler ile bilgi sunucusunun trafiğini ayırma imkanı sağlar. Bilgi sunucusu, şekilde gösterildiği gibi geçit-gateway ile yönlendirici-router arasında alt ağa yerleştirilir. Ağ geçidinin (gateway) bilgi sunucusu için uygun Vekil Sunucu servisleri sağladığını farzederek (ftp , gopher veya http gibi) yönlendirici (router), Güvenlik Duvarı doğrudan erişimi önleyebilir ve erişimleri Güvenlik Duvarı'nın denetlemesine tabi tutar. Bilgi sunucusunun bu şekilde yerleştirilmesi, davetsiz misafirlerin bilgi sunucusuna erişimine imkan vermediğinden ve çift taraflı geçit mekanizması ile de ağ sistemlerine ulaşımın engellenmesinden dolayı daha emniyetli bir yöntemdir.

Çift taraflı geçidin esnek olmayan yapısı bazı ağlarda dezavantaj olabilir. Vekil Sunucu haricinde bütün servisler bloke edildiği için var olan diğer servislere erişim imkanı olmaz. Erişilmesi gereken servisler için bu servisleri veya sistemleri geçidin internet tarafına yerleştirmek gerekir. Ancak ayrı bir yönlendirici, geçit ile asıl yönlendirici arasında bir alt ağ oluşturacak şekilde kurulabilir ve ekstra hizmetler gerektiren sistemler burada devreye sokulabilir.

Diğer önemli bir nokta Güvenlik Duvarının güvenli bir makina ve işletim sistemi üzerine kurulması gerekliliğidir. Ana sistemdeki açıklar Güvenlik Duvarı için boşa harcanan para demektir.

2.11.3. Perdelenmiş Kullanıcı Tipindeki Güvenlik Duvarı - Screened Host Firewall

"Çift taraflı geçit" tipindeki Güvenlik Duvarından daha esnekler. Ancak her zamanki gibi esneklik, güvenlik adına verilen bazı bedeller ile sağlanmıştır.

"Perdelemeli Güvenlik Duvarı", yönlendiricinin korunmalı durumdaki alt ağ tarafına yerleştirilen uygulama geçidi ile paket Filtrelemeli yönlendiriciyi birleştirir. Uygulama geçidi sadece bir ağ ara birimine ihtiyaç duyar . uygulama geçitlerinin Vekil Sunucu servisleri ağ sistemindeki bazı Vekil Sunucular için telnet ftp ve diğer veri paketlerini geçirebilir. Yönlendirici Filtreleri ve perdelemeler, uygulama geçiti ve ağ sistemlerine ulaşımı kontrol ettiğinden dikkat edilmesi gereken protokollerdir ve uygulama trafiğini aşağıdaki şekilde yönlendirirler

Yönlendirilmek üzere uygulama geçidine internet ağlarından gelen trafik kabul edilir, İnternet ağlarından gelen diğer tüm trafik geri çevrilir. Uygulama geçitiden gelmedikçe, yönlendirici içeriden gelen herhangi bir uygulama trafiğini reddeder.

"Çift taraflı geçitli" türü Güvenlik Duvarından farklı olarak, bu sistemdeki uygulama geçiti sadece bir ağ ara birimine ihtiyaç duyar ve uygulama geçiti ile yönlendirici arasında ayrı bir alt ağ (subnet) gerektirmez. Bu durum daha esnek ama daha emniyetsiz bir yapıdır. Örneğin ntp gibi daha az tehlikeli servisler, ağ sistemlerine yönlendiricinin içinden geçiş izni verebilirler. Eğer alt ağ sistemleri

internet sistemlerine dns erişimi gerektirirse dns protokolü bu alt ağı erişimi mümkün kılabilir.

2.12. Güvenlik Duvarı Tipleri

Eğer fazlasıyla data kaybı kullanıcı hatalarını oluşturan varsayımını ele alırsak Internetwork'u domainler içerisinde segmentasyon için kullanabiliriz. Kullanıcılar bu domainlere gerekli izin ve özel haklar oluşturulmadan giremezler.

Internetwork ağ trafiğini kontrol amaçlı olarak yarar sağlar. Bu işlemler bazen Yönlendirici veya köprülerin konfigürasyonu ile daha iyi bir şekilde sağlanabilir. Sonuçta Yönlendirici ve Köprülerde burada Güvenlik Duvarı gibi davranışı için Güvenlik Duvarı adı altında incelenebilir. Örneğin Yönlendirici tabanlı Güvenlik Duvarları buna güzel bir örnek teşkil eder. Gerçekte bunlar Güvenlik Duvarı değildir, sadece konfigüre edilerek Güvenlik Duvarı gibi çalışırlar. Biz anlatım sırasında güvenlik duvarlarını birde üç tip adı altında kategorilendirdik.

Üç tip Güvenlik Duvarı vardır.

- Yönlendirici Tabanlı
- Devre Katmanlı
- Uygulama Katmanlı

Son iki tip, ağ izolasyonu adı altında sınıflandırılabilir. Ağ izolasyonunun bir faydası kurumları büyük ağların adreslemesinde yeni adresleme oluşturup kolaylık sağlar.

2.12.1. Yönlendirici Tabanlı Filtreleme

Yönlendirici Tabanlı Güvenlik Duvarları konfigürasyon özelliklerine göre ağlar arası data yönlendirme trafiğini kontrol eder. Yönlendiriciler tek başlarına Güvenlik Duvarı olarak kullanılmaları sağlıklı olmaz çünkü yönlendirici tasarımı sonuçta diğer tip Güvenlik Duvarının özelliklerini karşılayabilecek yapıda değildir. Yönlendirici aynı anda sadece bir paketi inceler ve yönlendirir. Yönlendiriciler

tarafından kullanıların güvenlik politikasında “yasaklanmamış ne varsa izin var” olayıdır.

2.12.2. Devre Düzeyli Ağgeçitleri

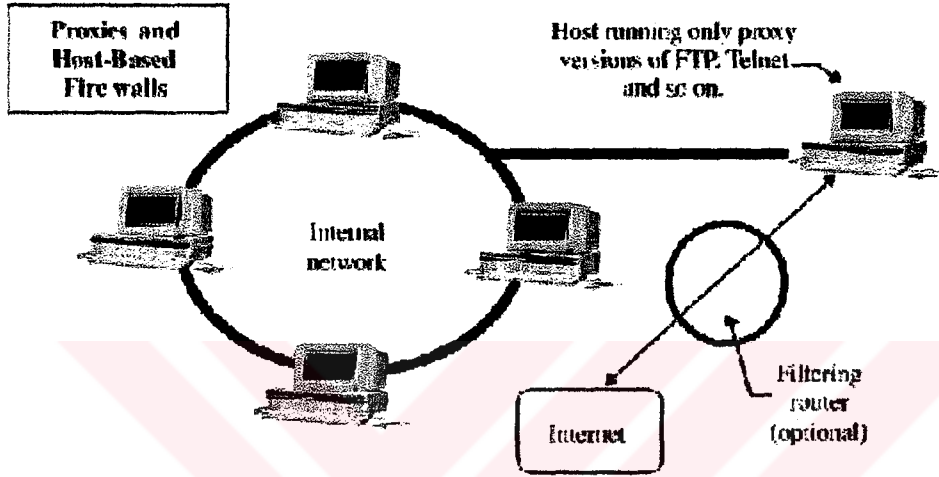
Paket başlığı yöntemi çok bilinen bir ağ katmanlı ataktır. Sonuç olarak Güvenlik Duvarı tarafından gelen ve giden trafiğin araştırılması işi daha üst protokollere bırakılır. Bu, ulaşım, oturum ve uygulama katmanlarında veri trafiğinin daha karmaşık bir şekilde değerlendirilmesi anlamına gelir. Devre düzeyli ağ geçitleri Güvenlik Duvarı kurmanın farklı yoludur. Devre düzeyli ağgeçidi uygulama düzeyli sistemlere benzer, fakat, arayüz sağlayan bir host yerine, dahili ve harici ağlar arasında oturum yapabilecek izole edilmiş bir alt ağ oluşturulur. Normalde bu ağ VPN ve internettten ulaşılabilir şekilde konfigüre edilir, fakat izole edilmiş ağ deki trafik bloke edilir. Bazı izolasyon ağları, interaktif oturumları ya da uygulama düzeyi ağ geçitlerini destekleyecek şekilde konfigüre edilmiş tek bir bastion host içerebilir.

