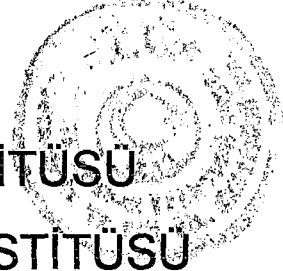


T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ



BİLGİSAYAR AĞLARINDA FİREWALL İLE GÜVENLİK

Mustafa UZUN
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

84115

TEZ DANIŞMANI
Yrd. Doç. Dr. E. Murat ESİN

T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

GEBZE

1999

Bu tez çalışması, G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 27.08.1999 tarih ve 99/125 sayılı kararıyla oluşturulan jüri tarafından ...~~Biyoloji~~...~~Mühendisliği~~... Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRI

ÜYE
(Tez Danışmanı)

: Yrd. Doç. Dr. E. Murat Esin

Muratt'ın

ÜYE

: Yrd. Doç. Dr. İbrahim Söğütçü



ÜYE

: Yrd. Doç. Dr. Gökhan Özer

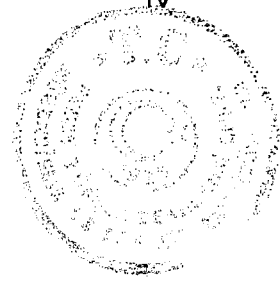


ONAY

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 27.09.1999 tarih ve 99/126 sayılı kararı.

İmza / Mühür





ÖZET

Bu tez çalışmasında yerel ve geniş bilgisayar ağlarında firewall tekniği ile güvenliğinin sağlanmasına çalışılmıştır.

Öncelikle ağ güvenliği için gerekli kavramlar ve tanımlar gibi tanıtım bilgileri verilmiştir. Yine ağ güvenliği için firewall bileşenleri açıklanmış ve basit bir firewall tasarımı gerçekleştirilmiştir.

Özel şirketin bilgi teknolojisi alt yapısı tanıtılarak güvenlik problemleri tespit edilmiştir. Bu problemleri gidermek için gerçek dünyadan bir firewall ürünü olarak Check Point Technologies firmasının FireWall-1 ürünü seçilmiştir. Ayrıca FireWall-1 seçilme kriterleri üzerinde durulmuştur. Bu yazılımın tanıtımı ve özelliklerinden bahsedilerek mevcut ağlara kurulumu üzerinde durulmuştur.

Tespit edilen güvenlik problemleri için örnek güvenlik politikaları belirlenmiş ve bu politikalar için gerekli ayarlamalar yapılmıştır.



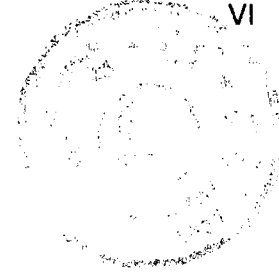
SUMMARY

In this study, it was tried to provide security in the internal and external network by firewall technique.

First of all, it was given information about the needed concepts and definitions for network security. Firewall components were explained and a simple firewall was designed.

The commercial firm was introduced and its security problems established. To avoid the security problems of this firm, a firewall product was chosen from the real world called Check Point Technologies FireWall-1 and then was given information about the criterion of this product. Then the product was introduced and talked about its features. It was told about implementation of the software to the current networks.

The sample security policies were determined for the security problems that were determined and the required configuration was made for these policies.



TEŞEKKÜR

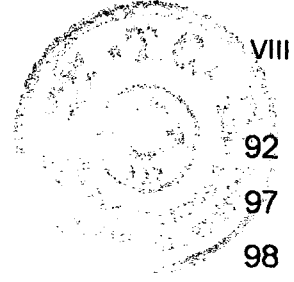
Bu tezi hazırlarken bana gerekli ilgi, alaka, kolaylık ve esnekliği tanıyan, yardımlarını hep yanımda gördüğüm, kıymetli danışman hocam Yrd. Doç. Dr. E. Murat ESİN'e, bu tezi seçmemde beni bilgilendiren ve yönlendiren değerli hocam Yrd. Doç. Dr. İbrahim SOĞUKPINAR'a, bana gerekli ilgiyi gösteren, kendisinden çok istifade ettiğim Prof. Dr. Oğuz MANAS'a, çalışmalarım sırasında tecrübelerinden yararlandığım arkadaşlarıma, bana sağladıkları samimi ortamdan dolayı Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü ve asistanlarına, tez için bana gerekli uygulama ve doküman desteğini sağlayan işyerime, tüm çalışma arkadaşlarıma, manevi desteğini hep yanımda gördüğüm nışanlım Servet YAKAR'a ve emeği geçen herkese teşekkürlerimi borç bilirim.



İÇİNDEKİLER DİZİNİ



	Sayfa
ÖZET	IV
SUMMARY	V
TEŞEKKÜR	VI
İÇİNDEKİLER	VII
SİMGELER VE KISALTMALAR	X
ŞEKİLLER DİZİNİ	XIII
ÇİZELGELER DİZİNİ	XVI
1 GİRİŞ	1
2 TEMEL KAVRAMLAR VE TANIMLAR	2
2.1. Giriş	2
2.2. İnternet Kavramı	2
2.3. İnternet Kavramı	16
2.4. Güvenlik Kavramı	20
3 AĞ GÜVENLİĞİ	30
3.1. Giriş	30
3.2. Neden İnternet Güvenlik Duvarları?	30
3.3. Ne Korunmaya Çalışılıyor?	31
3.4. Neye veya Kime Karşı Korunmaya Çalışılıyor?	35
3.5. Nasıl Korunabilir?	49
3.6. Güvenlik Stratejileri	57
3.7. İnternet Servisleri	64
4 GÜVENLİK DUVARI GELİŞTİRME	83
4.1. Giriş	83
4.2. Güvenlik Duvarı Tasarımı	83
4.2.1. Bazı Güvenlik Duvarı Tanımları	83
4.2.2. Güvenlik Duvarı Nasıl Çalışır	84
4.2.3. Ağ Adresi Çevirimi	87
4.2.4. Güvenlik Duvarı Mimarileri	87

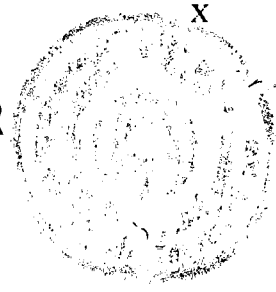


4.2.5. Değişik Güvenlik Duvarı Mimarileri	92
4.3. Savunma(Bastion) Hostu	97
4.3.1. Savunma Hostları Nasıl Çalışır	98
4.3.2. Genel Prensipler	100
4.3.3. Savunma Hostlarının Özel Çeşitleri	100
4.3.4. Savunma Hostu Tarafından Sağlanan Servisler	101
4.3.5. Savunma Hostu Geliştirme	102
4.4. Paket Filtreleme (Packet Filtering)	103
4.4.1. Neden Paket Filtreleme	103
4.4.2. Paketlerin Yapısı	104
4.5. Proxy Sistemleri	107
4.5.1. Proxy Sunucuları Nasıl Çalışır	110
4.5.2. Neden Proxy Sunucuları	111
4.5.3. Proxy Sunucu Terminolojisi	112
4.6. İki Örnek Güvenlik Duvarı Tasarımı	111
4.7. Ticari Bir Şirket İçin Güvenlik Duvarı Mimarisi	118
Tasarımı	
5 TİCARİ UYGULAMA	123
5.1. Giriş	123
5.2. Ürün İnceleme	123
5.2.1. Ürün Değerlendirme Kriteri	123
5.2.2. Güvenlik Duvarı Alırken	125
5.2.3. Ticari Güvenlik Duvarı Ürünleri	125
5.3. Ticari Şirket Tanıtımı	130
5.4. Ticari Ürün İnceleme(Check Point FireWall-1)	133
5.5. Check Point Firewall-1 Özellikleri	134
5.5.1. FireWall-1 Yöneticileri	135
5.6. Güvenlik Politikalarını Ayarlamak	139
5.7. Erişim Kontrolü(Access Control)	142
5.8. Kimlik Onaylama(Authentication)	147
5.9. Şifreleme(Encryption)	150

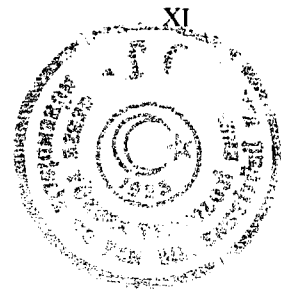
5.10. Adres Çevirme(Address Translation)	155
5.11. İçerik Güvenliği(Content Security)	158
5.12. Bağlantı Kontrolü (Connection Control)	161
5.13. Yaygın Yönetim(Enterprise Management)	163
SONUÇ	167
KAYNAKLAR DİZİNİ	169
ÖZGEÇMİŞ	170
EKLER	
EK 1. Güvenlik Duvarı Ürünleri	
EK 2. Güvenlikle İlgili Bazı Kaynaklar	



SİMGELER VE KISALTMALAR



AFS	Andrew File System
ARP	Address Resolution Protocol
ATM	Asencronous Transfer Mode
BIND	Berkeley Internet Name Domain
BISDN	Broadcasd ISDN
BSD	Berkeley Software Distribution
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CMIP	Common Management Information Protocol
COPS	Computer Oracle and Password System
CSRC	Computer Security Resource Clearinghouse
DCC	Direct Client Connections
DDN	Defense Data Network
DMZ	Demilitarized Zone
DNS	Domain Name Service
FAQ	Frequently Asked Questions
FDDI	Fiber Distributed Data Interface
FSP	File Service Protocol
FTP	File Transfer Protocol
GPS	Global Positioning System
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IAB	Internet Architecmture Board
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISP	Internet Service Provider
ISS	Internet Security Scanner

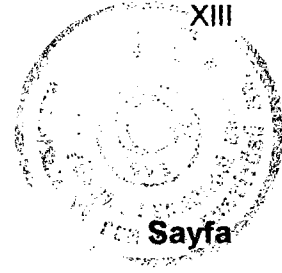


interNIC	Internet's Network Information Center
KPOP	Kerberos-supporting Post Office Protocol
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MBONE	Multicast Backbone
MIME	Multimedia Internet Mail Extensions
MTU	Maximum Transmission Unit
NAR	Network Address Rotation
NAT	Network Address Translation
NFS	Network File System
NIC	Network Information Center
NJE	Network Job Entry
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCMCIA	Personal Computer Memory Card International Association
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PROFS	Professional Office System
RFC	Request for Comment
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SAGE	System Administrators Guild
SATAN	Security Analysis Tool for Auditing Networks
SGML	Standard Generalized Markup Language
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNADS	SNA Distributed Systems
SNMP	Simple Network Management Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locators
VPN	Virtual Private Network
WAIS	Wide Area Information Service
WAN	Wide Area Network
WWW	World Wide Web



ŞEKİLLER DİZİNİ



Şekil

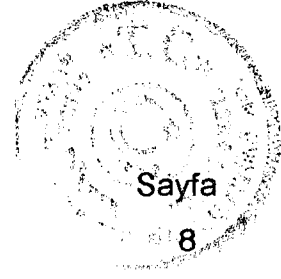
2.1. Firewall Ve Dahili Ağ	21
4.1. Çift Arayüzlü Sistem Mimarisi	88
4.2. Perdelenmiş Sistem Mimarisi	89
4.3. Perdelenmiş Alt-Ağ Mimarisi	90
4.4. İki Savunma Hostu Mimarisi	93
4.5. İç Ve Dış Yönlendiriciyi Birleştirme	94
4.6. Savunma Hostu Ve Dış Yönlendiriciyi Birleştirme	95
4.7. Çoklu Çevre Ağı(Çoklu Güvenlik Duvarı)	96
4.8. Savunma Hostu Tarafından Sağlanan Servisler	101
4.9. Veri Paketlenmesi	105
4.10. IP Başlık Ve Gövdesi	106
4.11. Vekil(Proxy) Sistemi	109
4.12. Perdelenmiş Alt-Ağ Mimarisi	114
4.13. Perdelenmiş Sistem Mimarisi	116
4.14. Ticari Bir Şirketin Güvenlik Ağ Mimarisi	119
5.1. Ticari Bir Şirketin Yapısı	132
5.2. İnternet Dünyası	133
5.3. Check Point Firewall-1 Pazar Payı	134
5.4. Check Point Firewall-1 Ödülleri	134
5.5. Check Point Firewall-1 Yöneticileri	135
5.6. Ağ Nesneleri Yöneticisi	135
5.7. Kullanıcı Yöneticisi	136
5.8. Servis Yöneticisi	136
5.9. Kaynak Yöneticisi	137
5.10. Zaman Yöneticisi	138
5.11. Sunucu Yöneticisi	138
5.12. Anahtar Yöneticisi	139
5.13. Güvenlik Politika Kriterleri	140
5.14. Güvenlik Politika Kriterleri_Servis Engelleme	140
5.15. Güvenlik Politika Hareketi Belirleme	141

5.16. Kayıt Defteri Ve İzleme Belirleme	142
5.17. Yeni Kural Tanımlama	143
5.18. Kaynak Yöneticisine Yeni Nesne Ekleme	144
5.19. Kaynak Yöneticisine Yerel_Ağ Ekleme	144
5.20. Hedef Belirleme	144
5.21. Servis Belirleme	145
5.22. Hareket Tarzı Olarak İşlemi Kabul Etme	145
5.23. Kayıt Defteri Tutulması	145
5.24. Tanımlanmış Kural	146
5.25. HTTP Kuralının Tanımlanması	146
5.26. Firewall Trafiğine Alarm Durumu Tanımlama	146
5.27. Kimlik Onaylama	147
5.28. Kimlik Onaylama İşlemi Başarılı	148
5.29. Kimlik Onaylama Eklenmiş Güvenlik Politikası	148
5.30. Sqlnet2'yi Kullanarak SQL Sunucuya Erişime İzin Veme	149
5.31. Kimlik Onaylama Metotları	149
5.32. Kimlik Onaylama Güvenlik Metotları	150
5.33. Şifreleme	151
5.34. Uzaktan Erişimlerde Koruma İçin Şifreleme	152
5.35. Hareket Olarak Şifreleme Seçilmesi	152
5.36. Sadece Şifreleme Gerektiren Servis Tanımları	153
5.37. Firewall-1 Şifreleme Teknikleri	153
5.38. Firewall-1 Certificate Authority Anahtar Yönetimi	154
5.39. Kimlik Onaylamayı Şifrelemeye Çevirme	154
5.40. Uzaktan Erişim İçin Şifrelemenin Tamamlanmış Hali	155
5.41. Ağa Yeni Kayıtlı Olmayan İstasyonların Eklenmesi	156
5.42. IP Adreslerinin Dönüştürülmesi	156
5.43. Adres Çevirme	156
5.44. Adress Dönüştürme Metodu	157
5.45. Adres Çevirmede IP Adresi Seçilmesi	157
5.46. Firewall-1 Adres Çevirme Kuralını Üretmesi	158
5.47. İçerik Güvenliği Olmaması Durumu	158
5.48. Firewall-1 İçerik Güvenliği Denetimi	159

5.49. İçerik Güvenliğinin Denetimden Geçmesi	159
5.50. İçerik Güvenliğinin Firewall-1 De Tanımı	160
5.51. İçerik Güvenliği İçin Harici Anti-Virüs Programı Seçimi	160
5.52. Tüm İstekleri Dengesiz Yükleme	161
5.53. Firewall-1'in Gelen İstekleri Dengeli Yüklemesi	162
5.54. Firewall-1'in Yük Dengeleme Algoritmaları	162
5.55. Firewall-1'in Yük Dengeleme İçin Hedefinin Değiştirilmesi	163
5.56. Firewall-1 Yönetim Seti	164
5.57. Firewall-1 Kural Editörü	164
5.58. Firewall-1 Kayıt Göstericisi	164
5.59. Firewall-1 Kayıt Defteri	165
5.60. Firewall-1 Gerçek Zamanlı Kayıt Defteri Kontrolü	165
5.61. Firewall-1 Gerçek Zamanlı Kayıt Defteri Göstericisi	166
5.62. Firewall-1 Sistem Durum Göstericisi	166



ÇİZELGELER DİZİNİ



Çizelge

2.1. İnternet Adreslerindeki Uluslararası Kısaltmalar	8
2.2. Bazı Ülke Kısaltmaları	9
2.3. Örnek Domain Adresleri	9
2.4. Yeni Domain Adresleri	9
3.1. Güvenlik Dereceleri Belirleme	56
3.2. Güvenlik İçin Gerekli İşlemler	57
4.1. Filtrelenecek Bazı Servis Ve Port Numaraları	107
5.1. Bilgisayarların Özellikleri Ve Kullanım Amaçları	131
5.2. Ağ Elemanlarının Özellikleri Ve Kullanım Amaçları	131



1 GİRİŞ

Bilgisayar ağı ve özellikle internet, kullanıcılara büyük olanaklar verirken ciddi güvenlik sorunlarını da beraberinde getirmiştir. Ağa bağlı bilgisayarlarda çalışanların bu güvenlik sorunları konusunda bilgili olmaları zorunlu hale gelmiştir. Ancak güvenlik ile kullanım kolaylığının çoğu zaman birbirleriyle çelişmesi ve kullanıcıların seçimlerini genellikle kullanım kolaylığından yana kullanmaları güvenlik önlemlerinin yerleşmesini engellemiştir.

İnternet dünyasında en önemli konu şüphesiz güvenlidir, özellikle ağların internete bağlanması ile güvenlik, uygulanması gereken zorunlu bir kural haline almaktadır, mevcut verilerin çalınması, web sayfalarının değiştirilmesi, internet üzerinde bir noktadan diğerine giden bir bilginin alınarak okunması ve daha bir çok problem güvenlik konusunun ne kadar ciddi olduğunu göstermektedir.

2 TEMEL KAVRAMLAR VE TANIMLAR

2.1. Giriş

Bilgisayar ağlarında güvenlik kavramının iyi anlaşılması için bir bilgisayar ağının temellerini oluşturan kavramların bilinmesi gerekir. Global bilgi sistemlerine, gelişen teknolojilere uzak kalmamak için bilgisayar ağları genelde dış dünyaya açılır. En azından kendi içinde bile olsa dış dünya standartlarının kullanıldığı sistemler üzerinden iletişim kurmak zorundadır. Bu durumda da bu ağ için güvenlik kavramı ortaya çıkar. Sonuçta hiç kimsenin bilmediği bir sistemi kullanmak, o sistemi bir nevi bilinmeyen bir güvenlik altında tutar. Bu konuda bir bilgisayar ağının dış dünyaya açılması halinde etkileşim içinde olacağı temel kavramlar üzerinde durulacaktır.

2.2. İnternet Kavramı

İnternet, birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır.

İnternet, insanların her geçen gün gittikçe artan, üretilen bilgiyi saklama/paylaşma ve ona kolayca ulaşma istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alandaki bilgilere insanlar kolay, ucuz, hızlı ve güvenli bir şekilde erişebilmektedir. İnternet bu haliyle bir bilgi denizine, ya da büyükçe bir kütüphaneye benzetilebilir. İnternete, bakış açısına bağlı olarak farklı tanımlamalar da getirilebilir:

- İnternet birçok insanın kendi arasında etkileştiği, bilgi değiş-tokuşu yapabildiği ve kendi yazısız kuralları olan büyük bir topluluktur. Bu, internetin sosyal yönüdür.
- Pek çok yararlı bilginin bir tuşa basmak kadar yakın olduğu dev bir kütüphanedir.

- Milyonlarca bilgisayarın bağılı olduğu çok büyük bir bilgisayar ve iletişim ağıdır.
- Kişilerin değişik konularda fikirlerini serbestçe söyleyebilecekleri ortamlar barındıran bir demokrasi platformudur.
- Evden alış-veriş, bankacılık hizmetleri, radyo-televizyon yayınları, günlük gazete servisleri vb gibi uygulamaları ile aslında internet aynı zamanda bir hayat kolaylaştırıcıdır. [Akgül, Mustafa, İnternet ve İntranet..., 1997]

Tüm bu tanımların arakesitinde yer alan ise bilgiye ulaşım ve onu paylaşım, sonrasında da elde edilen bilgiyi kullanımdır.

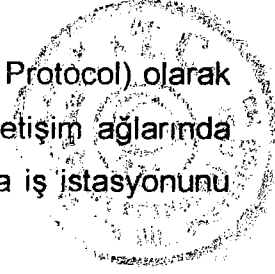
Sonuç olarak internet; önümüzdeki yıllarda üretilecek bilgilerin dolaşım sistemidir. Ticari boyutunun da ortaya çıkmasıyla yaşamla daha çok iç içe geçmeye başlamıştır.

2.2.1. TCP/IP Kavramı

Bilgi ağı üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dahilinde yapılmaktadır. Bu kurallara kısaca internet protokolleri, ya da TCP/IP protokoller ailesi denir. TCP/IP(Transmission Control Protocol/İnternet Protocol), bilgisayarlar ile veri iletilme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır. Bir başka ifadeyle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar

Bu protokollere örnek olarak, dosya alma/gönderme protokolü (FTP, File Transfer Protocol, Dosya Transfer Protokolü), Elektronik posta iletişim protokolü (SMTP Simple Mail Transfer Protocol, Basit Posta Transfer Protokolü), TELNET protokolü (internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen login protokolü) verilebilir. Adını sıkça duyduğumuz WWW(World Wide Web) ortamında birbirine link objelerin

iletilmesini saęlayan protokol ise HTTP(Hyper Text Transfer Protocol) olarak adlandırılmaktadır. TCP/IP protokolü aynı zamanda dięer iletiřim aęlarında da kullanılabilir. Özellikle pek çok farklı tipte bilgisayar veya iř istasyonunu birbirine baęlayan yerel aęlarda kullanımı yaygındır.



2.2.2. İnternet Ne Sunar?

İnterneti bir iletiřim aęı olarak tanımladıktan ve bu aę üzerinde bilgi dolařtıęını belirttikten sonra, internetin bu altyapı üzerinde neler sunduęunu tahmin etmek aslında o kadar da güç deęildir. Bu iletiřim aęının içinde bulunan her hangi iki bilgisayar arasındaki en temel iřlem çift yönlü bilgi aktarımıdır. Burada bilgiden kastedilen, bilgisayarlardan birinde bulunan bir dosya, bir bilgisayar programı ya da bir mesaj olabilir. İnternet, teknik olarak, TCP/IP protokolü ile desteklenen pek çok servis sunar. Örnek olarak, internet erişimi olan bir kullanıcı, eęer kendisine yetki verilmiřse, internete baęlı dięer herhangi bir bilgisayardaki bilgilere erişebilir, onları kendi bilgisayarına alabilir, kendi bilgisayarından da internet erişimi olan başka bir bilgisayara dosya/bilgi gönderebilir. Bu özellik, dosya transfer protokolü olarak bilinir. Benzer şekilde, internet üzerindeki kullanıcılar birbirlerine elektronik posta gönderebilirler. Bu da, posta iletim protokolü olarak bilinir. İnternet, deęişik protokoller aracılıęı ile, insanlara bilgiye erişim olanakları sunar. Yani, internet yardımıyla her çeřit bilgiye erişilebilir.

İçerik bakımından, internetin sundukları bazen insanın hayal gücünü zorlayacak boyutlara varmaktadır. Vizyondaki filmlerin kısa tanıtımları kolayca evdeki ekrana taşınabilir ya da Amerikan Kongre Kütüphanesi'nde tarama yapılabilir. Tübitak Arřivi'ne baęlanıp Bilim ve Teknik dergilerinin yeni ve eski sayıları taranabilir, yazıları okunabilir. Başka bir örnek olarak, katılmak istenilen bir bilimsel toplantıya, bildiri internet üzerinden gönderilebilir. Örnekleri arttırmak mümkündür. İnternette sunulanlar; onu kullananların istekleri, hayal güçleri ve gelişen internet teknolojisi ile hep çoęalmaktadır.

2.2.3. İnternet Yoluyla Erişilebilen Bilgiler, Programlar

İnternet ile erişilebilen bazı merkezlerde herkese açık arşivler vardır. Buralarda çok çeşitli bilgiler, çok çeşitli programlar bulunur. Bu bilgiler bir konferansın kayıt formu olabileceği gibi, piyasadaki bir ürünün tanıtım kılavuzu da olabilir. Bilgi amaçlı dosyalar, daha çok düz yazı düzenindedir ve grafik, ses, animasyon vb. ile içeriği zenginleştirilmiş olabilir. Bunlar daha çok, bir ürünün tanıtımı, kullanımla ilgili sorunları çözmede kullanıcıya yol gösterecek bazı destek bilgileri gibi bilgilerdir. Ayrıca, web tabanlı ortamlarda, firma reklamları ve ürün tanıtıcı reklamlara da rastlanılmaktadır. Bu tip arşivlerde en çok karşılaşılan dosyalar; çok değişik amaçlar ve değişik bilgisayar ortamları (PC, Mac, Unix vb) için geliştirilmiş binlerce çeşit ve yüzlerce giga byte yer tutan bilgisayar programlarıdır.

2.2.3.1. Halka Açık(Public Domain) Yazılımlar

Bu programları yazan kişiler, kendi programlarını herkesin alıp bedava kullanmasına izin verirler. Ancak, bazı durumlarda bu bedava kullanım kısıtlandırılır. Public Domain yazılımlarda aşağıdaki hususlar göz önüne alınmalıdır:

- Tamamı değiştirilmeden üçüncü kişilere kopyalanmalı,
- Eğer söz konusu eser bir başka yerde kullanılacaksa (örneğin bir başka eserde bundan yararlanılacaksa) yazarlarına bildirilmeli,
- Herhangi bir şekilde eserin dağıtımından dağıtım medyası masrafından fazla masraf alınmamalı (BBS'ler için).

2.2.3.2. Bedava(Freeware) Yazılımlar

Freeware yazılımlar limitsiz bir şekilde bunları alan kişiler tarafından kullanılabilir. Bu yazılımlar, parayla üçüncü şahıslara satılmamalıdır.

2.2.3.3. Sınırlı(Shareware) Yazılımlar

Shareware yazılımlarda ise, kullan, eğer beğenirsen bana belli bir miktar para gönder felsefesi geçerlidir. Bu miktar genellikle 10-30 ABD doları mertebesindedir. Shareware yazılımlar kaynak kodları ile birlikte dağıtılabılırler. Programı alan kişi, belirli bir süre (1 ay gibi) kullanır, eğer kullanmaya devam ederse bu parayı gönderir. Ancak, burada zorlayıcı bir mekanizma yoktur. Bazı durumlarda, kullanılan shareware program, süresi dolunca çalışmaz. Çoğunluk böyle programlara para ödememektedir. Ancak, shareware felsefesi her geçen gün daha fazla yerleşmektedir.

2.2.3.4. Tanıtım/Deneme(Tryware) Yazılımlar

Bazı ticari şirketlerin, yeni geliştirdikleri yazılımların sınırlanmış sürümleridir ve tanıtım amacıyla konurlar.

2.2.3.5. Postcardware Yazılımlar

Postcardware yazılımlar aynen freeware yazılımlar gibidirler. Bu yazılımları geliştirenlerin kullanıcılardan tek beklentisi ödeme olarak güzel bir kartpostalıdır.

2.2.3.6. Yama(Patch) Yazılımlar

Mevcut bir yazılımın (ticari ya da halka açık) bazı hatalarını düzeltmek, ve programı güncellemek amacıyla, ilgili firmaların (ya da kişilerin) çıkardıkları yama programlardır. Bu tip programlar, internet üzerinde sıkça dağıtılır.

2.2.4. İnternet Adresleri

İnternete bağlı her bilgisayarın kendine özgü bir adresi vardır. DNS (Domain Name System, Alan İsim Sistemi) olarak adlandırılan hiyerarşik bir isimlendirme internet adresi sistemi ile, internete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilir. DNS de bir TCP/IP servis protokolüdür. DNS, host olarak adlandırılan, internete bağlı tüm birimlerin yerel olarak bir ağaç yapısı içinde gruplandırılmasını sağlar. Bu şekilde, bütün adreslerin her yerde tanımlı olmasına gerek kalmaz. Örnek olarak, itu.edu.tr altında, ehb.itu.edu.tr vb. seklinde dallanmış bir çok adres olabilir.

2.2.5. İnternet Üzerinde İstenilen Bilgilerin Yerlerine Ulaşması

İnternete bağlı her ağ şu veya bu şekilde kendisine bağlantı sağlayan bir servis sunucusuna veya kuruma bağlıdır. Bu birleşme yerlerinde birden çok bağlantısı bulunan yönlendiriciler(router) bulunur. Bu düğüm noktalarında düğümün belirli kollarında hangi ağların bulunduğu dair bilgiler (ya routerlar arası haberleşme protokollerinden ya da sabit tanımlamalardan) yer alır. Bu tanımlara ek olarak bir de varsayılan(default) route tanımı bulunur, düğümde tanımlı bulunmayan adresler oraya yönlendirilir.

Tüm haberleşme bilgi paketleri şeklinde gerçekleşir. Her paketin başında nereden gönderildiği (IP adresi) ve nereye gönderildiği yer alır. Paketin içeriği kullanılan haberleşmeye göre büyük farklılıklar gösterir.

Bu yapı çerçevesinde, bilgiyi isteyen(istemci) ve bilgiyi gönderen (sunucu) olarak iki ana noktadan bahsedebiliriz. İstemci bilgisayar, bu isteğini protokollerde belirtilen bazı kurallar dahilinde istediği bilginin olduğu sunucu bilgisayara bildirir. Bu iki bilgisayar arasında bilginin geçtiği/yönlendirildiği başka bilgisayarlar da vardır.

2.2.6. İnternet Adreslerinde Görülen Kısaltmalar

İnternete bağlı kuruluşlar değişik gruplara ayrılabilir ve bir kuruluşun domain adresi, o kuruluş hangi gruba dahilse ilgili kısaltmayı bazı istisnalar dışında mutlaka içerir. Ayrıca, ülkelerin iki harfli tanıtım kodları da (Amerika Birleşik Devletleri ve Kanada çıkışlı adreslerin çoğu ve geniş bir kitleye servis sunan bazı birimler dışında) adresin sonuna eklenir. İnternet adresi, eğer özel amaçlı bir servise (ftp, gopher, www gibi) aitse, genellikle, bu durum, adresin başında kullanılan bir kısaltmayla verilir. Adreslerde kullanılan bazı kısaltmalar ve ne anlama geldikleri Çizelge 2.1.'de görülmektedir.

gov	Hükümet kuruluşları
Edu	Eğitim kurumları (üniversiteler gibi)
org	Ticari olmayan, kar amacı gütmeyen kuruluşlar
com	Ticari kuruluşlar
mil	Askeri kuruluşlar
net	Servis Sunucuları (İnternet Servis Sağlayıcıları gibi)
ac	Akademik kuruluşlar (bazı ülkelerde edu yerine kullanılmaktadır)
int	Uluslararası organizasyonlar, kuruluşlar
ftp	FTP Arşiv Sitesi (ön ek)
www	World Wide Web Sitesi (bazen web de kullanılır) -ön ek-

Çizelge 2.1. İnternet adreslerindeki uluslararası kısaltmalar

Ülkeler için de aynı yöntemle bazı kısaltmalar mevcuttur. (Çizelge 2.2)

tr	Türkiye	jp	Japonya	uk	İngiltere
ch	İsviçre	ca	Kanada	ru	Rusya
nl	Hollanda	de	Almanya	br	Brezilya
fr	Fransa	il	İsrail	no	Norveç
it	İtalya	id	Endonezya	bg	Bulgaristan
se	İsveç	hr	Hırvatistan	yu	Yugoslavya
fi	Finlandiya	gr	Yunanistan		

Çizelge 2.2. Bazı ülke kısaltmaları

Örnek domain adreslerinden bazıları ise aşağıda gösterilmiştir.

Hokudai.ac.jp (jp=Japonya)	Bilkent.edu.tr (tr=Türkiye)
Oak.oakland.edu	Servis.net.tr
<u>Www.microsoft.com</u>	<u>ftp.netscape.com</u>
<u>Tubitak.gov.tr</u>	Garbo.uwasa.fi (fi=Finlandiya),

Çizelge 2.3. Örnek domain adresleri

Genel olarak bu sınıflamaya uyulsa da, bazı domain adlarında daha farklı sözcük grupları da olabilir. (rl.ac.uk (uk=İngiltere), www2.itu.edu.tr gibi).

arts	Sanat ve kültür ile ilgili siteler
firm	Ticari Firmalar
info	Bilgi servisi sunan siteler
nom	Kişisel domainler için kullanılan adresler
rec	Eğlence siteleri
stor	Alışveriş merkezleri, ticari ürün satılan yerler
web	WWW ile ilgili servis sunan siteler

Çizelge 2.4. Yeni domain adresleri

2.2.7. İnternette Bilgi Hızları ve Band Genişliği

Band genişliği, bir iletişim ortamının taşıyabileceği bilgi miktarını gösteren bir ölçüdür. Söz gelişi, ses iletimi için band genişliği, iletebilen en yüksek ve en düşük frekanslar arasındaki farktır (Hertz). Bilgisayarlar arası haberleşme için de benzer şekilde, band genişliği, saniyede iletilen bit sayısı ile verilir.

İnternetteki bilgi iletim hızları çeşitlilik gösterir. Bilgisayarları ve değişik ağları birbirine bağlayan hatlar, kablo (çoğunlukla fiber optik), uydu ya da radyo link (yakın birimler için) bağlantılı olabilir. İnternette hat hızı, saniyede iletilen "bit" sayısı ile (bps, bit/san) ölçülür. Söz gelişi, 64 kilobit/saniye hızındaki bir hat saniyede 64kbit=65536 bit iletebilir. Bu da, ideal şartlarda, yaklaşık 8 kilobyte/saniye hızına denk gelmektedir. Söz gelimi, böyle bir hat ile, tam kapasite kullanımında, 1 Megabyte'lık bir dosya yaklaşık 2 dakikada iletilecektir. Bir birimin, bağlantılarında kullanabileceği en fazla hıza Band Genişliği denir. 64kbit/saniye bant genişliği olan bir hattı aynı anda 10 birime kullanılırsa, buna göre hız, en fazla hızın ortalama %10'una kadar düşer.

Günümüzde bağlantı hızları 9.6kbit/saniyelerden (modem bağlantısı) Gigabit/saniyelere kadar geniş bir aralıkta değişmektedir. Yurt dışındaki bağlantılarda, tipik hızlar, yaklaşık 5-10 Megabit/saniyeler mertebesinde iken, bu oran ülkemiz için, 64Kbit/san-2Mbit/saniyeler mertebesinde dir.

Bir hattın bant genişliğinin ne kadarının kullanıldığı, o hattın doluluk oranını verir. Eğer 64kbit/san.'lık bir hat, 1 saat boyunca, %100 çalışırsa; $3600 \times 64\text{kbit}$ 'lik veri aktarımı yapması gerekir. Gerçekte ne kadar veri aktardığını bulup bu iki sayıyı birbirine oranlanırsa, hattın, o saat için doluluk oranını bulunmuş olur. Bunu 1 ay boyunca yapılsa, hattın 1 ay boyunca ortalama % kaç doluluk oranı ile çalıştığı tespit edilebilir. Doluluk oranı ne kadar fazlaysa, o hattı kullananların veri aktarımları da o kadar yavaşlar.

2.2.8. ISDN

ISDN (Integrated Services Digital Network, Birleştirilmiş Servisler Sayısal Ağı), özellikle normal telefon hatları (ve diğer bazı ortamlar) üzerinden daha yüksek hızlı entegre ses (analog) ve veri (dijital) aktarılmasını sağlayan bir dizi iletişim protokolüne verilen addır. ISDN'de, her iki uçta da, modemin dışında, bazı özel adaptörler kullanmak gerekir. Bu şekilde, 64Kbps ve 128Kbps gibi hızlara (normal hatlar üzerinden) çıkmak mümkün olmaktadır.

ISDN'de iki temel seviye hızı vardır :

1. Basic Rate
2. Primary Rate.

Her iki seviyede de, iki farklı tip kanal bulunur : B (bearer) kanalları (sayıları birden çok olabilir) ve D (delta) kanalı (1 tane). B kanalları, her türlü ses, veri vb. taşırlar. D kanalı ise iletişimde kullanılacak kontrol ve yönlendirme bilgilerini taşır. Basic Rate seviyesi daha çok evden kişisel kullanımlar ve küçük şirketlerin kullanımları için tasarlanmıştır ve iki tane 64Kbps B kanalı ile 1 tane 16Kbps D kanalı içerir. Ulaşılabilecek en yüksek hız 128Kbps olmaktadır. Primary Rate seviyesi ise, daha yoğun kullanımlar için tasarlanmıştır ve 23 tane 64Kbps B kanalı (Avrupa için 30 tane) ve 1 tane 64Kbps D kanalı içerir. Ulaşılabilecek en yüksek hız ise yaklaşık 7Mbps'e kadar çıkar.

Yeni geliştirilen B-ISDN (Broadband ISDN) teknolojisi ise, Frame Relay'a bir alternatif olarak düşünülebilir. ISDN kullanımı (özellikle evden kişisel bağlantılarda) önümüzdeki yıllarda çok daha fazla yaygınlaşacağı eğilimindedir.

2.2.9. Frame Relay

Frame Relay, verilerin yüksek hızlarda dijital ağlar üzerinden iletilmesini sağlayan bir teknolojidir. Veriler, frame olarak adlandırılan paketler halinde iletilir. Frame Relay, veri aktarımı süresince, kesintisiz ve sadece o verinin iletileceği (dedicated) bağlantılar üzerinden yapılır. Frame Relay'de, iletilen paketler için iletim sırasında herhangi bir anda hata kontrolü yapılmaz. Verinin iletileceği nokta hata kontrolünden sorumludur.

2.2.10. ATM

ATM (Asynchronous Transfer Mode, Asenkron Transfer Modu), bir paket anahtarlama teknolojisidir. ATM, verileri byte büyüklüğünde hücrelere (cell) ayırır ve aynı anda 53 hücrelik paketler halinde iletir. ATM, daha çok donanım tabanlıdır ve yüksek veri işleme/iletme hızları elde edilebilir. En çok kullanılan standart hızlar, 155 Mbps ve 622Mbps'dir. 10Gbps hızlara kadar da çıkmıştır. (1996 sonu itibarıyla). ATM, BISDN protokolünün de en temel elemanıdır.

2.2.11. İnternet Dışında Yaygın Kullanılan Ağlar

Bunlardan en yaygın kullanılanları UUCP(Unix-to-Unix Copy) ve BITNET(Because It's Time Network)'tir. Bunların dışında da firma temelli Decnet, Ibmnet gibi, görev temelli, yerel vb. pek çok ağ vardır.

UUCP ağı, UUCP protokolü ile haberleşen sistemleri bünyesinde bulundurulur. Bu protokolde, iki sistem belirli aralıklarla (polling) birbirlerine bağlanır ve bu iki sistemden herhangi biri üzerinde birtakım planlı programlar çalıştırılır (mail aktarımı, dosya aktarımı, kısaca bir sistemden diğerine kopyalama).

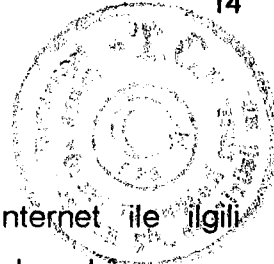
BITNET ise, birbirlerine NJE protokolü ile bağı sistemlerden oluşur. BITNET esas olarak ağaç(tree) şeklinde bir yapıya sahiptir. Statik bir yönlendirme vardır. Mail, sınırlı şekilde FTP ve Telnet (VTAM) desteği vardır. Mail, bir depola ve ilet mantığı ile bir düğümden komşusuna gider, oradan bir öteye gider. Hatlar kesildiği zaman, ya da makine yüklü olduğu zaman yolda bir yerde bekler. İnternet ile diğer ağlar arasındaki ileti trafiği için geçiş görevi yapan merkezlere internet gateway denir.

2.2.12. Elektronik Para (E-Para, E-Cash, Sanal Para)

E-para, tam olarak, kullanılan bilgisayarın sabit diskinde kişi adına bulunan ve internet üzerinde yapılan alışverişlerde harcanabilen paradır. Harcama yaptıkça, harcanan miktar toplamdan düşölür. E-para kullanımı pek yaygın değildir. Ancak, gelecekte sık kullanılacak bir araç olabilir.

Temel olarak, gidip, e-para servisi veren bir bankadan, kredi kartıyla ya da peşin ödemeye, bir miktar e-para alınır. Daha sonra, banka bu miktarı kişinin bilgisayarına transfer eder. İnternet üzerinden bir alışveriş yapıldığında da, eğer burada e-para geçiyorsa, sipariş formunda e-para ile ödeme yapılacağı belirtilir. Miktar otomatik olarak bilgisayardaki miktardan düşölür. Bütün bu işlemler, e-para servisi veren bankadan da kontrol edilir. Bazı uygulamalarda, e-para ödemesi doğrudan bankadan yapılır. Bu durumda, kişiye bir e-posta mesajı ile ilgili siparişi alıp almayacağı sorulur. Böylece, alışverişlerde, fiziksel olarak alışagelen para dolaşımı ortadan kalkar.

E-para sistemine birkaç örnek; Digital Cash (<http://www.digicash.com>), Cyber Cash (<http://www.cybercash.com>) ve First Virtual (<http://www.fv.com>). İlgili yerlere bağlanıp daha ayrıntılı bilgiler alınabilir.



2.2.13. İnternet Grubu(Internet Society)

İnternet Society(IS), 1992'de kurulan ve amacı internet ile ilgili gelişimler, yeni çalışmalar için bir nevi yol göstericilik olan, kâr amacı gütmeyen(non-profit) bir kuruluştur. IS, internet ile ilgili teknik çalışmaları yönlendiren ve denetleyen İnternet Architecture Board (IAB)'un çalışmalarını destekler. IAB'nin aktivitelerinden bir diğeri de, TCP/IP konusunda çalışmalar yapan İnternet Engineering Task Force (IETF) tır. IAB'nin diğeri aktiviteleri arasında, ağ teknolojileri ile ilgili çalışmalar yapan İnternet Research Task Force; IP adreslerinin verilmesi ile ilgili çalışmalar yapan İnternet Assigned Numbers Authority; ve DNS ile ilgili konularda çalışan İnternet Registry grubu gösterilebilir. İnternet Society web adresi : <http://www.isoc.org> . Buradan ilgili bütün linklere ulaşılabilir.