2.12.3. Uygulama Düzeyi Firewallar

Birçok Güvenlik Duvarı uygulama katmanında işleme yapabilmektedir ve genelde düşük seviyeli filtreleme imkanı sunarlar. Bunların biraraya gelmesiyle, Güvenlik Duvarı un güvenliği artar ve hackerlar engellenir. Güvenlik Duvarı oluşturma konusundaki diğer bir yaklaşım, yönlendirici yerine bir bilgisayar kullanmaktır. Bu gateway üzerinden geçen bütün aktivitelerin loglarının tutulması gibi birçok imkanlar sunar. Bazen bastion host diye adlandırılan, ağı koruyan, güvenli, ayırık olarak kurulmuş bir Güvenlik Duvarı, özenle tasarlanması sık sık kontrol edilmesi ve düzenli olarak denetlenmesi gereken kritik bir savunma noktasıdır.

Yönlendirici tabanlı Güvenlik Duvarları paketleri IP düzeyinde izlerken, hostlar trafiğin daha iyi denetlenebileceği uygulama düzeyinde kontrol ederler. Bununla birlikte herhangi bir uygulama kullanılamaz. Uygulama yazılımının ve işletim sisteminin kendisinin de güvenlik açıkları olabileceğini bilmek önemlidir.

Bu problemler ve potansiyel buglar içeren protokoller gözönüne alındığında, uygulama düzeyindeki Güvenlik Duvarları, özel uygulama ağgeçitleri ve servis Vekil Sunucuları kullanılmalıdır. Bununla birlikte Vekil Sunucunun cut-down özelliği yalnızca tasarlandığı uygulama ile birlikte çalışmasına izin verir. (Resim1 Vekil Sunucu ve host tabanlı Güvenlik Duvarları göstermektedir.)



Resim1. Proxies and host-based firewalls

2.13. Güvenlik Duvarı Yapıları

Güvenlik Duvarları biz ayrıca tanım olarak da (yapılarına) iki farklı kategoride de inceledik. Bir önce ki anlatıma göre de üç tip olarak anlatmıştık. Yapılarına göre incelediğimizde;

- Hardware
- Software

Software Güvenlik Duvarlarında genelde standart Üç Bacaklı (Veya Üç Ethernet Kartlı) olması uygun görülür (En az bir). Eğer NAT kullanacaksak bu sayı en az iki ethernet kartı kullanılmalı.

Burada Hardware olarak Roudguard Güvenlik Duvarı (CiPro HQ Serisi) ve CyberGuard Güvenlik Duvarı incelenmiş; software olarak da Altavista Güvenlik Duvarı ve CheckPoint Güvenlik Duvarı incelenmiş.



2.14. Test Kavramının İncelenmesi Ve Güvenlik Duvarlarında Testin Gerekliliği

Neden Test?

İnternet Güvenlik Duvarı'ları günümüzde güvenlik açısından önemli bir yer tutmaktadır. Piyasada bilinen Güvenlik Duvarı tipleri oldukça fazladır Bu Güvenlik Duvarı'lar tasarım açısından birbirlerinden farklılıklar göstermekte ve uygulama alanlarına göre tercih nedeni olmaktadır. Bazı Güvenlik Duvarları içerdikleri fonksiyonellik bakımından diğerlerinden üstün gözükselerde zayıflıkları olabilir. Dolayısıyla bir test yöntemi geliştirilip gerçekten görüldüğü kadar güvenli olup olmadığı araştırılmalıdır.

Güvenlik Duvarı üzerinden geçen internet paketlerini yönetir yani kontrol eder. Piyasada birçok farklı tipte Güvenlik Duvarı bulunmakta ve sonuçta bu Güvenlik Duvarı kullanan kurum veya kişiler Güvenlik Duvarı'nın arkasında bulunan ağlarına davetsiz şekilde girilmesinden endişe ederler[4, 9,13, 14].

2.15. Güvenlik Duvarları Testi Konulu Yapılan Çalışmalar

İlk olarak bahsedeceğimiz makale çevirisi Khalid Al-Twai ve İbrahim A. Al-Kaltham tarafından yapılan ve konusu "Evaluation and Testin of Internet Firewalls" olan yani "İnternet Güvenlik Duvarlarının Değerlendirilmesi ve Testi" konulu bir araştırmadır. Araştırmanın amacı internet güvenlik duvarlarının değerlendirilmesi ve piyasada iyi bilinen iki güvenlik duvarında ele alınarak test yöntemlerinin anlatımına yer verilmesidir. [4]

Anlatımda bazı mevcut Güvenlik Duvarı ürünlerini açıklanmış: 1) Trusted Information Systems Inc. Tarafından geliştirilen TIS Güvenlik Duvarı aracı 2)D.Koblas tarafından geliştirilen socks kütüphaneleri.

Bu ürünlerin ikisi de kamu etki alanlı güvenlik duvarlarıdır. Bunların tanımına kısaca bir göz atarsak;



TIS internet Güvenlik Duvarı Aracı (FWTK)

TIS internet Güvenlik Duvarı aracı Amerikan savunma bakanlığı tarafından organize edilen bir çalışmada hazırlanan software modullerinden ve konfigürasyon kılavuzlarından oluşur. Toolkit öğeleri beraber çalışacak şekilde tasarlanmıştır. Fakat tek başına veya diğer Güvenlik Duvarı öğeleriyle birlikte de kullanılabilir. Güvenlik Duvarı yazılımı Unix sistemlerde Berkeley soket arayüzüyle birlikte TCP/IP yi kullanır.

Socks Güvenlik Duvarı

Socks paketi bir internet soket servisidir. 3 bölümden oluşur: 1) client library rutinleri, 2) daemon, 3)Güvenlik Duvarı host üzerinden uygun ve güvenli bir ağ bağlantısını sağlayacak bir protokol.

Test Ortamları olarak; test yatağı tek bir güvenlik duvarının belli bir zamandaki performansını değerlendirmek üzere tasarlanmış. Bu bölümde güvenlik duvarlarının değerlendirilmesi ve kıyaslanmasıyla ilgili 3 farklı test yatağı kullanılmış. Bu üç test yatağının avantaj ve dezavantajlarını gösterilerek bunlar denenecek olan güvenlik duvarlarının çalıştığı hostlar ve ağ analizi ya da hack simülasyon araçlarının çalıştığı hostlar arasında kurulacak bağlantı sağlamak için omurga mimarisi oluşturmada kullanılmış. Daha sonra testlerin sonuçları incelenerek tablo oluşturulmuş.

Yapılan çalışmada bazı güvenlik değerlendirme araçlarının yardımıyla bazı Güvenlik Duvarı ürünleri değerlendirilmiş. Bazı test metotları geliştirilip iki Güvenlik Duvarı karşılaştırılması için kullanılmış; SOCKS ve TISFWTK. Bununla birlikte herbir Güvenlik Duvarı un farklı bir ortama ihtiyaç duyduğu ortaya çıkmaktadır. Örneğin bir uygulama düzeyi Güvenlik Duvarı olan FWTK, birleşik güvenlik ortamından daha çok akademik olarak tanımlanabilecek, daha fazla güvenlik ve daha az esneklik ortamı sunar. Diğer taraftan, aygıt düzeyi bir Güvenlik Duvarı olan SOCKS, birleşik güvenlik ortamlarından daha çok akademik görünen Daha fazla esneklik ve daha az güvenliğin olduğu bir ortam sunar. Bu deneyde iki Güvenlik duvarının otomatik değerlendirilmesini yapmak için SATAN güvenlik analiz aracını kullanılmış. SATAN bu proje başladığında çok yaygındı. Fakat şu



anda SATAN ın kontrol ettiği birçok güvenlik açığı güncel yazılımlarla düzeltilmiştir [6,12]. Yeni yazılımda da yeterince korunmayan alanlar bulunabilir.

Tablo.2.4. Konfigurasyon Ve Çalıştırma Kıyaslaması

Karşılaştırma Faktörleri	SOCKS v5	TIS FWTK 2.0
Yükleme öncesi konfigürasyon	Çok opsiyonlu,otomatik	Manuel(host sistem hakkında bilgi gerektiriyor)
Yükleme	Otomatik	Otomatik (Fakat tek öğeler ayrı ayrı değerlendirilmeli)
Programlar	Tek program	Ayrık küçük programlar
Etkilenen makinalar	Sunucu ve bütün dahili/harici istemci çalışma istasyonu	Yalnızca sunucu
Desteklenen mimariler	Tekli ve çoklu hostlar	Tekli ve çoklu hostlar
Host Güvenliği	Geliştirilmemiş	Geliştirilmiş
Istemciler	Aşağıdakilerden biri kullanılarak Sock uyumlu yapılmalıdır Statik Dinamik	Özel bir işlem gerekmiyor
Authenticate opsiyonları	Herhangi bir authenticate opsiyonu	Herhangi bir authenticate opsiyonu
Erişim kontrol opsiyonları	Aşağıdakileri tanımlayan kurallar tarafından; Kaynak ve varış host adresleri Kaynak ve varışın servis portu Kullanıcı adı/ password Arayüz adresi	Bireysel servisler tarafından; Kaynak host Kullanıcı adı/password Güçlü onaylama DNS kontrolü
Arayüz algılama	Ağ arayüzlerini algılar	Arayüzleri algılamaz
Etki Alanı Servisleri	Kontrol edilmez	IP adres spoofing etkisine karşı kontrol edilebilir
TCP tabanlı Servisler	SOCK uyumlu hale getirilerek kullanılabilir	FWTK ağ geçidi Poxy leri şunları kapsar: ftp, http, rlogin,telnet, X11 and plug-gw Netacl diğer TCP tabanlı servisleri kontrol etmede kullanılır.
UDP tabanlı servisler	Uygulanamaz	UDP servisler kullanılamaz. Bir çok UDP tabanlı hizmet sunucular iletme görevini yerine getirecek şekilde ayarlandıktan sonra kullanılabilir.
Karşılaştırma Faktörleri	SOCKS v5	TIS FWTK 2.0
Güvenlik Duvarı türü	Devre düzeyi	Uygulama düzeyi
Güvenlik duvarının başlatılması, restlenmesi ve durdurulması	SOCKs komutlarını kullanarak basitçe	İstenen servisleri seçebilmek için inetd.conf un değiştirilmesini ve inetd daemon unun resetlenmesini gerektirir.

İstemciler (Client)	Socket uyumlu uygulamaları kullanmak zorundalar	Diğer tarafa bağlanmadan önce FWTK sunucuya bağlanmak zorundalar.
Şeffalık	Kullanıcılar için %100 şeffaf hale getirilebilir	FWTK sunucuya bağlanması gereken kullanıcılar için şeffaf değildir.
Inbound bağlantılar	Yalnızca socks sunucu ve istemcilerden	Socks sunucu ve istemcilerde olabilen herhangi bir TCP/IP workstationından
Diğer Güvenlik Duvarıyla bağlantı	Socks istemciler FWTK sunucu aracılığıyla bağlanabilirler	FWTK istemciler Socks sunucu aracılığıyla bağlanamazlar
Güvenlik Duvarı host erişilebilirliği	Güvenlik Duvarı hosta erişmeye imkan tanımaz.	Farklı yollarla izin verilebilir veya engellenebilir.
İzin verilen servisler	Herhangi socket uyumlu uygulama ve servis	Yalnızca FWTK sunucu kontrolünde çalışan FWTK Vekil Sunucu servisleri ya da standart servisler

Tablo.2.5. SOCKS ve FWTK Kullanımı Kıyaslaması

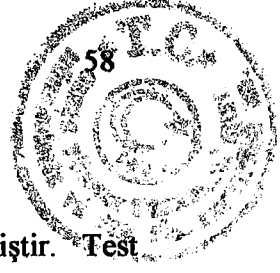
Artılar	Eksiler
Şeffaf	Devre düzeyi: Kontroller yalnızca bağlantı zamanında yapılabilir.
Socks istemciler Socket olmayan diğer TCP/IP tabanlı güvenlik duvarı aracılığıyla bağlanabilirler	Yalnızca socks sunucu ve istemcilerden gelen bağlantılar kabul edilir.
Authenticate ve şifreleme	Varış Socks Güvenlik Duvarı adresi local socks sunucu tarafından bilinmeli ve konfigürasyon dosyasında bulunmalıdır.
Kaynak/Varış Host/Port kombinasyonlarıyla erişim kontrolü	Local socks Güvenlik Duvarı adresi kendi istemcileri tarafından bilinmeli ve herbirinin konfigürasyon dosyasında bulunmalıdır.
Arayüz algılama	Yalnızca Socket uyumlu uygulama ve servisler Güvenlik Duvarı dan geçebilir.
Güvenlik Duvarı hosta bağlantı yapılamaz(Güvenlik duvarının türü devre düzeyi olduğu için bu avantaj olarak kabul edilir)	Çalıştığı hostun güvenliği artırılmaz.
	UDP desteğinin olmaması

Güzel bir çalışma sonucu iki firewall karşılaştırılmış ve yukardaki tablo oluşturulmuş. Bu deneyde iki Güvenlik duvarının otomatik değerlendirilmesini yapmak için SATAN güvenlik analiz aracını kullanılmış. SATAN bu proje başladığında çok yaygındı. Fakat şu anda SATAN ın kontrol ettiği birçok güvenlik açığı güncel yazılımlarla düzeltilmiştir. Yeni yazılımda da yeterince korunmayan alanlar bulunabilir.