2.2.14. İnternet Kullanım Etiği

Ağ üzerindeki her kullanıcının, servisleri, sistemleri kullanmaları konusundaki sorumluluklarını farketmeleri önemlidir. Kullanıcı, ağdaki her servise ulaştığında yaptığı hareketlerden sorumlu olmak zorundadır.

İnternet ya da kısaca Net, tek bir ağ değildir. Hatta bir birinde ayrı protokollere, yapılaraya sahip binlerce irili ufaklı ağların toplamıdır. İnternetteki bilgi akışı, bir çok değişik ağdan gelip geçmekte, ulaşacağı yere öylece varmaktadır. Bu yüzden, her kullanıcının, kendi bölgesindeki ağ yükünü dengede tutması gerekmektedir.

Bir ağ kullanıcısı olarak, başka bilgisayar ağlarına ulaşmaya izin verilmiş olabilir. Her ağın kendine ait sorumlulukları, kuralları ve yasakları vardır. Ağ üzerindeki izin verilmiş işlemler, bu ağdaki sorumlular tarafından her zaman izlenebilecek şekilde tasarlanmıştır. Fakat bir yerde izin verilen bir hareket, başka bir ağda yasaklanmış olabilir. Bu kuralları bilmek ve bunlara uymak, kullanıcının sorumluluğundadır. Ağın, özellikle internetin kullanımı, bir

ayrıcalıktır, bir hak değildir. Bu ayrıcalık, istenildiği zaman, kötüye kullanım ya da başka sebeplerle, elden alınabilir. Bu kötüye kullanım; bir sistemdeki gizli bilgileri hileli yollarla almak, kötü, anlaşılmaz mesajlarla diğerlerini rahatsız etmek, sistemin kaynaklarını kullanıp sistemi yavaşlatmak, ardarda mesajlar postalayarak başkalarının e-posta kutularını doldurmak, ağ üzerinde yasalarla belirlenmiş kuralların dışına çıkmak vs. olarak sayılabilir.

2.2.15. İnternetin Sosyal Boyutu

Yaygın bir görüşe göre internet, kişilerin sosyal yaşamlarında olumsuz etkilere sahiptir. Gerçek dünyadan farklı bir ortamda, sanal dünyada, insanlar arası ilişkiler değişmektedir. Çoğu durumda birbirleri ile etkileşen insanlar bir internet adresi, bir e-mail adresi vb gibi. Öte yandan internet, kişiler arasındaki mesafe, yaş, cinsiyet, ırk, kültür vb. gibi gerçek dünyada önemli olabilecek pek çok özelliği de ortadan kaldırmaktadır.

Yerinden alışveriş, yerinden bankacılık, hatta işe gitmeden evden çalışma vb. gibi kullanımlar insanın sosyal yaşamını etkileyebilecek unsurlardır.

2.2.16. İnternetin Ticari Boyutu

İnternetin 1990'ların başlarından itibaren bu kadar yaygınlaşmasının en temel nedenlerinden birisi ve belki de en önemlisi para kazandırabilecek potansiyele sahip bir imkan olmasıdır. Bu iletişim ağına bağlı bilgisayarlar yolu ile alışverişler yapılabilmekte, borsa/bankacılık işlemleri yerine getirilebilmektedir. Bu haliyle internetin ağ teknolojisi kimliğinin yanında bir de medya özelliğinden söz edilebilir. İnternet artık ciddi reklam paralarının dönmeye başladığı ve şirketlerin ürünlerini pazarladığı bir ortam haline gelmeye başlamıştır.



2.3. İnternet Kavramı

İnternet, bir şirket ya da kurumun daha iyi sonuçlar elde etmek amacıyla kendi yerel ağında klasik veri erişim ve transfer sistemi yerine internet teknolojisi kullanımına verilen isimdir. İnternet, maliyet düşürmede yardımcı olurken, günlük bilgilere kolay ve hızlı erişim imkanı sağlar.

İnternet, sadece belirli bir kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı bir ağıdır. Yani, küçük internet!, İnternetin daha özel bir hali. İnternetler gatewayler ile diğer ağlara bağlanabilir. Temel oluşturulma amaçları, kuruluş bünyesinde bilgileri ve bilgi işlem kapasitesini paylaşmaktır. İnternetler, şirket(ler) içi tele-konferans uygulamalarında ve farklı birimlerdeki kişilerin biraraya gelebildiği iş gruplarının oluşturulmasında da kullanılırlar.

İnternetler üzerinden HTTP, FTP vb gibi pek çok protokol uygulamaları çalıştırılabilir. Günümüzde, internetler içinde, web erişimi ile kaynakların kullanımı oldukça yaygındır.

Bazı şirketlerdeki internetlerden, güvenlik duvarı sistemleri üzerinden (bazı emniyet tedbirleri ile), internet çıkışı da yapılmaktadır. Bu sayede, her iki yönde de ileti trafiği kontrol edilebilmekte ve güvenlik sağlanmaktadır.

Bir internet; TCP/IP protokolünü transfer için kullanan özel bir şirket veya eğitimsel ağ olarak da tanımlanabilir. İnternet haberleşme için TCP/IP protokolünü kullanarak kurulur. IPX gibi diğer protokoller de TCP/IP ile beraber aynı ağda çalışabilir. TCP/IP protokolü pek çok donanım ve kablolu sistemlerinde çalışabilir. Bir internet oluşturmak, sistem için gerekli donanım alt yapısını çalışır hale getirmek değildir. En önemli şey yazılım kurallarının doğru olarak kurulup kullanılabilmesidir.

Intranetler diğer özel ağ teknolojileriyle beraber vardır. Çoğu şirketlerde var olan temel sistemler; Main Frame bilgisayar sistemleri, Mini bilgisayarlar, Novel Networkler, PC'ler ve çeşitli veri tabanları intranetle entegre edilebilirler. Çok sayıda aracın olması bunu mümkün kılar. CGI scriptleri intranetten temel veri tabanlarına erişim imkanını sağlarlar. Java programlama dili de intranetten veri tabanlarına erişimi gerçekleştirmek için kullanılabilir.

İnternetin gelişmesiyle beraber, şirketlerde artan sayıda kişiler bilgi toplamak veya iş yapmak amacıyla dünyanın çeşitli yerlerindeki insanlarla bağlantı kurmak için intraneti kullanmaktadır. İnsanların, interneti bu kadar ünlü yapan değer katıcı bileşenlerini tanıması uzun zaman almamaktadır. Bazı şirketlerin zamanında TCP/IP ağları yoktu ve bu protokol internete erişmek için gerekliydi. Bütün bilgi ve imkanların karışıklık oluşturmadan kullanılabilirdiği bir intranet oluşturulmasının pek çok faydaları vardır. TCP/IP tabanlı ağlar, insanların uzaktan ağa kolayca erişebilmelerini sağlarlar. Böylece bir şirket personeli evinden veya seyahat halinde iken şirketinin bilgisayar ağına bağlantı kurabilir. Bu yönüyle intranete bağlanma internete bağlanmaya benzer. İstenilen ortak internet servis sağlayıcı yerine yerel alan ağına bağlanmaktadır.

Güvenlik sistemi sayesinde intranet, internetten ayrılır. Bir şirketin intraneti güvenlik duvarı donanımlarla ve insanların özel amaçlarla internete çıkmalarını sağlayan yazılım ürünleriyle korunur.

Var olan bir ağ çeşitli yöntemlerle intranet olarak kullanılabilir. Web üzerinde bilgilerin yayınlanmasının kolaylığı, ortak bilgilerin postalanması verilebilecek popüler örneklerdendir. Ayrıca veri tabanının baştan sona kolayca oluşturulabilmesi için web ve java gibi bir programlama dili kullanılabilir.

Intranet insanların daha kolay ve daha etkili bir şekilde birlikte çalışmalarını sağlar. Groupware olarak bilinen yazılımlar da intranetin diğer bir parçasıdır. O, çalışanlara, çalışan ürünün çalışması için, güvenlik kurallarının konulması, video konferans yapabilmeleri, bilgi paylaşımı yapabilmeleri, aynı proje üzerinde iş birliği yapma imkanını verir. Bedava sunucu, istemci yazılımları ve haber grupları internetin gelişmesini teşvik etmiştir. Gelişmeler desteklenmiş ve internetin yakıtı olmuştur. Bilginin kolayca paylaşılabilmesi ve hangi insanların kimlerle haberleşeceği intranetin inşasında en önemli donelerdendir.

2.3.1. Intranetin Faydaları ve İnternette Farklı Yönleri

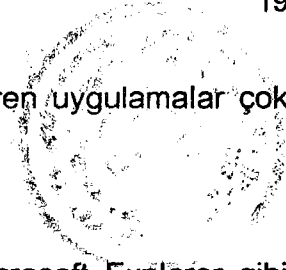
- İnternette internetin bütün kaynaklarına ulaşılabilirdi halde, internette intranetin sadece izin verilen kısıtlı kaynaklarına ulaşılabilir.

- Video konferans büyük miktarda verilerin gönderilmesine ihtiyaç duyduğu önemli bir uygulamadır. İnternetler gerek duyulan bu büyüklükteki bilgilerin transferi için son derece yüksek bant genişliği sağlayan donanımlar kullanılarak inşa edilmelidir.

- İnternet, şirkette bulunan diğer intranetlerle sık sık bağlantıya geçer. Bu ayrı ağlar alt-ağ olarak ifade edilir. Güvenliği arttırmak için intranetler arası bağlantılar asla internet üzerinden gerçekleştirilmez. Sadece özel kiralık devreler kullanılmalıdır. Eğer internet kullanılacaksa ek güvenlik önlemleri alınmalıdır.

- İnsanların e-mail ve kurumsal ilan tahtalarıyla birbirleriyle haberleştikleri ve birlikte çalışmak için kullandıkları çalışma grubu yazılımları en güçlü intranet yazılımları arasındadır. Şirketin farklı birimlerinin bilgi postalamasını sağlayan, personelin zaman cetveli gibi şirket formlarını

doldurmasını sağlayan, şirketlerin finansal bilgilerini veren uygulamalar çok faydalı ve popülerdir.



- İnternette kullanılan Netscape Navigator ve Microsoft Explorer gibi web tarayıcıları intranette de kullanılabilir. Bunlar gibi intranette kullanılan çoğu standart yazılımlar intranette de kullanılabilir. Özel amaçlı programlar genelde java dili ve CGI script'leri kullanılarak yazılırlar.

- İnternetler sipariş takibi, faturaların gönderilmesi ve ödemelerin yapılması gibi şirketler arası iş çevrimlerinin hızlandırılmasına olanak sağlamak için kullanılabilirler.

- İnternetler, internetteki bir kişinin sipariş vermesi gibi şirketlerin online çalışmasına olanak sağlayan en güçlü sistemlerdir. İnternette birisi bir sipariş verdiğinde sipariş bilgisi şirketin intranetine güvenli bir şekilde aktararak sipariş işlemi başlatılır.

- Hassas şirket bilgilerini korumak ve hacker'ları bilgisayar sistemlerinden uzak tutmak için güvenlik duvarı olarak adlandırılan güvenlik bariyerleri kullanılır. Güvenlik duvarı teknolojisi intranet kullanıcılarının internet kaynaklarının kullanabilmesini sağlayan yönlendiriciler, sunucular, diğer donanım ve yazılımlarla birlikte kullanılır. İnternetten intranete girişleri kontrol altına alan da güvenlik duvarı yazılımlarıdır.

2.3.2. İnternet Pazarı

İnternet pazarı, hızla gelişmekte olan bir pazardır. TCP/IP internetwork altyapısına sahip şirketler internet protokol paketi teknolojileri ve son olarak geliştirilen istemci/sunucu web teknolojilerinden yararlanarak çeşitli pilot projeleri hayata geçirmektedirler. Birçok şirkette, web sunucular kontrolsüz bir şekilde artmaktadır. Bunun en önemli nedenleri olarak NCSA ve CERN gibi kamusal web sunucu yazılımlarına erişimin kolay olması ve implementasyon ve kullanımın genel olarak kolaylığı ileri sürülmektedir.



2.4. Güvenlik Kavramı

İnternet dünyasında en önemli konu şüphesiz güvenlidir, özellikle ağların internete bağlanması ile güvenlik, uygulanması gereken zorunlu bir kural haline almaktadır. Mevcut verilerin çalınması, WEB sayfalarının değiştirilmesi, internet üzerinde bir noktadan diğerine giden bir bilginin alınarak okunması ve daha bir çok problem güvenlik konusunun ne kadar ciddi olduğunu göstermektedir. Güvenlik konusunda Güvenlik duvarları, Tunnelling, SSL çözümleri mevcuttur. Konu gereği ayrıntılı olarak güvenlik duvarı üzerinde durulacaktır.

2.4.1. Güvenlik Duvarı(Firewall) Kavramı

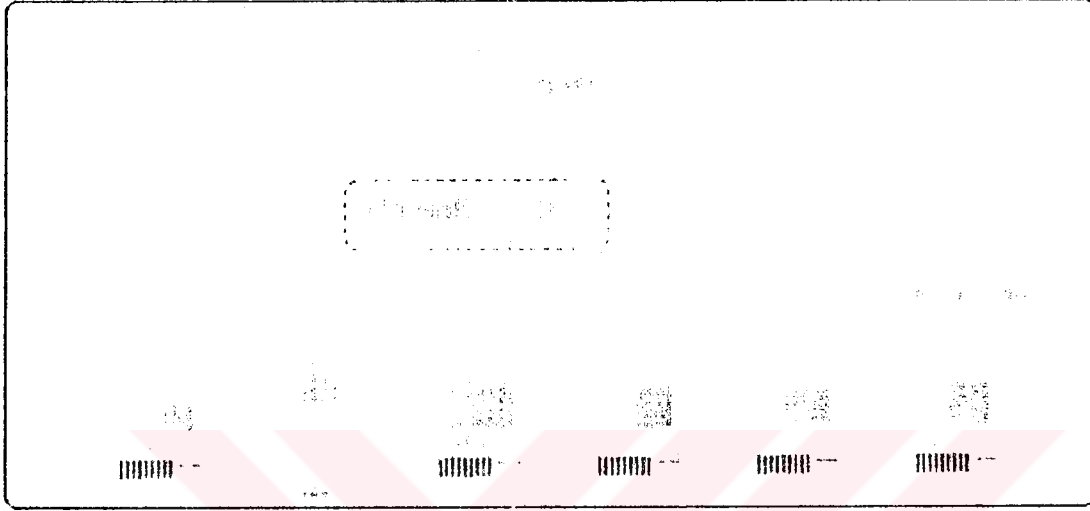
Güvenlik duvarı; basit anlamda bir ağ ile internet arasına yerleştirilen bir duvar gibidir. İnternet tarafından gelebilecek tüm saldırılara karşı ağı koruyan güvenlik duvarının temel prensibi, izin verilen ağların veya sistemlerin belirli bir ağa erişmesi diğerlerinin ise güvenlik duvarı üzerinde bloklanarak engellenmesidir. Güvenlik duvarı tamamen bir donanım olabileceği gibi bir yazılım da olabilir.

Diğer bir tanımla güvenlik duvarı, 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.

Güvenlik duvarları ağ güvenliğinin çok etkili bir tipidir. Binaların inşasında bir ateş duvarı, ateşin bir binadan diğerine sıçramasını engellemek için kullanılır. Teoride, bir internet güvenlik duvarı da aynı amaçlı çalışır. Pratikte ise, bir internet güvenlik duvarı modern binalardan çok herhangi bir kaleye ait sur hendeği gibi işlev görür. Bir çok amaca hizmet eder.

- İnsanların dikkatle kontrol edilen bir noktadan girmelerini sağlar.
- İnsanların diğer saldırılardan korunma sistemlerine yaklaşmalarını engeller,
- İnsanların dikkatle kontrol edilen bir noktadan ayrılmasını sağlar.

İnternet güvenlik duvarı çoğunlukla korunulan ağın internete bağlandığı yere yerleştirilir.(Şekil 2.1)

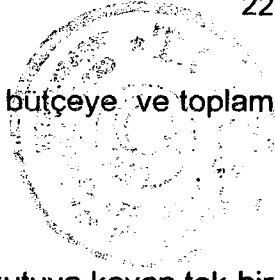


Şekil 2.1. Güvenlik duvarı ve dahili ağ (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.18).

İnternette ağa gelen ve ağdan internete çıkan bütün trafik güvenlik duvarından geçer. Güvenlik duvarı bu trafiğin kabul edilebilir olduğunu kontrol eder. Burada kabul edilebilirlikleri kasıt, gelen elektronik posta, dosya transferleri, uzaktan erişimler veya bunun gibi herhangi belirli sunucular arasındaki belirli hareketlerin kontrolüdür. Böylelikle gelen erişimler sitenin güvenlik politikasına uyar. Güvenlik politikaları her site için farklı olabilir. Bazıları yüksek oranda sınırlandırıcı olabilirken bazıları da olabildiğince açıktır.

Mantıksal olarak bir güvenlik duvarı; ayırıcı, sınırlayıcı ve analiz edicidir. Güvenlik duvarının fiziksel uygulaması siteden siteye değişir. Çoğunlukla güvenlik duvarı donanım parçaları kümesidir. Bu küme ise yönlendirici(router), bir ana bilgisayar veya uygun yazılıma sahip izleyici, bilgisayar ve ağ kombinezonundan oluşur. Bu ekipmanı ayarlamanın bir çok

yolu vardır. Bu ayarlama ilgili sitenin güvenlik politikasına, bütçeye ve toplam işlemlere göre değişiklik arz eder.



Bir güvenlik duvarı, bir çok yeni ticari parçaları aynı kutuya koyan tek bir fiziksel parçadır. Genellikle, bir çok parçadan oluşur ve bazı parçalar güvenlik duvarının bir fonksiyonu gibi çalışmanın yanında başka görevleri de yerine getirirler. İnternet bağlantısı hemen hemen çoğu zaman güvenlik duvarının bir parçasıdır.

Güvenlik duvarı önceki ifadelerde bir kalenin sur hendeğine benzetilmişti. Güvenlik duvarı da aynen bir kalenin hasar görebilmesi gibi zarar görebilir. Ağın içinde olan insanlara karşı bir koruma yapmaz. Dahili savunma ile birleştirilirse iyi çalışır. Ve güvenlik duvarı kendi dezavantajlarına da sahiptir. Bir tane oluşturmak para, çaba ve baş ağrıtabilecek davetsiz misafirler için gerekli sınırlamaların iyi yapılmasını gerektirir.

Güvenlik duvarı birtakım dezavantajlara ve sınırlandırmalara sahip olmasına rağmen bir ağı internete güvenli bağlamada ve o ağı korumada kullanılan en etkili yoldur. İnternet insanlara çok çeşitli olanaklar sağlar. Milyonlarca insan orada bilgiyi paylaşır. Yararları ortadadır. Bu bilgi otoyolunun popülaritesi insanları kendine çekmektedir. Bununla birlikte riskleri de ortadadır. Herhangi bir zamanda milyonlarca insan bir araya gelebilir ve herhangi birisi şehirde olabileceği gibi internette de suç işleyebilir. Bu şuna benzer: Herhangi bir otoyolda arabada bulunmak eğlenceli olabilir. Ama otoyola yakın yaşıyor veya çalışılıyorsa otoyolda gürültü, hava kirliliği ve tehlike vardır.

Bu durumda amaç; internetin iyi yönlerinden, yararlarından faydalanmak ve kötülerin zararlarından korunmak olabilir. Bu nasıl başarılabilir? Bunu için bulunulan ağın internete bağlı olduğu yeri iyi kontrol etmek gerekir. Bir güvenlik duvarı bunu yapmak için vardır ve çoğu durumlar için de bunu yapan en etkili araçtır. Sonuçta güvenlik duvarları etkili fayda sağlarlar fakat her güvenlik problemini de halledemezler.

2.4.1.1. Bir Güvenlik Duvarı Ne Yapabilir?

Güvenlik duvarları bir sitenin güvenliği için pek çok avantaj sağlar. Gerçekte, bazı avantajlarıyla güvenliğin ötesinde özellikler sağlar. Bunlardan bazıları;

- **Güvenlik duvarı, güvenlik kararları için odak noktasıdır:**

Güvenlik duvarı boğum noktası olarak da düşünülebilir. Dışarıya ve içeriye olan tüm trafik, bu tek ve dar olan kontrol noktasından geçmek zorundadır. Güvenlik duvarı, güvenlik kontrolünü bu kontrol noktasında yoğunlaştırdığından, ağ güvenliği için büyük miktarda güç kazandırır. Bu kontrol noktası da ağın internete bağlandığı yerdir.

Güvenliği bu yolla odaklama, güvenlik kararlarını ve teknolojilerini dağıtık düzende tutmaktan çok daha etkilidir. Güvenlik duvarları kurulum ve bakım için fazla miktarda para gerektirmelerine rağmen, en etkili yazılım ve donanım güvenliği açısından bir çok güvenlik kararından daha ucuza malolurlar. Kesinlikle yetersiz güvenliğe sahip olmaktan daha az pahalıdır.

- **Güvenlik duvarı, güvenlik politikasını yürütür:**

İnsanların internetten bekledikleri servislerin birçoğu doğal olarak güvensizdir. Güvenlik duvarı, bu servisler için adeta trafik polisi görevini yürütür. Güvenlik duvarı, sadece kabul edilen, içerisinde tanımlı kuralların olduğu servislerin geçmesine izin vererek site güvenlik politikasını yürütür. Örneğin; bir sitenin yönetimi şuna karar verebilir: NFS, NIS gibi servisler güvenlik duvarı ile kullanmak için çok risklidir. Bu servisleri hangi sistemin kullanmak istediği veya hangi kullanıcının istediği önemli değildir. Güvenlik duvarı, potansiyel olarak tehlike arzeden servisleri titizlikle kendi içinde tutar. Diğer bir site ise sadece bir dahili sistemin dış dünyayla iletişim kurmasına karar verebilir. Yine aynı site, belli bir tipteki veya belli bir gruba ait sistemlere erişim izni verebilir.

Güvenlik duvarı, çok daha karmaşık politikaların yürütülmesini de sağlar. Örneğin; güvenlik duvarındaki sadece belli sistemlerin internete veya internetten dosya transferine izin verebilir. Hangi kullanıcıların bu sistemlere erişimlerinin olduğunu kontrol ederek, hangi kullanıcıların bu imkanı olduğu kontrol edilebilir. Güvenlik duvarı kurmak için seçilen teknolojilere bağlı olarak, bu tip politikaların daha fazla veya az özelliğine sahip olunan bir sistem kurulabilir.

▪ **Güvenlik duvarı, internet aktivite hareketlerinin kaydını tutar:**

Tüm trafik güvenlik duvarından geçtiği için güvenlik duvarı, sistem ve ağ kullanımı veya kötü kullanımı hakkında bilgi toplamak için iyi bir yer sağlar. Tek bir erişim noktası olarak güvenlik duvarı, korunulan ağ ile harici ağ arasında ne olup bittiğini kaydedebilir.

▪ **Güvenlik duvarı, korunmasızlığı sınırlar:**

Bazen güvenlik duvarı, site ağının bir bölümünü diğer bir bölümünden ayrı tutmak için kullanılır. Böylece, bir bölümü etkileyen bir problemin ağ içine yayılması engellenmiş olur. Bazı durumlarda ağın bir bölümü diğerlerinden daha güvenilir yada daha hassas olduğu için bu işlem yapılır. Sebep ne olursa olsun, bir ağ probleminin tüm ağ iletişimini bozması sınırlandırılmış olur.

2.4.1.2. Bir Güvenlik Duvarı Ne Yapamaz?

Güvenlik duvarları ağ tehlikelerine, tehditlerine karşı mükemmel koruma sağlarlar. Fakat komple güvenlik çözümü değildirler. Belirli tehditler güvenlik duvarı kontrolü dışında olabilir. Bunlar;

▪ **Kendisine özel ayrıcalık verilmiş kötü niyetlilere karşı koruma yapamaz:**

Bir güvenlik duvarı firmayı, bir sistem kullanıcılarını müseccel bilgilerin ağ üzerinden firma dışına göndermesinden korur. Fakat aynı kullanıcı bu bilgileri herhangi bir disk, teyp veya kağıt üzerine bastırabilir ve evrak çantasında firma dışına çıkarabilir.

Eğer saldırgan güvenlik duvarı içerisinde ise, diğer bir tabirle tiki kümese girmişse, güvenlik duvarı teorik olarak hiçbir şey yapamaz. Dahili kullanıcılar verileri çalabilir, donanım ve yazılımları bozabilir ve güvenlik duvarının yanına hiçbir zaman gelmeden programları değiştirebilirler. Özel kullanıcı tehlikeleri host güvenliği ve eğitim gibi dahili güvenlik ölçümleri gerektirirler. Bu tür konular ise bu çalışma alanının dışındadır.

▪ **Güvenlik duvarı, kendisi vasıtasıyla olmayan bağlantılarda koruma yapamaz:**

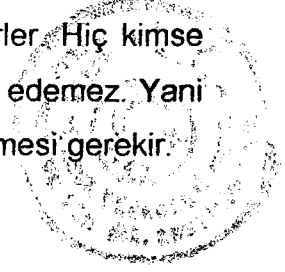
Güvenlik duvarı, kendisi üzerinden akan bir trafikte etkili bir kontrol yapar. Örneğin; eğer bir site güvenlik duvarı arkasında bulunan dahili bir sisteme dışarıdan çevirmeli bağlantı ile erişim yapmaya izin veriyorsa ne olur? Güvenlik duvarı için kesinlikle böyle bir modem bağlantısı ile giren bir davetsiz misafiri engelleyecek bir yol yoktur.

Bazen, teknik olarak uzman kullanıcılar ve sistem yöneticileri ağda kendi arka kapılarını geçici veya sürekli olacak şekilde kurarlar. Çünkü güvenlik duvarının kendilerine ve sistemlerine yapmış olduğu sınırlamalara sinir olurlar. Bu tür bir bağlantı konusunda güvenlik duvarı hiçbir şey yapamaz. Bu tamamen teknik olmanın dışında gerçek bir insan yönetimi problemidir.

▪ **Güvenlik duvarı, tamamen yeni olan tehlikelere karşı koruyamaz:**

Bir güvenlik duvarı pek çok güvenlik stratejisinde olduğu gibi bilinen tehlikelere karşı koruma yapmak üzere tasarlanmıştır. İyi tasarlanmış bir güvenlik duvarı, bir yere kadar yeni tehlikelere karşı da koruma yapabilir. Örneğin; birkaç güvenli servis dışında her servisi iptal etme işlemiyle güvenlik duvarı, insanların yeni ve güvenli olmayan servisler açmasına izin vermez. Bununla birlikte hiçbir güvenlik duvarı ortaya çıkan yeni tehlikelere karşı otomatik olarak savunma yapamaz. Periyodik olarak insanlar daha önceki güvenilebilir servisleri kullanarak veya daha önce hiçbir kimsenin

karşılaşmadığı saldırıları kullanarak yeni atak yolları keşfederler. Hiç kimse güvenlik duvarını bir kere kurup ondan sonsuz bir koruma ümit edemez. Yani her güvenlik duvarının günün gelişen şartlarına göre güncellenmesi gerekir.



▪ **Güvenlik duvarı, virüslere karşı koruyamaz:**

Güvenlik duvarları PC ve Macintosh virüslerini ağı dışında tutamazlar. Her ne kadar bir çok güvenlik duvarı tüm gelen trafiği dahili ağa geçiş izni var mı yok mu diye kontrol ediyorsa da, bu kontrol daha çok gelen verinin kaynak ve hedef adresleri, port numaraları, konusunda olur. Verinin içeriği -detayı- konusunda olmaz. Gelişmiş bir paket filtreleme veya proxy(vekil) yazılımında güvenlik duvarındaki bir virüs koruması pratik değildir. Çok fazla sayıda virüs ve bunların veri içerisinde çok fazla saklanma şekli vardır.

Güvenlik duvarından geçen rastgele bir veri paketindeki virüsü tespit etmek çok zordur. Bu şunları gerektirir:

1. Paketin bir programın parçası olduğunun farkına varılmalıdır.
2. Programın nasıl bir şey olduğu belirlenmelidir.
3. Değişikliğe virüsün neden olduğu belirlenmelidir.

Çoğu güvenlik duvarları farklı çalıştırılabilir düzende çoklu tipte makineleri korumaktadırlar. Bir program derlenmiş bir çalıştırılabilir veya bir metin(script) olabilir. Bundan başka, çoğu programlar taşımacılık için paketlenmişler ve çoğunlukla da sıkıştırılmışlardır. Elektronik posta veya Usenet haber servisleri yoluyla transfer edilen paketler ayrıca farklı yollarla ASCII formatında kodlanmışlardır.

Bütün bu sebeplerden dolayı, kullanıcılar güvenlik duvarı arkasından virüs getirmeyi sonlandırabilirler. O güvenlik duvarının ne kadar güvenli olduğu hiç fark etmez. Virüsleri güvenlik duvarı altında bloklama işlemiyle mükemmel bir iş yapılmış olsa da henüz virüs problemi çözülüş sayılmaz. Çevirmeli ağlar vasıtası ile ilan tahtaları sistemlerinden indirilmiş yazılımlar,

eve veya diğer sitelerden disketlerde getirilmiş yazılımlar, daha üreticide virüslenmiş yazılımlar internetteki virüslenmiş yazılımlardan daha yaygındır.

Virüs problemini halletmenin en pratik yolu host tabanlı bir virüs koruma programı ve virüslerin tehlikeleri ve onlara karşı alınacak tedbirlerle ilgili kullanıcı eğitimidir.

2.4.2. Tunnelling Nedir ?

Tünelleme iki ağ veya bir PC ile ağ arasında gidip gelen tüm verilerin güvenli bir hat üzerinden şifrlenmesi ve başka bir IP paketinin içerisine konmasıdır. Bu sayede internet üzerinden bir PC'nin bu ağa bağlanarak programlarını çalıştırması, veri alıp göndermesi veya ağların internet üzerinden birleştirilmeleri mümkün olmaktadır.

2.4.3. Özel Sanal Ağ(VPN, Virtual Private Network)

İnternet üzerinde hareket eden verilerin güvenli bir şekilde iletiltikleri noktalara varmasını sağlayan **güvenlik tünelleridir**. Bu tünel, servis sağlayıcı tarafında, ulaşım noktası ile şirket tarafında geçit kapısı, güvenlik duvarı gibi noktalar arasında kurulan bir özel ağdır. Uzaktan erişim yapan bir kullanıcı servis sağlayıcının POP noktası ile bağlantı kurar, burada paketler PPTP (Point-to-Point Tunnelling Protocol) tarafından kapsül içine alınır ve ulaşılacak noktaya ikinci katman tarafından iletilir. Bazı uygulamalarda Layer-2 Tunneling Protocol da devreye girer ve görev PPTP ile birlikte yerine getirilir. Son kullanıcıdan son kullanıcıya VPN de bazı zamanlar IETF tarafından ağ güvenlik standardı olarak görülen ve şifreleme, kimlik belirleme ve anahtar yönetim konularını içine alan Internet Protocol Security (IPSec) destekleyen bazı araçlar da kullanılabilir [Manas, Prof. Dr. Oğuz, Güvenlik Duvarları,1998].

Uzaktan Eriřim

Özellikle internet kullanımının yaygınlařması ile uzaktan erişim çok büyük bir önem kazanmıřtır. Bilgisayar ağılarını kullanarak işlem yapan çalışan sayısı çok büyük bir hızla artmaya başlamıřtır. İşte tipik uzaktan erişim kullanıcıları;

- 1- Seyahat anında řirketi ile iletişim kuran hareketli (Mobil) çalışanlar,
- 2- řirket duyuru tablolarına ulaşan müşteriler,
- 3- Master üretim programlarına uygun dağıtımı koordine etmeye çalışan satıcılar,
- 4-İnternet aracılığı ile bilgi kaynaklarına ulaşmaya çalışan kullanıcılar.

Birçok řirket kendi açık uzaktan erişim ağılarını kullanarak inanılmaz boyutlarda kazanç sağlamaktadır. Bununla beraber, kazançlardaki bu artış güvenlik riskindeki artışı da birlikte getirmiřtir. Bu durumda řirketler güvenlik duvarları ile kuruluşlarını güvenlik altına alma çabası içine girmişlerdir. Ancak bu uygulama LAN'daki řirketleri ve kullanıcıları korurken, uzaktan erişim kullanıcılarını bu şemsiyenin dışında bırakmıřtır.

Bunun sonucu olarak giderek artan oranda evinden veya gittiğı şehirde kaldığı otelden bilgisayarını kullanarak ağ üzerinden kurumuna ulaşarak çalışma yapan kullanıcılar için ayrı bir koruma sistemine gereksinim doğmuřtur. Bütün bu açıklamaların ışığında uzaktan erişimde güvenlik dendiğinde ařağıdaki üç özelliğın varlığına gereksinim duyulmaktadır.

1. Yeterli Bir Güvenlik

Güvenli sistem, görevli veya yetkili olmayan kişilerin bilgi kaynaklarına ağ aracılığı ile bağlanmasını engelleyecek ve görevli kullanıcıları şifrelerini kullanarak ağa bağlanmalarını sağlayacak bir yapıda olmalıdır. Ancak doğal olarak gerek kullanıcıların, gerekse kaynakların belirli gruplara ayrılması kaçınılmazdır. Bazı kaynaklar çok gizlidir ve bunların çok özel koruma altına alınmaları gerekmektedir. Bu çok özel verilere de doğal olarak çok özel kişilerin ulaşabilmesine izin verilmesi gerekmektedir.

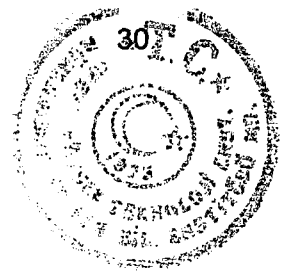
2. Kolay ve Güvenli Bir Yönetim

Şeçilen güvenlik sisteminin kurulması ve bakımı kolay olmalıdır. Ayrıca güvenlik sisteminin yönetim fonksiyonları kullanıcıların kolayca erişebilmesini engelleyecek güvenli bir yapıda olmalıdır.

3. Kullanıcılar İçin İletişimde Kolaylık

İster evden ister otel odasından ofise ulaşma, LAN'daki bir kullanıcı kadar kolay olmalıdır. Bunlara ek olarak güvenlik sistemi istendiğinde kolaylıkla genişleyebilmelidir.





3 AĞ GÜVENLİĞİ

3.1. Giriş

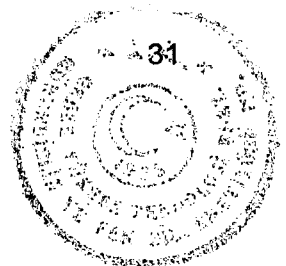
Genelde zor aşamalardan geçerek oluşturulan ağların güvenli olması, sürekli ve verimli çalışması istenir. Fakat günümüzde ağları tehdit eden bir çok tehlike söz konusudur. Hiç bir bilgisayar ağı yüzde yüz güvenli değildir. Mutlaka her ağa girilebilecek bir veya birçok deliği vardır ve saldırganlarca bulunmayı beklemektedir. Eğer ağın dış saldırganlara karşı emin olması isteniyorsa ağ tümüyle dış kullanıcılara karşı kapatılmalıdır. Doğal olarak bilgisayar ağını dış kullanıcılara kapatmak olanaksızdır. Kaldı ki bu sağlansa bile ağ iç kullanıcılara karşı da korunmak zorundadır. Bilgisayar ağını iç ve dış kullanıcılara kapatarak çözüm bulma yerine, oluşabilecek iç ve dış saldırılara karşı korumak için gerekli önlemleri almak en akılcı yoldur. Bu bölümde güvenlik gerekliliği, tehlikeler ve güvenlik için gerekli teorik stratejiler üzerinde durulacaktır.

3.2. Neden İnternet Güvenlik Duvarları?

İnternet bilgiye erişimi sağlamada ve bilgiyi paylaşmada olağanüstü teknolojik bir gelişmedir. Fakat aynı zamanda da bilginin kirlenmesini ve bozulmasına neden olabileceğinden dolayı da tam bir tehlikedir.

Güvenlik duvarı, güvenlik denetimini yaparken aynı zamanda bir ağın internete bağlanmasını sağlayan bir koruma şeklidir.

Güvenlik duvarlarının amacı, değişik saldırı yöntemlerini kullanarak ağlara sızmak isteyen kötü amaçlı kişilerin girişimini engellemektir. Güvenlik duvarları bu nedenle üzerlerinden geçen verilerin durumlarını belirler ve belirli kurallar çerçevesinde bunların girişine izin verir veya reddeder. Böylece ağlara kötü amaçlı kişilerin girişleri engellenir.



3.3. Ne Korunmaya Çalışılıyor?

Güvenlik duvarı, temel olarak koruyucu bir üründür. Bir güvenlik duvarı oluşturulurken ilk önce üzerinde düşünülmesi gereken neyin korunacağıdır. İnternete bağlanmakla;

- **Veriler:** Bilgisayarlarda tutulan bilgiler,
 - **Kaynaklar:** Bilgisayarların kendileri,
 - **Ünvan / İsim:** Kişi veya kuruluşların ünvanları,
- riske atılmış olunur. Bu kavramları inceleyecek olursak;

3.3.1. Veriler

Verilerin korunması gereken temel karakterleri şunlardır:

- **Gizlilik:** Diğer insanların bilmemesi gereken veya bilinmesi istenmeyen veriler,
- **Bütünlük:** Diğer insanların değiştirmemesi istenilen bilgiler,
- **Geçerlilik:** Kullanılması imkanı olan yani kullanılabilir bilgiler.

İnsanlar, gizlilik riski üzerinde gruplaşmaya meyillidirler ve bu hareket gerçekten büyük bir risktir. Bir çok işletmenin ürün tasarımları, finansal kayıtlar veya okul ve üniversitelerin öğrenci kayıtları gibi bilgisayarlarında tuttıkları çok gizli bilgileri vardır. Diğer yandan bir sitede gizli bilgileri tutan bilgisayarları internete bağlanan diğerlerinden ayırmak teknik olarak kolaydır. Bu yolla bilgiler ayrılabilirler ve internet erişimi olan hiçbir bilgi gizli olmaz. Bu durumda güvenlik için duyulan endişenin sebebi sorgulanmalıdır. Çünkü korunmaya çalışılan tek şey gizlilik değildir. Bütünlük ve geçerlilik için de endişe duyulmalıdır. Tüm bunlardan sonra, eğer veri gizli değilse, değişmesi sorun olmayacaksa ve herhangi biri tarafından erişilmesi önemli değilse neden bu bilgi bir diskte yer israfı yapsın ki!

Eğer veri özellikle gizli değilse ve bu bilgi bozulur veya değiştirilirse değerini kaybetmesi sorumluluğuna katlanır. Bu kayıpların bazıları

ölçeklenebilir değerdedir. Eğer veri kaybedilirse tekrar elde etmek için bu değer ödenir. Eğer bu veri bir şekilde satılmak isteniyorsa; verinin direkt satılan, üretilen nesnelerin tasarımları veya bir yazılım ürünü için olan kodun olup olmadığına bakılmaksızın satış kaybı olur. Ayrıca herhangi bir güvenlik olayıyla birleşik görülmeyen değerler de vardır. Verilerde istenmeyen değişiklik oldu mu? En ciddiisi de sistemlerde, verilerde, önemli olarak organizasyonlarda güven kaybıdır ki bu kullanıcı güveni, müşteri güveni, sermayedar güveni, ekip güveni, öğrenci güveni, halkın güveni üzerinde büyük rol oynar.

Güvenlik olayları diğer suç tiplerinin çoğundan farklıdır. Çünkü denetleme zordur. Bazen, birisinin siteye girdiğini anlamak çok zaman alabilir. Bazense hiç bir zaman bilinmeyebilir. Eğer birisi siteye girmeyi başarır ve sistem verilerine herhangi bir şey yapmamışsa bunu anlamak saatler hatta günler alabilir. Çoğu zaman tamamen her şeyi bozmak ve silmek amacına yönelik olan bir saldırıyı engellemek, sistemi bozmaya yönelik bir hareketi olmayan saldırıyı engellemekten daha kolaydır. Eğer her şey silinmişse, yedeklerden geri yüklemek –tabi yedek alındığı farz ediliyor– tekrar eski hayata döndürebilir. Fakat sisteme veya verilere herhangi bir şey yapılmamışsa ve anormal durum söz konusuysa, bunu anlamak için çok zaman harcanabilir.

3.3.2. Kaynaklar

Eğer bir sistem diskleri test için her hafta yeniden kuruluyorsa veya bunun gibi önemli olmayan bir veri varsa ve diğer insanlar bu bilgisayarları kullanıyorlarsa bir şekilde bu kullanırın bir takım avantajlar getirir. Çoğu insan kendi bilgisayarını kullanmak ister veya diğer insanlara para karşılığında kullandırır. Bilgisayar zamanını ve disk kullanımını başkalarına açan kişiler genellikle iyi ilişki ve teşekkür beklerler fakat bunu davetsiz misafirlerden bekleyemezler tabi ki. Bilgisayar kaynaklarında para ve zaman harcanır ve bu işi yapan kişi bu kaynakların nasıl kullanılacaklarına karar verme hakkına sahiptir. Davetsiz misafir sadece fazla kaynakları kullandıkları konusunda

sıkça tartışılır. Sonuçta onların zorla girişleri kurbanlarına herhangi bir parasal problem yüklemesin. Bu tartışmayla ilgili iki problem vardır:



Birincisi; davetsiz bir misafirin hangi kaynakların fazla olduğunu tespit etmesi ve sadece onları kullanması imkansızdır. Bu; sistemde okyanuslar gibi diske ve saatlerce kullanılmayan bilgisayar zamanına sahip olmak gibi bir şeydir. Fakat gerçekte, sistemin her bir bitini ve milisaniyesini kullanan bir animasyon komut dizisi başlatılmış olabilir. Davetsiz biri kaynakları istediğinde geri vermez. Bu bir bakıma; insanların arabalarını gece yarısından sabahın 6'sına kadar kullanmamaları varsayılırsa ve bunu herhangi birisinin sormadan bu arabayı kullanabileceği anlamına gelmeyeceği gibi bir durumdur. Bu durumda kişiler acilen arabalarına ihtiyaç duyarlarsa durum ne olacak!

İkincisi; herkes kendi kaynaklarını istediği gibi kullanma hakkına sahiptir. Bilgisayar kaynakları doğal kaynaklar değildir ve kullanılmadıkları zaman israf edilen veya bozulan sınırlı kaynaklar değildir.

3.3.3. Ünvan/İsim/Prestij

Davetsiz misafir internette başkasının yada hedefinin kimliğiyle görünür. Yaptığı her şey hedef aldığı kişi tarafından yapılıyor gibi görünür. Peki bunun sonuçları neler olabilir?

Çoğu zaman sonuçta, basitçe diğer siteler veya kanun koyucu ajan servisleri; neden sistemlerine girmeye çalıştıklarını sorarlar. Bazen sahtekarlar zaman kaybettirmekten çok daha pahalıya mal olabilirler. Birisini sevmeyen veyahut yabancıların hayatını zorlaştırmaktan zevk alan bir davetsiz misafir, bu kişilerden gönderiliyormuş gibi elektronik mektup gönderebilir veya haber mesajları postalayabilir. Genellikle inandırıcılıktan çok, nefret uyandırmayı hedef seçen bu kişiler eğer mesajlarına birkaç kişiyi inandırabilirlerse meydana gelecek bu olumsuz durumu temizlemek uzun

zaman alabilir ve insanı küçük düşürebilir. Uzaktan olsa bile inandırıcı herhangi birşey insanın ünvanına, kişiliğine sürekli olabilecek olan bir zarar verebilir. Bu konuya iyi bir örnek olması açısından aşağıdaki olaylar düşündürücüdür: Birkaç yıl önce bir sahtekar, binlerce alıcıya Texas A&M profesörü olarak, ırkçı yorumlar içeren nefret dolu bir elektronik posta göndermişti. Bu sahtekar asla bulunamadı ve profesör hala tepki mesajları almaktadır. Diğer bir olayda ise, Dartmouth'da bir öğrenci, bir profesörün imzasıyla imtihan döneminde, bir gece geç vakitte imtihan zamanı bir mail gönderir. Bir ailenin acil olarak hak talep etmesiyle gönderilen elektronik posta ertesi günün imtihanını iptal ettirdi. Ve bunu çok az öğrenci ortaya çıkardı.

Bir siteye girmeden de elektronik posta veya haber gönderilebilir fakat eğer uydurulmuş site tarafından gönderilmişse bunun uydurma olduğu çok kolay gösterilebilir. Dolayısıyla inandırıcı birisinin veya bir sitenin imzasını taşıyan bir mesajın etkisi de çok daha fazla olacaktır. Bir siteye girmeyi başarmış bir davetsiz misafirden gelen elektronik postalar tam olarak o siteye ait görünürler çünkü o mesajlar o sitenindir. Bir davetsiz misafir aynı zamanda harici bir bozucunun elde edemeyeceği kadar çeşitli ayrıntılar elde edebilir. Örneğin bu kişi o sitede sahip olunan tüm posta listesini ve postaların kime gönderildiğini görebilir.

Eğer bir izinsiz kullanıcı bir kişinin kimliğini kullanıyorsa, o siteye bu zorla giriş sitenin ünvanı için hiç de iyi değildir. O organizasyondaki kişilerin güvenini sarsar. Ek olarak, çoğu davetsiz misafirler sitedeki bilgisayarlardan diğerlerine erişebilirler. Böylelikle sonraki kurbanlar, o siteyi bilgisayar suçları için bir platform olarak görebilirler. Çoğu davetsiz misafirler, uzlaşmış siteleri korsan yazılımları vs. için dağıtım siteleri olarak kullanabilirler.

3.4. Neye veya Kime Karşı Korunmaya Çalışılıyor?



Burada cevap bulması gereken sorular şunlardır;

- Ne için üzülüyoruz?
- İnternette ne tip saldırılarla karşılaşılıyor?
- Bu saldırıları ne tip saldırganlar gerçekleştiriyor?
- Ne tür saldırı yöntemleri kullanılıyor?
- Basit hatalar(kazalar) ve vurdumduymazlık bunlara ne kadar etken?

3.4.1. Saldırı Tipleri:

Sistemler üzerinde birçok tipte saldırı şekli ve bu saldırıları sınıflandırmanın birçok yolu vardır. Burada saldırılar temel üç kategoride ele alınmıştır.

- Sistemlere zorla girmek.(Davetsiz misafirler).
- Servislerin devre dışı kalması.
- Bilgi hırsızlığı.

1. Sistemlere Zorla Girmek: Sistemlerdeki en yaygın saldırı tipi hedef sisteme zorla girmektir. Zorla ve gizlice girmekle insanlar bilgisayarları istedikleri gibi kullanabilirler. Çoğu saldırganlar girdikleri bilgisayarları yasal(geçerli) kullanıcılar olarak kullanmak isterler.

Saldırganların sisteme erişim kazanmak için düzinelerce yolu vardır. Bunlar; önemli bir işi gerçekleştirmek için sistem yöneticisinden şifreyi hemen değiştirmeyi istemek gibi sosyal mühendislik saldırılarından ve herhangi biri geçerli olana kadar denenen kullanıcı hesap ismi ve şifresini denemek gibi tahmin işinden, kullanıcı ismi ve şifre gerektirmeyen karmaşık yollarla sisteme girmeye kadar çeşitlilik gösterir.

Güvenlik duvarları zorla girmeyi bir kaç yolla engellemeye yardımcı olur. İdeal olarak, herhangi bir kullanıcı ismi ve şifresini bilmeden sisteme girmeyi

engelleyebilirler. Uygun bir şekilde biçimlendirilmiş olarak, sosyal mühendislikle veya tahmini olarak kolay kırılabilen ve dışarıdan erişilebilen kullanıcı sayısını düşürürler. Çoğu insan güvenlik duvarını tahmini olarak tespit etmek ve kullanılan saldırılardan korunmak için sadece bir kere girmeyi sağlayacak şekilde ayarlarlar. Bu şifreler kullanılmazsa dahi bir güvenlik duvarı sisteme olan giriş denemelerini kaydederek kontrol yeri tespit eder. Bu yolla tahmini saldırıları tespit etmekte yardımcı olur.

2. Servisin Devre Dışı Kalması: Servisi devre dışı bırakma saldırısının hedefi, insanları kendi bilgisayarlarını kullanmayı engellemektir. Örnek olarak mail bombardımanı gösterilebilir. Elektronik posta akışı bilgisayar ağını, diğer mesajların kullanamayacağı bir şekilde bastırır. Yani ağı devamlı meşgul eder ve internet bağlantısı kesilir. Ayrıca telefon servisi de bunu yeniden programlayan davetsiz misafirlerin kurbanı olur ve böylece telefonla arayanlar ülke dışı bir no.ya yönlendirilirler. Bazı durumlarda bu elektronik sabotaj, gerçek verilerin veya ekipmanın kapanması veya bozulmasına neden olsa da solucan olayında görüldüğü gibi daha sıklıkla bir akış şeklini takip ederler. Davetsiz misafir böylece sisteme adeta akar ve mesajlar, süreçler ve ağ istekleri gibi tüm gerçek işlemleri durdurabilir. Sistem veya ağ tüm cevaplama zamanını bu mesajlara ve isteklere ayırdığından diğer hiç bir işlemi tam olarak yerine getiremez.

Devamlı veri akışı, bir servisin devre dışı kalmasını sağlamak için en kolay yol iken daha akıllı bir saldırgan servisleri iptal edebilir, onları tekrar yönlendirebilir(rerouting) veya tekrar eski haline getirebilir.

Servisleri devre dışı bırakan saldırılardan korunmak imkansız yakın bir ihtimaldir. Örneğin; çoğu site sisteme ciddi bir şekilde girme olayı başarısızlıkla sonuçlanan durumlarda o kullanıcı ismini kullanılmaz hale getirir. Bu da saldırganların doğru olan şifreyi bulana kadar denemelerini engeller. Diğer yandan yöntem de, saldırganlara servisi devre dışı bırakmak için daha kolay bir yol olur. Şöyle ki; sisteme birkaç defa girmeyi denemeleri o kullanıcı isminin kilitlenmesine neden olur. Servisin devre dışı kalma

saldırıları kaçınılmazdır. Elektronik posta, telefon çağrıları veya paketler gibi dış dünyadan gelen şeyler kabul edilirse veri akımına uğramak olasıdır. Tanınmış bir kolej şakası olan pizza siparişi de bir şekilde servisi devre dışı bırakan bir olaydır. Bu olayda 24 pizzacıdan her birinden 2'şer adet olmak üzere tek bir kişi için pizza siparişi verilmesi o kişinin 42 siparişe boğuşacağı anlamına gelir. Elektronik dünyada da bir faks makinesinin herhangi birinin ses hattına bir şeyler göndermeye çalışması da kazara olmuş gibi bir servisi devre dışı bırakmadır. En önemli şey ise servisleri, herhangi birisine akım olduğu zaman diğerlerinin fonksiyonlarına devam etmelerinin sağlanması ve problemi halletmek için iyi bir şekilde ayar yapmaktır. Bereket versin ki kasıtlı olarak servisi devre dışı bırakma saldırıları çok popüler değildir. Çoğu saldırganlar açısından da tatmin edici olmayacak kadar basit olarak görülürler. Bu saldırılarda iz sürülebildiği için saldırganlar açısından risklidir ve saldırganlara herhangi bir bilgi sağlamazlar ve saldırganlar bilgisayarları kullanmazlar.

Servisleri devre dışı bırakan kasıtlı saldırılar genelde herhangi bir siteye kızgın ve kını olan kişiler tarafından yapılır. Çoğu sitede de böyle insanlar oldukça nadir bulunur.

3. Bilgi Casusluğu: Bazı saldırı tipleri de saldırganların bilgisayarları direkt olarak hiç kullanmadan veriye erişimlerine izin verir. Genellikle bu saldırılar dışarıya bilgi veren internet servislerinin; daha fazla bilgi vermesinde veya bilgiyi yanlış insanlara göndermesine neden olacak şekilde aşırı yüklenmesine neden olur. Birçok internet servisi yerel ağ üzerinde kullanılmak üzere tasarlanmıştır ve onları internette güvenli bir şekilde kullanmak için gerekli güvenlik derecesine veya tipine sahip değildirler.

Bilgi casusluğu, aktif veya özellikle teknik olmak zorunda değildir. Özel bilgiye erişmek isteyen insanlar basitçe telefonla ararlar ve gerekli bilgiyi sorarlar. Bu aktif bilgi hırsızlığıdır. Ya da telefonu dinleyebilirler. Bu da pasif hırsızlıktır. Benzer olarak, elektronik bilgiye sahip olmak isteyen birisi de onu sorgulayabilir (belki bir makine veya geçerli erişim almış bir kullanıcı gibi görünerek) veya ağı dinleyebilir ve o bilginin akışını bekleyebilir.

Çoğu insan bilgi çalmak için başkalarının bilgisayarlarına girmeye çalışır. Bu kişiler geçerli kullanıcı adları ve şifreleri ararlar. Bunların şansı ve diğerlerinin şanssızlığı olarak, bir bilgiyi elde etmek için ağın dinlenmesi en kolay yoldur. Kullanıcı ismi ve şifre bilgileri tahmin edilebilir bir şekilde çoğu ağ etkileşiminin başlangıcında bulunur ve bu bilgi aynı formda tekrar kullanılabilir. Herhangi birisinin telefona nasıl cevap verdiği bulunmak istenirse nasıl davranılır? Bir dinleyici yerleştirerek kolay ve emniyetli bir yol olacaktır ve telefon sisteminin merkezinde olan bir dinleyici, kısa bir süre içerisinde yüzlerce insanın binlerce konuşmasının duyulmasını sağlayacaktır.

Benzer olarak; genellikle koklayıcı(sniffer) olarak adlandırılan ağ dinleyicileri şifre bilgisini bulmakta çok etkilidir. Fakat diğer çeşit bilgileri elde etmede nadiren kullanılır. Bir site hakkında daha belirli bir bilgi elde etmek ya ekstra bir tarama ve sabır ya da istenilen bilginin güvenilir olarak verilen yerden ve verilen zamanda geçmesini gerektirir. Örneğin; eğer bir kişinin her Cuma öğleden sonra saat 2'de parasını çek ve birikim hesapları arasında transfer etmek için bankasını aradığı bilinirse, bu kişinin erişim kodlarını, hesap numaralarını bulmak için bu telefon çağrısını dinlemeye değer. Bununla birlikte, muhtemelen birisinin telefonunu bunun için dinlemeye değmez. Çünkü çoğu insan parasını telefonla transfer etmez.

Ağı dinlemek telefon dinlemekten çok daha kolaydır. Geleneksel olarak, bir bilgisayarı ağa bağlamak için kullanılan konnektörler de ağıdaki diğer cihazlar gibi davranış gösterir. Çoğu genel ağ teknolojilerinde ethernet ve token ring gibi, yerel alan ağındaki bir bilgisayar o ağıdaki tüm trafiği görebilir ve izleyebilir. İnterneti çaprazlayan trafik, herhangi bir yerel alan ağını da çaprazlayabilir. Ağ servis sağlayıcıları ve herkese açık erişim sistemleri izinsiz girmek için çok popüler hedeflerdir. O ağa yerleştirilmiş koklayıcılar, son derece başarılı olabilir çünkü bu ağlarda oldukça fazla veri trafiği vardır.

Tam olarak ayarlanmış bir güvenlik duvarı, istenildiğinden daha fazla bilgiye erişmeyi deneyen kişilere karşı koruma sağlayabilir. Bir kere bilgi internete gönderilmeye(açılmaya) karar verilmişse bununla birlikte kasıtsız

kişilere karşı bu bilgiye erişime karşı korunmak çok zordur. Bu riskler bir güvenlik duvarının verebileceği korumanın dışında olsalar bile, bu kavramlar tartışılabilir ve güvensizliği azaltmak için metotlar geliştirilebilir.

3.4.2. Saldırganların Çeşitleri

Bu bölümde saldırıda bulunan kişiler hakkında bilgi verilecektir. İnternette bulunan bu saldırgan kişileri kategorize etmek için bir çok yol vardır. Yıllardır görülen bu değişken saldırgan kişileri tam olarak gruplamak adilane bir şekilde yapılamaz ve bu şekilde hızlı bir özet yapmak klişeleşmiş bir görüşü belirtir. Yine de bu özet, saldırganları ana kategorilere ayırmakta faydalı olabilir.

Tüm saldırganların belirli karakteristikleri vardır. Yakalanmak istemezler, kendilerini gizlemeye çalışırlar. Eğer bir sisteme girmeyi başarmışlarsa, kesinlikle bu erişimi korumaya çalışırlar. Eğer imkan varsa erişim kazanmak için başka yollar geliştirirler. Saldırganların kendileri bulunsa da bu erişimin farkına varılamayacağını ümit ederler. Çoğu aynı şeyle ilgilenenlerle iletişim içindedir ve çoğu da bir sisteme saldırarak elde edilen bilgileri diğerleriyle paylaşır.

1. Joyriders(Çalıntı araba kullananlar): Bunlar eğlence arayan canı sıkkın kişilerdir. Bir yerlere girmeyi, hep oralarda ilginç verilerin olabileceğini düşünerek denerler. Ya da başkasının bilgisayarını kullanmak eğlenceli olacaktır veya daha iyi yapacak işleri olmadığından bu işlerle uğraşırlar. Bir kişinin kullandığı bilgisayar veya veriler hakkında bilgileri öğrenebilirler. Meraklıdırlar fakat aktif olarak kötü niyetli değildirler. Bununla birlikte, haberleri olmadan, bilgisizliklerinden veya kendi izlerini örtmeye çalışırken sıklıkla sistemi bozabilirler. Bu kişiler, özellikle iyi bilinen sitelere ve sıra dışı bilgisayarlara hayranlık duyarlar.

2. Zararlılar(Vandals): Bu kişiler bozmak için vardır. Kendilerince, etkileri bozdukları şeylerle doğru orantılıdır. Daha çok girdikleri sistemi



bozmakla bilinirler. Sevmedikleri bir kişiye ise zararları daha çoktur. Ve bu zararlarından dolayı hemen tanınırlar.

Eğer internet dünyası tarafından düşman olarak hedef olunmuşsa (Ör: Telefon şirketi veya hükümet gibi) veya bilgisayar ve zamanı olan insanlar kızdırılma eğilimindeyse (ör: başarısız öğrencilerle dolu olan bir üniversite, kızdırılmış müşterileri olan bilgisayar firmaları veya internette saldırgan ticari bir varlığa sahip olunması gibi) bu kişiler daha da problem olurlar. Geniş ve görünür olan herkes bunların hedefi olabilir. Eğer bazı komşular arasına büyük bir duvar koyarsanız, insanlar da sizin hakkınızda ne düşündüğü mesele olmadan o duvarı duvar yazılarıyla doldururlar.

Neyse ki bu zarar verenler oldukça nadirdirler. İnsanlar, genelde bilgisayarlara izinsizce sızmaya karşı herhangi bir konumda bulunmasalar bile onlardan hoşlanmazlar. Bu kişiler insanlara, onları bulma ve durdurma konusunda ilham verirler. Sıradan davetsiz misafirlerden farklı olarak bu zararlılar kısa fakat gösterişli kariyerleri vardır. Çoğu, hoş olmayan fakat görsel olarak tespit edilen ve onarılabilen bir şekilde zarar verirler. Çoğu durumlarda veriyi silmek veya herhangi bir kişinin bilgisayar donanımını çalıştırmak o kadar kötü bir şey değildir fakat bunların yaptığı şey budur. Aslında, kendini tanıtmak zekice bir harekettir fakat programlardaki veya finansal verilerdeki anlamlı değişiklikleri tespit etmek ve onarmak çok daha güç olacaktır.

Maalesef azimli bir zararlıyı durdurmak neredeyse imkansızdır. Herhangi bir siteye karşı kin besleyen bir kişi yakında veya daha sonraki bir zamanda istediğini elde edecektir. Kesin saldırılar zararlılar için cezbedicidir fakat diğer saldırgan tipleri için değildir. Örneğin; bir servisi devre dışı bırakma saldırıları sisteminizde herhangi bir yerlerde duruyor iken bile joyrider'lar için ilginç değildir.

Onlar için bir bilgisayardaki bilgiler, bilgisayarın internetteki varlığı ve bilgisayarda çalışan programlar daha önemlidir.

3. Puan Toplayıcılar(Score Keepers): Birçok davetsiz misafir çok eski bir geleneğin güncelleştirilmiş sürümünü içerisinde birbirini tutarlar. İzinsizce girdikleri sistem tiplerine ve sayılara dayandırılmış, haklarını kazanmakla övünürler. Joyrider'lar ve Zararlılar gibi ScoreKeeper'lar özel ilgi duydukları siteleri tercih edebilirler. İyi korunulan bir siteye girmek veya diğer yandan özellikle basit ve iyi siteler onlara daha da değer katar. Bununla birlikte, erişebildikleri herhangi bir şeye saldırabilirler. Kalite kadar çokluğa da önem verirler. Hiç bir şeye sahip olunsun istemezler veya herhangi bir sitenin karakteristiklerinin en azını bile umursamazlık etmezler. Kesin bilgiler elde ederler ve onları daha sonra çeşitli amaçlar için kullanırlar. Daha sonra tekrar geri gelebilmek için kendilerine bir yol bırakırlar. Ve bütün bunlar imkan dahilindeyse, bilgisayarları diğer makinelere saldırmak için birer platform olarak kullanabilirler.

4. Casuslar(Spies): Bu kişiler paraya ya da daha sonraki erişimlere dönüştürülebilen nesneleri çalarlar. Örneğin; Kredi kartı, telefon, ağ erişimi bilgisi gibi. Eğer sırları ele geçirirlerse satabileceklerini düşünürler. Böyle yapmayı deneyebilirler fakat bu onların ana işi değildir.

Herkesin bildiği gibi ciddi bilgisayar casusluğu geleneksel casusluk çemberinin dışında, çok nadir olan bir olaydır. Yani; eğer profesyonel casussanız, sizi ve bilgisayarlarınızı izleyen başka profesyonel casuslar da mutlaka vardır. Casusluk çok zor fark edilebilir. Bilgi hırsızlığının herhangi bir iz bırakmaya ihtiyacı yoktur ve izinsiz girişler görsel olarak nadir olsa bile anında tespit edilebilir. Bilgisayarlara giren birisi verileri kopyalar ve hiçbirşeyi rahatsız etmeden her şeyi olduğu gibi bırakıp ayrılır.

Pratik olarak, çoğu organizasyon casusların başarılı olmalarını engelleyemezler. Hükümetlerin bilgisayarlardaki hassas bilgileri korumak için aldığı tedbirler kompleks, pahalı ve kullanışsızdır. Bu yüzden, bunlar en kritik kaynaklarda kullanılırlar. Bu tedbirler, elektromanyetik kalkanlar, dikkatli erişim kontrolleri ve güvensiz ağlara kesinlikle bağlantı olmaması gibi işlevleri içerirler.

Bu çeşit saldırganlara karşı korunmak için neler yapılabilir? İnternet bağlantısının bir casus için bilgi elde etmede kullanılabileceği en kolay yol olmadığından emin olunmalıdır. Bazı çocukların bilgisayarlara girmesini ve casuslara satmakla değer kazanacak bilgilere ulaşmasını hiç kimse istemez. Hiç kimse rakiplerinin kendi verilerine tereyağından kıl çeker gibi sahip olmasını istemez. Bazıları, herhangi bir kişinin fiziksel olarak erişebileceği verileri, ağ erişiminden korumanın amaçsız ve sebepsiz olduğunu söylerler. Fakat bir saldırgan için fiziksel erişim, ağ erişiminden daha pahalı ve risklidir.

5. Aptallık ve Kazalar: Aptallık olarak açıklanmaya elverişli olan bir şey asla kötülüğe atfedilmemelidir. Çoğu felaketlere kötü niyet sebep olmaz. Bunlar kaza veya aptalca hatalar sonucunda ortaya çıkarlar. Yapılmış bir çalışma, güvenlik olaylarının %55'inin saf ve eğitimsiz kullanıcıların yapmamaları gereken işleri yapmaları sonucunda ortaya çıktığını göstermiştir.

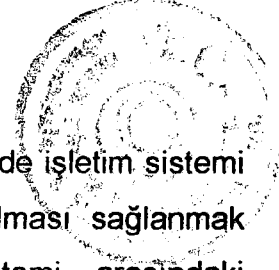
Servislerin devre dışı kalma olayları, çoğu kez tümüyle saldırılarla olmaz. Yapılan yanlış bir hareket de servisi devre dışı bırakabilir. Örneğin; bir posta sunucusu geniş bir kullanıcıya sahip posta listesine tek fakat yanlış bir posta göndermesiyle birlikte yüz binlerce hata mesajının meydana gelmesine sebep olur. Ve bu hata mesajları posta servisini kilitleyebilir.

Benzer şekilde; bir şirketin kendi verilerini kazayla bozması ya da tüm dünyaya yayması, yaygın olan bir durum değildir. Güvenlik duvarları bu tip bir problemi engellemek için tasarlanmışlardır. Gerçekte insanın kendisini kazalarda veya aptalca işler yapmaktan korumasının bilinen belirli bir yolu yoktur. Ne yazık ki, insanların bir amaç için birilerine saldırmasıyla veya basit hataların yapılmasıyla ortaya çıkan sonuçlar benzerdir.

3.4.3. Saldırı Yöntemleri

Ağları tehdit eden saldırı çeşitleri ise, yukarıda izah edilen saldırı tiplerinin fiziksel olarak gerçekleştirilme şeklidirler.

1. İletişim Protokollerini Kullanan Saldırılar



▪ **Port Bombing:** Port bombalama kullanıldığı takdirde işletim sistemi üzerine kurulmuş olan güvenlik duvarının devre dışı kalması sağlanmak istenir. Bu nedenle güvenlik duvarı ile işletim sistemi arasındaki konfigürasyon çok önem taşır.

▪ **IP Sahtekarlığı(Spoofing):** Saldırgan kurumun güvenliği ve yüksek yetkiye sahip makinaların IP adreslerini kullanarak sahte paketler yollamakta ve güvenilir makina kimliğine bürünmektedir. Bu atak güvenlik duvarlarını aşmak için en çok kullanılan yöntemdir ve öteki tip ataklar için dayanak noktası oluşturur. Bu saldırı da hacker sistem filtrelerini aşarak sisteme izinsiz girer; mesela birisine gönderdiği mesajı sanki başka yerden veya kişiden gelmiş gibi gösterebilir.

▪ **TCP Dizi Numarası Atağı:** Eğer TCP dizisi tahmin edilirse, saldırgan güvenli makina adresli kaynaklı sahte paketler yollayarak IP adreslerine dayalı onaylama kullanan rsh ve rlogin gibi servisleri ele geçirebilir.

▪ **ICMP Atakları:** ICMP protokolu internet protokolünün önemli bir parçasıdır ve ağ problemi oluştuğunda kullanılır. Sentetik, sahte ICMP paketleri gönderen saldırgan ağı kullanamaz hale sokabilir (Source Quench, Destination Unreachable gibi) ve yönlendirme yollarını değiştirerek sistemin çökmesine yol açabilir.

▪ **Ölümcül Ping:** Nerede ise tüm işletim sistemlerinde ve bazı yönlendiricilerde 65.508 byte'tan daha büyük geçersiz ICMP paketleri sistemin donmasına ya da yeniden boot edilmesine yol açar.

▪ **TCP SYN Seli Atağı:** Saldırgan hedef makinaya çok sayıda TCP bağlantısı kurarak geçici olarak servis dışı bırakma atağını gerçekleştirir. Bir port SYN paketleri tarafından bombardıman edilir. Her SYN paketi, hedef

makinanın o oturum için bir ara bellek ayırmasını zorunlu kıldığı için port kullanılamaz hale gelir ve servis dışı kalır.

▪ **IP Parçalama(Fragmentation) Atağı:** IP başlığı dışında, her paket bir kimlik ile parçaları açıkça tanımlayan ve sırasını gösteren parça görelî konum numarası içerir. Parçalanmış paketler TCP port numarasına göre yönlendirme yapan paket süzgeci güvenlik duvarları için tehlike yaratırlar. Zira sadece ilk parça TCP port numarasını taşır ve sonraki parçalar süzgeçten geçirilemez. Bir saldırgan (hacker) anlamsız IP parçaları üreterek paket süzgecini aşabilir ve tehlike yaratabilir. Bu sistemde ise güvenlik duvarı ağ içine giren ve onayı alınmış paketlerin sadece nerden geldiğini bilmesi için gereken kısmına bakması ve gelen bu paketin diğer kısımlarını kontrol etmemesi mantığı ile çalışır, bu sayede ağdan içeri giren paketin diğer küçük modülleri, iç ağ hakkında gereken bilgiyi toplamış olur, bu sebepten kesinlikle fragment edilmiş paketlerin güvenlik duvarından geçişine izin vermemek gerekmektedir.

▪ **İnternet Yönlendirme Atakları(RIP):** 8 bit opsiyon alanı kullanılarak IP paketleri gözetleme ve test amaçları için kullanılabilir. Kaynak yönlendirmesi opsiyonu, birinin bir paketin hedefe ulaşması için izleyeceği belirli veya karmaşık yolu tanımlamasını sağlar. Bu opsiyon yönlendiricinin kendi yolu yerine kullanılır. Eğer bir güvenlik duvarı bu opsiyonu engelleyemezse, kaynak yönlendirilmiş bir paket güvenlik duvarının tanımladığı kuralları rakatlıkla geçebilir. Benzer bir atak ise iki nokta arasındaki bağlantıyı ortada koşullanmış saldırganın üstünden geçirmek mantığına göre kurulmuştur.

▪ **UDP Sahtekarlığı ve Kıkılama (Sniffing):** UDP paketleri kolayca oluşturulabildiğinden saldırgan içerdeki bir makineye ait IP adresli UDP paketleri yollayarak istenilen uygulamayı çalıştırabilir. Saldırganlar aynı zamanda varolan UDP bağlantılarını sunucu uygulamasının haberi olmadan çalabilirler. Sniffing esas olarak; internet üzerinde dolaşan (text,düz yazı olarak) şifre ve kullanıcı isimlerini alarak daha sonra bu kullanıcı yerine sisteme girmeyi hedefler, bu amaç için hackerlar internetten sürekli mesaj paketleri toplayarak bunların içeriğini kontrol ederler.

▪ **UDP Portunu Servis Dışı Bırakma Atakı:** UDP paket fırtınası oluşturarak hedef makinada performans düşüklüğüne sebep olur ve ağda tıkanmaya yol açar.

▪ **Rastgele Port Taraması:** Saldırganın hedef porta bir dizi basit paketler yollayıp gelen cevaba göre hangi portların açık olduğunu gerçek bir bağlantı kurmadan öğrenmesi tekniğidir. Böylece hedef makinadaki servisler hakkında bağlantı kurmadan bilgi edinilmiş olmaktadır.

▪ **ARP Atakları:** Kötü niyetli bir makina, gerçek alıcının ARP isteğini alıp geriye cevap vermesinden önce göndericiye yanlış ARP cevapları yollayabilir. Böylece gönderici, kendi trafiğini gerçek hedef yerine kötü niyetli makinaya, bilmeden yollar.

▪ **Ortadaki Adam Atakları:** Bu atak, saldırganın ağ üstünden geçen paketlere erişimi olmasını gerektirir. Genellikle ağ paket koklayıcıları, yönlendirme ve ulaştırma protokolleri kullanarak bunu gerçekleştirirler. Bu atakların olası kullanımı arasında; bilgi hırsızlığı, devam eden bir oturuma katılarak içteki ağın kaynaklarına ulaşabilme, trafik analizi yaparak organizasyonun ağı ve kullanıcıları hakkında bilgi toplama, servis dışı bırakma, ulaşılan veriyi değiştirme ve ağ oturumlarında sahte bilgiyi araya sokma uygulamaları yer alır.

2. Kimlik Onaylama Atakları

▪ **Kullanıcı Parolası Atakları:** Kullanıcı parolası atakları zor kuvvet, truva atı programları, ağ paketi koklayıcıları ve toplum sahtekarlığı kullanılarak gerçekleştirilebilir.

3. Uygulama Katmanı Atakları

▪ **Uzaktan Login İle Saldırıları:** Telnet, rlogin veya rsh gibi uygulamalar saldırıya açık uygulamalardır. Bir telnet oturumunda iletilen her

şey açık yazı olarak yollandığından ağ koklayıcıları sayesinde telnet loginlerinin ve kullanıcı şifrelerinin saldırganların eline geçmesine olanak sağlamaktadır.



Başka bir atak ise; istemci telnet uygulamasını kullanıcı kimlikleri ve şifrelerini gizlice kayıt eden bir truva atı ile değiştirebilir. Rsh ve rlogin uygulamaları güvenilir bir makinede çalışan kullanıcı kimliğine bürünmüş saldırganın uzaktan bir komutu çalıştırmasına olanak sağlayabilir.

- **DNS Atakları:** Eğer bir saldırgan DNS inaddr.arpa tablosunu değiştirecek güvenilir makinanın domain ismini kendi internet için tanımlayabilirse rlogin veya rhs kullanarak sisteme saldırabilir. DNS ataklarının ikinci hedefi saldırganlara iç ağın kurulması, yapısı ve adreslenmesi hakkında yararlı bilgi sunan bölge dosyalarıdır.

- **SMTP Atakları:** İletiler(mesajlar) iki ileti aktarım aracısı arasında SMTP kullanılarak yönlendirilirler. Son yıllarda, saldırganların kullandığı bir çok güvenlik deliği saptanmıştır. Bu atakların arasında; SMTP arka kapı komut atağı(Sendmail portu üzerinden hedef makinaya sızma), SMTP arabellek üzerine yazma atağı(yerel kullanıcının izinsiz süper kullanıcı hakkına sahip olması), SMTP takma isim atağı(Saldırgan decode@hostname adresine sistem dosyalarını silmesi için özel olarak kodlanmış elektronik postayı yollayabilir) gösterilebilir.

- **MIME Atakları:** MIME ile kodlanmış elektronik postanın otomatik olarak okunması, .rhosts gibi sistem dosyalarını silmek amacı ile kullanılabilir. Ayrıca MIME iletisini alan sistemin uygun dosya alanları doğru olarak oluşturulmamışsa, MIME obsiyonunu kullanan saldırgan dosyaları okuyabilir.

- **NFS Atakları:** NFS, dosyaların sadece yerel makinalar için dışarıya verilmesini sağlayıcı bir şekilde kurulmalıdır. Eğer NFS standart RPC tarafından kullanılıyorsa, dosya saplarının koklayıcılar tarafından kayıt edilme tehlikesi vardır. Saldırgan daha sonra içerdeki NFS istemcisinin adresini kullanarak o dosya sistemine ulaşabilir.

▪ **Ağ Zaman Protokolü Atakları(NTP):** Ağ üzerindeki bilgisayar sistemlerini senkronize etmek amacı ile kullanılır. Eğer hedef makinadaki zaman ayarı değiştirilirse, zamanı geriye alıp sisteme bir defa kullanılabilecek kullanıcı parolası girerek, giriş yapılabilir.

Bir zaman ayarı sunucusunu taklit etmek, gönderilmiş zaman iletilerini tekrar yollayarak bir zaman ayarı sunucusunun iletilerini değiştirmek, bir zaman sunucusunun paketlerini silmek ve ağda tıkanıklığa yol açarak gönderilen zaman iletilerini geciktirmek, NTP protokolünü kullanarak yapılan ataklardır.

▪ **Bilgi Sızdıran Ataklar:** Bu ataklar **finger**, **whois**, **echo**, **ping**, **SNMP** veya **traceroute** servisleri kullanarak iç ağ hakkında bilgi edinilmesi temeline dayanır.

▪ **URL Sahtekarlığı:** WWW sunucu sistemlerine girmenin yaygın bir yolu, URL'lerin sunucunun /etc/passwd veya .rhosts gibi sistem dosyalarını aktaracak şekilde değiştirilmesidir. URL'nin kullandığı port numarasını değiştirerek, o port üstündeki uygulamaların beklenmedik bir şekilde davranmaları sonucunda bir güvenlik boşluğunun açılması sağlanabilir.

▪ **CGI Atakları:** Bir çok CGI programı giriş dizgesini işledikten sonra gerekli komutu çalıştıracak yetenektir. Eğer CGI değişkeni UNIX kabuğuna direkt olarak geçirilirse, tehlikeli sonuçlar doğabilir. En kolay yollardan biri olan bu yöntem ile web sunucu üzerine bağlanılarak CGI programları aracılığı ile sisteme girilebilir, bu sayede mesela web sunucu üzerine farklı bir sayfa gönderilmesi, virüslerin aktif hale getirilmesi gibi ataklar yapılabilir. Bunun engellenmesi için web sunucuların kendilerine gelen paketleri kendi ağlarında hiçbir yere göndermemeleri sağlanmalıdır.

▪ **X-Windows Sistem Atakları:** Saldırgan, bir makinanın X-Windows sunucusuna bağlanmaya çalışır. Eğer X-Windows sunucusunda zayıflık varsa, tuşa basmalar yakalanıp kullanıcının haberi olmadan uzaktan komutlar çalıştırılabilir.

▪ **Kötü Niyetli Java ve ActiveX Uygulamaları:** Bu ataklar zararlı programların ağ üzerinden aktarılması ve kullanıcının tarayıcısına yüklenmesi sonucu gerçekleştirilir. Ancak bir saldırganın gerçekleştirmesi yerine, kullanıcının zararlı uygulaması içeren bir HTML sayfasını seçmesi sonucu başlatılırlar ve her tarafa uyarlanabilir bir program diliyle yazıldıklarından dolayı herhangi bir işletim sistemi veya donanımına bağlı değildirler. İnternet üzerinde programlama yapılarak java appletleri sayesinde gerçekten çok etkili problemler yaratılabilir. Bir appletin internette alınması bir virüsün download(kendi makinemize indirilmesi) edilmesiyle benzerdir. Bu sayede WEB sitelerinin bozulması, değiştirilmesi veya silinmesi mümkün olabilir.

▪ **Sistem Kayıt(Log) Seli:** Saldırgan güvenlik duvarına çok sayıda giriş yaparak log dosyasının dolmasını ve sonuç olarak sistemin kapanmasını sağlar.

4. Diğer Saldırı Yöntemleri

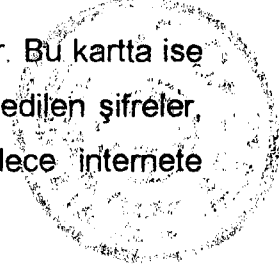
▪ **Telephone Entry:** Telefon sistemleri bilgisayar sistemine girmenin kolay yollarından biridir. İnternete telefon ile ulaşmak isteyenler için arayan ve geri arayan (call back) sistemler mevcuttur. Bu sayede sisteme benzer telefon tonu gönderilerek modemin tekrar geri aranması sağlanabilir. Bu sayede de hacker sisteme girebilir.

▪ **Ftp Bouncer Attack:** Bu sayede ftp sitesine diğer bir güvenilen site üzerinden ulaşan kimse sisteme kolayca girer ve hedeflediği siteye ulaşabilir.

▪ **Trojaning:** Bu yöntemle hack edilen sistem içersinde bir kullanıcının bir program çalıştırarak dışardaki hacker'ın sisteme girmesi yöntemidir. Örneğin; Netbus, BackOrifice gibi...

▪ **Social Engineering:** Bu yöntem ise en enteresan olanlardan biri olsa gerektir. Örneğin bir grup insanla girilen bir sohbette konu şifrelerden

açılıyor. Gün bittiğinde herkes bir diğerine kartını vermiş oluyor. Bu kartta ise kişinin e-mail adresi, kullanıcı adı ve sohbet esnasında elde edilen şifreler, bilgisayar adları ve bilgisayar sistemi var. Geriye ise sadece internete bağlanmak kalıyor.



3.5. Nasıl Korunabilir?

İnsanlar, saldırı çeşitlerine göre; güvenlik olmayan, kapalılık, anlaşılmazlık yöntemiyle güvenlik, host güvenliği ve ağ güvenliği gibi değişik savunma modelleri veya yaklaşımlar geliştirmektedirler.

3.5.1. Güvenlik Yok

En basit bir yaklaşım imkanı güvenlik için hiç bir çapa sarfetmemek ve satıcının sunduğu ürünle gelen minimum güvenliği kullanmaktır. Bu çalışmada bu yaklaşım tarzı baştan reddedilmiştir.

3.5.2. Karmaşıklıkla Güvenlik Sağlamak

Bir başka güvenlik modeli ise karmaşıklık, kapalılık yöntemiyle olan güvenliktir ki, bu modelle bir sistem güvenli varsayılır. Çünkü hiç kimse bu sistem hakkında hiç bir şey bilmez. Onun varlığı, içeriği, güvenliği ölçeklendirilmesi veya herhangi bir özelliği hakkında bilgi yoktur. Bu yaklaşım nadiren uzun süre çalışır. Çekici bir hedefin cazibesi her zaman yeni bir saldırı ve sistemi çözme yolu üretilmesine sebep olabilir.

Bir çok kişi saldırganların kendilerini her halukarda bulacaklarını farzederler. Bunlar küçük bir şirket veya ev bilgisayarının davetsiz misafirlerin ilgisini çekmeyeceklerini sanırlar. Fakat gerçekte, çoğu davetsiz misafir olağanüstü hedefleri seçmez. Onlar sadece girebildikleri kadar fazla makineye girmeye çalışırlar. Onlara göre, küçük işletmeler ve ev makineleri

kolay hedeflerdir. Buralarda muhtemelen çok fazla beklemeler fakat zorla makinelere girmeye kalkışabilirler ve izlerini kaybettirmeye çalışırken de makinelere zarar verebilirler.



İnternete bağlı herhangi bir ağda işlev görmek için, bir site en az minimum miktarda kayıt tutmalıdır ve bu kayıt bilgilerinin çoğu da herhangi birine sadece soru için açıktır. Bir site, ağda her zaman servisleri kullanır ve herhangi birisi onların orada olduğunu bilebilir. Davetsiz misafirler, bazı sitelerin güvenlik ölçeklendirmelerinin olmaması ümidiyle yeni bağlantıları izlerler. Bazı siteler görünüşe göre yeni site kayıtlarında temel olan otomatik araştırmalar raporlarlar.

Bazı insanların güvenlik duyarlı sitelerinin tanımlamak için ne kadar yol olduğu insanları muhtemelen çok şaşırtmaktadır. Örneğin; hangi donanım ve yazılımların kullanıldığını, hangi sürüm işletim sisteminin çalıştığını bilmekle, davetsiz misafirler ne tür güvenlik deliklerini kullanabilecekleri hakkında önemli ipuçları elde ederler. Bu bilgileri genelde host kayıt işlemleriyle veya bilgisayara bağlanmaya çalışarak elde ederler. Çoğu bilgisayar kendisine bağlanılmadan önce üzerindeki işletim sistemi tipini açığa vurur. Böylelikle davetsiz misafir içeri girmek ihtiyacı hissetmez.

Davetsiz misafirlerin çok zamanı vardır ve bütün olasılıkları deneyerek bilinmeyen sistemler hakkında bilgi elde etmeye çalışırlar. Uzun vadede, kapalılığa bel bağlamak akıllıca bir güvenlik seçimi değildir.

3.5.3. Host Güvenliği

Muhtemelen en genel güvenlik modeli host güvenliğidir. Bu modelle, her host makineye ayrı ayrı güvenliği sağlanır ve her çapadan kaçınılır veya özel bir host'un etkileneceği tüm güvenlik problemleri hafifletilir. Host güvenliğinde yanlış olan taraf; kişisel bilgisayarlarda çalışmaması değil, çok fazla makineye ölçeklendirilememesidir.

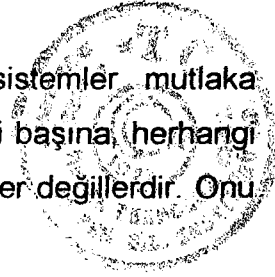
Gelişmiş bilgisayarlılık ortamında etkili host güvenliğinin en büyük engeli karmaşıklık ve o ortamın farklılığıdır. Çoğu gelişmiş çevreler, her makinenin kendi işletim sisteminin ve kendi güvenlik probleminin olduğu değişik satıcılardan alınmış makineler içerir. Bir sitenin bilgisayarları tek bir satıcıdan alınmış olsa bile, aynı işletim sisteminin değişik sürümlerinin önemli ölçüde değişik güvenlik problemleri bulunur. Bütün makineler tek bir satıcıdan ve işletim sistemleri de aynı sürümü içerseler bile, farklı konfigürasyonlar(farklı servisler kurulu olduğundan dolayı) değişik alt sistemleri ortaya çıkarırlar ve farklı güvenlik problemlerinin olmasına sebep olurlar.