57

Bir diğerk akademik çalıřma da H.Joseph Wen (School of Management, New Jersey Institude of Technology, Newark, USA) ve Jyh-Horng Micheal Tarn (Information Systems, Department of Business, Chowan College, Murfreesboro, USA) tarafından yapılan Internet Güvenlięi: Güvenlik Duvarı Seçimindeki Hususlar (A Case Study of Firewall Selection) konulu çalıřmadır[2]. Bu çalıřmada da yine Güvenlik Duvarı mimarileri incelenmiř ve güvenlik duvarı seçiminde dikkat edilmesi gereken hususlar anlatılmıřtır. Genel olarak paket filtreleme, kullanıcı onaylama (User Authentication), Uyarı Denetimi gibi özellikler incelenmiř.

Yapılan arařtırmalarda göz önünde tutulduğunda; Güvenlik Duvarların testi ve deęerlendirmesi organizasyon için doęru, uygun ve fonksiyonellik olarak tatmin edicilik için yardımcı olur. Teoride belirtilen özelliklerin pratikte işlevi görölür. Firewall için en önemli özelliklerinden birisi de performansdır. Özellikle yoğun trafięi olan firewallar bazı saldırı teknikleriyle hizmet veremeyecek duruma gelebilirler. Günümüz teknolojisi hızla gelişmekte ve her geçen gün hackerlar tarafından yazılımlar geliştirilmekte ve sistemlere zarar verilebilmektedir. Bu yüzden mevcut sistem iyi tanınmalı ve güncellemeler zamanında yapılmalıdır.



3. KURT TEST YÖNTEMİ

Geliştirilen test yöntemine KURT Test Yöntemi adı verilmiştir. Test Programıyla birlikte aşağıda ki bölümleri kapsamaktadır.

Donanımsal (Yapısal) Test

Yazılımsal Test

Güvenlik Testi

Performans Testi

Yönetimsel Test

Kullanışlılık Testi

3.1. Güvenlik Duvarlarında Test Yöntemi Ve Güvenlik Duvarı Testleri

Bazı Güvenlik Duvarları paket filtreleme tekniği kullanırlar ve bu filtreleme değişken yeteneklerde de kullanılabilir. Bu yüzden Güvenlik Duvarının test edilip değerlendirilmesi gerekmektedir. Güvenlik Duvarların testi ve değerlendirmesi organizasyon için doğru, uygun ve fonksiyonellik olarak tatmin edicilik için yardımcı olur.

Bu inceleme sırasında Güvenlik Duvarlarda ki günümüzde ki en çok tercih edilenler arasından seçilerek incelenmiştir.

Ayrıca Güvenlik Duvarlarının;

- Desteklediği Platformlar
- Update mekanizması
- Kontrol mekanizması
- WEB site tracking
- Security Policy
- Virus Scanning
- Database erişimi
- Network Address Translation (NAT)
- Encryption
- GUI tabanlı yönetim



- Uyarı mekanizması
- gibi konulara dikkat edilir.

Şu ana kadar incelenen test yöntemlerinde bazı programlar kullanılmış. Örneğin “Evaluation and Testing of Internet Firewalls” [4] konulu çalışmada SATAN programı kullanılmış. Ancak birkaç program yardımıyla yapılan testler yetersiz kalabilmektedir. Test yöntemi kavramı geniş bir alana yayılmaktadır. Çünkü sadece belirli bir konunun araştırılmasından öte yapıyı her yönüyle ele alınmasını gerektirir. Geliştirilen test yöntemi olan KURT Test Yöntemi öncelikle kategorilere ayrılmış ve sadece deneysel değil, gözlemsel testide içermektedir. Ayrıca sadece güvenlik duvarı değil, beraberinde tüm sistemin analizinde önemine dikkat çekilmekte. Donanımsal (Yapısal) Test, Yazılımsal Test, Güvenlik Testi, Performans Testi, Yönetimsel Test, Kullanışlılık Testi gibi. Hepsi kendi içerisinde ayrı bir test yöntemi gibidir. Ayrıca test yönteminde öncelikle bir test yönteminin nasıl olması gerektiği gibi konulara da değinilmektedir. [7,9]

3.2. Güvenlik Duvarı Testleri

- Donanımsal (Yapısal) Test

Mevcut konumunun incelenmesi ve analizi

Donanımsal test, mimari yapının incelenmesi ve analiz edilmesidir. Güvenlik Duvarlarının mimari içinde ki yerinin güvenlik ve performans açısından yeterliliğinin testidir. Çünkü bir mimaride firewall ağ üzerinde bulunduğu yer itibariyle üzerinden geçen ağ trafiği, onun performansını ve güvenlik içeriğini etkileyecektir.

- Yazılımsal Test
- Güvenlik Testi
- Performans Testi
- Yönetimsel Test
- Kullanışlılık Testi

3.2.1. Donanımsal (Yapısal) Test

Donanımsal test, mimari yapının incelenmesi ve analiz edilmesidir. Güvenlik Duvarların mimari içinde ki yerinin güvenlik ve performans açısından yeterliliğinin testidir. Çünkü bir mimaride Güvenlik Duvarı ağ üzerinde bulunduğu yer itibariyle üzerinden geçen ağ trafiği, onun performansını ve güvenlik içeriğini etkileyecektir.

3.2.2. Yazılım Testi

Güvenlik Duvarı yazılımının hangi programlama dilinde yazılı olduğu ve bununla birlikte yazılımın artı ve eksilerinin incelenmesi.

3.2.3. Güvenlik Testi

Güvenlik testinin amacı; konfigürasyonu yapılan güvenlik duvarının internet ortamında iyi bilinen yüzlerce atak formlarına karşı güvenilirliğini test etmektir. Bu tür testler için gerek internet ortamında gerekse firmalar tarafından programlar satılmakta ve desteği verilmektedir.

3.2.4. Performans Testi

Performans testi, güvenlik duvarının data trafiğinde paket/zaman başarımlı oranı testidir. Data trafiğinde ki iletişim sırasında gelen ve giden dataları check etme süresi, bellek durumu, datanın yoğunluğuna göre başarımlı göz önünde tutulur. Güvenlik duvarları kendi aralarında da yapılarına göre elbette ki farklı performanslar gösterir. Bir yazılım güvenlik duvarı ile donanım güvenlik duvarı arasında bu durum daha açıkça görülür. Ayrıca performans testinde limit değerlere (Veya sınır değerler) yakın değerlerde olan trafik akışında güvenlik duvarının göstereceği performans, oluşabilecek hataların test edilmesi gerekmektedir.

3.2.5. Yönetimsel Test

Güvenlik Duvarı konfigürasyonunun yönetimsel testidir. Güvenlik Duvarlarının yönetilebilirliği ve kurulum kolaylığının testidir. Arayüzeylerin anlaşılabilirliği, konfigürasyon sırasında oluşabilecek hatalar, uyarılar önemlidir. Her konuda olduğu gibi burda da anlaşılabilirlik önemlidir. Kişi önceden yaptığı konfigürasyonu kolaylıkla analiz edebilmelidir.

3.2.6.Kullanışlılık Testi

Kullanışlılık Testi; kurulum kolaylığı, konfigürasyon, yönetim, dokümanlama işlemi, yardım menüsü ve raporlama özelliğinin test edilmesidir. Bu konu hakkında uzman kişinin görüşü bakımından ele alınır. Bu konu altında AltaVista Güvenlik Duvarı 97 ile Check Point Güvenlik Duvarı incelenirse;

3.2.6.1 AltaVista Güvenlik Duvarı 97

AltaVista Güvenlik Duvarı 97; özel ağlarla internet arasında veya güvenli kalması gereken TCP/IP uygulamaları arasında güvenli bağlantı sağlayan, kolay yönetilebilen, ileri raporlama ve alarm özelliklerine sahip bir güvenlik yazılımıdır. Sağladığı olanaklar açısından aşağıdaki özelliklere sahiptir.