Ve tüm makineler mutlak olarak aynı olsalar da, bazı sitelerde az sayıda makinenin hepsinin güvenliğini sağlaması zor olur. Öndeki ve çalışan önemli bir miktarı etkili olarak çalışır ve host güvenliği sağlayabilir. Tüm işler doğru yapılmış olsa da, satıcı yazılımlarındaki böcekler(bug) veya bazı işlevler için uygun güvenlik yazılımının olmayışından dolayı host güvenliği başarısız olabilir.

Host güvenliği herhangi bir makineye erişen herkesin becerisine ve iyi niyete bağlıdır. Makine sayısı artarken yetkili kullanıcı sayısı da artar. Bir makinenin güvenliğini sağlamak onu bir ağı bağlamaktan çok daha zordur. Böylece güvenli olmayan makineler ağıda beklenmeyen sürprizler olarak ortaya çıkabilirler. Herhangi birine danışılmadan makine satın almak veya iletişim kurmak ihtimali beklenmesi gerçeği önemsizdir. İnsanlar eğer ihtiyaç hissederlerse doğru olarak ödüyormuş bilgi buluşları ve ağ iletişim entrikaları geliştirebilirler.

Bir host güvenliği modeli, küçük sitelere veya son derece iyi güvenlik gereksinimleri olan siteler benzerler. Gerçekte, tüm siteler kendi güvenlik planlarına host güvenliği seviyeleri dahil etmelidirler. Eğer bir sonraki konuda anlatılacak olan ağ güvenliği benimsenirse konfigürasyondaki kimi sistemler en güçlü host güvenliğinden yarar sağlayacaklardır. Örneğin; eğer dahili ağ ve sistemlerin etrafında bir güvenlik duvarı kurulmuşsa, host güvenliğine

ihtiyaç duyacak dış dünyaya karşı korumasız olan sistemler mutlaka olacaktır. Buradaki problem ise host güvenlik modeli kendi başına, herhangi bir fakat küçük veya basit siteleri koruyan fiyat etkili modeller değildir. Onu çalışır halde tutmak çok fazla sınırlama ve insan gerektirir.



3.5.4. Ağ Güvenliği

Çevrenin genişlemesinden, çeşitliliğinin artmasından ve bu ortamın host temelli güvenliğini sağlamanın daha fazla zorlaşmasından dolayı, çoğu siteler ağ güvenliği modeline geçmektedirler. Ağ güvenlik modeli ile çeşitli host'lara ve sağladıkları servislere erişim; ağ kontrolü hepsini ayrı ayrı korumak yerine tek noktada toplanır. Ağ güvenlik yaklaşımları, kuvvetli gerçekleyici yaklaşımları(bir defa sorulan şifreler gibi) ve özellikle hassas verileri şifreleme teknikleriyle koruma yaklaşımları kullanarak dahili sistemleri ve ağları korumak için güvenlik duvarları içerirler.

Bir site ağ güvenlik modelini kullanarak güvenlik çapalarından büyük bir güç elde ederler. Örneğin; bu çalışmada anlatılacak olan tek bir güvenlik duvarı ile ağdaki yüzlerce, binlerce hatta milyonlarca makine korunabilir. Hem de kişisel makinelerin host güvenlik seviyesi ne olursa olsun. Fakat bu host güvenliğini hafife almak demek değildir. İyi bir host güvenliği ölçeklendirmesi ile internete bağlı önemli makineler direkt olarak korunabilirler. Host güvenliği dahili makinelerde korunma sağlamak ve internetten gelen saldırılar haricindeki güvenlik problemlerinde kullanılabilirler.

3.5.5. Güvenlikte Belirlenmesi Gerekli İşlemler

1. Güvenlik Politikasının Belirlenmesi

Gerçek güvenlik, ağ tasarımı, bilginin gizlilik derecesini ve kullanıcı hakları ile uygulama sınırlarını hesaba katan sağlam bir güvenlik politikası ile

başlar. Politika, güvenliğin temelini oluşturur, zira kurumun önemli gördüğü ve korunması gerekli bilgileri tehdit eden hareketleri belirler. Güvenlik politikasının oluşturulmasında sorulacak temel sorular şunlardır:

- Kime, nereye, ne zaman, nereden ve hangi yetki ile izin verilecektir ?
- Hangi aktiviteler tehdit olarak görülüyor ve güvenlik riski oluşturuyorlar?
- Ne tip gözden kaçmalar ve dikkatsizlikler olabilir?
- Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?

Dış ve iç güvenlik için problem yaratan ağ sistem zayıflıkları:

- **Protokoller:** Bilgisayarlar, bilgisayar ağları aracılığı ile haberleşirler. Bu haberleşmenin temel alt yapısını protokoller oluşturur ve bir kurumun bilgisayar ağı içinde birden fazla protokol kullanılabilir. Protokollerin yapıları gereği saldırganların kullanabileceği pek çok delik bulunabilir.

- **Yazılım:** Protokollerin dışında, işletim sistemleri, bilgisayarlar, ağlar arasında, kısaca tüm bilgisayar ağ işlemi yürüten yazılımlar da bu tip saldırılar için zayıf noktalardan biridir.

- **Kuruluş:** Kuruluştaki kusur genellikle donanım ve yazılımların etken olarak nasıl kullanılabileceğinin bilinmemesinden kaynaklanmaktadır.

2. Fiziksel Güvenlik

Belki de en önemli güvenlik konularından biridir. Kullanmakta olunan ağın fiziksel olarak güven altına alınması gerekmektedir. Zira fiziksel olarak tahrip edilmiş ağ da artık güvenlik diye bir sorun kalmayacaktır.

3. Erişim Kontrolü

Güvenlik duvarının en önemli görevlerinden biri ağımıza girmek üzere baş vuran her paketin içeri alınıp alınmayacağına karar vermesi yanında,

hangi uygulamanın bizim için daha doğru olacağına karar vermesidir. Başka bir deyişle güvenlik duvarı dışardan gelen bir paketlerin oturum isteklerinin belirlenen güvenlik politikalarına uygunluğunu belirler. Böylece dışarıdan ağa bağlantılarda ağ protokolleri, yazılımlar, ağ yapısındaki eksiklikler ve hatalar ve problemlerden kaynaklanan erişim kusurlarını kullanarak yetki alan saldırganları engellemeye çalışır.

4. Kimlik Onaylama

Bu işlem yetkili kişi ve bölümlerin serbestçe haberleşmelerini sağlarken, saldırganların erişimini engeller. Kullanılan onaylama yöntemi kullanıcının nereden ve nasıl onaylandığına bağlıdır. İnternet ve diğer uygulamalar için en popüler onaylama yöntemleri 'neredeler , neleri var ve ne biliyorlar'dır. Ancak IP adres onaylaması veya neredeler yöntemi, IP adres sahtekarlığı(spoofing) kullanılarak kolayca alt edilebilmektedir.

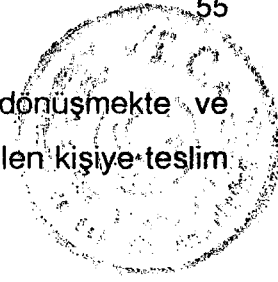
5. Şifreleme

Bu yöntem veri bütünlüğünün garantilenmesinde en güçlü koruma yöntemlerinden biridir. Eğer şirket bilgilerine uzaktan erişim söz konusu ise veya şirket intranetini kullanılıyorsa, ağda ek bir koruma sağlamak üzere şifrelemeyi kullanmada büyük yarar olacaktır. Ancak şifrelemede en önemli bağlantı noktası anahtarlardır. Bunlar verilerin şifrlenmesi ve açılmasında kullanılır. Ancak bu anahtarların nasıl yönetilecekleri çok büyük bir önem taşımaktadır ve çok sayıda bağlantılar için otomatik anahtar yöntemi kullanılması gerekmektedir.

Şifrelemenin Esasları

İki nokta veya iki kişi arasında haberleşmenin en güvenli yolu şifrelemedir. Şifreleme çok eski zamanlardan beri haberleşmede kullanılmış ve bugün artık bilgisayar iletişiminde de yaygın olarak kullanılabilir hale gelmiştir. Bir kullanıcının göndereceği açık ileti (Cleartext Message) şifreleme

tekniki kullanarak şifrelenmiş iletiye(Ciphertext Message) dönüşmekte ve iletilmektedir. Karşı sistem bunu çözmekte ve iletilmesi istenilen kişiye teslim etmektedir.



Şifreleme bir matematiksel algoritmaya dayalı olarak iletinin anlaşılabilir bir forma değiştirilmesini sağlar. Temelde bu tip matematiksel algoritmalar, şifrelemeyi yapabilmek için bir anahtar seçimine gereksinim duyarlar. Bu anahtar düzeyinde açık ileti kodlanarak çözülmesi zor bir hale dönüştürülür. Şifreleme algoritmaları iki grup altında toplanırlar:

- **Simetrik Algoritmalar:** Bu modelde şifrenin hazırlanması ve çözülmesi için aynı anahtar kullanılır. Bu tip algoritmalar gizli anahtar algoritması diye de adlandırılırlar. Başka bir deyişle şifreli iletinin çözülebilmesi için alıcının, kullanılan anahtarı daha önceden bilmesi gerekir.

- **Asimetrik Algoritmalar:** Bunlar Anonim Anahtar(Public Key) Algoritmaları diye de anılırlar. Bunlarda şifreleme için kullanılan anahtarlar ile şifre çözümünde kullanılan anahtarlar farklıdır. Bu nedenle bu algoritma tipinde şifreleme için kullanılan anahtar bilinse dahi (zaten bu anahtar açıktır ve herkez tarafından kolaylıkla öğrenilebilir), bu anahtarı kullanarak şifreyi çözmek için kullanılan anahtarı elde etmek olanaksızdır. Böylece anonim anahtarlar ile şifrelenen bilgiler ancak özel anahtar(Private Key) ile açılabilir.

Bu tip algoritmalarda özel anahtarla şifrelenen iletilerin anonim anahtarlar ile çözülme zamanı, simetrik algoritmalarinkine kıyasla çok daha uzundur. Bu zaman, ileti uzunluğu ile üssel olarak artar.

Bu nedenle anonim anahtar yöntemi birçok uygulamada simetrik şifreleme yöntemi ile birlikte kullanılır. Örneğin elektronik postaların şifrelenip gönderilmesinde en yaygın kullanılan yöntemler hem simetrik hem de asimetrik yöntemleri içerenlerdir.[Manas, Prof. Dr. Oğuz, Güvenlik Duvarları, BT/Haber 1998.]

6. İzleme

Güvenlik politikasının belirlenmesi ve uygulamaya başlanmasından sonra bütün sistem parçaları ve personelin güvenlik politikasına ne dereceye kadar bağlı kaldıklarının çok dikkatli bir şekilde izlenmeleri gerekir. Denetimin yapılması hem problemlerin doğmasını engelleyecek hem de eğer bir güvenlik sorunu doğarsa gerekli bilgi elde hazır olacaktır.

7. Güvenlik İçin Özet Adımlar

Güvenlik hangi methodla sağlanmaya çalışılırsa çalışılsın her güvenlik için belirlenmesi gereken olmazsa olmaz denebilecek olan şartlar vardır. Bu şartların yerine getirilmemesi güvensizlik anlamına gelmemekle beraber istenilen kalitede güvenlik için önceden belirlenmelidirler. Bunlar;

- Önce güvenlik derecelerinin belirlenmesi;

Güvenlik konusu	Yüksek	Orta	Düşük
İstenmeyen ziyaretçilerin intranete erişimi			
Mahrem veriler			
Virüslerden korunma			
İç verilerin içerde tutulduğundan emin olmak			
Rekabetçilerin verilere erişimi			
İçerden gelebilecek istenmeyen erişimler			
Diğer			

Çizelge 3.1. Güvenlik dereceleri belirleme

- Sonra bu güvenlikleri sağlamak için gerekli işlemlerin belirlenmesi;

Güvenlik için önlemler	Evet	Hayır
Veri şifrelemesi		
Güvenlik Duvarları		
Sunucu Mirorlanması		
Şifreli koruma		
Kuralların korunması için gerekli duyurular		
Diğer		

Çizelge 3.2. Güvenlik için gerekli işlemler

3.6. Güvenlik Stratejileri

Güvenlik duvarlarını tartışmaya başlamadan önce, güvenlik duvarı geliştirmede ve site güvenliğinde kullanılan bazı temel stratejileri anlamak çok önem arz etmektedir. Bunlar insanı şaşırtan ifadelerin açığa vurulması değil, sadece doğruların yaklaşımıdır.

3.6.1. En Az Yetki(Least Priviliage)

Belki de en temel güvenlik prensibi ki bu sadece bilgisayar veya ağ güvenliği değil, her türlü güvenliği içeren en az yetkidir. En az yetki demek ise kullanıcı, yönetici, program, sistem vs. gibi bir nesnenin görevini yerine getirmek için sadece gerekli yetkileri kullanması daha fazlasını kullanmaya yetkili olmamasıdır. En az yetki, saldırılara karşı korunmasızlığı ve özel saldırıların verdiği zararları en aza indiren önemli bir ilkedir.

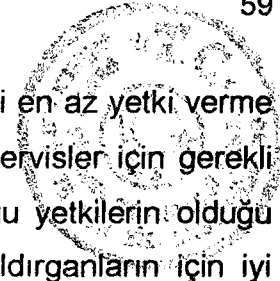
İnternette her kullanıcının muhtemelen tüm internet servislerine erişmeye ihtiyacı yoktur. Her kullanıcı bir sistemdeki her dosyaya erişip onlarda değişiklik yapmak durumunda değildir. Ayrıca makinelerin en yetkili kullanıcı(root) şifrelerini bilmek zorunda da değildir. Yine her sistem tüm diğer sistemlerin dosyalarına erişmek durumunda değildir.

En az yetki ilkelerini uygularken her iş için gerekli yollar ve yetkiler belirlenir ve bunlar çerçevesinde görevler yerine getirilir. Örneğin: Yazdırma sistemini başlatan birisine asla en yetkili kullanıcı (root) şifresi verilmemelidir. Bunun yerine yazdırma sistemini yeniden başlatmaya yetkili bir program yazılabilir.

Tüm yaptığı iş korunan bir dosyaya yazmak olan bir programın kullanıcı tanımını en yetkili kullanıcı yapmamalıdır. Bunun yerine o dosyaya bazı gruplara yazma yetkisi verilmeli ve o programın o grup tarafından çalıştırılması sağlanmalıdır.

Dahili sistemlerin güvenlik duvarı makinelerinin herhangi birisine sadece yedekleme yapabilmesinde güvenmemelidir. Bunu yerine güvenlik duvarının dahili sisteme güvenmesi sağlanmalıdır veya güvenlik duvarı makinesine yerel bir yedekleme ünitesi(teyp sürücü) takılmalıdır. Böylece o kendi yedeklerini alabilir.

İnternetteki en çoğu yaygın güvenlik problemlerinin en az yetkinin takibindeki başarısızlıklardır. Örneğin; büyük ve karmaşık olan bir posta gönderme programında bir böcek(bug) olsun. Bu program posta gönderirken kendi yetkisini en yetkili (root) seviyesine çevirdiği varsayılırsa, bu anda posta gönderme programına birçok saldırı avantaj sağlayabilir. Çünkü root olarak çalışmaktadır. Posta gönderme saldırganların çok dikkatini çeken yüksek değerli bir hedeftir. Bu tür kompleks programlar yetki gerektirdikleri zaman, bu programı karışık parçalardan yetki ihtiyacı olan parçalara ayırma ve parçaları izole etme yolları aramalıdır.



Siteleri korumak için kullanılan birçok çözüm yöntemi en az yetki verme taktiğidir. Örneğin; bir paket filtreleme sistemi istenilen servisler için gerekli paketlere izin verir. Programların mutlaka gerek duyduğu yetkilerin olduğu çevre birimlerinde güvensiz programları çalıştırmak saldırganların için iyi birer hedef oluştururlar. Bu yüzden yetki olması gereken yerde güvenlik olmazsa oradaki yetki karşı saldırı için kullanılabilir.

En az yetkiyle donatmada iki problem vardır. Birincisi, kullanılan programların ve protokollerin tasarım özelliği olmadığı zaman en az yetkiyi uygulamak kompleks olabilir. En az yetkiyi devreye sokmakla doğruyu elde etmek çok zor olabilir. Örnek olarak; birisine arabanızı belli bir süre kullanmak için vermiş olabilirsiniz. Ve arabanızın benzin deposunun kapağı açılması için anahtar gerekmiyor. Sadece araba içerisinde bir kontrolle açılıyor. Verilen kişi de bunu bilmiyor. Çünkü bir yerde belirtilmemiş. Bu durumda arabaya gerektiğinde benzin koyması onun için karmaşık bir hal alabilir. İkinci olarak, herhangi bir uygulama en az yetkiden de daha az olarak uygulanabilir. Bu durumda da arabanın benzin depo kapağı ise anahtarla açılıyor. Araba verilirken o kişiye depoya benzin koyması söylenmiş fakat bu arada anahtarı verilmemiş. Bu kişi benzin doldurmaya çalışırken kendisine anahtarın verilmediğinin yani deponun kullanma hakkına sahip olmadığına farkına varır. Bu da en az yetki verirken gerektiğinden az olduğunu gösterir.

3.6.2. Derin Savunma(Defense in Depth)

Diğer bir güvenlik stratejisi ki yine herhangi bir güvenlik için, derin savunmadır. Tek bir güvenlik mekanizmasına bağlı kalınmamalıdır. Bunun yerine daha güç görünse de birden fazla mekanizma kurulmalıdır. Herhangi bir tek güvenlik mekanizmasının çökmesi, olduğu gibi bir sitenin çökmesi demektir ki bu da o sitenin prestijini sarsar. Genelde her evin kapısında bir kilitle beraber bir zincir veya başka bir kilit vardır. Aynı şekilde çoğu arabada kilitten başka alarm sistemleri de mevcuttur. Bu da tek güvenlik yerine birden fazla güvenliğin daha etkili olduğundadır. Çalışmada anlatılan konu güvenlik duvarları olmasına rağmen güvenlik duvarları internet güvenlik problemlerine

tam bir çözüm sağlamazlar. Gerekli riski ve gücü riske eden bir kişi herhangi bir güvenliği aşmayı başarabilir. Buradaki ipucu, saldırı hareketini saldırgan açısından çok riskli veya çok pahalı hale getirmektir. Bu da yedekleme ve gerekli olan çoklu savunma mekanizmalarını bir araya getirerek yapılabilir. Bunlar da ağ güvenliği(güvenlik duvarı), host güvenliği(özellikle bastion host) ve insan güvenliği(kullanıcı eğitimi, dikkatli sistem yönetimi, vs.) gibi yöntemler olabilir. Tüm bu mekanizmalar önemlidir ve güvenlikte çok etkili olabilirler. Fakat tüm inanç onlara bağlanmamalıdır.

3.6.3. Boğum Noktası(Choke Point)

Boğum noktası, saldırganları, denetleme ve kontrol edilebilen dar bir kanal kullanmaya zorlar. Hayatta boğum noktasına örnek olabilecek çok örnek vardır: köprülerde ücret ödeme turnikeleri, süper marketlerde ödeme yerleri, sinemalarda bilet gişeleri gibi.

Ağ güvenliğinde site ile internet arasındaki güvenlik duvarı (burada site ile internet arasında sadece bu bağlantının olduğu varsayılıyor) boğum noktası gibidir. Bu arada internetten gelebilecek saldırılar, bu saldırılara karşı savunma görevi üstlenecek kanal boyunca gelmek durumundadırlar. Bu tip saldırılar bu durumda dikkatle izlenebilir ve görülebilirlerse bu saldırılara cevap da verilebilir.

Boğum noktası, eğer bir saldırgan onu aşacak etkili bir yol bulduğunda kullanışsızdır. Eğer bir evde arka tarafta mutfak kapısı açıksa, neden daha da güçlendirilmiş ön kapıyı zorlama zahmetine girilsin ki. Bu durumda her saldırgan mutfak kapısını dener. Benzer şekilde olaya ağ güvenliği olarak bakılırsa, eğer saldırabilecek ve başarılı olunabilecek yüzlerce telefon hattı varsa neden güvenlik duvarına saldırılsın ki!

Bir boğum noktası tüm yumurtaları aynı sepete koymaya benzer. Bu ilk bakışta kötü bir fikir gibi olsa da buradaki püf noktası o sepet dikkatle korunabilen bir sepet olur. Alternatif yol ise dikkati diğer bir çok saldırı üzerine

dağıtmaktır. Bu yolla her tür saldırıya karşı savunma yapacak tam bir koruma yapılamaz ve birini savunurken diğerinden gelen saldırılar başarılı olabilir.

3.6.4. Güçsüz Bağlantı(Weakest Link)

Güvenliğin temel bir prensibi bir zincirin en zayıf halkası kadar ve bir duvarın da en zayıf noktası kadar kuvvetli olmasıdır. Akıllı saldırganlar bu noktalardaki zayıflıkları keşfeder ve buralardan saldırmada ısrar ederler. Bu zayıf noktaların bulunup elenmesiyle ancak saldırılara karşı güçlü bir güvenlik sağlanabilir.

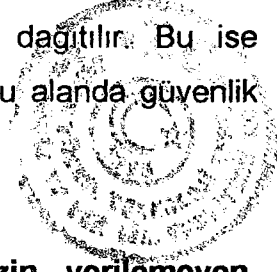
3.6.5. Güvenli Başarısızlık Durumu(Fail-Safe Stance)

Güvenliğin diğer temel prensibi, sistemlerin mümkün olabilen en kapsamlı bir şekilde emniyete sahip olmalarıdır. Yani sistemler başarısız olurlarsa, öyle bir yolla başarısız olmalı ki bu saldırganlara izin verici değil engelleyici olmalıdır.

Güvenli başarısızlıklar, alışık olunan geniş uygulamalarla diğer bir prensiptir. Elektrik cihazları herhangi bir başarısızlık durumunda kapanmalarına yönelik tasarlanmışlardır. Örnek olarak; asansörler herhangi bir elektrik güç kesilmesi durumunda fren sistemini devreye sokarlar, elektrikli kapı kilitleri de elektrik kesilmesi durumunda insanların binalarda mahsur kalmamaları için kilit özelliğini iptal ederler.

Çoğu uygulama güvenli bir şekilde başarısız olur. Örneğin, bir paket filtreleme yönlendirici(router) başarısızlık durumunda herhangi bir paket geçişine izin vermez. Eğer bir vekil(proxying) program bozulursa artık herhangi bir servis sağlamaz. Diğer yandan, bazı paket filtreleme sistemleri paketlerin, paket filtreleme uygulamasının çalıştığı ve parçalı olarak servis veren bir makineye iletilmesine izin verirler. Bu yol bazı sistemlerde çalışır. Eğer paket filtreleme uygulaması bozulur veya makine açılış sırasında

çalışmazsa paketler uygulamalara sağlanan servislerle dağıtılır. Bu ise güvenli başarısızlık durumu değildir ve engellenmelidir. Bu alanda güvenlik kararlarına uygun olan iki temel durum vardır:



1. Varsayılan Engelleme Durumu: Özellikle izin verilemeyen, yasaklanmıştır.

Bu yöntem güvenli başarısızlık olarak görüldüğü için kullanılır. Bilinmeyen zarar vereceği teorisi üzerine hareket eder. Bu yöntemle ilk olarak her şey engellenir. Daha sonra neye izin verileceği belirlenir ve sadece izin verilen servisler çalışır. Bunun için;

- Kullanıcıların istediği servisleri incelenir.
- Bu servislerin güvenlik durumları iyice düşünülüp araştırılır.
- Sadece anlaşılan, güvenli sağlanabilen ve gerçekten ihtiyaç olan servislere izin verilir.

2. Varsayılan İzin Durumu: Özellikle yasaklanmayana izin verilir.

Çoğu kullanıcı ve yöneticiler varsayılan izin durumunu tercih ederler. İlk önce her şeye izin verme ve hassas, belirli, sorun çıkaran hareketleri ve servisleri engelleme gerekliliği eğilimindedirler. Örneğin;

- NFS' e güvenlik duvarı vasıtasıyla izin vermemek
- WWW'nin güvenlik problemleri hakkında eğitim almış ve farkında olan kişilere bu servise erişimi kapatmak.
- Kullanıcılara yetkili olmadıkları sunucularda herhangi bir ayar yapma izni vermemek.

3.6.6. Yaygın Katılım(Universal Participation)

Tam olarak etkili olmak için, çoğu güvenlik sistemleri bir sitenin personelinin yaygın katılımını gerektirir. Eğer birisi basitçe güvenlik mekanizmalarından çekinirse, bir saldırgan güvenlikten hariç tutulmuş bu

kişinin sisteminden bu kişiye saldırabilir ve daha sonra onun makinesinden yani içerden tüm siteye saldırabilir. Örneğin; eğer bir sitede bir kişi güvenlik duvarından kaçınmak için, güvenlik duvarını sitesi ile internet arasında arka-kapı bağlantısı yapan saçma bir yük olarak görüyorsa, bu güvenlik duvarı dünyadaki en iyi güvenlik duvarı bile olsa siteyi koruyamaz.

Daha fazlası sıradan isyan biçimleri güvenliğin yıkılmasına neden olur. Güvenlikle ilgili olabilecek her türlü tuhaf olayların rapor edilmesi gerekir. Sonuçta her şey görülemez. İnsanların iyi şifre seçmeleri, onları düzenli olarak değiştirmeleri ve arkadaşlarına, akrabalarına vs. vermemeleri gerekmektedir.

Peki herkesin katılımı nasıl sağlanabilir? Katılım herkesi bunun iyi bir fikir olduğuna ikna etmekle gönüllü, uygun yetkili ve güçlü birisinin işbirliği ile gönülsüz veya bu ikisinin karışımı şeklinde olabilir. Belli ki gönüllü olan katılım gönülsüzce yapılabileceğine göre kuvvetle tercih edilmelidir.

3.6.7. Savunma Değişimi(Diversity of Defense)

Nasıl derin güvenlik sağlamak için farklı sistemleri kullanarak ek güvenlik sağlanabiliyorsa, farklı tipteki sistemler kullanılarak da ek güvenlik sağlanabilir. Eğer kullanılan tüm sistemler aynı ise bunlardan birisine girmeyi bilen bir kişi muhtemelen tümüne birden girmeyi bilir.

Savunma değişiminin ardındaki fikir, farklı üreticilerin güvenlik sistemlerini kullanmaktır. Bu genel bir hatanın tüm savunma sistemini etkilemesini önler. Farklı savunma sistemlerini sağlamak ve kurmak, daha zor olacak, kurması daha uzun zaman alacak ve tek bir sistemi veya benzer sistemleri alıp kurmaktan çok daha pahalı olacaktır. Bunun için birden fazla sistem satın alınması ve desteklenmesi gerekecektir. Ve ayrıca bu sistemleri öğrenmek ekibin ayrı bir zaman ve çaba harcamasını gerektirecektir.

3.6.8. Basitlik veya Sadelik(Simplicity)



Basitlik iki sebepten dolayı güvenlik stratejisidir.

- Nesneleri basit tutmak onları kolayca anlamayı sağlar. Eğer herhangi bir şey anlaşılmıyorsa, onun gerçekte güvenli mi değil mi olduğu bilinemez.
- Komplekslik, kuytu yerler her çeşit nesnenin saklanması sağlar.

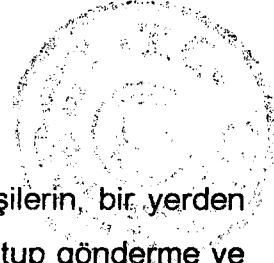
Kompleks programların daha fazla hatası vardır ve bu hatalar güvenlikle ilgili de olabilir. Hata olmasa veya bunlar güvenlikle ilgili olmasalar bile, bir defa insanlar verilen sisteme kararsız davranmakta ümitli oldular mı, onların tanıma ümitlerini öldüren ve bu problemler ortaya çıktığında güvenlik problemlerini rapor eden o sistemden hemen her şeyi kabul ederler.

3.7. İnternet Servisleri

İnternet servisleri, internet üzerinden değişik amaçları yerine getirmek için sağlanan servislerdir. Bu servisler mutlak bir korunma gerektirirler. Çoğu sitenin desteklediği ve hemen her internet kullanıcısının yararlanmak istediği standart servisler vardır. Gerçekte bu servisler olmadan internete bağlı olmanın da bir anlamı yok gibidir. Fakat bu servisleri kullanmanın da getirdiği potansiyel güvenlik problemleri vardır.

Gerçekte bu servislerin hiçbiri güvenli değildir. Her biri kendisine has zayıf güvenlik önlemlerine sahiptir ve bunlar değişik saldırılar karşısında altüst olabilirler. Kullanıcılara bir servis hizmeti sağlanmaya başlamadan önce o servisin kullanıcılar açısından önemi ortaya konmalı ve tehlikelere karşı ne gibi güvenlik önlemleri alınacağı belirlenmelidir. Bu servislerin miktarı çok olduğundan, sadece standart olarak kullanılan baş servisler hakkında bilgi verilecektir.

3.7.1. Elektronik Posta(E-Mail)



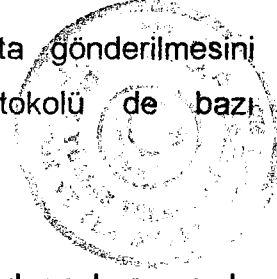
Bilgisayar ağlarının oluşturulma nedenlerinden biri, kişilerin, bir yerden diğerine hızlı ve güvenli bir şekilde elektronik ortamda mektup gönderme ve haberleşme isteğidir. E-posta(elektronik posta), bu amaçla kullanılan servislere verilen addır. İnternet ve diğer ağlar üzerinde kullanılan pek çok e-posta sistemleri mevcuttur. Bunlardan bazıları;

- SMTP (Simple Mail Transfer Protocol, Basit Posta Transfer Protokolü)
- IBM PROFS (Professional Office System, Profesyonel Ofis Sistemi)
- SNADS (SNA Distributed Systems, SNA Dağıtık Sistemleri)
- VaxMail

Standart SMTP, bir mektup gönderildiğinde bu mektubu, gideceği yere ulaşana dek yönlendirerek iletir(routing). Eğer mektubun son varış noktasına ulaşamıyorsa(bağlantı kopukluğu) SMTP daha sonraki bir zamanda aynı mektubu tekrar göndermeye çalışır. Eğer uzun bir süre sonra mektup hala gönderilememişse göndericiye bir hata mektubu ile birlikte mektubu geri gönderir. Bunun önüne geçmek için kullanılan sisteme POP(Post Office Protocol, Posta Ofisi Protokolü) ya da şu anki haliyle POP3 adı verilir. POP3 servisi bir posta kutusu vazifesi görür ve gelen mektupların gideceği yere aktarılması yerine bu kutuda tutulmasına imkan tanır. Daha sonra, kullanıcı bu POP servisine bağlanıp kendi mektuplarını kendi sistemine aktarır.

İkinci kullanım, mantık olarak yukarıdaki ile aynı olmasına rağmen işlevsel olarak farklıdır. Bu internet kişisel bağlantılarında karşımıza çıkar. Evden, işyerinden yapılan **SLIP/PPP** türü bağlantılarda gelen mektupları almak ve okumak için POP3'ü destekleyen e-posta programlarının(Outlook, Eudora, Netscape Mail vb.) kullanılması çok büyük avantajlar sağlar. Bu şekilde, bilgisayarın açılmasından sonra posta kutusundaki tüm mektuplar kısa sürede alınır, sonra bağlantı kapatılır ve mektuplar okunabilir. Bu zaman kazandırması açısından önemlidir.

Son zamanlarda, farklı sistemler arasında e-posta gönderilmesini sağlama için X.400 isminde bir mesajlaşma protokolü de bazı merkezlerde(özellikle Avrupa ve Kanada) kullanılmaktadır.



E-posta, başlangıçta sadece düz yazı mesajlar göndermek amacıyla geliştirilmişken, 1995'li yıllardan sonra geliştirilen tekniklerle, e-posta içinde kompozit yapıların (resim, ses, video, html dokümanları, çalışabilir program vb.) kullanımı mümkün hale gelmiştir.

E-postanın kullanım yerlerinden biri de e-posta tabanlı bilgi alma servisleridir. On-Line tarama yapmak yerine, bir e-posta mesajı içinde gerekli komutları vererek tarama yapmak ve sonuçları yine e-posta ile istemek bazı durumlarda çok kullanışlıdır.

3.7.2. Dosya Transferi:

1. FTP(File Transfer Protocol, Dosya Transfer Protokolü): İnternete bağlı bir bilgisayardan diğerine veya her iki yönde de dosya aktarımı yapmak için geliştirilen bir internet protokolü ve bu işi yapan uygulama programlarına verilen genel addır. İlk geliştirilen internet protokollerinden biridir. FTP protokolü ile bir bilgisayardan bir başka bilgisayara dosya aktarımı yapılırken, o bilgisayar ile etkileşimli aynı anda(on-line) bağlantı kurulur ve protokol ile sağlanan bir dizi komutlar yardımıyla iki bilgisayar arasında dosya alma/gönderme işlemi yapılır.

2. TFTP(Trivial File Transport Protocol, Basit Dosya Transfer Protokolü): Diski olmayan makinelerin dosya transferi yapmak için kullandıkları FTP protokolünün daha basitleştirilmiş halidir. O kadar basittir ki donanım olarak da uygulanabilir ve bu yüzden herhangi bir belgelemeyi desteklemez. Bir ağın dışına TFTP erişimi vermek için herhangi bir sebep yoktur. Alışıl gelmiş olduğu gibi zaten kullanıcılar dosyalarını genelde TFTP kullanarak transfer etmezler.

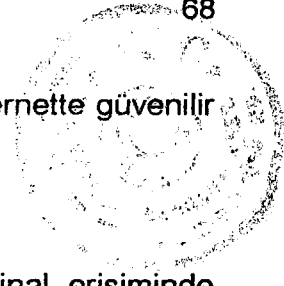
3. FSP(File Service Protocol, Dosya Servisi Protokolü): FTP'ye alternatif olarak geliştirilen bir protokoldür. FTP'ye olan en büyük üstünlüğü,yarıda kalan bir dosta transferi işlemine kaldığı yerden daha sonra devam edilmesine izin vermesidir. Hat hızları arttıkça bu protokol popülaritesini yitirmiştir.

4. UUCP(Unix-to-Unix CoPy, UNIX'ten UNIX'e Kopya): Modemler üzerinden kullanılan daha eski bir dosya transfer protokolüdür ve hala aralıklı internet bağlantısı yapılan Usenet haber ve posta transferinde kullanılmaktadır. Böyle siteler internete bağlandıkları zaman servis sağlayıcısından postaları almak için TCP protokolü üzerinde UUCP kullanırlar. Yaygın olduğundan beri çok az site dosya erişimi için anonim UUCP servisi sağlarlar. Bir dosya transfer protokolü olarak internet bağlantısı olmayan ve modem kullanan kişilerin ilgi alanına girer.

3.7.3. Uzaktan Terminal Erişimi ve Komut Çalıştırma

1. Telnet: İnternet ağı üzerindeki bir makineye uzaktan bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel bir addır. Bağlanılan makineye girebilmek(login) için orada bir kullanıcı isminin(user name) ve telnet erişim programının olması gerekir. Telnet erişim programları günümüzde işletim sistemlerinin çoğunda işletim sistemi ile birlikte gelmektedir. Tamamen bir terminal ekranı üzerinde çalışılır. Grafik değildir. Sadece karakter tabanlı uygulamalara erişimi sağlar. Telnet internete bağlı herhangi bir siteden belli bir hazırlık yapmadan uzaktan erişim sağlar. Telnet daha önceleri güvenli bir servis olarak algılanmıştır çünkü kullanıcıların kendilerini sisteme tanıtmaları gerekir. Yani sistemde tanımlı olmaları gerekir. Fakat telnet iki uç arasındaki verileri herhangi bir veri şifrelemesine tabi tutmadan gönderdiği için dinlenebilir ve korsan saldırılarına maruz kalabilir. Bu sebepten telnet şu anda uzak sistemlerden erişimde en tehlikeli servislerden biri sayılır. Telnet, ancak uzak makine, arasındaki tüm

ağ ve yerel makine güvenli ise güvenlidir. Bu da, telnetin internette güvenilir olmadığı anlamına gelir.



2. Rlogin, Rsh ve On: Telnet yanında uzaktan terminal erişiminde kullanılan programlardır. Bu programlar, tekrar kendini tanıtmayı gerektirmeden güvenilir birimlerde kullanılırlar. Bağlanılan makine, bağlantı kurulan makineden verilere güvenir. Güvenilir makine modeli internette kullanmak için tam uygun değildir. Çünkü bulunan ağın dışındaki ana makinelere genelde güven olmaz. Gerçekte, paketlerin belirttikleri yerden geldikleri konusunda emin olmak zordur. Bu servislerin, güvenlik duvarı tarafından korunulan bir ağ içerisinde dahili güvenlik politikasına bağlı olarak kullanılmaları daha uygun olabilir.

On ise, bununla birlikte tüm güvenlik kontrolünü istemci programa yerleştirir ve herhangi birisi bu kontrolleri es geçerek bu istemciyi kullanabilir. Bu yüzden güvenlik duvarı ile korunuluyor bile olsa yerel alan ağında bu programı kullanmak güvenilir değildir. Bu servisle, herhangi bir kullanıcı herhangi bir komutu başka bir kullanıcı olarak çalıştırılabilir.

3.7.4. Word Wide Web

WWW, Web, ya da W3 yazı, resim, ses, film, animasyon gibi pek çok farklı yapıdaki verilere kompakt ve etkileşimli bir şekilde ulaşmayı sağlayan bir çoklu hiper ortam sistemidir. Hiper ortam, bir dökümandan başka bir dökümanın çağrılmasına(navigate) olanak sağlar. Bu ortamdaki her veri, başka bir veriyi çağırabilir. Bu veri aynı doküman içinde başka bir yerde olabildiği gibi, fiziksel olarak başka bir yerde de olabilir. Bütün bu farklı yapıdaki veriler uygun bir standart ile bir arada kullanılıp bir Web Listeleyicisinde(Web Browser) görüntülenebilir. Web'in diğer bir işlevi de, ftp, gopher, news, wais gibi bazı internet servislerini kendi içerisinde barındırmasıdır.



Web sistemleri, kullanıcıları platformdan bağımsızdır. Bir Macintosh Pc ya da Unix Web Listeleyicisi aynı sayfaları, aynı şekilde alırlar. Sayfaların alındığı web servisleri de farklı bilgisayar platformlarında olabilir. Web yapısının bu kadar çok kabul görmesinin bazı sebeplerini sıralamak gerekirse:

- Herşeyden önce web, açık bir sistemdir. Platform, bilgisayar, işletim sistemi vb. bağımlı değildir.
- Web üzerinden pek çok bilgi kaynağına kolayca erişilebilir.
- Web uygulamaları geliştirmek ve bunları kullanıma sunmak çok kolaydır. Çoğu durumda, uzmanlık gerektirmez.
- Web ortamları son derece dinamiktir. Java ve ActiveX kullanarak, tamamen konfigüre edilebilir istemci uygulamaları geliştirmek mümkündür. Bir firma, Java kullanarak, ürün tanıtımları için dinamik bir şekilde kendiliğinden oluşan uygulamalar geliştirebilir ve sayfa içerikleri kendiliğinden değişebilir. Bir kullanıcı, isteğine bağlı bir şekilde, bağlandığı bir veri tabanından bilgileri istediği gibi farklı gruplarda isteyebilir(client side corporation).

3.7.5. HTTP ve HTML

Web'in en ilginç yönlerinden biri de çok basit olmasıdır. Bir web dökümanına ulaştığımızda herşey dört ana fazda gerçekleşir:

1. Bağlantı,
2. Ne istenildiğinin web servisine iletilmesi,
3. Cevap,
4. İlgili sayfaya yapılan bağlantının kesilmesi.

Bu ana safhalar, web üzerinde iletişimin kurallarını tanımlayan bir protokolü oluştururlar. Bu protokole de, HTTP(Hyper Text Transfer Protocol) denir. Bağlantı safhasında, web erişiminde kullanılan bir web listeleyici ilgili bilginin olduğu web servisine bağlanır. Bu servislere HTTP servisleri de denir. Bağlantı sağlandıktan sonra web istemci programı http servisine isteğini



bildirir. Bu istek, http, ftp, e-mail gibi bazı protokol kurallarını içerir ve bu işlemlere genel olarak navigate de denir. Bu isteği alan http servisi de istenilen işlemi yapar ve cevabı gönderir. Eğer istek gerçekleştirilemezse bir hata mesajı ile karşılaşılır. Son safhada ise http servisine yapılan bağlantı kesilir.

Web Listeleyicileri, navigate işlemini HTML(Hyper Text Markup Language) denen bir programlama dili yorumlayıcısı kullanarak yaparlar. HTML, ana hatları SGML(Standard Generalized Markup Language) ile belirlenmiş bir döküman formatlama dilidir. Bu dil, daha çok yazılı bir dökümanı formatlamak ve bir objeden başka bir objeye linkler sağlamak ile ilgili komutlar içerir.

Son yıllarda, HTML içinde, salt döküman formatlama dışında işler yapan CGI, Java, JavaScript gibi unsurlar da kullanılmaktadır. Ayrıca, 2.0'dan sonraki sürümlerde, tablo kullanımı, doldurulabilir form kullanımı, frame vb. gibi pek çok yenilik göze çarpmaktadır.

3.7.6. URL(Uniform Resource Locators)

URL, Web Browser'lar içinden bir web servisine ya da diğer bazı internet servislerine yönlendirme yapılabilmesini sağlayan bir komut formatıdır. URL'ler bir bakıma, internet üzerinde erişebileceğimiz servisleri belirtmek, tanımlamak için kullandığımız adreslerdir. Web Browser içinden Open URL ya da Open Location şeklinde bir seçenek üzerinden uygun URL satırları verilerek, web, ftp, news, gopher, wais, telnet erişimi yapılabilir. Unix için Lynx kullanarak, bu URL'ler bir parametre gibi verilir (lynx <URL satırı>) ya da ilk sayfadan GO seçilir. URL satırlarının genel formatı :

<servis>://<adres>[:port_numarası]/<dizin>/dosya_adi

şeklindedir. <servis> yerine web için http; gopher için gopher; wais için wais; haber grupları için news; telnet için telnet yazılmalıdır. Aşağıda bazı örnek kullanımlar gösterilmiştir [Akgül, Mustafa, İnternet ve İntranet; Araçlar ve Olanaklar 1997].

Web Erişimi: <http://www.tubitak.gov.tr/form/index.html>;

Gopher: <gopher://gopher.itu.edu.tr:70/11/inet-turkey>;

News: <news:comps.os.linux>;

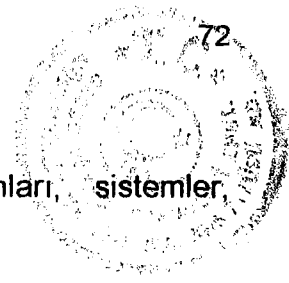
FTP: <ftp://ftp.metu.edu.tr/pub/mirrors/cica/winsock> (anonymous FTP);

URL satırlarına dikkat edilirse, http, gopher, news ve ftp şeklinde tanıtıcı kelimeler URL satırlarının başına gelmektedir. Bunlar, bağlanılacak servise yapılacak bağlantı türünü (ftp, telnet, web gibi) belirtir. //dan sonra gelen ise, bağlanılacak makina adı ve istediğimiz bilginin dizin/dosya adı bilgisidir.

3.7.7. Usenet

Usenet, dünya üzerindeki milyonlarca ağ kullanıcısının(internet/bitnet vb.) çok değişik konularda haberler, yazılar gönderdiği bir tartışma platformudur. Bu platform, konularına göre belirli bir hiyerarşide oluşturulmuş tartışma öbeklerinden (news group, haber grubu) oluşur. Kullanıcı, iletisini, içerik olarak en uygun öbeğe gönderir. Kullanıcıların gönderdiği postalar internet için, NNTP isimli bir internet protokolü kullanılarak iletilir. Bir kişinin gönderdiği ileti, hiyerarşik bir yapıda dağıtılır ve dünya üzerindeki internet erişimi olan kişiler tarafından bir Usenet servis sağlayıcısı aracılığı ile okunabilir. Usenet ileti trafiği internet hatlarının yanında, UUCP, BITNET bilgi hatları üzerinden de iletilebilir. Dolayısıyla, Usenet internete özgü değildir ama arakesiti büyüktür.

Usenet Servis Sağlayıcıları, diğer bazı Usenet servis sağlayıcılarına NNTP ile sık aralıklarla bağlanarak kendi merkezlerine yeni iletileri alırlar. Bir iletinin yeni olup olmadığı, mesaj numarasına bakılarak anlaşılır.



Usenet üzerinde olan bazı üst tartışma öbekleri;

- comp: Bilgisayar donanımı, bilgisayar programları, sistemler, programlama dilleri ve teoriler.
- sci: Doğal ve uygulamalı(mühendislik vb.) bilimler.
- soc: Sosyal konular, değişik kültürler ve ülkeler.
- talk: Pek çözölemeyen konularla ilgili oluşturulmuş öbekler.
- news: Usenet haberleri ile ilgili genel konular.
- misc: Diğer konular (işsizlik, çocuk bakımı, tüketici hakları, al-sat grupları vb).
- rec: Eğlence, hobi, spor, müzik, oyunlar vb.
- humanities: Edebiyat, güzel sanatlar ve benzeri konular.
- alt: Ciddi ya da çok sulu/gayrı ciddi hemen her konuda pek çok öbek.
- biz: Ticari ürünler, şirketler, servisler.
- clarinet: On-Line günlük gazete (ücretli)
- k12: İlk ve orta dereceli okullardaki eğitim ile ilgili konular.

3.7.8. İsim Servisi (DNS,Domain Name Service)

İsim servisi, insanların kullandıkları host makineleri ile makinelerin kullandıkları IP numara adresleri arasında çeviri yapan servistir. İnternetin ilk zamanlarında, sitelerin internet üzerinde kullanılan her makinenin isim ve numaralarını tutmak kolaydı. Fakat milyonlarca makinenin internete katılmasıyla bu artık imkansız hale geldi. Bunun yerine, DNS her siteye sadece kendi hostlarının bilgilerini tutmasına ve diğer sitelerin bilgilerini de bulmalarına izin verir. DNS, kullanıcı seviyeli olan bir servis değildir. Fakat SMTP, FTP, Telnet ve kullanıcıların kullandığı diğer görsel servislerin temelini oluşturur.

DNS servisi kullanmaktaki ana risk ise planlanandan daha fazla bilginin dışarı verildiğidir. Örneğin; DNS kullanılan donanım ve yazılım hakkında ve saldırganların bilmemesi gereken bilgiler ekler. Gerçekte, bir saldırgan tarafından, dahili makinelerin isimlerinin bilinmesi istenmez.



DNS'i dahili olarak kullanmak ve daha sonra bekleme için host isimlerine güvenmek, ortamı, gizli bir DNS sunucu kurabilen davetsiz bir misafir için korunmasız yapar. Bu bazı metotların kombinasyonu ile önlenabilir:

- Servislerde daha güvenli olma ihtiyacı olan belgelemede host isimlerinden çok IP adreslerini kullanmak.
- Çoğu güvenli servislerde hostların yerine kullanıcıların doğruluğunu kanıtlamak.

Her bir internet adresine dört haneli bir numara karşılık gelir. a.b.c.d şeklindeki bu numaralara IP numaraları denir. Burada; a, b, c, d 0-255 arasında değişen bir tam sayıdır. (32 bit adresleme sistemi). Örnek olarak titan.ehb.itu.edu.tr için bu numara 160.75.27.250 'dir.

Her internet adresinin ilk kısmı bulunduğu domain'in network adresini, son kısmı ise makinenin (host) numarasını verecek şekilde ikiye bölünür. Bir bilgisayar ağında bulunan makinelerin miktarına göre makine numarası için ayrılan kısmın daha büyük veya daha küçük olması gerekebilir. Değişik ihtiyaçlara cevap verebilmesi açısından IP adresleri aşağıdaki şekilde gruplanmıştır.

- Class A ağ adresleri 1.0.0.0 adresinden 127.0.0.0 adrese kadar olan aralığı kaplarlar. Her ağda kabaca 1.6 Milyon makine bulunabilir.
- Class B ağ adresleri 128.0.0.0 adresinden 191.255.0.0 adresine kadar olan aralıktadır. 16065 ağ adresi ve her ağda kabaca 65500 makine bulunabilir.
- Class C ağ adresleri 192.0.0.0 adresinden 223.255.255.0 adresine kadar olan aralıktadır. Her biri 254 makineden oluşan yaklaşık 2 milyon ağ adresi barındırır.
- Class D, 224 ve 254 arasında kalan adresler herhangi bir ağ tanımlamazlar, ileri kullanımlar için rezerve edilmişlerdir.

Bu domain adreslerinin dağıtımı ağ bilgi merkezi(NIC) tarafından yapılır, daha sonra her domain sahip olduğu adresi kendi ihtiyaçlarına göre

parçalararak dağıtabilir. Son zamanlarda, sınırlı sayıdaki internet adres uzayının bitebileceği düşüncesi ile, yeni bir adresleme stratejisine doğru da gidilmektedir.



Bu IP numaralarına karşılık düşen bir makine ismi de bulunur. Bu sayede makinelerin isimleri daha kolay akılda kalır. Her domainde o domaine ait IP numaraları ile bu isimler arasında geçişi sağlayan bir servis bulunur. Bu servis aynı zamanda diğer domainlere ait isimleri ilgili isim servislerine(DNS) sorarak öğrenir.

Örneğin; Class B ağ numarasına sahip 160.75.0.0 domaininde bulunan tüm IP numaraları 160.75. ile başlar. Dikkat edilirse bir host numarası 1 den 254 e kadar 254 farklı değer alabilir. Zira 0 ve 255 bu numaralandırmada özel anlamlar içerirler. 0(sıfır), ağı tanımlarken 255 de o ağdaki tüm hostları tanımlar. 127.0.0.1 adresi ve 127.0.0.0 ağı test ve geliştirme için kullanılır. 127.0.0.1 adresi her makinenin kendisini tanımlar buraya gönderilen her şey, sanki bir başka ağdan geliyormuş gibi o makineye geri dönecektir. Bu sayede herhangi bir ağ bağlantısı olmadan bazı denemeler yapılarak ağ yazılımları geliştirilebilir.

DNS, ayrıca, internet adresini nümerik adrese çevirir. Domainler hiyerarşik DNS adresleme sistemi içindeki farklı yapıları temsil ederler. Her domain kendi içinde bağımsız bir topluluktur. Doğal olarak, herkes kafasına göre geliş güzel internet domain ismi ve IP numarası alamaz. Ağ Bilgi Merkezi(NIC)'ne bunun için başvurmak gerekir.

3.7.9. Proxy(Vekil) Servisleri

Proxy servisi, internet üzerindeki yerel bir ağ ya da internete bağlı bir bilgisayar ile dış dünya arasındaki ilişkiyi sağlayan bir yardımcı geçiş (gateway) sistemidir. İki amaç için kullanılabilirler:



1. Bir proxy servisi (sunucusu), kişi adına kişiden aldığı internetten bilgi alma isteklerini yürütür ve sonucu yine kişiye iletir. Ancak, aynı anda, bu bilgilerin bir kopyası da (cache), bu proxy sunucusu üzerinde tutulur ve bir dahaki erişimde kullanıcının istediği bilgiler doğrudan ilgili siteden değil de, proxy servisinden gelir. Dolayısıyla, iletişim daha hızlı olur. İnternete erişim için mutlaka bir proxy servisine ihtiyaç yoktur, ancak, en yakın bir servis noktasındaki proxy servisinin kullanılması, internet erişimini bir hayli hızlandıracaktır. Özellikle evinden modemle internete erişenler için, proxy servislerini kullanmak performansı artırır. Çünkü, istenilen bilgiler, dış bağlantı hızı daha fazla olan proxy bilgisayarları kişi adına alır, kişi de kişisel bağlantıyla bu bilgilere daha hızlı erişmiş olur.

2. Güvenlik duvarı güvenlik sistemlerinin kullanıldığı yerlerde, kullanıcıları çıkışları tek bir makine üzerinden olabilir. Bu durumda proxy servis makinesi sadece bir aracı olarak çalışır.

Proxy servisi kullanmanın avantajı çoktur. Herhangi bir siteden istenilen bir bilgi (web sayfası, ftp dokümanı vb.) eğer kullanılan proxy servisinde henüz depolanmamışsa, bu bilginin olduğu siteden alınır ve kişiye iletilir. Ancak, daha sonra başka bir kullanıcı aynı bilgiyi istediğinde, ilgili doküman/bilgi proxy servisinde depolandığı(cache) için, doğrudan oradan kişiye iletilir ve erişim de çok daha hızlı olur. Proxy servisleri, uluslararası internet bağlantılarındaki yoğunluğu azaltmak, erişimleri hızlandırmak ve ağı daha etkin kullanmak için çok yararlı araçlardır.

3.7.10. Gerçek Zamanlı Konferans Servisleri

İnternette farklı sayıda gerçek zamanlı konrefans servisi bulunur. Bunlar; Talk, IRC(İnternet Relay Chat) ve MBONE(Multicast Backbone, çoklu yayın omurgası) üzerinden sağlanan çeşitli servislerdir. Tüm bu servisler insanların diğer insanlarla etkileşim kurmalarını sağlarlar. Elektronik posta, Usenet haberleri gibi servisler asenkron iletişim için tasarlanmışlardır.



Bunlar, kullanıcılar sisteme bağlı olduğunda etkileşim sağlanabilen servislerdir. Gelecek sefer tekrar sisteme girdiklerinde e-posta ve haber iletileri onları bekliyor olacaktır. Diğer yandan gerçek zamanlı konferans servisleri, on-line(hatta) olan kişilerin etkileşimi için tasarlanmışlardır.

1. Talk: İnternette kullanılan en eski gerçek zamanlı konferans sistemidir. Çoğu UNIX işletim sisteminde vardır ve iki kişinin konuşmasını sağlar. Bir kullanıcı <talk diğer_kullanıcı@host> komutunu kullanarak bu servise dahil olabilir. Diğer kullanıcının ekranında istekte bulunan kullanıcının mesajı belirir. Bu mesaj karşı kullanıcının talk yapmak istediğini ve nasıl karşılık verileceğini içerir.

Talk, kolej öğrencileri ve değişik sitelerde bulunan arkadaşlar arasında sıklıkla kullanılmasına rağmen internette yabancılar arasında yaygın olarak kullanılmaz.

Talk'ın kendisi için gerçekte herhangi bir ağ güvenlik suçlaması yoktur. Bu konudaki olumsuz yanı, güvenlik deliklerini kasıtlı olarak açmaksızın güvenlik duvarına erişim izni vermesi olabilir.

2. Internet Relay Chat (IRC): IRC, bir çok kişinin aynı anda etkileşimli mesajlarla haberleşebildiği bir platform ve bunu sağlayan programlara verilen genel addır. IRC'de, belirli bir konuda konuşmak, tartışmak isteyen insanlar kanal olarak adlandırılan ve genellikle bir konusu olan alanlarda toplanırlar. Birisinin yazdığı bir mesaj, o kanaldaki herkese iletilir.

IRC, ancak bir servis üzerinden kullanılır. Dünyada bir çok IRC servisi vardır. Bulunulan sistemden bu servislerden birine erişmek için, özel bir protokol kullanan IRC yazılımlarının sistemde yüklü olması gerekir. Bir IRC servisine bağlanmak için verilecek komut, genellikle <irc>'dir. Grafik ara birimli işletim sistemlerinde, menüler ve ikonlar üzerinden gidilerek bağlantı sağlanır. Bu programlara en güzel örnekler: Netscape Chat, Mirc, Virc vb.

IRC Servisi veren bütün siteler birbiriyle bağlıdır ve normal olarak, hangi IRC servisine bağlanırsanız bağlanın aynı kanalları görürsünüz. Ancak, bu global networke bağlı olmayan yerel IRC servisleri de olabilir.



3.7.11. Ağ Yönetim Servisleri

Ağları yönetmek ve bakımını yapmak için çeşitli servisler vardır. Bu servisleri çoğu kullanıcı direkt olarak kullanmaz. Bunların çoğu hiçbir zaman duyulmamış olabilir fakat ağ yöneticileri için çok önemli araçlardır.

En önemli iki ağ yönetim aracı **ping** ve **traceroute** dur. Her ikisi de ilk uygulamalar olan UNIX programlarında isimlendirilmişlerdir. Fakat günümüzde tüm internet desteği veren platformlarda bazı formlarda mevcuttur. Kendi protokolleri yoktur fakat aynı temel protokol olan internet kontrol protokolü (ICMP) kullanırlar. ICMP, tüm internet hostlarının kullandığı TCP/IP protokolünün gerekli bir parçası olarak düşük seviyede uygulanmıştır.

1. Ping: Basit olarak erişimi test eder. Verilen bir adrese paket gönderip alabilme konusunda bilgi verir ve sıklıkla bu paketin gönderilip alınmasının ne kadar zaman aldığını da gösterir.

2. Traceroute: Sadece verilen bir adrese erişim bilgisi yanında aynı zamanda verilen paketlerin izlediği yol hakkında da bilgi verir. Bu belli bir site ile hedef arasındaki bazı ağ problemlerinin analizinde çok yararlı olan bir servistir.

3. SNMP(Simple Network Management Protocol,Basit Ağ Yönetim Protokolü): Merkezi olarak ağ ekipmanını kolay yönetmek amacıyla tasarlanmış bir protokoldür. Bu ekipmanlar ise router, bridge, concentrator, hub ve hostlar dahi olabilir. SNMP yönetim istasyonları SNMP vasıtasıyla ağ ekipmanından, verilen bir ara yüzün çalışır durumda olup olmadığı, bu ara

yüz vasıtasıyla kaç byte veri taşındığı, bu ara yüzde ne kadar hata olduğu vb. konularda bilgi alınabilir. SNMP yönetim istasyonları aynı zamanda hassas ağ ekipmanını da bu ekipmanı çalıştırmak ve durdurmak ve gerekli ayarlamaları yapmak gibi işlerde kontrol edebilir. Ağ ekipmanı SNMP vasıtasıyla SNMP yönetim istasyonlarına herhangi bir hattın bozulduğu veya verilen bir hatta çok sayıda hata oluştuğu gibi acil bilgileri rapor edebilir.

SNMP kullanmadaki en büyük güvenlik riski ise her hangi bir kimse ağ ekipmanının kontrolünü ele alabilir ve onun ayarlarında kendi amacı doğrultusunda istediği değişiklikleri yapabilir. Örneğin; paket filtreleme servisini durdurabilir, yönlendirmeyi(routing) değiştirebilir veya basitçe mevcut ayarları silebilir.

3.7.12. Zaman Servisi

NTP(Network Time Protocol, Ağ Zaman Protokolü) mevcut sistemde büyük bir kesinlikte saat ayarlaması yapan bir internet servsidir. Farklı makineler arasında zaman senkronizasyonu yapmak çoğu açıdan çok önemlidir. Güvenlik açısından farklı makinelerin log dosyalarında tutulmuş tam zamanları incelemek, sistemde meydana gelmiş bazı anormal durumların analiz edilmesinde büyük yardım sağlar. Senkronizasyonu yapılmış saatler, aynı zamanda saldırganların sistemde herhangi bir etkileşimi kaydetmesini ve daha sonra tekrarlamasını engellemek için de gereklidir. Eğer zaman işaretleri etkileşimde kodlanırsa ikinci defa olacak bir işlem tekrarında bunlar zaman açısından yanlış olacaktır. Pratik açıdan bakılırsa senkronizasyon edilmiş saatler NFS'i de başarılı kullanılması açısından gereklidir.

NTP internet dahilinde kullanılmamalıdır. İnsanların NTP servisini internette kullanma sebebi, son derece kesin(doğru) saatlere sahip hostların sadece kendi aralarında senkronize olmadığını bunun yanında kesin doğru olmasını sağlar. Bu doğruluğu da NTP servisi uluslararası zaman



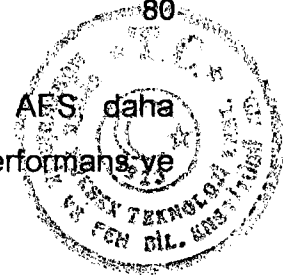
standartlarına göre sağlar(Birleşik Devletler Ana Atom Merkezi, GPS(Global Positioning System)). Harici bir zaman servisi olmadan sahip olunan bütün bilgisayarlar tamamen yanlış zaman ayarına sahip olabilir. Harici bir servis kabul etmek siteyi korumasız kılar. NTP saatleri çok hızlı olarak taşıyamayacağı için aynı zaman içinde bir saldırıya (playback saldırı) karşı korunmasız kalınabilir. NTP zaman kaynakları için radyo sinyalleri kullanmak çok pahalı bir yöntem değildir. Bununla birlikte kimlik onaylama(authentication) protokolü için saatleri senkronize etmede NTP kullanılıyorsa, harici referansları kullanmak yerine kendi NTP servisi satın alınmalı ve bütün zaman servisleri dahili olarak sağlanmalıdır.

3.7.13. Ağ Dosya Sistemleri

Fiziksel olarak başka makinelere bağlı olan dosya sistemlerine diğer bilgisayarları monte etmek(mount) için birkaç protokol vardır: NFS(Network File System, Ağ Dosya Sistemi) ve AFS(Andrew File System, Andrew Dosya Sistemi) UNIX işletim sisteminde en çok kullanılan dosya sistemleridir.

- **NFS(Network File System, Ağ Dosya Sistemi):** NFS, yerel alan ağlarında kullanılmak üzere tasarlanmış, hızlı cevap verme, yüksek güvenilirlik, zaman senkronizasyonu yapabilen ve makineler arasında yüksek güvenilirlik derecesi gibi özellikler sağlar.

NFS'in bazı ciddi güvenlik problemleri vardır. Eğer NFS tam anlamıyla ayarlanamamışsa, bir saldırgan basit olarak sistemlere kendini monte edebilir. NFS'in çalışma yöntemi, istemci(client) makinelerin, o sunucuya herhangi bir login işlemi gerekmeden veya şifre sorulmadan, sunucudaki dosyalara erişme ve onlarda değişiklik yapabilmesi şeklindedir. Çünkü NFS, işlemlerin hareketlerini tutmaz. Başkalarının sunucudaki dosyalara tam erişiminin olup olmadığı bilinmeyebilir.



- **AFS(Andrew File System, Andrew Dosya Sistemi):** AFS, daha geniş ağlar arasında kullanılmak üzere tasarlanmıştır ve zayıf performans ve daha az güvenilirlik derece toleransı daha iyidir.

AFS, kimlik onaylama(authentication) ve seçenekli olarak şifreleme kullanır ve internet dahil geniş alan ağları için kullanılır. NFS çoğu UNIX işletim sisteminin bir parçası olarak dağıtılır fakat AFS üçüncü parti üründür. Bundan dolayı, AFS'nin kurulum ve bakım için önemli teknik uzmanlık gerektirir.

3.7.14. Pencere(Window) Sistemleri

Çoğu UNIX makineleri X11 pencere sistemi temeline göre çalışan pencere sistemleri sağlar. Ağ erişimi X11'in önemli bir özelliğidir. Çoğu programlar grafik ara yüzüne sahiptir ve kullanışlıdır. Uzaktan terminal erişimi ise çok daha az yararlıdır. X11 uzaktan erişimli grafik sağlar.

X11 sunucular davetsiz misafirler için özendirici birer hedeftirler. X11 sunucusuna erişebilen bir davetsiz misafir şunları gerçekleştirebilir:

- **Ekran Görüntülerini alabilir:** Bu kullanıcıların monitör ekranlarında görülen grafiklerdir.
- **Klavye Tuş Vuruşlarını okuyabilir:** Bunlar kullanıcı şifrelerini içerebilir.
- **Klavyeden Tuş Vuruşlarını gerçekleştirebilir:** Bunda ise sanki kullanıcı bu tuşlara basmış gibi olur. Ve verilen anlamlı bir komut ise bilgisayarca işlenir. Tüm haklara sahip bir kullanıcının ekranında bunların yaptırılması tehlikesinin boyutları ise çok büyüktür. Bu yüzden X11'in internette kullanılması güvenli değildir.

3.7.15. Yazdırma Sistemleri

Sistem V yazdırma sistemi, **lp**, **lpr**, the **BSD**(Berkeley Printing System Berkeley Yazdırma Sistemi) uzaktan yazdırma özelliği içerirler. Bu bir bilgisayardan başka bir bilgisayara fiziksel olarak bağlanmış yazıcıdan çıktı almayı sağlar. Yerel alan ağında bu son derece arzu edilen bir özelliktir. Böylelikle sahip olunan makine sayısı kadar yazıcının olması gerekmez. Bununla birlikte internet yoluyla veri göndererek uzaktan yazdırma özelliği son derece güvensiz ve etkili bir yol değildir. Herhangi bir sitede internet yoluyla bir şey yazdırmak gerekiyorsa veya başka bir siteyi bu sitenin yazıcını kullanması gerekiyorsa, bu sitelere posta alıntısını yazdıracak özel sahte veya takma posta adları vermek mümkündür. Bu bir çok firmanın geniş alan ağlarında, önemli derecede güvenilir olduğu için kullandığı bir metottür.

3.7.16. Diğer Bilgi Servisleri

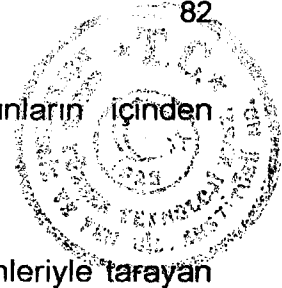
1. Gopher: Genellikle metin tabanlı(düz yazı) bilgilere menüler yardımıyla kolayca ulaşılmasını sağlayan bir sistem ve bu sistemin kullandığı TCP/IP protokolüne verilen genel addır. Bu çeşit bir menü yapısı dizin-alt dizin ilişkisine benzer. Ana menüdeki her bir madde seçildiğinde onun altında ya başka menü(ler) ya da görüntülenebilir bir döküman vardır. Bu şekilde istenilen bilgilere menüler takip edilerek ulaşılır.

Gopher menüleri yardımıyla, FTP merkezlerindeki programlar, ses, resim dosyaları, text vb. gibi pek çok bilgiye erişilebilir. Gopher menüsündeki maddeler, bir merkezdeki kullanıcıların isim/adres bilgilerini sorgulayan bir sistem bile olabilir. Gopher aynı zamanda diğer internet servislerine (**ftp**, **telnet**, **wais**, **www**, **finger**, **archie**) gateway'lik te yapabilir.

2. WAIS (Wide Area Information Service, Geniş Alan Bilgi Servisi):

WAIS değişik bilgi servislerindeki bilgilere ulaşmak için geliştirilen bir servis ve bu bilgileri indekslemek için kullanılan sisteme verilen isimdir. Bu servisi kullanan programlar verilen bir anahtar kelimenin (keyword) içinde geçtiği

dökümanların listesini isterler. Daha sonra program, bunların içinden seçeceği dosyanın/dosyaların bir kopyasını isteyebilir.



3. Archie: Anonim FTP sunucularını dosya ve izin isimleriyle tarayan bir internet servsidir. Archie sunucuları Telnet ve e-posta yoluyla atanmış archie istemcilerine servis sağlar. Archie servis sağlayıcıları kullanıcıların atanmış archie istemcileri kullanmalarını tercih eder çünkü sunuculara fazla yüklenmek istemezler.

4. Finger: Aranan makinede kullanıcı hesabı olan bir kişi hakkında bilgi arama servsidir. Hakkında bilgi aranan kullanıcının o an sisteme bağlı olması gerekmez. Bu bilgiler; kişinin gerçek adı, kullanıcı ismi, telefon numarası, ofisinin yeri, son olarak ne zaman ve nereye bağlandığı ve kullanıcı tarafından belirlenen bir mesaj gibi bilgiler olabilir. Eğer sorguda herhangi bir isim belirtilmemişse, o anda sorgulanan makineye bağlanmış olan kullanıcıların isimlerini verecektir. Bu da davetsiz misafirlere, bağlı kullanıcıları tanımlama veya gateway sistemleri gibi çok değerli bilgiler sağlar.

5. Whois: Finger servisi gibidir fakat hostlar, ağlar, domainler ve yöneticiler hakkında da halka açık bilgiler elde edilebilir. Varsayılan olarak whois istemcileri internet dominler ve ağ yöneticileri hakkında bilgi sağlayan interNIC'te sorgulama yaparlar.



4. GÜVENLİK DUVARI GELİŞTİRME

4.1. Giriş

Daha önceki bölümlerde internet güvenlik duvarları ve bunların koruma yapabileceği ve yapamayacağı konular üzerinde durulmuştu. Bu bölümde ise ana güvenlik duvarı kavramları üzerinde durulacaktır. Güvenlik duvarı bileşenleri, sitelerde günümüzde kullanılan güvenlik duvarı mimari çeşitleri hakkında bilgi verilecektir.

4.2. Güvenlik Duvarı Tasarımı

4.2.1. Bazı Güvenlik Duvarı Tanımları

Güvenlik duvarı mimarileri ve bileşenleri hakkında günümüzde tamamlanmış ve tutarlı bir terminoloji mevcut değildir. Bu konuda insanların tanım amacıyla kullandıkları yollar farklılık arz eder. Bununla birlikte aynı terimler ağ alanlarında başka anlamları da belirtebilirler. Bu sebeple burada yapılacak tanımlar tamamen güvenlik duvarı kapsamında düşünülmelidir.

- **Güvenlik duvarı (firewall):** Korunulan ağ ile internet arasında veya diğer ağ kümeleri arasında erişimi sınırlayan bileşenler bütünüdür.

- **Host:** Ağa eklenmiş bilgisayar sistemi.

- **Savunma(Bastion) Host:** Saldırılara karşı korunmasız olan ve bu yüzden yüksek derecede korunmaya ihtiyacı olan bilgisayar sistemidir. Çünkü genellikle internete açıktır ve dahili ağ kullanıcılarının ana bağlantı noktasıdır.



▪ **Çift Arayüzlü Sistem(Dual-homed host):** En az iki ağ ara yüzüne sahip genel amaçlı bilgisayar sistemidir.

▪ **Paket(Packet) :** İnternetteki temel iletişim ünitesi.

▪ **Paket Filtreleme(Packet Filtering):** Bir ağa gelen ya da ağdan giden veri akışının bir sistem tarafından seçimli olarak kontrol edilmesi olayı. Paket filtreleri, paketleri, bir ağdan diğerine iletilirken izin verir ya da bloklar. Bu genellikle internette dahili ağa doğru olur.

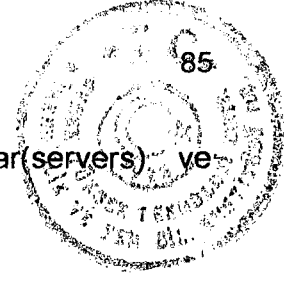
▪ **Çevre Ağı(Perimeter Network):** Korunulan ağ ile harici ağ arasına ek bir güvenlik katmanı oluşturmak için eklenmiş ağıdır. Çevre ağı zaman zaman DMZ (De-Militarized Zone) olarak da adlandırılır.

▪ **Vekil(Proxy) Sunucu:** Dahili istemcilerin tarafında harici sunucular ile bilgi dağıtan program. Proxy istemcileri proxy sunucusu ile haberleşir.

4.2.2. Güvenlik Duvarları Nasıl Çalışır?

Tüm intranetler saldırılara karşı korumasızdırlar. İnternetlerin altında yatan TCP/IP mimari yapısı internetle aynıdır. İnternet maksimum açıklık ve iletişim için geliştirildiğinden, intranetlere saldırı için kullanılabilecek sayısız teknikler vardır. Bu saldırılar şirketlerin çok önemli bilgilerini ve de parasını bile kapsayabilir. Saldırıları şirketin bilgisayar kaynaklarını ve servislerini bozabilir veya tanınmaz hale getirebilir. Saldırganlar şirket kaynaklarını kullanabilmek için intranete zorla girebilir veya şirket çalışanı gibi davranabilir.

Güvenlik duvarları intranette olup internet kaynakları kullanılırken davetsiz misafirlerin intranete erişimlerini kapatan donanım ve yazılım kombinasyonudurlar. Bir sitenin güvenlik derecesi ihtiyacına ve güvenlik duvarına harcanacak zaman, para, kaynaklara bağlı olarak çok çeşitli vardır.



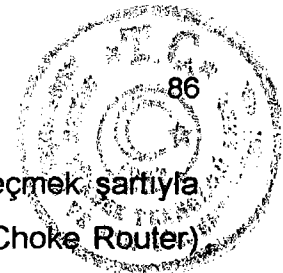
Çoğu birkaç elemanı kullanarak oluşturulmuştur. Sunucular(servers) ve yönlendiriciler(routers) güvenlik duvarlarının birincil parçalarıdır.

Çoğu güvenlik duvarları bir çeşit paket filtreleme(packet filtering) kullanırlar. Paket filtrelemede bir perdeleme yönlendiricisi(screening router) veya filtreleme yönlendiricisi(filtering router) intranet ve internet arasında hareket eden bütün veri paketlerine bakar.

Intranetteki proxy sunucuları intranetteki birinin internetteki herhangi bir sunucuya erişmek istediği zaman kullanılırlar. Kullanıcının bilgisayarından gelen bir istek direkt olarak internete gönderilmeden önce proxy sunucuya gider. Proxy sunucu internetteki bağlantıyı sağlar, İnternette bilgiyi alır ve daha sonra bilgiyi intranetteki istekte bulunan kişiye gönderir. Arada gidip-gelmek gibi davranarak, proxy sunucuları trafiği filtreleyebilirler ve internet ve intranet arasındaki tüm trafiğin kaydını tutarak güvenlik bakımını yapabilirler.

Savunma hostları, FTP istekleri gibi internetten gelen tüm istekleri tutan güçlendirilmiş sunuculardır. Gelen istekleri tutan basit bir savunma hostu saldırıların izlenmesini ve güvenliğin sağlanmasını kolaylaştırır. Herhangi bir sistem çökme anında tüm ağın yerine sadece basit savunma hostu problem yaşar. Her farklı internet servis isteği için bir adet olmak üzere birden çok savunma hostu kullanılabilir.

Güvenlik duvarları internet üzerinden atılmış saldırılara karşı intraneti korurlar. Onlar bir interneti ticari bilgiye erişimden, zarar vermeden ve bilgisayar kaynak ve servislerini devre dışı bırakmaktan korumak için tasarlanmışlardır. Ayrıca FTP gibi tehlike oluşturulan internet servislerine, intranetteki kişilerin erişimlerini engellemek için de tasarlanmışlardır.



1. İnternet bilgisayarları sadece bir güvenlik duvarından geçmek şartıyla internete erişimlerine izin verirler. İstekler boğucu yönlendiriciler(Choke Router) veya dahili filtreleme yönlendiricisi(Internal Filtering Router) de denilen dahili perdeleme yönlendiricisinden geçmek zorundadır. Bu yönlendirici paket trafiğinin uzaktan yönetilme yöntemiyle izlenmesini de engeller. Boğucu yönlendirici, paketlerin kaynağı ve hedefi gibi bilgi için tüm paketleri inceler.

2. Yönlendirici bulduğu bilgiyi filtreleme tablosundaki(filtering table) kurallara göre karşılaştırır ve paketi bu kurallara göre geçirir veya engeller. Örneğin, bazı servislerin(rlogin gibi) çalışmasına izin verilmez. Yönlendirici, paketlerin şüpheli internet bölgelerine gönderilmesine de izin vermeyebilir. Yönlendirici, e-mail haricinde internet ve dahili ağ arasında taşınan her paketi bloklayabilir. Sistem yöneticileri hangi pakete izin verileceğini ve hangilerinin engelleneceğini belirleyen kuralları koyarlar.

3. Bir intranet güvenlik duvarı tarafından korunduğunda, e-mail gibi genel dahili intranet servisleri ticari veri tabanlarına web servislerine ve grup kullanımlarına erişebilir.

4. Perdelenmiş alt-ağ güvenlik duvarları (screened subnet firewalls), harici filtreleme(exterior filtering) yönlendirici veya erişim(access) yönlendirici de denilen harici perdeleme(exterior screening) yönlendirici vasıtasıyla intraneti korumak için bir yol daha vardır. Yönlendirici, dahili perdeleme(interior screening) yönlendiricinin kullandığı aynı çeşit teknolojiyi kullanarak internet ve dış ağ arasındaki paketleri perdeleyebilir. Dahili perdeleme yönlendiricisine onaylanan aynı kurallara dayanarak paketleri perdeleyebilir ve dahili yönlendiricinin işlevini yapamaması durumunda bile ağı koruyabilir. Ayrıca bununla birlikte özellikle bütün hostları korumak için tasarlanmış, paketlerin perdelenmesi için de ek kurallar içerebilir.

5. Bir intraneti gelecek saldırılardan korumanın bir yolu olarak da, savunma hostu bir alt ağ ve güvenlik duvarı olan çevre ağa yerleştirilir. Eğer savunma host çevre ağ yerine intranette olursa ve çökerse, davetsiz misafirler intranete erişim kazanabilirler.

6. Bir savunma hostu ftp, e-mail ve herhangi veri ya da istekler gibi tüm servisler ve internetten gelen bağlantılar için ana bağlantı noktasıdır. Savunma hostları tüm bu istekleri yerine getirir ve internetteki kişiler sadece bu sunucuyla bağlantı kurabilirler ve herhangi bir intranet servisine direkt olarak bağlantı kuramazlar. Bu yolla internet sunucuları saldırılardan korunur. Savunma hostları proxy sunucuları gibi davranmaya ayarlanabilirler.

4.2.3. Ağ Adresi Çevirimi(NAT,Network Address Translation)

Özellikle iç kullanıcılar için küresel (global) IP adresleri var olmadığı durumlarda, internete bağlantı için bütün iç IP adreslerinin yeniden oluşturulmasından kurtulmakta NAT çok önemli bir görev yerine getirmektedir. Bunun için üç ayrı metot vardır:

1. Durağan (Static),
2. Hareketli (Dynamic),
3. Tek (Single).

Bunlardan ilk ikisi hemen tüm güvenlik duvarlarında bulunur. Tek adres aktarımı ise, ki bu özelliğin varlığı o güvenlik duvarı için büyük üstünlük sağlar, özel(private) ağ üzerinde bulunun tüm kullanıcılara, aradaki aygıtlar aracılığı ile aynı küresel adrese sahip olma olanağı getirir.

4.2.4. Güvenlik Duvarı Mimarileri

Çeşitli güvenlik duvarı bileşenlerini değişik kombinasyonlarda kullanarak farklı mimariler elde edilebilir. Temel olarak üç adet mimari ve bunların varyasyonları üzerinde durulacaktır.

1. Çift Arayüzlü Sistem Mimarisi

En az iki ağ ara yüzüne sahip çift arayüzlü sistem bilgisayarı çevresine kurulur. Böyle bir host, ara yüzlerin eklendiği ağlar arasında yönlendirici olarak görev yapabilir. IP paketlerini bir ağdan diğerine yönlendirebilir. Bununla birlikte bu tip bir güvenlik duvarı kurmak için bu işlem iptal edilir. Yani IP paketleri bir ağdan(internet) diğerine(dahili ağ veya korunulan ağ) direkt olarak yönlendirilmezler. Güvenlik duvarı içindeki sistemler ve güvenlik duvarı dışındaki sistemler (internette) bu çift arayüzlü sistem ile haberleşebilir. Fakat bu sistemler kendi aralarında direkt olarak haberleşemezler. Aralarındaki IP trafiği tamamen bloke edilmiştir. Bu tip güvenlik duvarının ağ mimarisi oldukça basittir. Çift arayüzlü sistem, internet ile dahili ağ arasında durur ve bağlantı kurar. (Şekil 4.1)



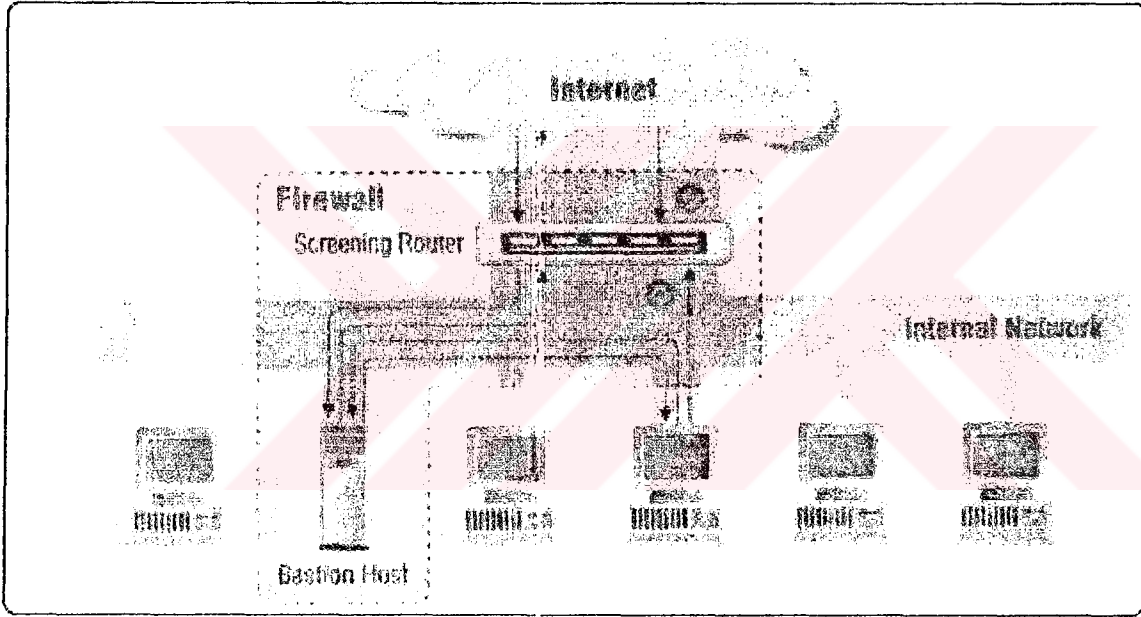
Şekil 4.1. Çift arayüzlü sistem mimarisi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.64).

Çift arayüzlü sistem çok yüksek seviyede kontrol sağlar. Eğer harici ve dahili ağ arasında paketlerin iletilmesine izin verilmiyorsa, dış kaynağa sahip,

dahili ağdaki herhangi bir paketin güvenlik probleminin kanıtı olduğundan emin olunabilir. Bir çift arayüzlü sistem, servisleri sadece proxy olarak veya kendisine direkt olarak kullanıcı kaydı tutarak sağlar.

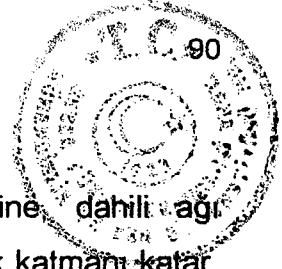
2. Perdelenmiş Sistem (Screened Host) Mimarisi

Nasıl ki çift arayüzlü sistem, çoklu ağ arasında servis sağlar fakat yönlendirme işlemi kapalıdır, perdelenmiş sistem mimarisi de sadece dahili ağa bağlanmış fakat bölümlendirilmiş yönlendirici kullanan hosttan servisleri sağlar. Bu mimaride birinci güvenlik paket filtreleme ile sağlanır. (Şekil 4.2)



Şekil 4.2. Perdelenmiş sistem mimarisi(Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.18).

Savunma host dahili ağda yer alır. Perdeleme yönlendiricisindeki paket filtreleme, internetteki hostların, savunma hostu, dahili ağda bağlantı kurabilecekleri tek sistem olarak görmelerini sağlayacak bir şekilde kurulur. Böylece belli tipteki bağlantılara izin verilir. Herhangi harici bir sistem dahili sistemlere erişmeye çalıştığında bu hosta bağlanmak durumundadır. Savunma host bu yüzden yüksek derecede güvenlik bakımına gerek duyar.