Avantajlar ;

- Servisler açısından güvenilir uygulamalara sahiptir (FTP, Telnet, WWW, Mail, News, RealAudio ve Finger)
- Kurulumu kolaydır (Adım adım instolasyon)
- Yönetimi kolaydır (Güvenlik Duvarı logları uzaktan izlenebilir, servisler Start/Stop edilebilir, gerçek zaman monitoring, gerçek zaman raporlama, istatistik ve alarm analizleri, çok sayıda güvenlik duvarı yönetimi uzaktan yapılabilir).
- Altavista Güvenlik Duvarı 97; Dual-DNS sunucu olarak konfigüre edilebilir (Grafic User Interface tabanlı konfigürasyon kullanılarak, name servislerin; internal servis veya external servis olduğu anlaşılabilir).
- Alarm özellikleri açısından ileri çözümler sunmaktadır (Yeşil, sarı, turuncu ve kırmızı renkleri üzerinde çeşitli alarm tipleri tanımlanarak, herhangi bir kötü niyetli girişimin durumu ekranda izlenebilir. Sistem yöneticisine mail gönderilmesi sağlanabilir).
- Altavista Güvenlik Duvarı 97; Uniform Resource Location (URL) bloklamaya izin verir
- (URL'nin bloklama yaptığı www servisleri şunlardır: HTTP, Gopher, FTP, SSL)
- Konfigürasyonu ve kontrolü en kolay güvenlik duvarlarından biridir(GUI olanakları ile)

- Altavista Güvenlik Duvarı 97; hem Windows NT hem de UNIX işletim sistemleri üzerinde çalışabilmektedir. Ancak en iyi performansı, DIGITAL UNIX işletim sistemi üzerinde çalışırken göstermektedir (IP paket filtreleme, Enhanced www Vekil Sunucu, generic UDP Vekil Sunucu ve DMZ desteği; Altavista Güvenlik Duvarı 97'nin windows NT işletim sistemi üzerinde çalıştırılması durumunda verilmemektedir)

Dezavantajlar ;

Altavista Güvenlik Duvarı 97; çok büyük networkler için elverişli değildir (Kim olduklarına bakılmaksızın, Güvenlik Duvarı dışındaki her bağlantıya benzer davranır; sistem yöneticilerine özel ayrıcalıklar tanınmaz) 2 LAN arabirimi kullanmaktadır (Tüm diğer Güvenlik Duvarları en az 3 LAN arabirimi kullanmaktadır)

3.2.6.2 Checkpoint Güvenlik Duvarı

Check Point Güvenlik Duvarı-1; internet, intranet/extranet ve uzaktan erişim sağlayan kullanıcılar için, çok güçlü onaylama, kodlama ve ağ address translation (NAT) yetenekleriyle güvenlik hizmetleri sunan bir yazılımdır. Sağladığı olanaklar açısından aşağıdaki özelliklere sahiptir.

Avantajlar ;

Grafiksel olarak log görüntüleme olanaklarını sunmaktadır (Güvenlik Duvarına yapılan tüm bağlantı girişimlerinin ve geçerli olan bağlantıların izlenmesi olanaklıdır).

“Inspection Module” yardımı ile veri, tüm paket katmanlarında incelenebilir. Bu modülle; paketin IP adresi, port numarası bilgileri elde edilebilir, bir bağlantı gerekirse reddedilir.

Merkezi yönetim olanaklarıyla; ağlar, kullanıcılar, sunucular için güvenlikle ilgili parametreler güncelleştirilebilir, bağlantı isteklerine ilişkin loglar analiz edilebilir, görüntülenebilir, print edilebilir.

Her kullanıcı için; FTP, TELNET, HTTP, RLOGIN servislerinin kullanımına yönelik sınırlama getirilebilir. Ancak özel konfigürasyonlarla, sistem yöneticilerine bazı ayrıcalıklar tanınabilir.

“Network Address Translation” özelliği ile, geçersiz veya gizli IP adreslerinin internal olarak kullanılması sağlanabilir. Bu özellik, internet’e tek bir IP adresinden ulaşılabilir (Dinamik olarak bir port numarası geçersiz IP adreslerini, geçerli bir tek IP numarasına çevirir); böylece internal olarak binlerce IP adresi kullanılabilir. Host veya sunucular IP adresleri yerine, isimleriyle temsil edilebilir; bu özellik de güvenliği artıran unsurlardan bir tanesidir.

FTP, SMTP ve HTTP uygulamalarına ilişkin virüs taraması yapılabilir (Dosya ve mail)

Güvenlik Duvarı gruplarının tek bir başlık altında konfigure edilmesi olanağını sunmaktadır. Grafik User Interface (GUI) kullanılarak, Güvenlik Duvarı gruplarına ve paket filtreleme yapan yönlendiricilere ilişkin kurallar enterprişe’da install edilebilir.

VIRTUAL PATH NETWORK (VPN) KULLANILARAK, INTERNAL VEYA INTERNET ÜZERİNDE güvenli haberleşme yapılabilir.

HTTP, URL ve içerik tabanlı filtreleme, güvenlik alanında en önde gelen konulardandır. İçerik tabanlı filtreleme; Java ve ActiveX programlarının yerel ağa girmesine engel olmak amacıyla kullanılmaktadır.

Dezavantajlar ;

DIGITAL UNIX işletim sistemini desteklememektedir.

Sonuç olarak;

Altavista Güvenlik Duvarı 97; hem Windows NT hem de UNIX işletim sistemleri üzerinde çalışabilmektedir. Ancak en iyi performansı, DIGITAL UNIX işletim sistemi üzerinde çalışırken göstermektedir (IP paket filtreleme, Enhanced www proxy, generic UDP proxy ve DMZ desteği; Altavista Güvenlik Duvarı 97’nin windows NT işletim sistemi üzerinde çalıştırılması durumunda verilmemektedir)

CheckPoint Güvenlik Duvarı-1; Windows 3.51, Windows 4.0 ve UNIX (Sunos, Solaris ve HP-UX) işletim sistemlerini desteklemekte, ancak DIGITAL UNIX işletim sistemini desteklememektedir

3.3.Test PC

Testi yapacak olan PC'yi aslında saldırı yapan hacker PC olarak ta tanımlayabiliriz. Bu PC si ilgili resimlerde de görüleceği gibi Ağ üzerinde belirlenen konumlarda bilinen tüm saldırı teknikleriyle hedef ağa saldırır.

Test PC si genel olarak aşağıda belirtilen genel ağ yapıları içerisinde olarak gerekli test işlemlerini yapar.

Mevcut korunmasını istediğimiz ağı güvenli ağ, dış ağıda güvensiz ağ olarak tanımlarız.

Aşağıda ki şekilde Test PC si güvensiz ağ üzerinden Güvenilir ağa atak yapmaktadır.

Örneğin bir port taraması yapabilir. Böylelikle açık ve kapalı portlar test edilmiş olur. Bunu şimdilik LANPortScan programı ile yapacağız. Bu programda taranacak IP aralığı verilerek açık bulunan portlar tespit edilir.

3.4.Test Yöntemi

Test yöntemimiz önceki test yöntemlerine bazı yönlerden benzerlik taşımasına rağmen genel olarak test yönteminin geliştirilmesi açısından yeni analizler içermektedir. Bir test yönteminin nasıl olması gerektiği ile ilgili anlatımlara öncelikle yer verilmiştir. Daha sonra da güvenlik duvarı öncelikle tek başına ele alınmakta ve incelenmekte, bununla beraber güvenlik duvarı tarafından korunan sistemin de bir bütün olarak ele alınmasıyla test yöntemi uygulanmakta. Testi yapacak olan PC'yi aslında saldırı yapan hacker PC olarak ta tanımlayabiliriz. Bu PC si ilgili yerel ağ üzerinde belirlenen konumlarda bilinen tüm saldırı teknikleriyle hedef ağa veya hedef ağ içerisinde ki bir hedef PC'ye saldırır.

Yazılan bir programla güvenlik duvarı test edilmekte ve analizler yapılmakta. Ayrıca uzman kişiler tarafından da tüm sistemin incelenmesi gerektiğinin önemi belirtilmektedir.

Yazılan program öncelikle güvenlik duvarı üzerinde ki açık portları taramakta ve bu portlardan gelebilecek saldırılara karşı kullanıcıyı bilgilendirmekte ve öneri sunmaktadır.

Güvenlik duvarına yüksek miktarda data gönderilerek tanımlanan kuralların (rule) işlevi engellenmeye çalışılmıştır. Bu sayede güvenlik duvarının performans testi yapılmaktadır.

3.5.Test Programın Yapısı

Programın amacı bir güvenlik duvarının ve beraberinde tüm sistemde ele alarak güvenlik testini yapmaktır. Program tasarlanırken amaç, tamamiyle yeni bir hack programı yazmak değil, bilinen en popüler hack programları da araştırılıp bunların içerisinde en iyi ve etkili olanlarının analiz edilip VisualBasic 6 yazılan bir test programına dahil edilmesidir. Ayrıca bu programla Güvenlik Duvarı üzerinde tanımlanan kurallar (rule) test edilmektedir.

Programda özellikle port tarama programlarına ilk başta yer verilmekte ve genel testler de bunlarla yapılmakta. Mevcut açık portlar belirlenmekte ve bu portlardan gelebilecek saldırı türleri hakkında bilgilendirme yapılmaktadır. Portun açık olmasının ne gibi riskler taşıdığı ve sonuç olarak öneriler sunulmaktadır.

Ayrıca Güvenlik Duvarına program tarafından yüksek miktarda veri gönderilerek meşgul edilmekte ve kural (rule) tanımlamaların sağlıklı çalışması önlenerek oluşabilecek hata ve açıklar analiz edilmeye çalışılmakta.

Ayrıca test programı sadece Güvenlik Duvarını değil Güvenlik Duvarının olduğu tüm sistemi ele alınarak tasarlanmıştır.

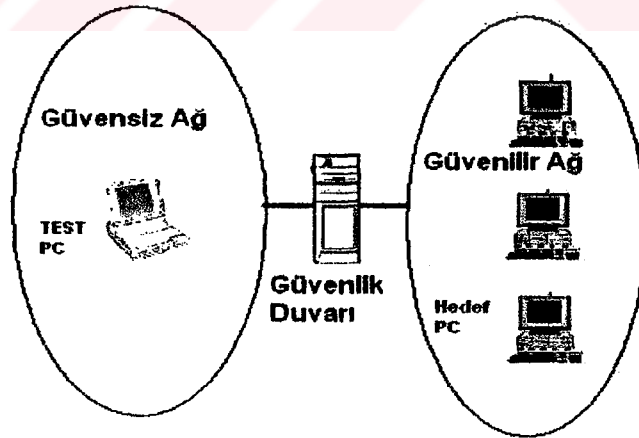
4.TEST YÖNTEMİNİN UYGULANMASI

Test yönteminin uygulanması için öncelikle test ortamı incelenir. Çünkü güvenlik duvarının sistem içinde ki yeride çok önemlidir. Sistemin genel olarak yapısı incelenirken donanımsal ve yazılımsal olarak incelenmelidir. Çünkü güvenlik duvarının izin verdiği bir erişimden bilgisayarınızda ki backdoor dan zarar verilebilir ya da sistem açıklarından zarar verilebilir.

4.1.Kurt Test Yönteminin Uygulanması

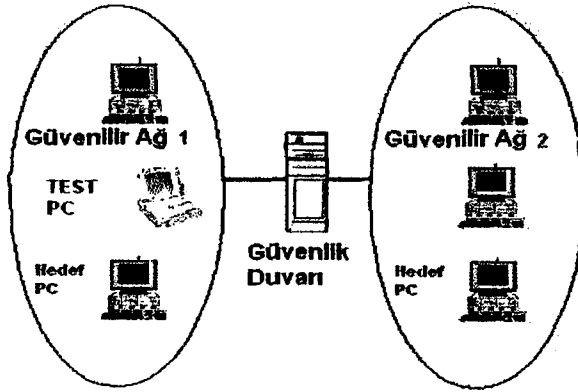
Mevcut korunmasını istediğimiz ağı güvenli ağ, dış ağda güvensiz ağ olarak tanımlarız.

Aşağıda ki şekil4.1.'de Test PC si güvensiz ağ üzerinden Güvenilir ağa atak yapmaktadır.Örneğin bir port taraması yapabilir. Böylelikle açık ve kapalı portlar test edilmiş olur.



Şekil.4.1. Test Bilgisayarının Güvensiz Ağ Üzerinden Güvenilir Ağda ki Hedef PC'yi Güvenlik Duvarı Üzerinden Testi

Şekil.4.2.'de ise mevcut güvenilir birden fazla ağın olduğu bir ağda her iki güvenilir ağ arasında ki bir güvenlik duvarı üzerinden hedef PC ye atak yapılarak test yapılmaktadır.



Şekil.4.2. Test Bilgisayarının Güvenilir Ağ-1 Üzerinden Güvenilir Ağ-2 de ki Hedef PC'yi Güvenlik Duvarı Üzerinden Testi

Daha sonra da güvenlik duvarı öncelikle tek başına ele alınmakta ve incelenmekte, bununla beraber güvenlik duvarı tarafından korunan sistemin de bir bütün olarak ele alınmasıyla test yöntemi uygulanmaktadır.

Yazılan programla (KURT Test) güvenlik duvarı test edilmekte ve analizler yapılmakta. Ayrıca uzman kişiler tarafından da tüm sistemin incelenmesi gerektiğinin önemi belirtilmektedir.

Yazılan program öncelikle güvenlik duvarı üzerinde ki açık portları taramakta ve bu portlardan gelebilecek saldırılara karşı kullanıcıyı bilgilendirmekte ve öneri sunmaktadır.

Güvenlik duvarına yüksek miktarda data gönderilerek tanımlanan kuralların (rule) işlevi engellenmeye çalışılmıştır. Bu sayede güvenlik duvarının performans testi yapılmaktadır.

Ayrıca Güvenlik Duvarı konfigürasyonunu yapan sistem yöneticisi de sonuçta tanımladığı kuralların (rule) istenilen şekilde olup olmadığını test etmesi gerekmektedir. Çünkü Güvenlik Duvarı hatalı konfigürasyonunuz sonucu istenilen şekilde hizmet edemeyebilir. Sorumlulukda burada tamamiyle konfigürasyonu yapan sistem yöneticisine aittir.