3. Perdelenmiş Alt-Ağ(Screened Subnet) Mimarisi

Perdelenmiş Alt-Ağ mimarisi screened host mimarisine dahili ağı internetten ayıran çevre(perimeter) ağı ekleyerek, ek bir güvenlik katmanını katar. Savunma(Bastion) host'ları ağda en fazla saldırıya maruz kalan makinelerdir. Çevre ağındaki savunma host'unu izole etmekle, dış etkiler azaltılmış olur. En basit screened subnet mimarisinde iki adet yönlendirici(router) mevcuttur. Biri çevre ağı ve dahili ağ arasındadır, diğeri ise çevre ağı ve harici ağ(çoğunlukla internet) arasındadır. Bir davetsiz misafir bu tip bir yapıyı kırmak ve dahili ağa ulaşmak için bu iki yönlendiriciyi geçmek zorundadır.



Şekil 4.3. Perdelenmiş Alt-Ağ mimarisi(iki yönlendiricili) (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.68).

Bu mimarinin parçaları olarak da şu başlıklar verilebilir:

Çevre(Perimeter) Ağı: Güvenliğin başka bir katmanıdır. Korunulan dahili ağ ile harici ağ arasında ek bir ağıdır. Bir saldırgan güvenlik duvarına erişmeyi başarsa, çevre ağı, saldırgan ve dahili sistemler arasında ek bir koruma katmanı oluşturur. Çoğu ağlarda, seçilen bir makinede o ağıdaki tüm makinelerin trafiğini görmek olanaklıdır. Bu, çoğu ethernet tabanlı ağlar için doğrudur. Token ring ve

FDDI ağ topolojileri için de bu geçerlidir. Dolayısıyla ağ izleyen birisi bu ağdaki tüm trafiği dinleyebilir. Çevre ağında, çevre ağı içerisinde bulunan savunma hostuna girmeyi başaran birisi sadece o ağdaki trafiği izleyebilecektir.

Savunma(Bastion) Host: Perdelenmiş alt-ağ mimarisi ile, çevre ağına bir yada daha fazla savunma hostu eklenir. Bu host, dış dünyadan gelen bağlantıların ana temas noktasıdır.

- Gelen e-posta(SMTP) oturumları için elektronik postayı siteye dağıtmak,
- Sitenin anonim ftp sunucusuna gelen ftp bağlantıları,
- Site hakkında gelen DNS sorgulamaları vs.

Dışarı-giden(Outbound) servisler(dahili istemcilerinden internetteki sunuculara) şu yollarla takip edilir:

- Dahili istemcilerin harici sunuculara direkt olarak erişimlerinin sağlanması için, paket filtreleme işleminin harici ve dahili yönlendiricide de kurulması.
- Dahili istemcilerin harici sunuculara dolaylı olarak erişimlerinin sağlanması için proxy sunucularının savunma host'ta çalışacak şekilde kurulması.

Her iki durumda da paket filtreleme, bastion host'a, internetteki host'lara bağlanmaya ve onlardan bağlantı kabul etmeye izin verir.

İç/Dahili Yönlendirici(Interior Router): Bu yönlendirici, dahili ağı hem internetten hem de çevre ağından korur. Genellikle boğum(choke) yönlendiricisi olarak adlandırılırlar. Bu yönlendiriciler güvenlik duvarı için olan paket filtrelemenin çoğunu yaparlar. Belirlenen servislere internete erişim için izin verirler. Bu servisler, proxy'lerden çok paket filtreleme ile daha güvenli bir şekilde desteklenen ve güvenle sağlanan servislerdir. Savunma hostu ile dahili ağ arasında sağlanan servisler, internet ile dahili ağ arasında izin verilen



servislerden gereklilik olarak farklıdır. Savunma hostu ile dahili ağ arasında sağlanan servislerin sayısını belli bir limitte tutma sebebi, savunma hostundan gelen saldırıların sayısını azaltmak içindir. Bu servisler bir saldırganın dahili sistemlere erişmek için kullanacağı servisler olduğundan güvenliği için dikkat sarfedilmelidir.

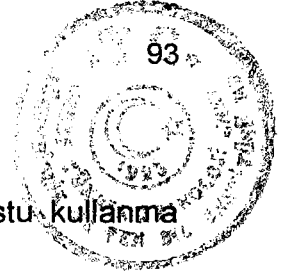
Dış/Harici Yönlendirici(Exterior Router): Teoride bu yönlendirici, çevre ağını ve dahili ağı internetten korur. Pratikte ise, dış yönlendiriciler, çevre ağında giden herşeye izin verme eğilimindedirler ve çok az paket filtreleme yaparlar. Dahili makineleri korumak için olan paket filtreleme kuralları her iki yönlendirici için de aynıdır. Kurallarda bir hata olursa, bu, saldırganın erişimine izin verir.

Sıklıkla dış yönlendirici harici bir grup tarafından sağlanır(örneğin internet sağlayıcısı) ve ona olan erişim sınırlandırılmış olabilir. Harici bir grup yönlendiricisine muhtemelen çok az genel paket filtreleme kuralı koyacaktır ve komplike ve sıklıkla değişen kural kümesi koymayacaktır. Dolayısıyla harici yönlendiricilere kendi yönlendiriciler kadar güven duyulmayabilir.

Dış yönlendiricilerdeki gerçek özel paket filtreleme kuralları, çevre ağındaki makineleri koruyan kurallardır. Genel olarak, çevre ağındaki hostlar, host güvenliği vasıtasıyla korunduğu için çok fazla güvenliğe gerek yoktur. Dış yönlendiricinin genellikle yerine getirdiği güvenlik görevi kaynak adreslerin taklidi olan internetten gelen paketlerin bloklanmasıdır. Bu tür paketler dahili ağdan geldiği iddia edilir fakat aslında onlar internetten gelmektedirler.

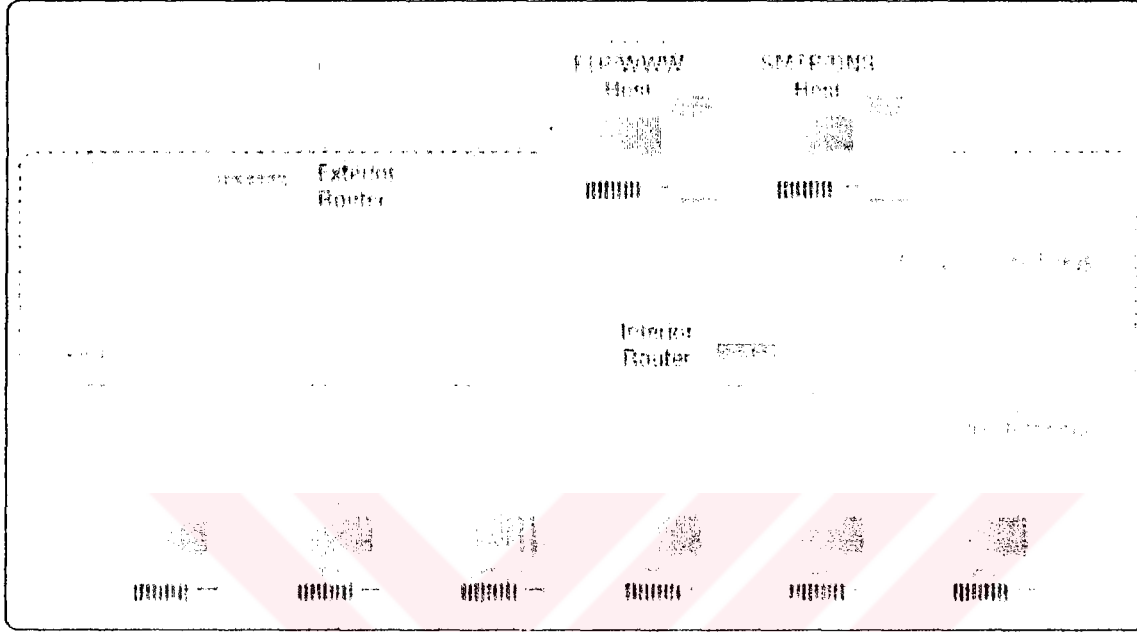
4.2.5. Değişik Güvenlik Duvarı Mimarileri

Güvenlik duvarı mimarilerini geliştirmede istenen özelliklere, donanım, bütçeye, ve güvenlik politikasına uygun esnek bir çeşitlilik söz konusudur.



Çoklu Savunma Hostu Kullanma

Genelde güvenlik duvarı mimarilerinde tek bir savunma hostu kullanma eğilimi olsa da birden fazla savunma hostu kullanılabilir. (Şekil 4.4)

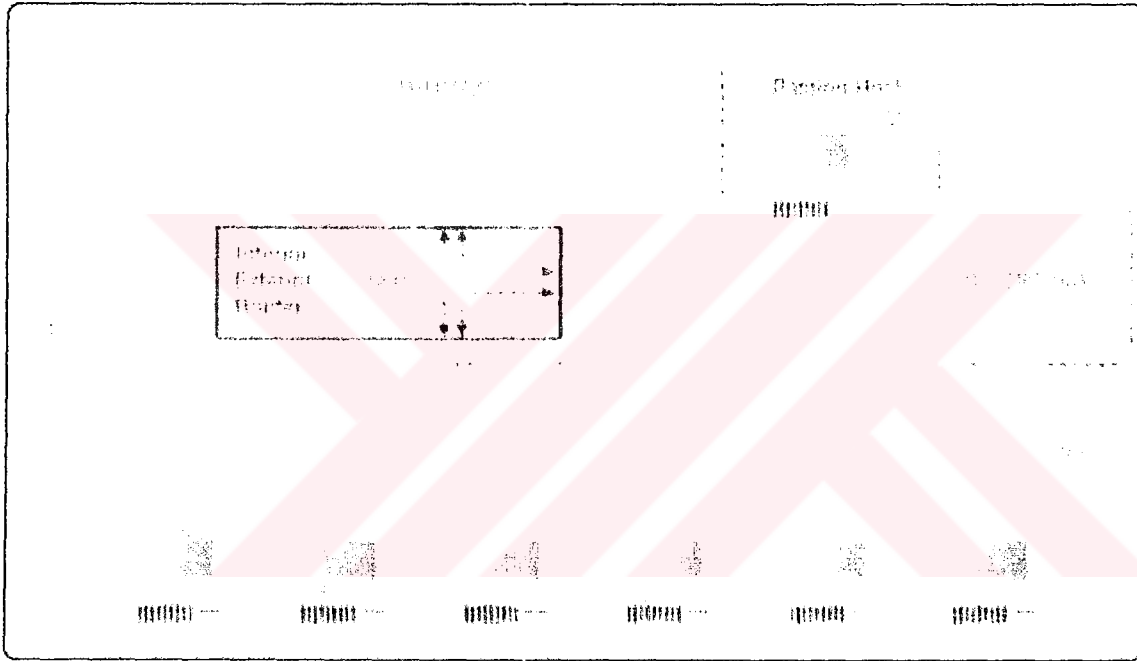


Şekil 4.4. İki savunma hostu mimarisi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.72).

Biri dahili kullanıcılar için önemli olan servisleri(SMTP sunucuları, proxy sunucuları vs.), diğer biri kullanıcılar için önemli olmayan ve internet servislerini(anonim ftp sunucusu gibi) sağlıyor olabilir. Böylelikle dış kullanıcıların aktivitelerinden dolayı sitenin kendi kullanıcıları etkilenmez. Bu mimari performans sebeplerinden dolayı da yapılabilir. Fakat bu sistemde çoğu servis belirli sunucular için ayarlanmalıdır. Güvenlik duvarı konfigürasyonu birden fazla savunma hostuna sahipse, bunlardan biri çalışmaz hale geldiği zaman servisler diğerinden sağlanacak şekilde ayarlanabilir. Fakat burada sadece bazı servislerin bunu desteklediği unutulmamalıdır.

İç ve Dış Yönlendiriciyi Birleştirme

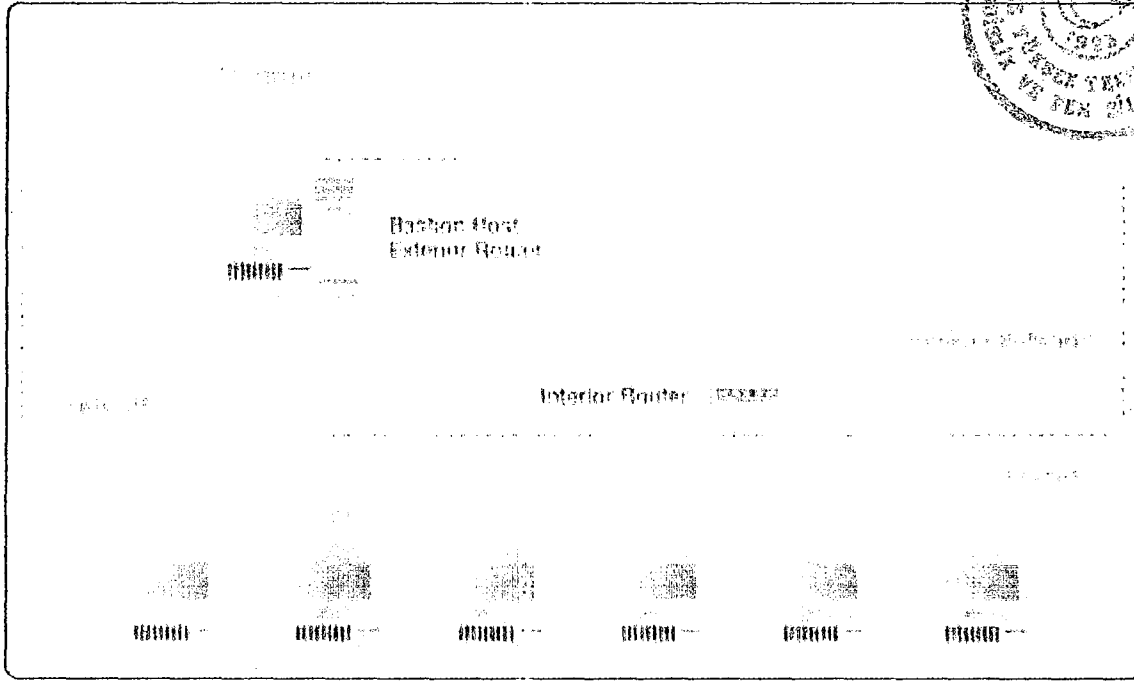
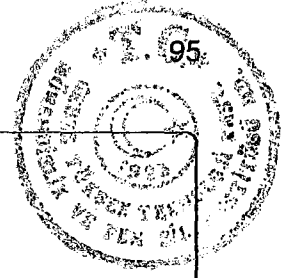
İç ve dış yönlendiriciler tek bir yönlendiricide birleştirilebilir. Çevre ağı yine mevcuttur ve dahili ağa bir bağlantı vardır. Trafiğin bir kısmı direkt olarak dahili ağ ve internet arasında akar. Diğer trafik ise çevre ağı ile internet veya çevre ağı ile dahili ağ arasında akar. Bu mimari perdelenmiş sistem mimarisi gibi tek yönlendirici olması sebebiyle siteyi savunmasız hale getirir. Genel olarak yönlendiriciler hostlardan daha kolay korunurlar fakat içinden çıkılmaz da değildirler. (Şekil 4.5)



Şekil 4.5. İç ve dış yönlendiriciyi birleştirme (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.73).

Savunma Host ve Dış Yönlendiriciyi Birleştirme

İç ve dış yönlendiricilerin birleştirilmesinin aksine, bu mimari önemli derecede savunmasız değildir. Savunma hostu internette açığa çıkarır ve korunması ise sadece kendi arayüz paketinin yaptığı filtreleme(eğer varsa) ile gerçekleşir. Bu yüzden ayrıca bir korumaya gerek duyulur. (Şekil 4.6)



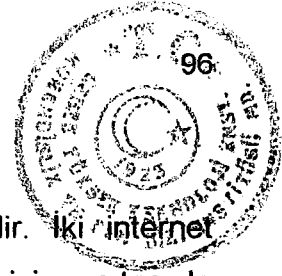
Şekil 4.6. Savunma hostu ve dış yönlendiriciyi birleştirme (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.75).

Çoklu Dış Yönlendirici Kullanma

Aynı çevre ağına çoklu dış yönlendirici bağlamanın birkaç sebebi vardır:

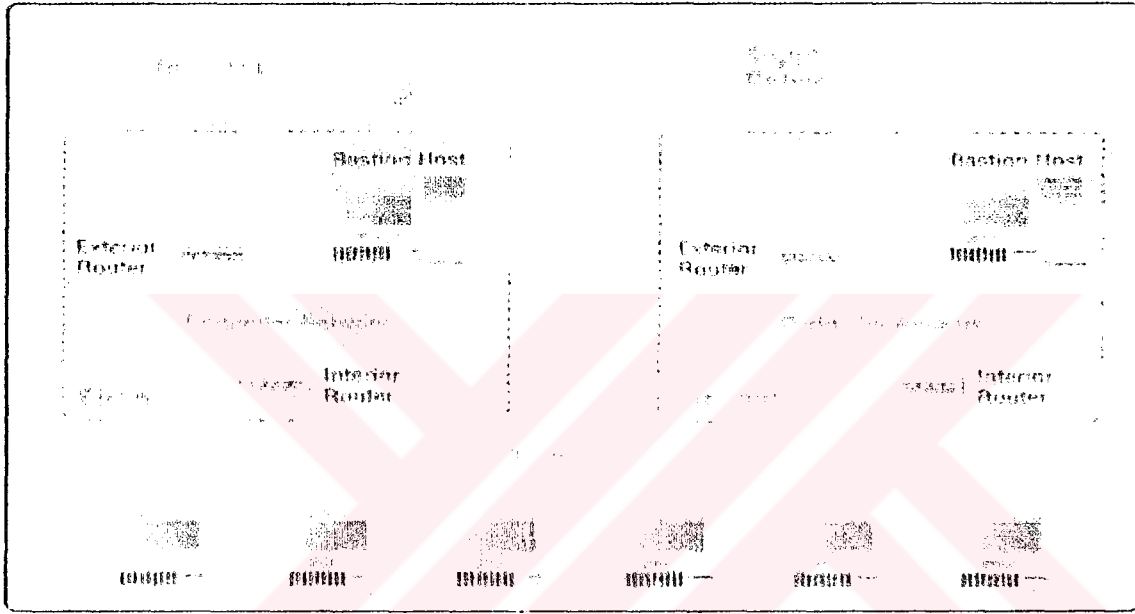
- İnternete çoklu bağlantı vardır.
- İnternete bir bağlantı ve ayrıca diğer sitelere farklı bağlantılar vardır.

Aynı dış ağı kullanan çoklu dış yönlendiriciyi eklemek önemli bir güvenlik problemi oluşturmaz. Farklı filtreleme yapabilirler fakat bu dış yönlendiricilerde kritik değildir. Bu tür mimarilerde şuna dikkat edilmelidir: Eğer çevre ağındaki savunma hostuna girilirse, giren, hangi trafiği görebilecek? Örneğin birisi girerse, bu kişi site ile bayisi arasındaki özel trafiği görebilecek mi? Eğer öyleyse, o zaman, tek çevre ağına çoklu dış yönlendirici yerine, çoklu çevre ağı kurmak düşünülebilir.



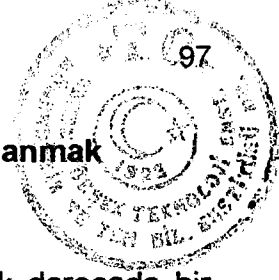
Çoklu Çevre Ağı Oluşturma

Birlikte çalışma sağlamak için çoklu çevre ağı kurulabilir. İki internet bağlantısı fazla hassasiyet yapmaz ve onlar aynı yönlendirici vasıtasıyla çalıştırılabilir. İki dış yönlendiriciyi, iki çevre ağını ve iki iç yönlendiriciyi koymak, sistem ile internet arasında tek bir çöküş noktası olmamasını garantiler. (Şekil 4.7)



Şekil 4.7. Çoklu çevre ağı(çoklu güvenlik duvarı) (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.81).

Çoklu çevre ağı özel olmak açısından da kurulabilir. Böylelikle gizli ve güvenilir veri bir ağda kullanılır. İnternet bağlantısı ise diğerinden kullanılır. Bu durumda iki ağ da tek bir iç yönlendiriciye bağlanabilir. Çoklu çevre ağına sahip olmak, aynı iç ağı paylaşan çoklu iç yönlendiriciye sahip olmaktan daha az risklidir.



Çift Arayüzlü ve Perdelenmiş Alt-Ağları sistemlerini Kullanmak

Bu mimarileri bir araya getirmekle güvenlikte önemli olacak derecede bir artış meydana getirilebilir. Bunu yapmak için çevre ağı bölünür ve dual-homed host yerleştirilir. Yönlendiriciler sahtekarlığa karşı koruma sağlarlar. Ayrıca dual-homed host trafiği başlattığı yerde çökmelere karşı koruma yapar. Bu host aynı zamanda bağlantılarda paket filtrelemeden daha iyi kontroller sağlar. Bu çok katmanlı koruma sağlayan mükemmel bir güvenlik duvarıdır.

4.3. Savunma (Bastion) Host'lar

Bir intraneti korumanın en iyi yollarından biri, güvenlik duvarı ile iyice sağlamlaştırılmış bir bastion host'u veya bastion sunucusu kullanmaktır. Bir bastion host'la; internetten intranete olan tüm erişimler bastion host vasıtasıyla elenmeyi gerektirir. Tüm erişimleri tek veya bir grup sunucuda yoğunlaştırmak dahili intraneti korumakta daha kolaylık sağlar.

Bastion host intranet servislerini kendisi sağlamaz. Intranet servisi için internetten bir istek aldığı anda önce bastion hosttaki proxy sunucusuyla bağlantı kurar ve bastion host bu isteği internet sunucusuna gönderir. İnternet sunucusu bilgiyi bastion hosttaki proxy sunucuya gönderir. Bastion host da bilgiyi intranetteki kullanıcıya gönderir.

Savunma host güvenliği sağlamak için çoğu temel servisin dışında tüm servislerden arındırılmalıdır. Tipik bir ağ sunucusu, login, dosya, yazdırma, ve diğer sunuculara da bağlanma dahil, diğer servisleri de sağlar. Bastion host'ta bu servisler yasaklanmıştır. Sistemde kullanıcılar tanımlı değilse birisinin şifreleri kullanarak sisteme girmesi zordur. Sistemde az servisin olmasıyla, eğer birisi sisteme girerse, yapılabileceği çok az şey olur.



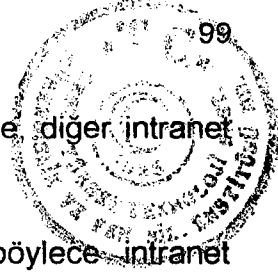
Daha fazla güvenlik için, savunma hostları özel alt-ağa hostu iyice izole edecek şekilde yerleştirilebilirler. Böylece birisi ağa girerse, sadece bu alt ağa ulaşabilir, intranetin geri kalanına ulaşamaz. Filtreleme yönlendiricileri özel alt ağdan gelen paketleri yeniden incelemek suretiyle, sadece izin verilen isteklerin intranete geçmesine izin verdiğiinden emin olur.

Güvenlik ölçümleri; intraneti ve sunucuyu korumakla birlikte, birisi ağa girmek istediğinde intranet yöneticilerini uyarabilir. savunma hostu kendisine olan tüm erişimleri kaydeder ve bunların bir yedeğini de seri porttan bağlı başka bir makinede tutabilir. Böylece kimse yedeğe erişemez ve sistem yöneticileri sisteme sızmalar için yedeği inceleyebilirler.

4.3.1. Savunma Hostları Nasıl Çalışır?

Bir savunma hostu (savunma sunucusu da denir) intranet güvenlik duvarındaki ana savunmalardan biridir. Güvenlik duvarı içinde olan güçlü bir sunucudur ve internet ile intranet arasındaki ana bağlantı noktasıdır. İzole edilmiş, ana bağlantı noktası olarak savunması geliştirilmiş sunucuya sahip olan ağlarda intranet kaynakları internetle başlayan saldırılardan korunabilir.

- Savunma hostları üzerlerindeki tüm ağ servisleri gerektiğinde iptal edilebilir olarak geliştirilmiştir. Sunucunun yaptığı tek şey belirli internet erişimine izin vermektir. Savunma hostunda hiçbir kullanıcı tanımlı olmamalıdır. Böylece kimse giremez, kontrolü alamaz ve intranete erişim sağlayamaz. Bir sistemin uzaktaki bir ağdaki sisteme erişimini sağlayan ağ dosya sistemi (NFS), iptal edilmiş olmalıdır. Böylece davetsiz misafirler savunma sunucusuna ve intranetteki dosyalara erişimi sağlayamazlar. Savunma hostlarını kullanmanın en güvenli yolu, onları intranet güvenlik duvarının bir parçası olarak kendi alt ağına



koymaktır. Onları kendi ağlarına koymakla, eğer içlerine girilirse diğer intranet kaynaklarına bir zarar gelmez.

- Savunma sunucular tüm aktiviteleri kaydeder ve böylece intranet yöneticileri intranetin saldırıya uğradığını söyleyebilirler. Güvenlik sebebiyle sistem yedeklerinin iki kopyasını tutarlar. Bir kopyanın bozulması veya karıştırılmasına karşılık diğer kopya yedek olarak çalışır. Yedeğin güvenli kopyasını tutmanın bir yolu savunma sunucusunu, tek görevi güvenli yedek kaydını izlemek olan bir bilgisayara seri porttan bağlamaktır.

- Otomatik denetleme, yetkilendirilmiş yazılımlardan daha gelişmiştir. Otomatik denetleme düzenli olarak savunma sunucularının sistem kayıtlarını kontrol eder ve şüpheli bir gidişat bulduğunda alarm verir. Örneğin; birisi üç defadan fazla sisteme girmeyi denemişse alarm verilebilir.

- Bir güvenlik duvarında birden fazla savunma hostu bulunabilir. Her savunma hostu intranet için bir veya birden fazla internet servisini sağlayabilir. Bazen savunma hostu bir kurban makine gibi kullanılabilir. Savunma hostu belirli internet servisi dışında tüm servislerden arıtılmış olabilir. Kurban makineler, proxy veya filtreleme kullanılmak suretiyle gerçekleştirilemeyen veya güvenlik özellikleri bilinmeyen internet servislerini sağlayabilirler. Servisler diğer servislerle beraber savunma hostu yerine kurban makineye konulur. Bu yolla sunucuya girilirse diğer savunma hostlarının etkilenmemesi sağlanır.

- Savunma hostuyla intranet arasına filtreleme yönlendiricisi yerleştirmek ek bir güvenlik sağlar. Bu yönlendirici internet ve intranet arasındaki tüm paketleri, izin verilmeyenleri engellemek suretiyle kontrol eder.

- Bir savunma sunucu, web sayfası göndermek veya e-mail dağıtmak gibi bir servis için istek alırsa sunucu isteği kendisi yerine getirmez. Bunun yerine isteği, uygun olan başka bir intranet sunucuya gönderir. Intranet sunucu isteği alır ve gerekli bilgiyi bastion sunucuya geri gönderir. Bastion sunucu da bilgiyi internetteki istek sahibine gönderir.

- Bazı bastion sunucular kendilerine karşı bir saldırının olup olmadığını kontrol eden denetleyici programlar içerirler. Denetlemenin çeşitli yolları vardır.

Denetlemenin bir yolu bastion sunucudaki bir programın herhangi bir yetkisi olmayan bir kişi tarafından değiştirilip değiştirilmediğini kontrol eden sonuç kontrolü yapan program kullanmaktır. Bir checksum programı sunucudaki çalıştırılabilir(executable) bir programın boyutuna dayalı bir sayı hesaplar. Daha sonra düzenli olarak sonucun değişip değişmediğini yeniden hesaplama yaparak kontrol eder. Eğer değişmişse birisi yazılımı saldırı sinyali üretecek kadar değiştirmiştir demektir.

4.3.2. Genel Prensipler

- **Basitlik :** Bir savunma hostu ne kadar basit olursa güvenliği o kadar kolay sağlar. Savunma hostunun sağladığı herhangi bir servis yazılım veya konfigürasyon hataları içerebilir ve bunlar güvenlik problemleri oluşturabilirler.
- **Saldırı için hazırlıklı olma:** Her ne kadar güvenlik sağlamak için çok çapa harcansa da yine de sisteme girmeler olabilir. Bunun için her zaman daha kötüsü beklenmeli ve planlı olunmalıdır. Her zaman eğer bu hosta saldırı olursa diğer ağın güvenliğinin sağlanması konusunda ne yapılmalı sorusuna cevap verilmelidir.

4.3.3. Savunma Hostlarının Özel Çeşitleri

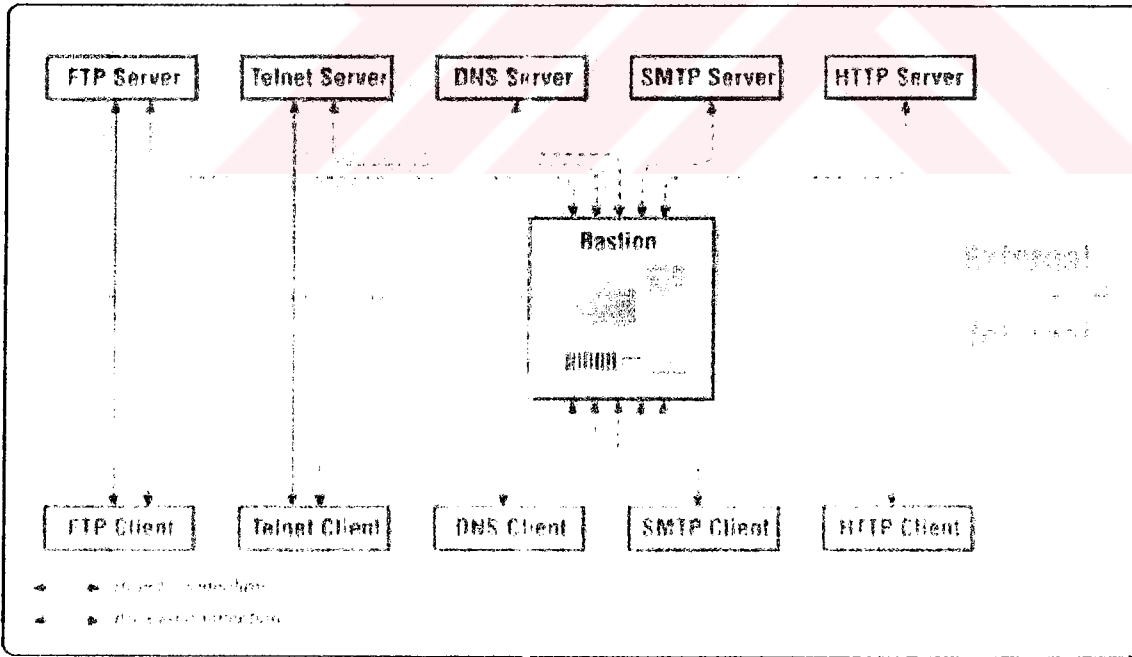
- **Yönlendirme Yapmayan Çift Arayüzlü Sistemler:** Çoklu ağ bağlantıları vardır. Fakat aralarında trafik geçişi yoktur. Böyle bir host kendisi güvenlik duvarı veya güvenlik duvarı kompleksinin bir parçası olabilir.
- **Kurban Makineler:** Proxy veya paket filtreleme ile güvenli bir şekilde sağlaması zor olan servisler veya güvenlik özellikleri bilinmeyen yeni servisler çalıştırılmak istenebilir. Bu amaçla, bir kurban makine yararlı olabilir. Bu makine, üzerinde korunması gereken herhangi bir şey olmayan veya davetsiz misafirin

kullanabileceği bilgilerin olduğu hiçbir makineye erişimi olmayan bir makine olabilir. Sadece kullanımı için gerekli olan minimum servisleri içerir.

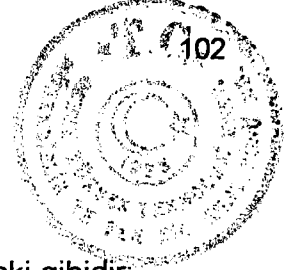
▪ **Dahili Savunma Hostları:** Çoğu konfigürasyonlarda, ana savunma hostu belli dahili host'larla özel etkileşimlerde bulunur. Örneğin; bir postayı dahili bir posta sunucusuna, Usenet haberlerini dahili haber sunucusuna iletebilir. Bu makineler ikincil savunma hostlardır ve dahili hostlardan daha çok savunma hostları gibi ayarlar edilir ve korunurlar.

4.3.4. Savunma Hostu Tarafından Sağlanan Servisler

Savunma hostları bir sitenin internete bağlanması için gerekli olan herhangi bir servisi sağlar. (Şekil 4.8) Savunma hostuna kullanılması tasarlanmayan servisler kurulmamalıdır. Örneğin; dahili host'lardan makine açma(boot) servislerini sağlamamalıdır.



Şekil 4.8. Savunma Hostu tarafından sağlanan servisler(Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.100).



4.3.5. Savunma Hostu Geliştirme

Bu tip bir mimari geliştirmede izlenecek olan strateji aşağıdaki gibidir:

1. Makineyi Koruma : Makine korumasında aşağıdaki işlemler gerçekleştirilir.

- Minimum temiz bir işletim sistemiyle başlanmalıdır,
- Tüm sistem hataları(bug) ayıklanmalıdır,
- Kontrol listesi kullanılmalıdır,
- Sistem kayıtlarının güvenliği sağlanmalıdır.

2. Gereksiz Servislerin İptali: Sistem için gerekli olan servislerin kurulması gereksizlerin iptali için şu konulara cevap verilmelidir:

- Servisler nasıl yönetilir?
- Servislerin iptali nasıl yapılır?
- Hangi servisler çalışmalıdır?
- Hangi servisler iptal edilmelidir?

3. Servisleri Kurma ve Değiştirme:

- Servisleri koruma için TCP/IP Wrapper kullanma

4. Üretim için Yeniden Şekillendirme:

- Çekirdeği yeniden şekillendirme ve kurma,
- Gereksiz programların silinmesi,
- Dosya sistemlerini sadece_okunabilir hale getirmek.

5. Güvenlik Denetimi Çalıştırmak

4.4. Paket Filtreleme(Packet Filtering)

Paket Filtreleme, ağı giren ve ağıdan çıkan verileri kontrol ederek çalışan bir ağ güvenlik mekanizmasıdır. Bilgi ağı içerisinde transfer etmeden önce küçük parçalara ayrılır. Bunların her biri ayrı olarak gönderilir. IP ağı sistemlerinde bu küçük bilgi parçaları paket olarak adlandırılır. IP ağlarında tüm veri transferi bu şekilde olur. İnternet ağı üzerinde dolaşan paketler, IP paketleridir.

IP ağlarını birbirine bağlayan temel alet yönlendirici(router)'dir. Bir yönlendirici, başka amacı olmayan adanmış bir donanım parçası veya genel amaçlı UNIX veya PC sisteminde çalışan yazılım parçası olabilir. Paketler hedeflerine ulaşınca kadar ağlar arasında bir yönlendiriciden diğerine transfer edilirler. Bunlar genellikle yönlendirici üzerinde uygulanırlar. Paketler yönlendiriciye nereye gideceklerini söylerler fakat nasıl gideceklerini söylemezler. Yönlendiriciler, yönlendirme protokollerini(RIP) kullanarak kendi aralarında haberleşirler. Daha sonra paketleri hedeflerine ulaştırmak için en kısa yolu bulma(OSPF) yöntemini kullanarak yönlendirme tabloları oluştururlar.

4.4.1. Neden Paket Filtreleme?

Paket filtreleme, verinin aşağıdaki kriterlere göre kontrol edilmesini(izin verme veya reddetme) sağlar.

- Verinin geldiği adres,
- Verinin gittiği adres,
- Veriyi transfer etmek için kullanılan oturum ve uygulama protokolleri.

Paket filtreleme, hiç kimsenin telnet kullanmamasını, herkesin SMTP vasıtasıyla posta göndermesini, herhangi bir makine dışındakilerin haber (NNTP) göndermemesini sağlayabilir. Fakat herhangi bir kullanıcıya telnet kullanma izni verip diğerlerine kısıtlama yapamaz. Ayrıca bazı dosyaları transfer edebilir diğerlerini edemez diye de bir durum olmaz. Çünkü, kullanıcı ve dosya, paket filtreleme sisteminin tanımlayacağı bir durum değildir.

Paket Filtrelemenin Avantajları

- Bir perdeleyici yönlendirici dahili ağın korumasına yardımcı olur.
- Paket filtreleme, kullanıcı bilgisi veya işbirliğine gerek duymaz.
- Paket filtreleme, bir çok yönlendirici tarafından desteklenmektedir.

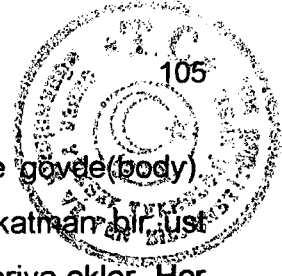
Paket Filtrelemenin Dezavantajları

- Mevcut filtreleme araçları mükemmel değildir.
- Bazı protokoller paket filtrelemeye tam olarak uygun değildir.
- Bazı politikalar, normal paket filtreleme yönlendiricilerle yürütülmeye tam hazır değildir.

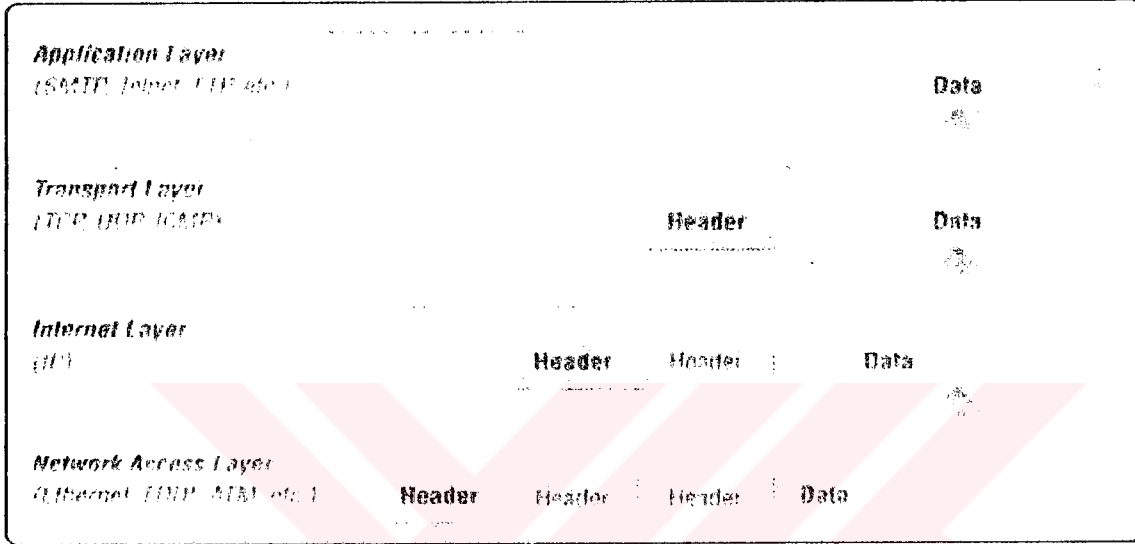
4.4.2. Paketlerin Yapısı

Paket filtrelemeyi iyi anlamak için ilk olarak paketlerin yapısı ve TCP/IP protokol yığnında(stack) her katmanda nasıl tutulduğu anlaşılmalıdır.

- Uygulama katmanı(Application Layer: FTP, Telnet, HTTP gibi),
- İletim Katmanı(Transport Layer: TCP veya UDP),
- İnternet Katmanı (IP)
- Ağ Erişim Katmanı(Network Access Layer: Ethernet, FDDI, ATM gibi)



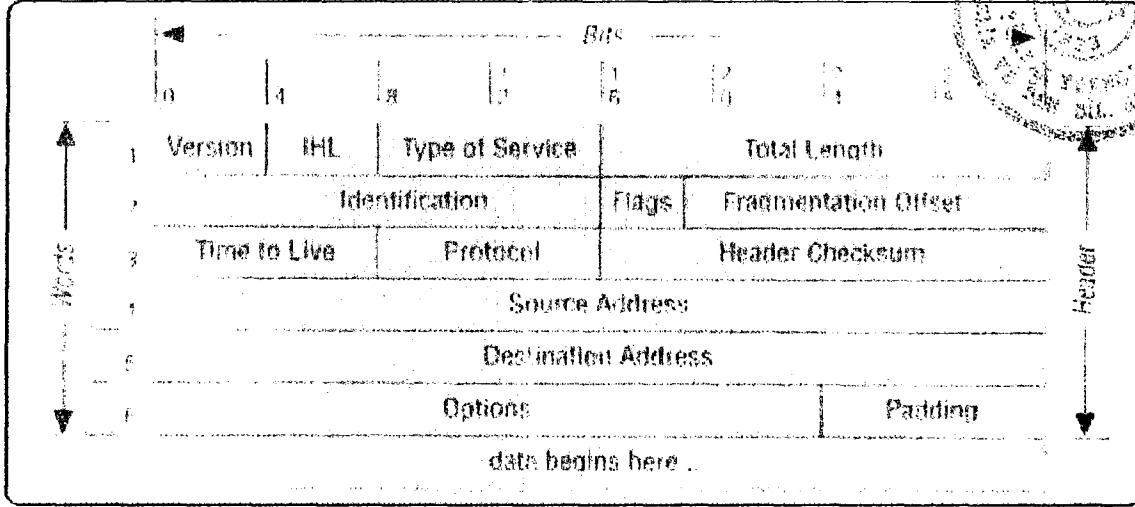
Her katmanda paketlerin iki kısmı vardır. Başlık(header) ve gövde(body). Başlık protokol bilgilerini içerir. Gövdede ise veri bulunur. Her katman bir üst katmandan aldığı bilgiyi veri olarak algılar ve kendi başlığını bu veriye ekler. Her katmanda paket üst katmanlardan gelen tüm bilgileri içerir. Şekil 4.8'de veri paketlenmesi olayı görülmektedir.



Şekil 4.9. Veri paketlenmesi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.139).

IP katmanında, IP paketi iki parça yapılır. IP başlığı ve IP gövdesi. IP başlığı dört parça bilgi içerir: (Şekil 4.9)

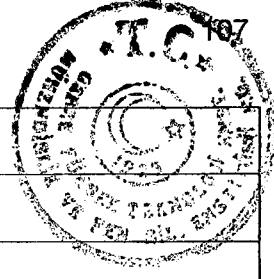
- **IP kaynak adresi:** 4 byte uzunluğundadır.(192.168.1.60)
- **IP hedef adresi:** IP kaynak adresi gibidir.
- **IP protokol tipi:** TCP, UDP, ICMP veya başka bir tip.
- **IP özellikler alanı:** Hemen hemen boştur. Fakat verilen paket için IP kaynak yönlendirmesini ve IP güvenlik özelliklerini içerir.



Şekil 4.10. IP başlık ve gövdesi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.141).

Paket filtrelemede belli protokollerin ve alanların filtreleneceği kararı, ağ erişim politikasına göre değişebilir. Çizelge 4.1'de korunmasız, saldırıya açık ve siteye girerken ve çıkarken güvenlik duvarında filtrelenen bazı servislerin port numaraları görülmektedir.

Servis	Port	Açıklama
FTP	20,21	Sıklıkla belli sistemlere sınırlandırılmıştır.
TFTP	69	Disketsiz iş istasyonları boot etmek için kullanılır.
TELNET	23	Sıklıkla belli sistemlere sınırlandırılmıştır.
SMTP	25	Sıklıkla merkezi e-posta sunucusuna sınırlandırılmıştır.
DNS	53	Host isimlerini, bilgilerini içerir. IP spoofing yapılabilir.
RIP	520	Direkt paket yönlendirmede dinlenebilir.
X Windows	6000+	Tuş vuruşlarında X window, bilgi sızdırabilir.
RPC	111	Sistem bilgisi(şifreler gibi) çalmada kullanılabilir.



Rexec	512	Kimlik onaylanmamış erişime izin verebilir.
Rlogin	513	Kimlik onaylanmamış erişime izin verebilir.
Rsh	514	Kimlik onaylanmamış erişime izin verebilir.
UUCP	540	Kimlik onaylanmamış erişime izin verebilir.
NNTP	119	Ağ haberlerine erişmek ve onları okumak için.
Gopher	70	Proxy servisleri ve uygulama gateway ile kullanılmalıdır.
http	80	Proxy servisleri ve uygulama gateway ile kullanılmalıdır.

Çizelge 4.1. Filtrelenecek bazı servis ve port numaraları.

Güvenlik açısından paket filtreleme tipi güvenlik duvarları kurulurken yönetici; hangi tip verilerin, adreslerin ve çok yük getirecek işlerin reddedileceği yönünde yönlendirici üzerinde kuruluşu yapabilir. Ancak IP sahtekarlığı(Spoofing) tekniğini kullanan şifre çözücüler(hackers), IP başlığındaki bu adresleri çözümleyerek yönlendiricilerden kolaylıkla geçebilirler. Ayrıca bu yazılımın esas görevi yönlendirme olan yönlendiricilere bir ek yük getirmekte ve başarımın (performance) düşmesine neden olmaktadır.

4.5. Proxy Sistemleri

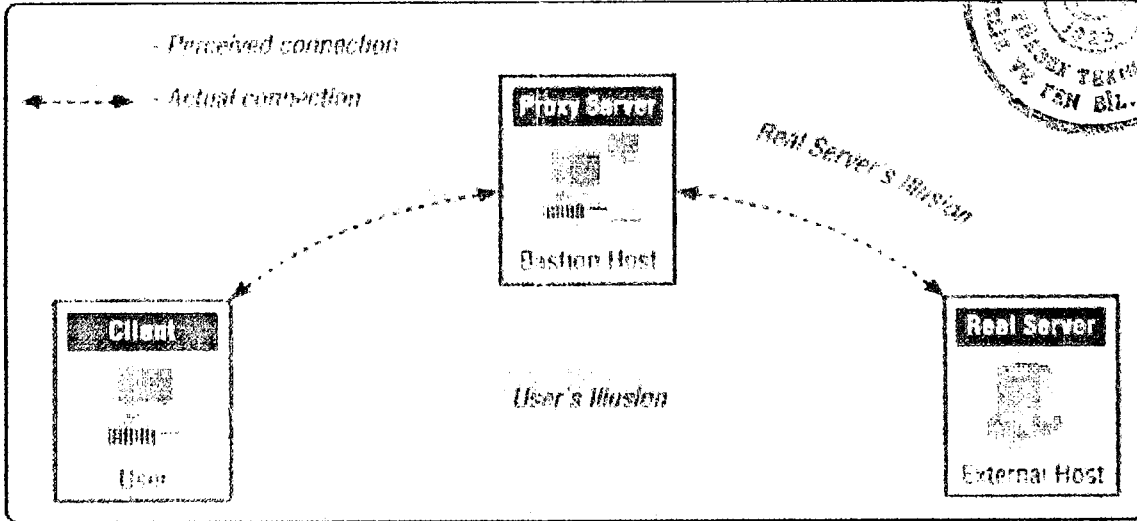
Bir intranetten internete pek çok şekilde bağlantı kurulabilir. Intranetten internet sayfalarına erişimi en performanslı hale getirmek, bağlantının gerçekleştirdiği bağlantı hattının yükünü azaltmak için proxy sunucu kullanımı çok yaygın bir uygulamadır. Bazı intranetler ise direkt router'lar aracılığıyla intranete bağlıdırlar. Proxy, bir host veya host grubunun internete erişimini sağlar.



Intranetteki kişilerin direkt olarak internet sunucu ve kaynaklarına erişimlerinde çok ciddi riskler vardır. Bir intranet kullanıcısı, kendi bilgisayarına ve intranete zarar veren bir dosya elde edebilir. Ayrıca, intranet kullanıcıları internete sınırsız haklarla bağlandığı zaman, bir intranet bilgisayarının ve sunucusunun çalışmasını bozacak harekette bulunan davetsiz misafirlerden korunması, intranet yöneticileri için daha da zorlaşır.

Bu tür bir erişimin engellenmesi için kullanılan ortak bir çözüm proxy sunucular kullanmaktır. Bu sunucular güvenlik duvarı arkasına, genellikle savunma(bastion) host üstüne yerleştirilir. Bunlar intranet kullanıcılarının internete kolay erişimlerini ve ağ güvenliğini korumakla ilgili iki işlevi dengelerler. İnternetteki bir kullanıcı, internette bilgiye ulaşmak veya bir web sayfasını ziyaret etmek gibi bir kaynağa erişmek isterse, internete direkt olarak bağlantı kuramazlar. Bunun yerine bir proxy sunucuyla bağlantı kurarlar ve proxy sunucuları internete bağlantıyı sağlarlar. (Örnek; web sunucu) Web sunucu proxy sunucuya ilgili sayfayı gönderir ve proxy sunucu da intranetteki kullanıcıya sayfayı gönderir.

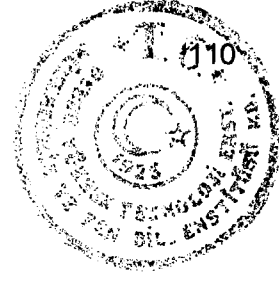
Proxy sunucuları yaptıkları tüm hareketleri kaydederler ve böylece intranet yöneticileri saldırıları kontrol edebilirler. Proxy sunucuları başka yararlar da sağlarlar. Web sayfaları kendi hafızalarından ara bellek olarak tutarlar böylece intranetteki birisi, daha önce eriştikleri bir web sayfasına tekrar ulaşmak istediğinde web sayfası direkt olarak proxy sunucudan getirilir ve istekte bulunan bir kişi internete açılmak zorunda kalmaz. İtranet bağlantıları, internet bağlantılarından daha yüksek hızlarda olmasından dolayı, web sayfalarına, internet kaynaklarına cevap süresi hızlanır. Bununla birlikte, stok takip gibi zamana duyarlı ürünler için bu erişim güncel olmayabilir. Çünkü yedeklenmiş(cached) web sayfaları konuyla ilgili en son sürümü içermeyebilir. (Şekil 4.11)



Şekil 4.11. Vekil(Proxy) sistemi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.191).

Tek bir intranette birden fazla proxy sunucu olabilir. Web, telnet, ftp ve diğer intranet servisleri için parçalı proxy sunucuları olabilir. İnternette bazı servisler sıklıkla proxy sunucular gerektirirler. Örneğin, bu telnet ve ftp'yi kapsayan herhangi bir şeyi içerebilir çünkü bunlar dosya transferi içerirler ve bir proxy sunucu üzerinde olması daha iyidir. Intranet yöneticisi, bu servisleri tamamen kapamaya veya proxy yazılımları yeni teknolojiyi içerene kadar kullanıma izin vereceğine karar vermelidir.

Bazen özel proxy istemci(client) yazılımları proxy servisleriyle uyum içinde kullanılmayı gerektirir. Bu problem olabilir. Çünkü tüm işletim sistemlerinin bütün intranet servisleri için proxy istemcileri yoktur. Bunlar kullanımı zor olan, standart olmayan istemci yazılımları içerebilir. Daha iyi bir yaklaşım ise, Netscape Navigator gibi standart bir yazılımı kullanmak ve yazılıma proxy sunucuların yerini belirten bir konfigürasyon kullanmaktır. Yazılım ve sunucu bundan sonrasını hallederler.



4.5.1. Proxy Sunucuları Nasıl Çalışır?

Birçok internet güvenlik sisteminin entegre parçası proxy sunuculardır. Proxy sunucu bir yazılımdır, güvenlik duvarı arkasında yer alan bir sunucudur ve intranet bilgisayarları ile internet arasında trafiği kontrol eder. Proxy sunucuları sıklıkla savunma(bastion) hostları üzerinde çalışırlar. Intranetteki birçok özel bilgisayar yerine sadece proxy sunucu internetle iletişimi kurar ve böylece güvenlik daha iyi sağlanır. Çünkü güvenlik, intranetteki birçok bilgisayar yerine tek bir sunucuda daha iyi sağlanır. Intranet yöneticileri ftp, telnet , web gibi birçok servisin kullanımı için proxy sunucuları ayarlayabilirler. Ayrıca intranet yöneticileri hangi internet servislerinin proxy sunucu vasıtasıyla gönderileceğine ve hangilerinin gönderilmeyeceğine karar verirler.

1. Intranetteki bir bilgisayar herhangi bir web sunucudan bir web sayfası getirmek için dış dünyadan(internet) bir istekte bulunursa, direkt internet sunucuyla bağlantı kurmaz, proxy sunucuyla bağlantı kurar. İnternet sunucu sayfayı daha sonra intranetteki bilgisayara ileten(forwarding) proxy sunucuya gönderir.

2. Proxy sunucuları, intranet ve internet arasındaki tüm trafiği kaydederler. Örneğin, Telnet proxy sunucusu intranetteki her telnet ortamındaki tuş vuruşlarını izler ve internetteki harici sunucunun bu tuş vuruşlarına karşı nasıl davrandığını da izler. Proxy sunucuları IP adresleri, erişim tarih ve zamanını, URL, indirilmiş(downloaded) byte miktarını bunun gibi pek çok şeyin kaydını tutabilir. Bu bilgi ağa karşı yapılmış herhangi bir saldırıyı analiz etmek için kullanılabilir. Ayrıca bu bilgiler, intranet yöneticilerine, çalışanlar için daha iyi erişim ve servis vermelerinde yardımcı olur.



3. Bazı proxy sunucuları özel proxy istemcileriyle (clients) çalışmak zorundadır. Popüler olarak proxy sunucu Netscape gibi standart istemciler kullanırlar. Bağımsız bir paket kullanıldığında, bu proxy sunucularla çalışması için konfigürasyon menüsünden özel olarak ayarlanmalıdır. Böylece intranet çalışan istemci yazılımını kullanabilir. İstemci yazılımı internet yerine bir proxy sunucuya gidip veriyi almayı sağlar.

4. Proxy sunucular, istekleri internet ve intranet arasında karşılamaktan daha fazla şeyler de yaparlar. Güvenlik tasarımlarını da tanımlayabilirler. Örneğin; bir ftp proxy sunucusu dosyaları internetten intranetteki bir bilgisayara gönderilmesi için ayarlanabilir, fakat dosyaların bir ticari ağdan internete gönderilmesini engelleyemezler. Bu yolla intranet yöneticileri kuruluş dışındaki kişilerin çok önemli kuruluş bilgilerini almalarını engelleyebilirler veya virüs içirme tehlikesi olan dosyaların yerel ağa indirilmesini engelleyebilirler.

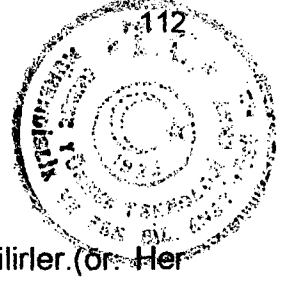
5. Proxy sunucuları, verileri kaydederek bazı internet servislerinin performanslarını arttırmak için de kullanılabilirler. Örneğin, bir web proxy sunucusu, birçok web sayfasını yedekleyebilir. Böylece intranetteki bir kişi bu web sayfalarından birine ulaşmak istediğinde bu sayfayı, yavaş olan internet hatlarından almak yerine çok daha hızlı olan intranet hatlarından proxy sunucu vasıtasıyla alabilirler.

4.5.2. Neden Proxy Sunucuları?

Proxy sunucularının birtakım avantajlarının yanında bazı dezavantajları da mevcuttur.

Proxy'nin Avantajları

- Proxy servisleri, kullanıcının internete direkt erişimlerini sağlarlar.
- Proxy servisleri, internete ulaşımındaki hareket kayıt işlemlerinde iyidirler.



Proxy'nin Dezavantajları

- Proxy servisleri, proxy olmayan servislerle yavaş ilerlerler.
- Proxy servisleri, her servis için farklı sunucular gerektirebilirler.(ör. Her protokol için)
 - Proxy servisleri, istemcilerde, prosedürlerde veya her ikisinde değişiklikler yapılmasını gerektirebilir.
 - Bazı servislerle çalışmayabilirler.(ör. *talk*)
 - Proxy servisleri, tüm protokol zayıflıklarından koruyamazlar.

4.5.3. Proxy Sunucu Terminolojisi

1. Uygulama Seviyeli Proxy'ler(Application Level Proxies): Belirli uygulama için sağladığı proxy servisleri hakkında bilgisi olan bir sistemdir. Uygulama protokolünde komutları anlar ve yorumlar. Özellikleri arasında ise; bilgi saklama, sağlam kimlik onaylama ve kayıt tutma, daha az kompleks filtreleme kuralları gösterilebilir.

2. Çevrim Seviyeli Proxy'ler(Circuit-Level Proxies): Bu tipte ise istemci ve sunucu arasında uygulama protokolünü yorumlamadan bir çevrim oluşturulur.

3. Adanmış Proxy'ler(Dedicated Proxies): Tek bir protokol gibi hizmet eder. Pratikte uygulama seviyeli gibi hareket ederler.

4. Genel Proxy'ler(Generic Proxies): Çoklu protokole hizmet eder. Pratikte ise çevrim seviyeli gibi hareket ederler.

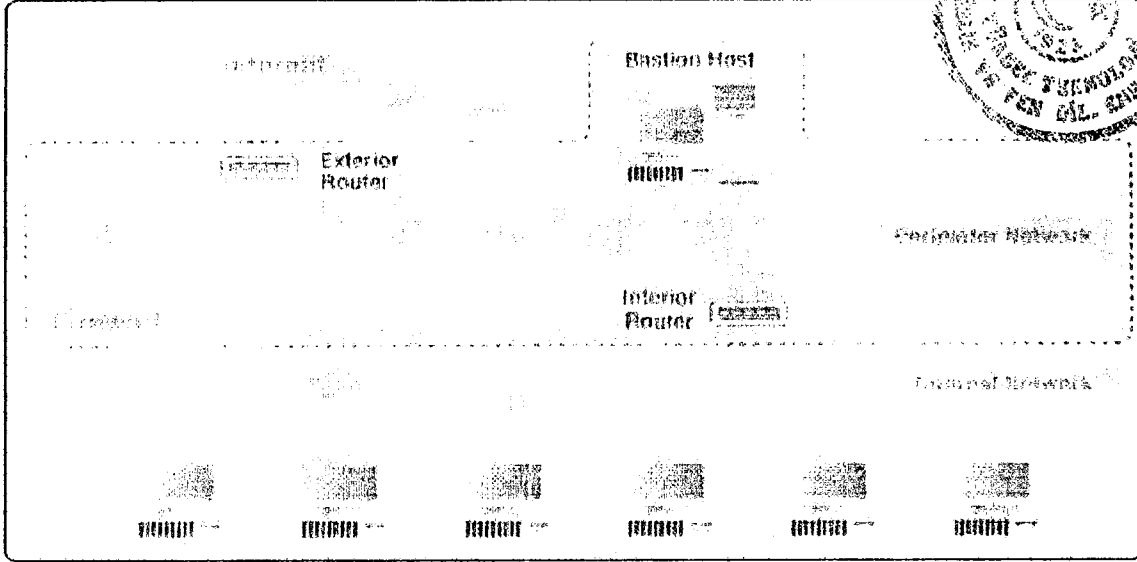
5. Akıllı Proxy'ler(Intelligent Proxies): Bir proxy gelen isteklerin dışında çok daha fazla iş gerçekleştirebilir. Örneğin; CERN HTTP proxy sunucusu verileri depolar ve böylece aynı veri için birden fazla istek olursa, bu verileri internetten getirmez.

4.6. İki Örnek Güvenlik Duvarı Tasarımı

Bu bölümde temel güvenlik duvarları için iki konfigürasyon örneği üzerinde durulacaktır. Gerçek dünyada güvenlik duvarları bu örneklerden çok daha kompleks olabilir. Bu örneklerde sağlanan servisler terminal erişimi, ftp, e-posta, Usenet haberleri, www ve DNS gibi sadece temel servisler olacaktır.

1. Perdelenmiş Alt-Ağ Mimarisi

En yaygın kendin-yap tipinde güvenlik duvarı mimarisidir. İyi güvenlik sağlar. Bu mimaride iki yönlendirici ve tek yönlendirici çeşidi vardır. Temel olarak iki arayüz yönlendirici çifti veya tek üçlü arayüz yönlendirici kullanılabilir. (Şekil 4.11) Tek yönlendirici perdelenmiş alt-ağ mimarisi hemen hemen iki yönlendirici perdelenmiş alt-ağ mimarisi kadar iyi çalışır ve fiyat olarak daha ucuzdur. Bununla birlikte her arayüzde gelen ve giden paket filtrelemeyi gerçekleştiren bir yönlendiriciye ihtiyaç duyulabilir. Bu örnekte daha basit olduğundan dolayı iki yönlendiricili olan seçilmiştir. Bu tip bir güvenlik duvarının parçaları şunlardır: Çevre ağı, dış yönlendirici, iç yönlendirici, savunma host. Dahili ağda ise posta sunucusu, Usenet haber sunucusu, DNS sunucusu ve çeşitli internet servisleri için istemci olsun. Bu dahili servislerin herbiri direkt(paket filtrelemeyle) veya dolaylı(savunma hostlarında proxy sunucularla) olarak sağlanır.



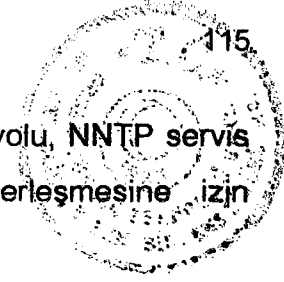
Şekil 4.12. Perdelenmiş alt-ağ mimarisi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.322).

Servis Konfigürasyonu

- **Telnet:** Giden Telnet istekleri paket filtreleme veya proxy ile sağlanabilir. Gelen Telnet servislerini güvenli bir şekilde sağlamak ise daha zordur. Eğer gerekli ise gelen Telnet ekstra bir kimlik onaylama kullanılarak savunma hostunda sağlanabilir.

- **FTP:** Ftp servisleri için pasif modda paket filtreleme ve yine pasif modda proxy desteği sağlanabilir.

- **SMTP:** Güvenli bir SMTP sunucusu savunma hostuna yerleştirilir. Daha sonra DNS kayıtları kullanılarak gelen tüm posta direkt savunma hostuna gönderilir. Daha sonra tüm posta tek dahili güvenli bir SMTP sunucuya iletilir. Başka yol olarak güvenli SMTP sunucusu direkt dahili posta sunucusuna yerleştirilebilir ve gelen posta ona yönettirebilir. Fakat SMTP sunucusuna girilirse dahili ağ tehlikede olur.



- **NNTP:** Güvenlik duvarı ile NNTP kurmanın en basit yolu, NNTP servis sağlayıcısının dahili Usenet haber host'uyla direkt haberleşmesine izin vermektir.

- **HTTP:** Dahili istemcilere http servisini sağlamak için yine paket filtreleme veya proxy sunucuları kullanılabilir. Paket filtreleme http sunucularına sadece standart portlardan erişime izin verir. Proxy ise tüm http sunucularına ulaşmalarına izin verir.

- **DNS:** Güvenlik duvarı ile DNS en iyi bir çift sunucu ile sağlanır. Biri savunma hostunda diğeri ise dahili ağdadır. Bu örnek için savunma hostundaki DNS sunucusu ikinci domain sunucudur ve birinci sunucu dahili ağdadır.

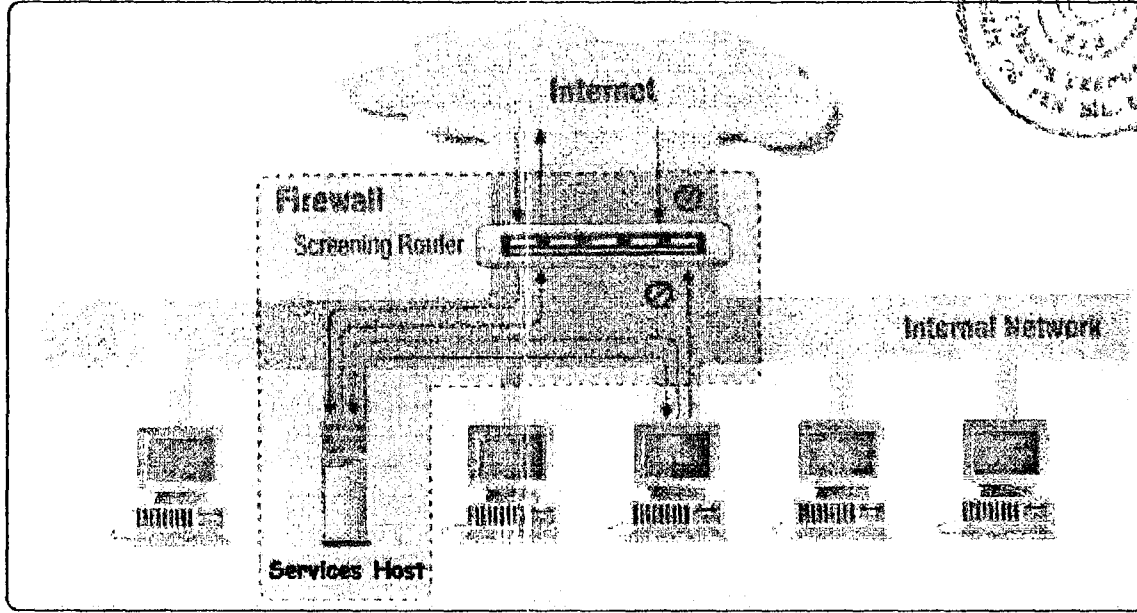
2. Perdelenmiş Sistem Mimarisi

Perdelenmiş alt-ağ mimarisine göre daha az güvenli, daha ucuz alternatif olan bir mimaridir. (Şekil 4.13) Sıklıkla çok önemli bütçe kısıtlaması yapan küçük işletmeler tarafından kullanılır. Bu mimaride çevre ağı, iç yönlendirici ve sıklıkla bastion host yoktur. Yönlendirici, dahili ağı korur ve ağa olan erişimi kontrol eder. Servis hostu(savunma hostu yerine) ise dış dünyayla etkileşmek içindir. Bu host site için genellikle posta sunucusu, Usenet haber sunucusu ve DNS sunucusu olur. Muhtemelen de dosya sunucusu, yazdırma sunucusu, vs. olabilir. Sitenin sahip olduğu tek sunucu makine de olabilir. Bu örnekte aşağıdaki kriterlere göre hareket edilecektir:

- Servis hostu sitenin posta sunucusu, haber sunucusu ve DNS sunucusudur fakat sitedeki tek makine değildir.

- Kullanıcılar güvenlik duvarında herhangi bir şey kaçırma konusunda güvenilirdir ve internet hareketlerini takip etmeye ve kayıt etmeye gerek yoktur.

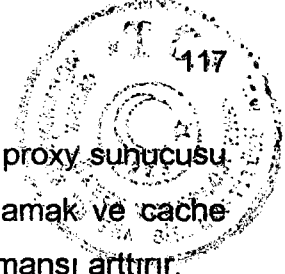
- Gerçek IP adresleri kullanılıyor.



Şekil 4.13. Perdelenmiş sistem mimarisi (Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.18).

Servis Konfigürasyonu

- **Telnet:** Telnet paket filtreleme ile güvenli ve uygun olarak sağlanabilir.
- **FTP:** Eğer dahili istemciler pasif FTP modunu destekliyorlarsa, FTP güvenli ve uygun bir şekilde paket filtreleme ile sağlanabilir. Pasif modu kullanmayan istemciler için Servis Host'una FTP proxy sunucusu kurulmalıdır. Eğer gerekirse pasif ve normal mod da desteklenebilir. Burada pasif mod desteklenmiştir.
- **SMTP:** Bu mimaride, SMTP kurmak için muhtemelen sadece tek bir iyi yol vardır. Gelen posta servis host'una yönlendirilmelidir. Gelen postanın direkt olarak dahili makinelerle gönderilmesi ise asla tavsiye edilmeyen bir yoldur.
- **NNTP:** SMTP gibi, NNTP kurmanın muhtemelen iyi tek bir yolu vardır. O da, dahili başka bir makineyi Usenet haber sunucusu yapmak ve NNTP'nin direkt ona yönelmesine izin vermektir. Böyle olursa servis host'u haber sunucusu olur.



- **HTTP:** Direkt olarak paket filtreleme ile dolaylı olarak da proxy sunucusu ile sağlanabilir. HTTP'yi dolaylı olarak proxy sunucusu ile sağlamak ve cache kullanmak istenen durumdur. Bunun da tek sebebi vardır. Performansı artırır.

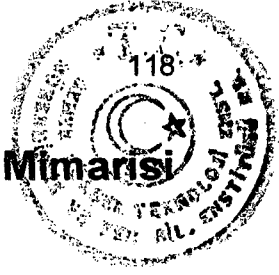
- **DNS:** DNS sunucusunun yerleştirilebileceği en iyi yer servis host'udur. Bu durumda şunlar kabul edilir:

- Servis host'u birinci DNS sunucusudur.
- Domain için harici bir DNS sunucusu vardır. Örneğin servis sağlayıcısında.
- Herhangi bir DNS bilgi gizlenmesi yapılmayacaktır.

Sonuçlar

Kurulum için perdelenmiş sistem mimarisi perdelenmiş alt-ağ mimarisinden daha ucuzdur fakat daha az güvenlidir. Tasarımda herhangi bir birlikte çalışma ve güvenli-çöküş yoktur. Perdelenmiş sistem mimarisinin sağladığı servisler daha azdır ve ne servisleri ne de güvenliği daha da arttırabilir.

İki mimari arasındaki fark; güvenlikte, ölçeklenebilirlikte ve servislerde olmak üzere çok büyüktür. Perdelenmiş sistem mimarisinde herhangi bir şey arttırılamaz. Mimari değişikliği yapılmadan destek makineleri bile arttırılamaz. [Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, 1995, s.18]



4.7. Ticari Bir Şirket İçin Güvenlik Duvarı Mimarisi Tasarımı

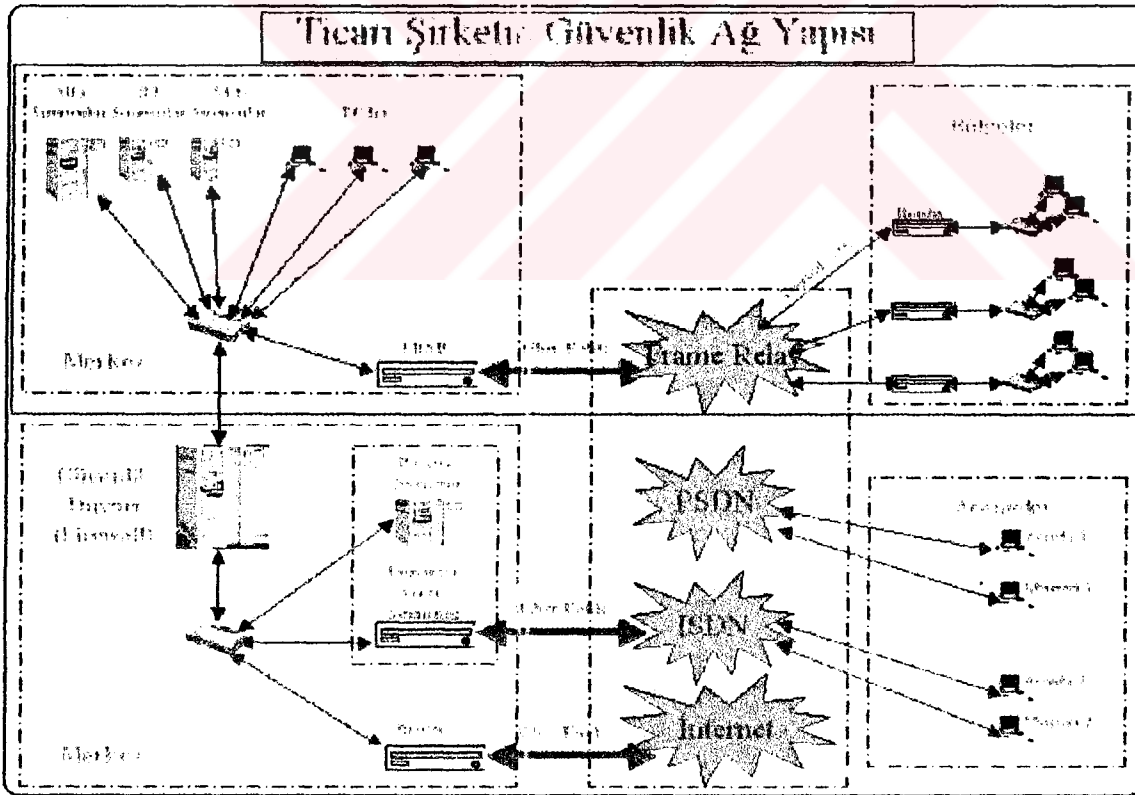
Uygulama olarak tasarlanan güvenlik duvarı mimarisi, yerel ve geniş alan ağına sahip olan bir şirketin, mevcut olan güvenlik duvarı mimarilerinin şirketin ağ yapısına göre özelleştirilmesi ile gerçekleştirilmiştir.

Mevcut olan ağ yapısı şirket içi yerel ağ ve bölgeler olmak üzere geniş alan ağ yapısını oluşturur. Bu ağ yapısında bölgeler tamamen özel kiralık hatlarla merkeze bağlı olduğu için bölgeler güvenlik açısından şirket içi olarak tasarlanmıştır. Bu ağ yapısı Şekil 4.14'de gösterilmiştir. Bölgelerin merkeze bağlantıları güvenli bağlantı olarak düşünülmüştür. Zira ağ mimarisi gereği şirket genel merkezindeki istemci bağlantılarından farklı değildir. Bu yüzden kurulan güvenlik mimarisinde bölgeler direkt olarak güvenlik duvarı ile iletişim içinde değildir. Bu hali hazırdaki mevcut durumu oluşturur.

Şirketin sağladığı servisleri arasında internet servis sağlayıcılığı(İSS) da yer almaktadır. Bu amaçla acentelerine ve gerekli görülürse dış müşterilere web, elektronik posta gibi servisler sağlamak amaçındadır.

Güvenlik ise tamamen dışarıdan normal ticari işlemleri veya internet erişimi için bağlanacak olan acenteler ve internet amaçlı bağlantı sağlayacak muhtemel müşteriler ve internet dünyası vasıtasıyla gelebilecek saldırılar için amaçlanmıştır. Mevcut sisteme internetten gelebilecek her türlü saldırı bu yolla olacaktır. Bu amaçla bu çeşitli saldırıları engellemek ve sistemin kesintisiz hizmet vermesini sağlamak için bir güvenlik duvarı sistemi kurulmuştur. Tasarımda düşünülen güvenlik şunları kapsayacaktır:

- Dışarıdan gelen tüm trafiğin istenildiği gibi yönetilebilmesi,
- Dışarıya giden tüm trafiğin istenildiği gibi yönetilebilmesi,
- Müşterilere sağlanan servislerin güvenli olması,
- Mevcut saldırılara karşı koruma sağlanması,
- Yeni saldırılarla karşı karşıya kalınma durumlarında ise saldırıya maruz kalan servis veya servislerin güvenli bir şekilde devre dışı kalması,
- Şirket verilerinin ve kaynaklarının korunmasını sağlaması,
- Sistemin devamlılığının sağlanması,
- Sistemin basit olması,
- İç ve dışı doğru olan trafiğin kaydının tutulabilmesi ve bu kayıtların raporlamasının iyi olması.



Şekil 4.14. Ticari bir şirketin güvenlik ağ mimarisi



Bu güvenlik duvarı sistemi, bahsi geçen mevcut mimariler içinden çift arayüzlü güvenlik duvarı mimarisinin şirket için özelleştirilmiş halidir. Normal olarak çift arayüzlü mimari daha önce de belirtildiği gibi, güvenlik amaçlı olarak kullanılacak olan bilgisayarın çevresinde en az iki ağın olmasından meydana gelir. Bu sistemle kurulan bilgisayar acentelerden, müşterilerden veya diğer internet kullanıcılarından gelen bilgi paketlerini arayüzlerin bağlı olduğu ağlar arasında yönlendirme işi de yapabilir. IP paketlerini şirket içinden dış dünyaya veya dış dünyadan gelen paketleri de dahili ağa yönlendirebilir. Fakat bu mimari sistemini kurmak için bu yönlendirme fonksiyonu iptal edilir. Böylelikle bir ağdan gelen paketler diğerine direkt olarak yönlendirilmezler. Güvenlik duvarı dahili ağdaki sistemleri ve bölgelerdeki sistemleri dış dünyadan ayırır.

Kurulan güvenlik sistemi donanım ve yazılımdan meydana gelmektedir. Sadece donanım olan sistemler de mevcuttur. Güvenlik olarak yazılımın da seçilmesi hem kontrol hem de tutulan kayıtların analizi bakımından esneklik sağlamaktadır. Seçilen güvenlik yazılımının kontrol mekanizması sağlanan servisler ve tasarlanan güvenlik politikası gibi özellikleri tam desteklemesidir. Ağlar arası olan hareketlerin kayıtlarının raporlaması oldukça kolaydır.

Bu sistemin istenilen güvenlik politikaları açısından özellikleri şunlardır:

- **Basitlik :** Çift arayüzlü güvenlik duvarı sisteminin çok basittir. Basitlik güvenlik stratejileri içinde yer alan en önemli unsurlardan biridir. Kurulan sistemin basit olması onun daha iyi anlaşılmasını sağlar. Bu sistem hem donanım olarak hemde yazılım olarak basittir. Bu sistem dahili ağ ile internet arasına kurulmuş çok basit bir sistemdir. Perdelenmiş güvenlik duvarı mimarisi ve perdelenmiş alt-ağ mimarisi donanım olarak daha komplekstir. Perdelenmiş güvenlik duvarı mimarisi ayrıca bir perdeleme yönlendiricisine ve savunma sistemine ihtiyaç duyar. Perdelenmiş alt-ağ mimarisinde ise bu yönlendirici çevre ağı oluşturulması bakımından ikiye çıkar ve güvenlik artarken karmaşıklık da artar.



▪ **Kontrol :** Çift arayüzlü güvenlik duvarı sistemi yüksek seviyede kontrol sağlar. Harici ve dahili ağ arasında paketlerin iletilmesine izin verilmek istenmezse, dış kaynak içerikli bir paketin dahili ağda olması bir güvenlik problemi. Bu sistem, özel bir servisin doğru çeşit bilgi içermeyen bağlantılarını iptal edebilir. Paket filtreleme, bu seviye kontrol konusunda zorlanır. Perdelenmiş sistem mimarileri ise temelde paket filtrelemeye dayanır. Bu sistemde savunma hostunun kontrolünün iyi yapılması ve güvenliğinin çok iyi sağlanmış olması gerekir. Perdelenmiş alt-ağ sistem mimarilerinde ise dahili ve harici yönlendiricilerin ayrı ayrı kontrolü gerekir. Güvenlik olarak daha etkilidir. Saldırganlar iki yönlendiriciyi aşmak durumundadırlar fakat kontrol daha kompleks hale gelmiştir. Bu sistem aynı zamanda çift kontrol gerektirmesi bakımında performans düşüklüğü oluşturabilir.

▪ Çift arayüzlü güvenlik duvarı sistemi çoklu ağlara bağlı olarak servis sağlayabilir. Fakat yönlendirme kapalıdır. Perdelenmiş sistemde ise sadece dahili ağa bağlı olarak bölümlendirilmiş yönlendirici kullanarak servis sağlar. Birincil güvenlik paket filtreleme ile sağlanır. Bu mimari paketleri internetten dahili ağa açtığı için risk taşımaktadır. Savunma bilgisayarı dahili ağda olduğundan buna erişim durumunda tüm ağ saldırısının elinin altında olur. Bu konuda perdelenmiş alt-ağ mimarisi çevre ağı oluşturarak çift koruma sağlar. Herhangi bir saldırı ilk anda sadece çevre ağını dinleyebilir ve böylece dahili ağ korunmuş olur.

▪ Seçilen çift arayüz mimarisinde, güvenlik açısından, gerekli boşlukların doldurulması yazılım olarak sağlanır. Bu yazılım sayesinde gerekli yetkiler ve politikalar tanımlanır. Tanımlanan bu politikalar donanımla bütünleşik olarak ağ trafiğini kontrol eder. Diğer mimariler güvenlik olarak bu sistemden daha iyi durumdadır.

▪ Çift arayüz mimarisi diğer mimarilerden maliyet açısından daha avantajlıdır. Bu mimarinin seçilmesinde bu da göz önünde bulundurulmuştur.

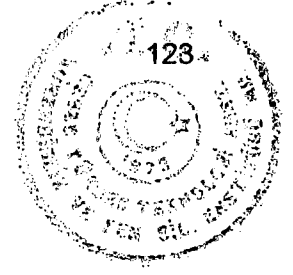
▪ Çift arayüz mimarisi, servisleri sadece vekil(proxy) olarak veya kullanıcıların sisteme direkt bağlanmalarıyla sağlar. Kullanıcı hesapları da

kendileri güvenlik problemleri içerirler. Çoğu kullanıcılar bu sistemi bağlanarak(login) kullanmayı güvenli bulmazlar. Proxy sistemi daha az problemlidir. Fakat istenilen servisleri sağlaması ve performans açısından kullanılması oldukça faydalıdır.

Seçilen yazılım ürününün özellikleri ise şunlardır:

- Yazılım olarak seçilen ürünün kurulumu ve yönetimi oldukça basittir.
- Tanımlanan güvenlik politikaları konusunda üstün kontrol sağlar.
- İstenilen seviyede güvenlik politikalarını tanımlar.
- Yönetimi oldukça kolaydır.
- Uzaktan yönetim özelliği ile her yerden yönetim yapılabilir. Uzaktan yönetimde istemci ise sunucu arasında yine kendi güvenlik sistemini kullanır. Veriler şifrelenir.

- Grafik arabirimi desteği de kullanımı kolaylaştırmaktadır.



5. TİCARİ UYGULAMA

5.1. Giriş

Bu bölümde ticari sahada iş yapan bir şirketin karşılaştığı güvenlik problemini nasıl çözdüğü üzerinde durulacaktır. Bu ürün seçilirken göz önünde bulunan kriterler hakkında bilgi verilecektir. Ayrıca ticari alanda güvenlik duvarı pazarında bulunan üç ürün hakkında bilgi verilecektir.

5.2. Ürün İnceleme

Bu bölümde, ticari olarak dünya çapında dikkat çeken üç adet güvenlik duvarı ürünü incelemeye alınmıştır. Tüm bu ürünler testlerde gereken güvenliği göstermişlerdir fakat sahip oldukları arayüzler ve özellikler farklıdır. Ticari bir şirket için ise bir güvenlik duvarı ürününün güvenilirliğinin yanında kullanılışı ve yönetimi oldukça önem arzeder. Bu yüzden bir ürün alınmadan önce onun bu hususiyetleri iyi tespit edilmelidir.

5.2.1. Ürün Değerlendirme Kriterleri

1- Güvenlik

Pek çok adet servis için en yüksek güvenlik sağlayan güvenlik duvarı seçilmelidir. Bu duvar aynı zamanda web, e-posta ve ftp servisleri için güvenlik sağlamalı ve gelişmelere açık olmalıdır. Bunun için dört soru yöneltilmelidir;

- a- Hangi güvenlik duvarı teknolojisini kullanılıyor?
- b- İşletim sistemi güvenlik altına alınıyor mu?
- c- NAT kaç tip bulunuyor ?
- d- SNMP hassaslığı var mı ?



Güvenlik duvarının uygun olduğuna emin olmak gerekir. Unutulmamalıdır ki çok az ürün iki farklı ağ arayüzünü destekler.

2- Tümlleşme (Integration)

Aşağıdaki soruların yanıtlarını aramada yarar vardır;

- 10 kullanıcıdan daha az ofisler için çözüm var mı ?
- Çoklu uyarılama var mı ?
- Dial-up desteğı var mı ?

3- Kurulması ve Kullanımı

Güvenlik duvarının kurulması ve kullanımı kolay olmalıdır. Eğer çok karmaşık ve kurulması kolay olmayan bir yazılım seçilirse, kuruluş için kurum dışı desteklere gereksinim doğar ki, bu da ek bir gider demektir. Ayrıca kullanımı da çok kolay olmalıdır. Kuruluşu izleyen ve kurumca verilen eğitim, kurum elemanları değışse bile ek eğitimlere gereksinme bırakmayacak kadar kullanımı kolay olmalıdır. Bunun için ise şu sorular yöneltilebilir;

- Kuruluşu son kullanıcı tarafından yapılabilir mi?
- Kuruluş için ne kadar süre gerekir?
- Yönlendirme tablolarında düzenlemeler gerekir mi?
- Kullanım ne derecede kolaydır?
- NAR(Network Address Rotation) var mı?