Programda özellikle port tarama programlarına ilk başta yer verilmekte ve genel testler de bunlarla yapılmakta. Mevcut açık portlar belirlenmekte ve bu portlardan gelebilecek saldırı türleri hakkında bilgilendirme yapmaktadır. Portun açık olmasının ne gibi riskler taşıdığı ve sonuç olarak öneriler sunmaktadır. Örneğin eğer güvenlik duvarı üzerinden yerel ağa port 25 yani SMTP portu açık hale getirilmişse bu port 25 den gelecek tüm saldırılara yerel ağ açık demektir. Bu yüzden port 25 açık olsa bile mail sunucu dışında ki tüm sunucuların SMTP Servisleri stop edilmelive güvenlik duvarında da sadece IP olarak mail sunucular için bu port açık olmalıdır. Program böyle bir açık bulursa bu gibi ayrıntılı öneriler sunmaktadır.

Ayrıca Güvenlik Duvarına program tarafından yüksek miktarda veri gönderilerek meşgul edilmekte ve kural (rule) tanımlamaların sağlıklı çalışması önlenerek oluşabilecek hata ve açıklar analiz edilmeye çalışılmakta.

Ayrıca test programı sadece Güvenlik Duvarını değil Güvenlik Duvarının olduğu tüm sistemi ele alınarak tasarlanmıştır.

4.2.Yerel Ağın Tanınması

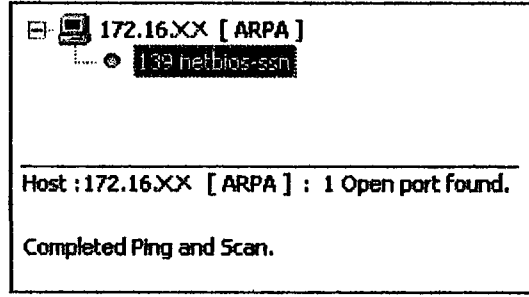
Yerel Ağın tanınması sunucu ve istemcilerin işletim sistemleri ve donanımlarının bilinmesi, ki bu bir kurum için her zaman bilinmesi gerekli olan bir konudur ve bunun için bir durum listesi oluşturulmalıdır. Yerel ağda bulunan güvenlik duvarı tipi, anahtar, hub, yönlendiricilerinde bilinmesi gereklidir. Örneğin bir yönlendirici de güvenlik duvarı olarak yerel ağı koruyabilir.

4.3.Port Tarama Sonuçları

Port tarama program üzerinde bulunan port tarama butonuna basıldığında karşımıza birden fazla port tarama programları çıkar. Bunlar sonuçta aynı işi yapmalarına karşın yazılımları ve analiz ayrıntıları farklıdır. Yani kimi basit bir tarama yaparken diğeri daha ayrıntılı bir inceleme yapmaktadır. Biz Zorlu Holding bünyesinde bulunan Vestelnet Online Communications and Information Inc. 'nin iki güvenli ağ arasında bulunan CheckPoint Güvenlik duvarının testini yaptığımızda;

Önemli Not: IP'ler ve Host isimlerigüvenlik amacıyla tam olarak yazılmamıştır.

Verilen bir posta sunucunun ip'sini yerel ağımızdan port taraması yapılmıştır.



Şekil.4.5. Güvenlik Duvarına Yapılan Port Taraması Sonuçları

Sadece bir tek portu açık olarak görüyoruz. Çünkü biz aslında güvenlik duvarına değil onun kurulu olduğu sunucuyu test edebiliyoruz burada. Güvenlik duvarı o sunucuda bir yazılımdan ibarettir.

4.4.Güvenlik Duvarlarında Tanımlanan Kuralların Testi

Sistem Yöneticisi kural (rule) tanımlarken hata yapabilir. Bu yüzden güvenlik duvarında ki arayüzlerin kullanım kolaylığı önemlidir. Sistem yöneticisi bir IP'ye hak tanımlarken örneğin IP yazımında hata yapabilir veya önceden tanımlamış olduğu bir kural artık kullanılmıyor olabilir. Bu gibi durumlarda sistem yöneticisi periyodik kontroller yapmayı ihmal etmemelidir. Örneğin virüs içeren bir web sayfası yasaklansın. Bu sayfa deneme amaçlı olarak www.virusweb.com olsun. IP numarası 216.156.16.72 dir.

Bu sayfaya yerel ağdan erişim güvenlik duvarı üzerinden configure edilerek yasaklansın. Daha sonra test PC'si yerel ağdan bu sayfaya bağlanmaya çalışarak sayfanın gelip gelmediğini kontrol eder. Yapılan testte sayfa gelmemektedir. Daha sonra yerel ağ haricinde ki bir ağ üzerinden sayfanın gelip gelmediği test edilir. Yaptığımız testte sayfa bu durumda gelmektedir. Bu şekilde basit bir kural test edilmiş olur.

4.5.Mevcut Ağın Meşgul Edilmesi Ve Performansın Değerlendirilmesi

Güvenlik duvarı sonuçta gelen isteklere cevap verme kapasitesi sınırlıdır. Biz program vasıtasıyla yüksek miktarda veri göndererek güvenlik duvarını sürekli



meşgul ettik ve veri gönderme işi birden fazla bilgisayar tarafından yapıldı. Çünkü bir güvenlik duvarını sadece bir tek PC'den meşgul etmeye çalışmak yetersiz olacaktı. Belirli bir veri gönderdiğimizde güvenlik duvarını kullana diğer PC'lerin veri alışverişleri yavaşlamış ve mevcut ağda rahatsız edici bir yavaşlama oluşturduk. Bu sırada güvenlik duvarının gelen isteklere cevap verme süresi, cevap verebilme yeteneği bize onun performansını göstermektedir.

Örneğin deneme amaçlı olarak Windows NT Sunucu üzerine kurulu bir PC'ye CheckPoint Güvenlik Duvarı kurduk ve bu PC'ye test programımız ile yüksek miktarda veri gönderdik. Güvenlik duvarı olan PC bir süre sonra ağda mevcut diğer PC'lere ping dahi atamaz duruma geldi.

Normal şartlarda ping komutuna

Reply from 212.29.65.X: bytes=32 time=20ms TTL=125

gibi yanıt alınır. Ancak ağ meşgul edildiğinde;

Reply from 172.16.7.182: bytes=65500 time=550ms TTL=128

Request timed out.

Reply from 172.16.7.182: bytes=65500 time=240ms TTL=128

Request timed out

Request timed out

gibi yanıt alınır. Yani Sunucunun ağ iletişimi engellenmiş olur.

4.6. Analiz Sonuçlarının İncelenmesi

Sonuç olarak güvenlik duvarının testi, sistemimin güvenliğinden emin olunmasını sağlar. Yani sayısal bir işlemin sağlanması gibi. Programda manuel olarak yapmamız gereken bazı testlerde kullanıcı için kolaylaştırılmıştır. Yasaklanan bazı sitelerin gerçekten gelip gelmediği gibi engellemeler otomatik olarak gözlemlenebilmektedir.

Port tarama ve Ağın meşgul edilerek kuralların test edilmesi bu çalışmanın temelini oluşturmaktadır. Yerel ağda bulunan açık portlarla güvensiz ağa karşı açılan portların farklı olduğunda yaptığımız testte gördük. Ancak bu sistem yöneticisi ve kurumun sistem güvenliğinden sorumlu kişilerin bilgisi dahilinde olan birşeydir.



Sistem yöneticisi sonuçta içerden gelebilecek saldırılara karşı da önlem almak zorundadır. İstatistiklere göre kurum içinden yapılan saldırı oranı kurum dışından yapılan saldırı oranından yüksektir. Daha önce ki test yöntemlerinde genelde bir program ile (örn. SATAN) ile test edilmiş. Bunun için özel bir program yazılmamış. Biz test yöntemini belirli kategorilere ayırıp geliştirdiğimiz bir program aracılığıyla da hem kullanıcıya gerekli uyarı bilgileri sunan hem de manuel testleri program tarafında yapılabilir hale getirilir. Ayrıca KURT test yönteminde tüm sistemin ele alınması gereğinin önemini belirtilmiştir. Test yöntemini belirli kategorilere ayırmış ve bunlar; Donanımsal (Yapısal) Test, Yazılımsal Test, Güvenlik Testi, Performans Testi, Yönetimsel Test, Kullanışlılık Testi. Mevcut donanımı donanım testi içerisinde, işletim sistemlerinin oluşturduğu açıkları güvenlik testi içerisinde, performansını performans testi içerisinde incelemiştir. Ayrıca Güvenlik Duvarlarının yönetilebilirliği ve kurulum kolaylığının testi olarakta yönetimsel test olarak bir yöntem belirlenir. Bu yöntem de arayüzlerin anlaşılabilirliği, konfigürasyon sırasında oluşabilecek hatalar, uyarılar incelendi. Güvenlik Duvarının kullanıcı açısından kurulum kolaylığı, konfigürasyon, yönetim, dokümanite işlemi, yardım menüsü ve raporlama özelliğinin test edilmesi olarakta kullanışlılık testi yapılır.

Yapılan çalışmalarda belirli iki güvenlik duvarları karşılaştırılmış. Oysa yapılan çalışmada iki güvenlik duvarının karşılaştırılmasından ziyade tüm sistem ele alınarak güvenlik politikası oluştururcasına test yöntemi uygulanmış. Yani sadece bir programa bağlı kalmamış.



5. SONUÇ

Bir ağda yeterli güvenliği sağlamak için basit şifrelerden kompleks güvenlik duvarlarına kadar değişen güvenlik seviyeleri vardır. Güvenlik seviyesi artırıldıkça, ağa bağlı kaynaklarında güvenliği de o derece artırılmış olur. Tabi bu arada maliyette artmaktadır.

Mevcut ağ korumanın en iyi yolu bir güvenlik duvarı kullanmaktır. Güvenlik duvarı, üzerinden geçen ağ trafiğini analiz eder ve raporlar.

Güvenlik duvarının performansı ağ yapısı için çok önemlidir. Performans, kurumların hızla gelişen haberleşme teknolojisi içerisinde ihtiyaç duyulan en önemli kavramlar içerisinde yer alır.

Güvenlik duvarının konfigürasyonu uzmanlık isteyen bir konudur. Konfigürasyon arayüzünün de kolay anlaşılır ve yönetilebilir olması gereklidir. Hatalı bir konfigürasyon tüm ağı riske atar ve kurum güvenliğini maddi ve manevi yönden zarara uğratabilir.

Bu gibi durumlar göz önüne alınarak bir güvenlik testi yapılması gerekmektedir. Özellikle güvenlik duvarının konfigürasyonunun ve performansının test edilmesi önem taşır. Bu manuel olarak da yapılabileceği gibi mevcut geliştirilmiş programlar da kullanılabilir.

Test yöntemi hazırlanacağı zaman sadece güvenlik duvarı değil ağ yapısı bütünüyle ele alınmalıdır. Güvenlik duvarının ağ içerisinde konum ve işlevi önemlidir. Gereksiz kural tanımlamalarından kaçınılmalı, performans verimi sürekli göz önünde tutulmalıdır.

KURT Test yönteminde yardımcı bir program tasarlanarak güvenlik duvarı test edilmekte ayrıca kullanıcıyı belirli konularda bilgilendirmektedir. Örneğin açık bulunduğu bir port hakkında oluşabilecek durumlar hakkında kullanıcıyı bilgilendirmekte. Manuel olarak yapılan bazı işlemler program tarafından yapılmaktadır.



Ayrıca güvenlik duvarının testi içerisinde güvenlik duvarı tercihinde dikkat edilmesi gereken hususlara da yer verilmişti.

Bunlar;

- Desteklediği Platformlar
- Update mekanizması
- Kontrol mekanizması
- WEB site tracking
- Security Policy
- Virus Scanning
- Database erişimi
- Network Address Translation (NAT)
- Encryption
- GUI tabanlı yönetim
- Uyarı mekanizması

gibi. Güvenlik duvarı tercihinde test yönteminin önemi de büyüktür.

Geliştirilen test yöntemi geniş bir uygulama alanına sahip olması avantajdır. Kullanıcı test programı sayesinde kendisinden kaynaklanan hataları da görebilmeli ve mevcut sistemi daha iyi analiz edebilmesine yardımcı olmalıdır. Bu konuda kullanıcıya en çok yardımcı olacak olan KURT Test Yöntemi içerisinde ki port tarama programıdır. Çünkü saldırılar açık portlar üzerinden gelmekte ve bu portların kontrol edilip gereksiz portların kapatılması gereklidir. Sistem içerisinde ki her bir sunucunun işlevine göre port açılmalı ve sadece port bazında güvenliğinde yeterli olmayacağının da bilinmesi gereklidir. İşletim sisteminin de bazı açıkları (backdoor) bulunabilir ve bunların kapatılması için sürekli sistemin güncelleştirilmesi ve güvenlik yamalarının yapılması gereklidir.

KAYNAKLAR



- [1] Indrek Peri, "Firewalls-Security in Distributed Systems" Helsinki, 14 November 2000
- [2] H.Joseph Wen and Jhy-Horng Micheal Tarn, "Internet Security:a case of firewall selection" ,Information Management & Computer Security, 6/4 [1998] 178/184
- [3] Dennis Steinauer, Stuart Katzke and ShirleyRadack, "Basic Intrusion Protection The First Line of Defense", IT Pro, January | February 1999
- [4] Khalid Al- Tawil and Ibrahim A.Al-Kaltham, "Evaluation and Testing of Internet Firewalls", International Journal of Network Management, 1999, 9, pp:135-149.
- [5] Cheswick / Bellovin, "Firewalls and Internet Security", Addison-Wesley, 1994
- [6] Farmer D, Venema W. Satan frequently asked questions (faq),
<http://wzv.win.tue.nl/satan/demo/docs/FAQ.html>, April 10 1995.
- [7] Firewall Mailing List Archieves- <http://www.netsys.com/firewalls/>
- [8] Testing Methodologies <http://www.netsys.com/firewalls/firewalls-9508/0066.html>)
- [9] Reto E.Haeni, "Firewall Penetration Testing", January 1997
- [10] Chris Brenton, " Mastering Network Security", SYBEX Inc. 1999
- [11] Computer Emergency Response Team.IP Spoofing Attacks and Hijacted Terminal Connections. CA-95:01, January 1995
- [12] D. Farmer and W. Venema. SATAN Documentation, Apr. 1995
- [13] C. Claus. Internet Security Scanner. <http://www.iss.net>
- [14] G.Vigna A. Topological Characterization of TCP / IP Security. Technical Report TR-96,156, Politecnico di Milano, November 1996. (Test)
- [15] B. Chapman and Z. E.Zwicky. Building Internet Firewalls. O'Reilly & Associates, 1995.