4- Başarımı (Performance),

5- Yerine Getirdiğı Görevler,

6- Görüntüleme, Raporlama ve Uyarı Konusunda sağladıkları ,

7- İletişim Yönetim Araçları,

8- Band Genişliğı ve Üretkenlik Yönetimi Konusundaki Etkinlikleri,

9- Çeşitli Adette Kullanıcı İçin Fiyat.



5.2.2. Güvenlik Duvarı Satın Alırken

- **Fiyat:** Donanım ve yazılım içeren toplam sistemlerin maliyetini ifade eder.
- **Satılan Nesne:** Güvenlik Duvarları, günümüzde dahili ağlar ile internet arasındaki bağlantılarda güvenlik sağlamada satılan en iyi çözümlerdir.
- **Hesaplı Güvenlik Duvarı:** İyi fiyatlar acente sözleşmeleriyle elde edilebilir. Bununla birlikte fiyat güvenlik duvarı alırken baş etken olmamalıdır. Performans ve özellikleri çok daha önemlidir.
- **Özellikleri Belirleme:** Güvenlik Duvarları uzaktan kontrol edilmek isteniyorsa bu gerekliliği belirtilmelidir. Diğer güzel bir özellik, tüm ağ istemcilerine yazılım kurma ihtiyacını ortadan kaldıran transparan proxy sistemi gerekir. Ayrıca grafik kullanıcı arayüzü ya da Unix stili bir sistem kullanılacağı belirlenmelidir.

İlk kuşak güvenlik duvarları paket filtreleme veya proxy servisleri metotlarından birini kullanıyorlardı. Bu temel fonksiyonlar değişmedi fakat kullandıkları metotlar gelişti. Tartışılacak tüm güvenlik duvarları, paket filtreleme, proxy servisleri kullanma veya her ikisini birden kullanabilirler. Fakat çoğu eski tarz güvenlik duvarlarından çok daha gelişmiş ve kolay yönetme yöntemleri geliştirilmiştir. Transparent proxy servisi, VPN(Virtual Private Network) bunlardan bazılarıdır.

5.2.3. Ticari Güvenlik Duvarı Ürünleri

Ticari ürün olarak dünyada kullanım olarak yaygın olan ve kendini ispat etmiş ürünlerden üç tanesi çeşitli kriterlere göre incelenecektir. Bu ürünlerin geniş bir listesi EK-1'de verilmiştir. Burada şu unutulmamalıdır ki, ürünler zamanla daha da gelişmekte ve yeni teknolojilere yönelmektedirler. Bu durumda buradaki kriterler geçmiş ve günümüz şartlarına göre değerlendirilmiştir. Güncel

bilgiler ışığında ürünlerin dünyadaki yeri, geçen zamana göre bu ürünlerde olan gelişim eğilimine göre, takip edilmelidir.



1. Check Point FireWall-1

FireWall-1, **Check Point Software Technologies** şirketinin geliştirdiği ve bir endüstri standartıdır. Açık tasarımı nedeniyle hemen hemen her türlü güvenlik duvarı beklentileri karşılar. FireWall-1 iki modüle sahiptir:

1. **İnceleme Modülü:** Güvenlik politikasını, log olaylarını işleme alır.
2. **Kontrol Modülü:** İletişimin devamını sağlar. Bu modül ayrıca lisan yönetimi, yönetici ve istemci kuruluşu, uzaktan erişim modülleri, IP'lerin gönderilmesi, güvenlik sunucuları ve SMTP güvenlik sunucusunu da yönetmektedir.

FireWall-1, geniş bir raporlama ve logging sağlar. Log kütükleri ile ilgili bilgi, paketler üzerinden taşınır. Bu bilgiler ağ trafiğinde neler olduğuna dair çok açık görüşler ortaya koyar.

FireWall-1 güvenlik politikası, ağ nesnelerinden, protokol çeşitlerinden, kullanıcı tanımlı servisler ve kurallardan oluşur. Bu politika menüsündeki bütün yönetim fonksiyonları ile birlikte çalışır. Ağ nesneleri, servisleri, kaynakları, sunucuları, kullanıcıları, zaman ve anahtarlar yönetim elemanlarının ilk adım tipleridir. Yönetilebilirliğindeki üstünlüğü ve genel olarak uygunluğuna karşılık, kuruluşundaki güçlük nedeniyle deneyimli personel gereksinmesi onun eksik bir yönü olarak görülebilir.

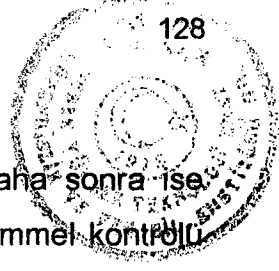
Microsoft Windows 95 üzerine kurulan ve Windows NT veya Unix tabanlı Check Point güvenlik duvarları uzaktan yönetme aracı bu ürünler arasındaki büyük bir gelişmedir.

▪ **Kurulum:** Ürünü, Microsoft Windows NT üzerine kurmak için sadece kurulum sihirbazındaki adımları takip etmek yeterli olmaktadır. Unix üzerine kurmakta ise biraz rahatlık vardır. Kullanıcıya ürün ve istenen konfigürasyon hakkında bir takım soruların yer aldığı bir metin(script) kurar. Metin daha sonra Unix RC metinlerinde gerekli modifikasyonları icra eder. 3.x önceki versiyonlarında farklı olarak Unix kernel(çekirdek)'in dahili otomatik IP izleme işlemini durdurabilir. Bu sistem açılış sırasında kural veri tabanına herhangi bir şey olursa, olabilecek potansiyel güvenlik akışını elimine eder. CheckPoint FireWall-1 kurulum için tatminkar bir puan sunar.

▪ **Yönetim:** CheckPoint'in yönetim grafik ara yüzü çok açıktır ve yeni kurallar ve güvenlik politikaları tanımlamak olabildiğince kolaydır. Paket filtreleme kurallarının grafiksel sunumu sezgiseldir ve kolaysa anlaşılabilir. Ayarlamalarda yanlışlıkla olacak bir hata ihtimalini minimize eder. Bu ürünün uzaktan koruma yönetimi özelliği sayesinde, ağ yöneticileri güvenlik duvarı konfigürasyonlarını kontrol edebilir ve gerekli değişiklikleri bulundukları yerden yapabilirler. Uzaktan yönetim aracı güvenlik duvarı ile şifrelenmiş paketler aracılığıyla haberleşir.

Paket filtreleme kuralları oluşturmak kolaydır. Check Point FireWall-1 tüm trafik çeşitiyle birlikte gelir. Temel HTTP servislerinden RealAudio'ya kadar servisleri destekler. Basit olarak yapılması gereken kaynak, hedef, trafik tipi ve hareketi seçmektir. Diğer detaylar güvenlik duvarı tarafından kontrol edilir. Kullanıcılar ve gruplar eklemek ve onlar için kurallar tanımlamak, paket filtreleme kuralları eklemek kadar kolaydır.

▪ **Esneklik:** Firewall-1'in esnekliği diğer ürünlerle karşılaştırıldığında iyi bir puan almıştır. Proxy hostları, paket filtreleme, ve sanal gerçekleştirme konfigürasyonu sunar. UDP desteği vardır. Kimlik onaylama Secure/ID diğer veya birkaç yöntemle yapılır. Zaman ve tarih temelli ayar sunar. Ağ trafiği konusunda yöneticilere çok fazla kontrol imkanı sağlar.



- **Güvenlik:** İlk kurulumda hiç bir trafiğe izin vermez. Daha sonra ise sadece kuralları tanımlanan trafiğe izin verir. Güvenlik için mükemmel kontrolü vardır.

2. CyberGuard FireWall 3.0

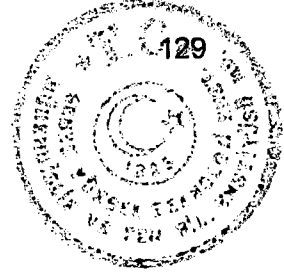
Harris Computer Systems Corp. (HCSC) şirketinin CyberGuard Firewall 3.0 ürünü alanında en gelişmiş ürünlerden biridir. Standart Intel Corp. platformlarında çalışmakta ve çok işlemcili sistemleri desteklemektedir.

- **Kurulum:** Çok kolay bir kurulum hayal etmek güçtür. Her ne kadar güvenlik politikaları bilinse de bu ürün gerekli konfigürasyonları yapabilir.

- **Yönetim:** Yönetim konsolu gerekli ayarlamaların yapılması için çok iyi geliştirilmiştir. Paket filtrellemeyi kolay anlaşılabilir bir tabloda gerçekleştirir. Kurallar yukarıdan aşağıya çalıştırılırlar. Yeni kurallar koymak kolaydır. IP adres çevirimi ve IP spoofing taraması tek bir kontrol kutusu(check box) ile yapılır ve anında aktif olur.

- **Esneklik:** Proxy'ler ve paket filtreleme özelliklerini desteği çok esnek bir çözümdür. IP adres çevirimi başka bir araçtır ve yöneticilere, güvenlik duvarını özel çevre için ayarlamalarını sağlar. Proxy'ler RealAudio ve birkaç UDP de dahil her protokol için sanal olarak vardır. Geniş anlamda kimlik onaylama mevcuttur. Zaman ve tarih temelli konfigürasyon desteği vardır.

- **Güvenlik:** İlk olarak herhangi bir trafiğe izin vermemektedir. Daha sonra ağ kuralları tanımlandıktan sonra izin verilen trafiği dahili veya harici ağa geçirir.



3. Guardian

Guardian **NetGuard**'ın Windows Nt 4.0 üzerine geliştirdiği bir endüstri standardıdır. Guardian güvenlik duvarı sistemi iki temel modülden oluşur:

- 1- Guardian Manager,**
- 2- Guardian Acenta (Agent)**

Guardian ağ güvenliğini **MAC Katmanlı – Stateful Inspection Teknolojisi**” kullanarak gerçekleştirmektedir. Teknolojisi TCP/IP protokolünün en üst katmanında ve Network Address Translation (NAT)'da paketlerin kontrol edilme mantığına göre kurulmuştur. Böylece hem işletim sistemi güvenliği sağlanır hem de başarımlar yüksek olmaktadır.

- **Yönetim:** Guardian acentası iç ve dış ağlar arasında bulunurken, Guardian yöneticisi ağ üzerinde uzak noktadaki her hangi bir yerde bulunabilir. Yönetici, verileri görüntülemek için acenta ile şifrelenmiş bir ilişki kurar. Acenta, ağ iletişiminin durumunu gösteren gerçek zamanlı grafik gösterimlerinin, yöneticiler istiyorsa, görüntülenmesini sağlar.

- **Esnelik:** Guardian'ın NAT stratejisi, ağ adres gönderimi için kuralları devam ettirme esasına dayanır. Guardian'ın sağladığı özellikleri aşağıdaki şekilde özetleyebiliriz:

1. Kullanıcıların bağlantılarından doğan sorunları gerçek zamanlı olarak görüntüler,
2. Ağ başarımlar problemini belirler,

3. Yürümekte olan oturumlarda uyarı ve log'ları anında görüntüler,
4. Geçmişte olan bilgileri MS Access veri tabanında saklar ve yöneticiye hali hazırda oturumun devamı anında bu bilgilere ulaşma olanağı sağlar,
5. Guardian, güvenlik duvarı stratejisine etki etmeden geçici kuralların dinamik uygulamalarını olanaklı kılar,
6. Guardian, band genişliği ve kontrolünü olanaklı kılar,
7. Guardian, diğer kullanıcı tanımlı servisler kadar TCP/IP ve UDP'yi de destekler.

▪ **Güvenlik:** Ağ için gerekli kural tanımlamaları yapıldıktan sonra istenilen trafik kontrolü ve güvenlik oluşmaktadır.

5.3. Ticari Şirket Tanıtımı

Uygulama yapılan şirket sigortacılık sektöründe hizmet vermektedir. Bu sektörde hizmet veren diğer şirketlerle kıyaslama yapılırken oldukça iyi bir bilgi işlem teknolojisine sahip olan şirketin bilgisayar sistemleri, temel olarak üç bölümde incelenebilir.

1. Genel Müdürlük: Bilgi işlem merkezi(BİM) genel müdürlükte bulunmaktadır. BİM'de ethernet network ile haberleşen yedi adet sunucu bilgisayar vardır. Şirketin diğer birimlerinde PC ve dummy terminal istemciler kullanılmaktadır. Genel müdürlük iki binadan oluşmaktadır. İki bina arasındaki iletişim fiber optik bağlantısı ile gerçekleştirilmektedir. Uygulama programları BİM personeli tarafından C, Oracle ProC, Microsoft Visual C++ kullanılarak geliştirilmektedir.

Bilgisayarların kullanım amaçları, teknik özellikleri ve network ürünleri aşağıdaki çizelgelerdedir.

Kullanım Amacı	Teknik özellikleri	İşletim Sistemi
Oracle Veritabanı Sunucusu	Digital Alpha 4100	Digital Unix
Uygulama Sunucusu	Digital Alpha 2*2100	Digital Unix
Uygulama Geliştirme Sunucusu	Digital Alpha 2100	Digital Unix
Dial-up iletişim Sunucusu	Intel PentiumII	SCO Unix
Dosya ve Yazıcı Sunucusu	Intel PentiumII	MS Windows NT
FireWall Sunucu	Intel Pentium	MS Windows NT
Web, Mail Sunucusu	Intel PentiumII	MS Windows NT

Çizelge 5.1. Bilgisayarların özellikleri ve kullanım amaçları

Kullanım Amacı	Teknik özellikleri
Frame Relay Erişim Cihazı	Motorola Vanguard 6560 Router Pro
ISDN dial-up iletişim sunucusu	Cisco AS500 Router
TT için Fiber Optik PCM sistemi	Siemens DSMX 2/32 PCM Sistemi
BackBone switch	Cisco Catalyst 2916
Kiralık ve dial-up devre bağlantı	Çeşitli marka ve sayıda modem

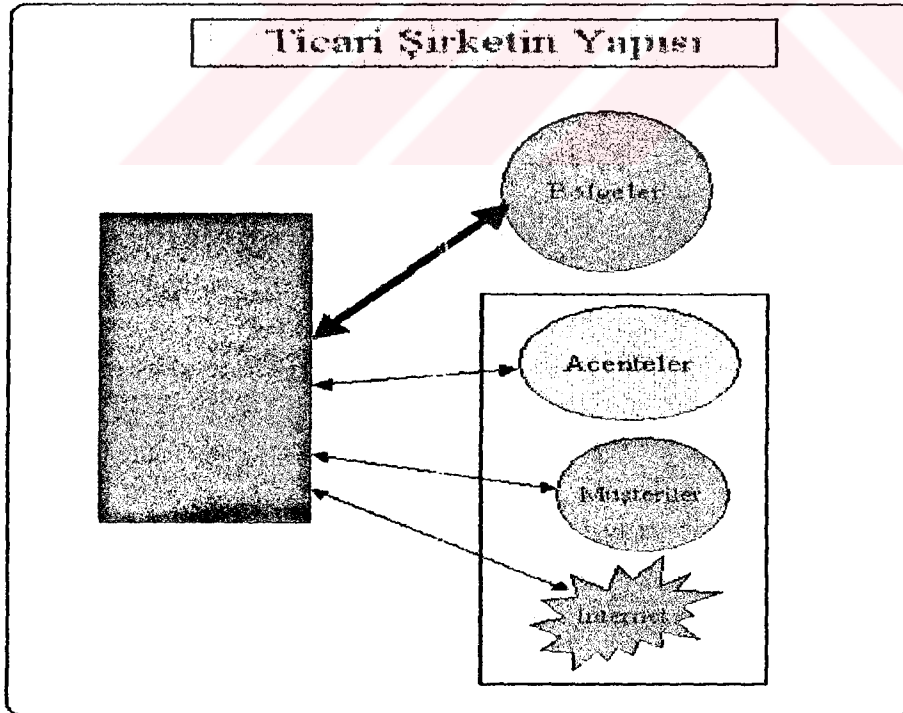
Çizelge 5.2. Ağ elemanlarının özellikleri ve kullanım amaçları

2. Bölge Müdürlükleri: Bölge müdürlüklerinde sunucu bilgisayar yoktur. Frame Relay üzerinden merkezi bilgisayar sistemi ile iletişim gerçekleştirilmektedir. İstemci olarak PC'ler kullanılmaktadır. Frame Relay erişim cihazı olarak Motorola Vanguard 320 kullanılmaktadır. Ayrıca bölge müdürlüklerinin PBX santralleri motorola routerlar yardımıyla frame relay devreleri üzerinden genel müdürlükteki PBX santrali ile haberleştirilmektedir. Böylece telekom telefon şebekesine çıkmadan telefon görüşmeleri gerçekleştirilmektedir.

3. Acenteler: Acentelerin kullanımı için MS Windows 9x üzerinde çalışan bir acente otomasyon programı geliştirilmiştir. Bu program windows'un çevirmeli ağ bağlantısını kullanarak, merkezi bilgisayar sistemindeki iletişim sunucuları yardımı ile uygulama sunucusuna bağlanarak on-line işlem yapılmasını sağlamaktadır. Program Visual C++ kullanılarak grafik tabanlı olarak geliştirilmiştir.

Tüm bu bilgiler ışığında şirket, kurmuş olduğu intranet yapısıyla internete açılmak durumundadır. Bunun için de güvenlik en önemli bir etken durumuna gelmiştir. Gerekli güvenliği de satın aldığı ve dünyada geniş kullanım alanı olan, kendisini ispat etmiş Check Point FireWall-1 ürünüyle sağlamaktadır. Bu çalışma da aslen bu güvenlik sorununa nasıl çözüm bulunduğu üzerinedir.

Yukarıda tanıtılan şirkette seçilen ürün; kendi dalında dünya pazarı pastasındaki diliminin büyüklüğü, referansları, kurulum sonrası desteği ve bakım, güvenilirliği ve fiyat şartları ışığında Check Point FireWall-1 olmuştur.

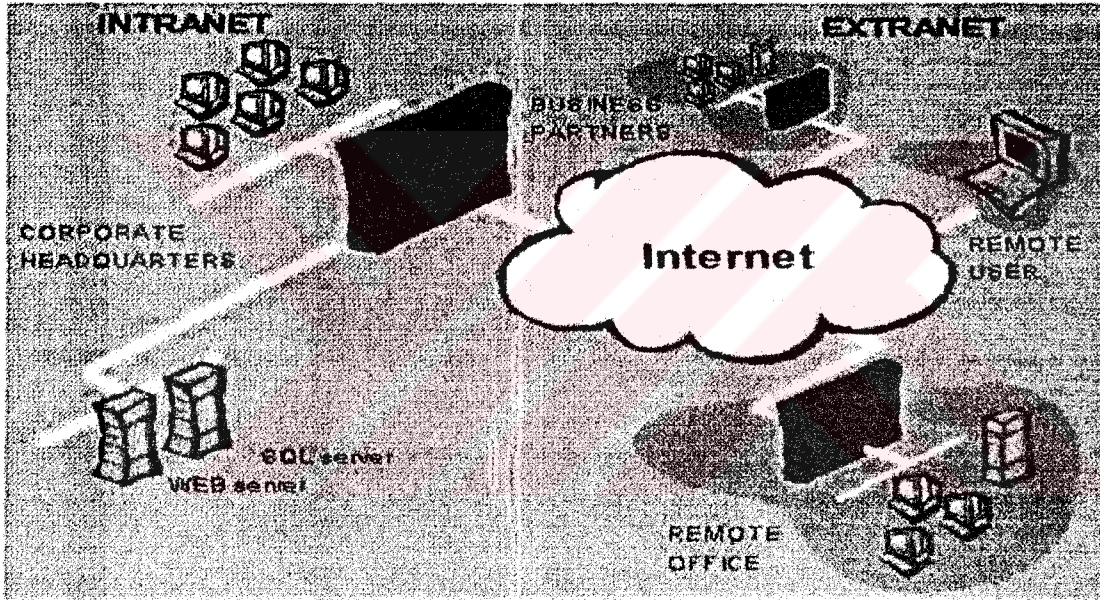


Şekil 5.1. Ticari bir şirketin yapısı

5.4. Ticari Ürün İnceleme(Check Point Firewall-1)

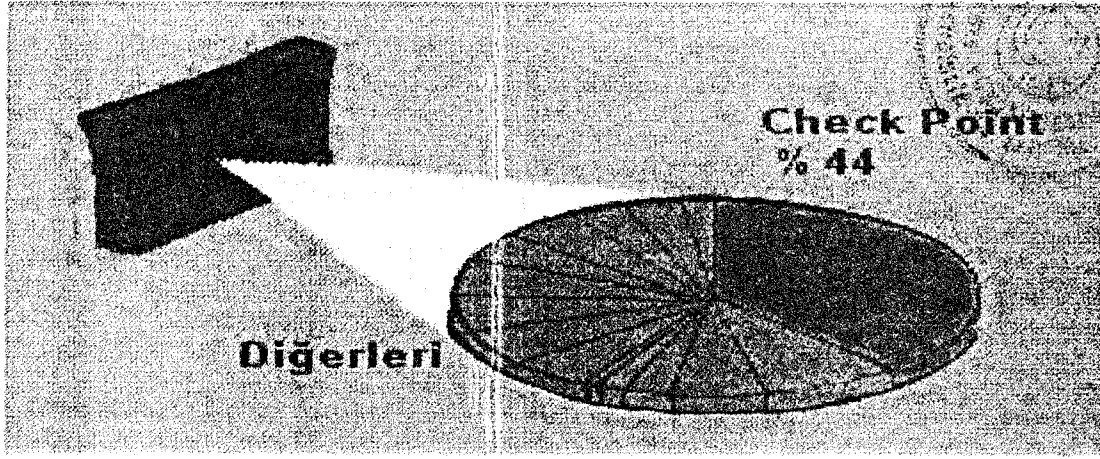
▪ İnternet teknolojisi bir şirkete imkanlar dünyasının kapılarını açar: İnternet üzerinden yapılan işlemlerin çeşitliliğinin sürekli gelişmesi ve hacminin artması şirketleri bu konuda yatırım yapmaya iten etken olmuştur. Mali açıdan internet üzerinde sağlanan gelirler şirketler için artık yeni bir iş alanı haline gelmiştir.

▪ CheckPoint Firewall-1, nesneye-dayalı bir mimari içerir ve ağ elemanlarını kolay ve mantıksal olarak yönetmeyi sağlar.



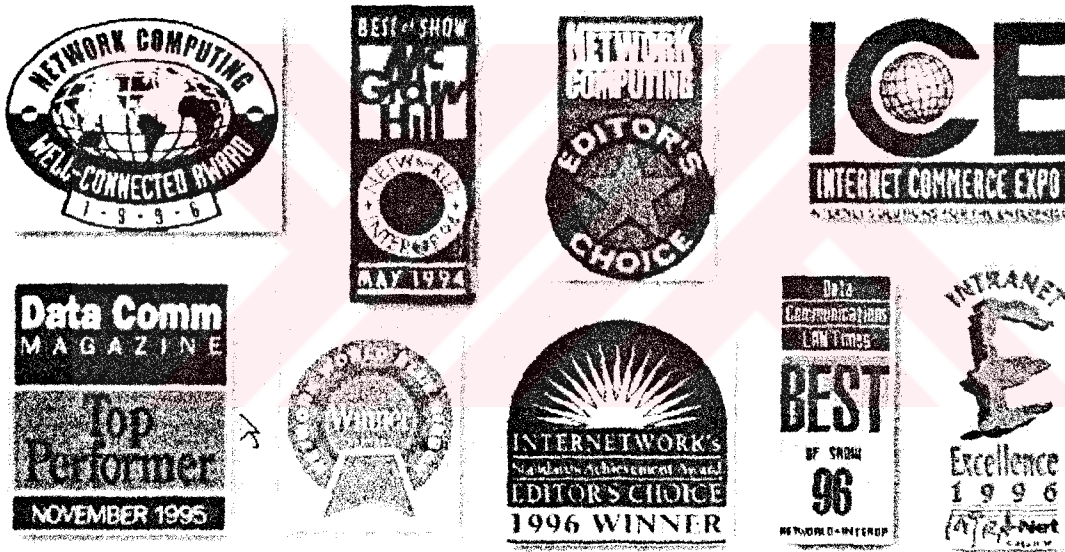
Şekil 5.2. İnternet dünyası (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

- Finansal topluluğun favorisidir.
- Endüstri analistlerinin ağ/sistem güvenliği konusundaki seçimidir.
- CheckPoint Firewall-1, ihtiyaç duyulan güvenli bağlantıyı kurar ve bunu açık pazar lideri olarak ispatlanmış çözümlerle sağlar. (Şekil 5.3)



Şekil 5.3. Check Point Firewall-1 pazar payı (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

- CheckPoint Firewall-1, birçok ödül almıştır. (Şekil 5.4)



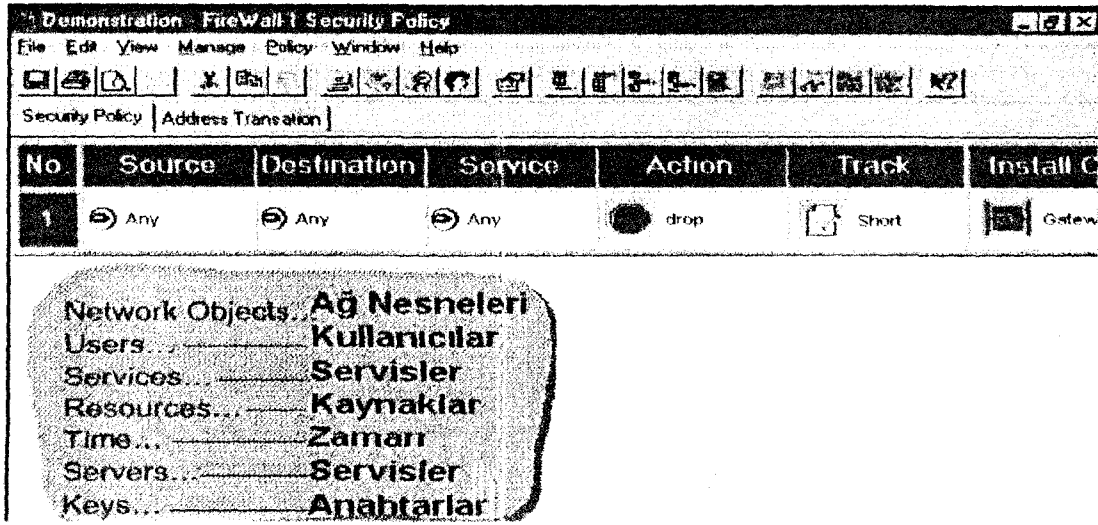
Şekil 5.4. Check Point Firewall-1 ödülleri (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

5.5. Check Point FireWall-1 Özellikleri

Check Point FireWall-1 tamamen nesneye dayalı bir mimari üzerine inşa edilmiştir. FireWall-1, çeşitli yöneticiler içerir.

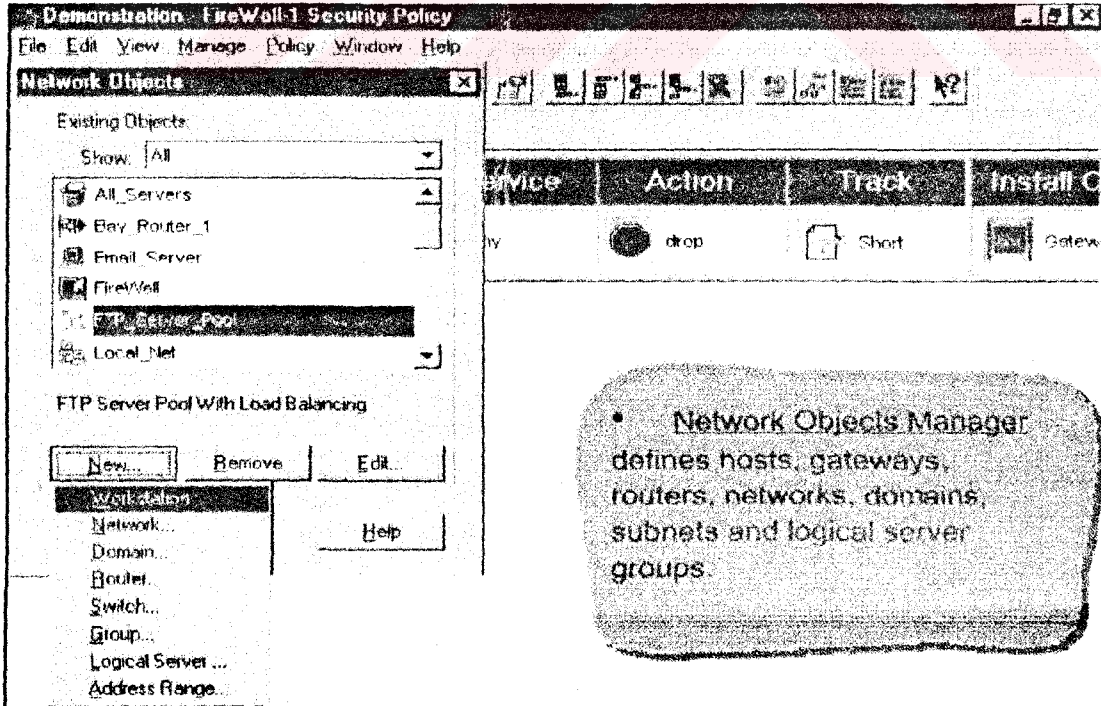
5.5.1. FireWall-1 Yöneticileri

FireWall-1 yedi tane yöneticiye sahiptir. (Şekil 5.5)



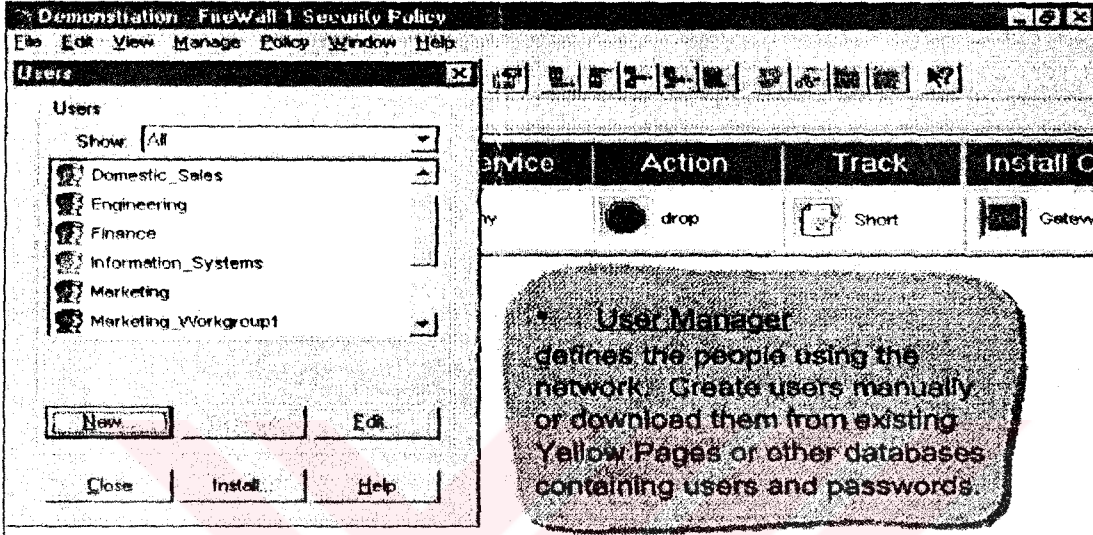
Şekil 5.5. Check Point Firewall-1 yöneticileri (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

1. **Ağ Nesneleri Yöneticisi:** Host, gateway, router, ağ, domain, altağlar ve mantıksal sunucu gruplarını tanımlar.



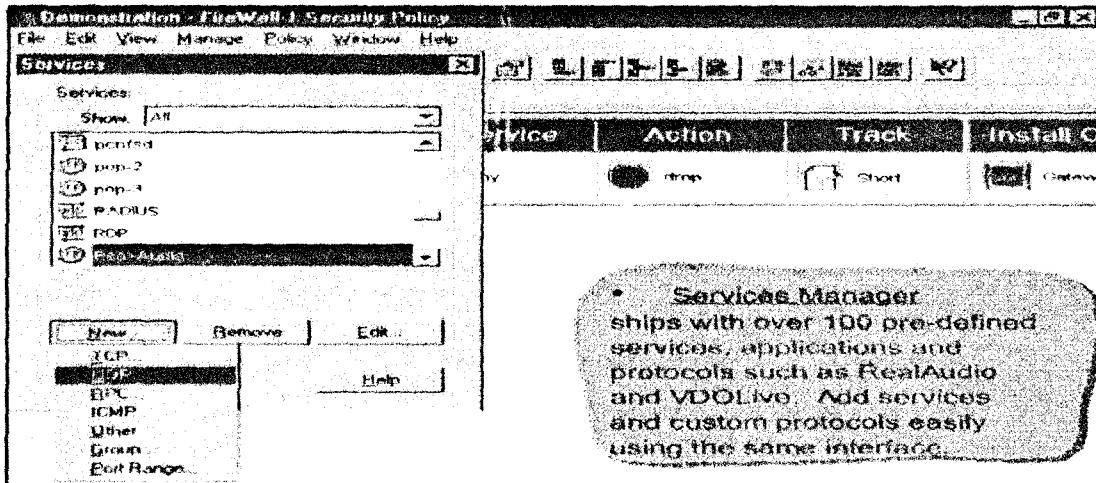
Şekil 5.6. Ağ nesneleri yöneticisi (Check Point FireWall-1, 1997).

2. Kullanıcı Yöneticisi: Kullanıcı yöneticisi, ağı kullanan insanları tanımlama işlemini yapar. Kullanıcıların elle tanımlanmalarını veya var olan Sarı Sayfalardan ya da diğer veri tabanlarından kullanıcı isimleri ve şifreleri ile beraber indirilmelerini sağlar. Tanımlanan bu kullanıcıların haricindeki kullanıcı isimleri bu sisteme erişme, ya da dahil, ağda bulunan kişilerin ağ dışına veri göndermesi engellenmiş olur. (Şekil 5.7)



Şekil 5.7. Kullanıcı yöneticisi (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

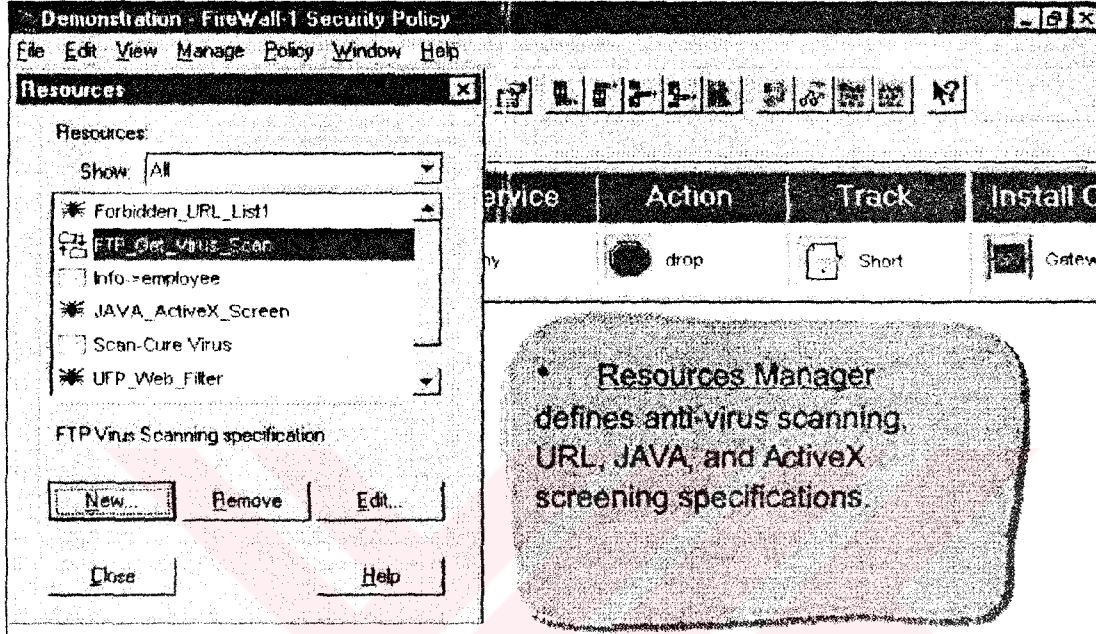
3. Servis Yöneticisi:



Şekil 5.8. Servis yöneticisi (Check Point FireWall-1, 1997).

Tanımlanmış 100 üzerinde servisle, uygulamalarla ve RealAudio ve VDOLive gibi protokollerle hazır halde gelir. Aynı arayüz kullanılarak servisler ve özel protokoller kolaylıkla eklenebilir. (Şekil 5.8)

4. Kaynak Yöneticisi:

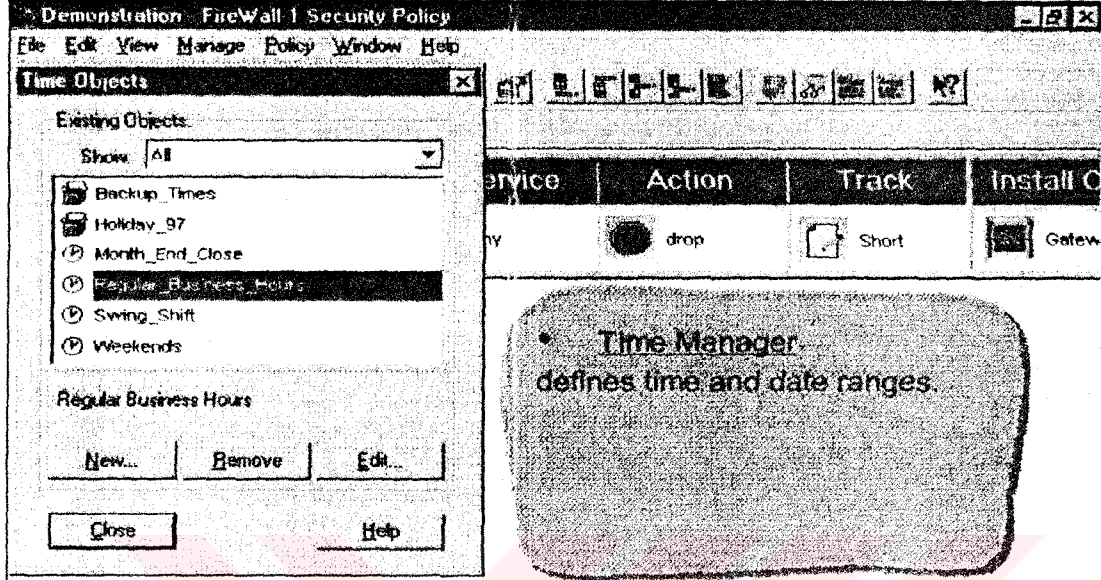


Şekil 5.9. Kaynak yöneticisi (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

▪ **Anti-Virüs Tarama:** FireWall-1, kendisi bir anti virus programı değildir. Fakat sistemler de internetten gelen her türlü virüsle karşı karşıyadır. Bir virüs bir kere sisteme girdi mi geri dönüşümü kolay olmayan zararlar verebilirler. Bu, bir bakıma sisteme davetsiz misafirlerin girmesi gibidir. Hatta ağdaki trafik etkileşimine göre on'ardan daha fazla zarar da verebilir. Ve zararı tasarlanma şekline göre ani olabileceği gibi daha sonraki zamanlarda belli şartların gerçekleşmesi anında ortaya çıkabilir. İşte virüslerden korumak amacıyla ağa dışardan gelen paketlerin virüs taramasından geçirilmesi gerekir. FireWall-1 de bunu gerçekleştirmektedir. Kendisine kullanılacak anti-virüs programı belirtilir. Böylelikle FireWall-1 ağa gelen ve giden paketleri virüs taramasından geçirir.

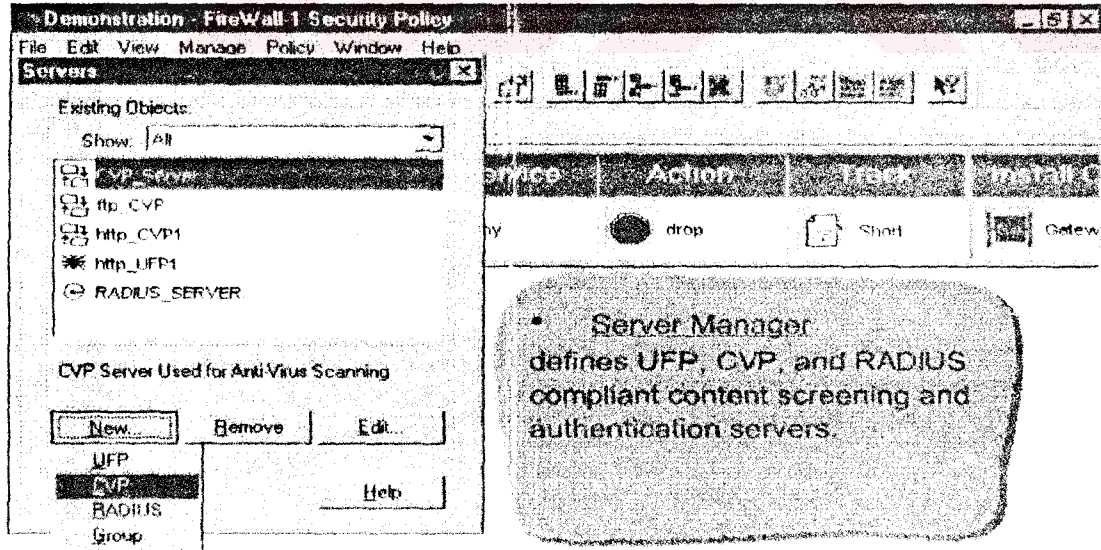
▪ FireWall-1, ayrıca yine aynı yöntemle gelen paketleri, URL, JAVA ve ActiveX gibi eleme şartlarından geçirebilir.

5. Zaman Yöneticisi: Zaman ve Tarih değişim aralıklarını tanımlar.



Şekil 5.10. Zaman yöneticisi (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

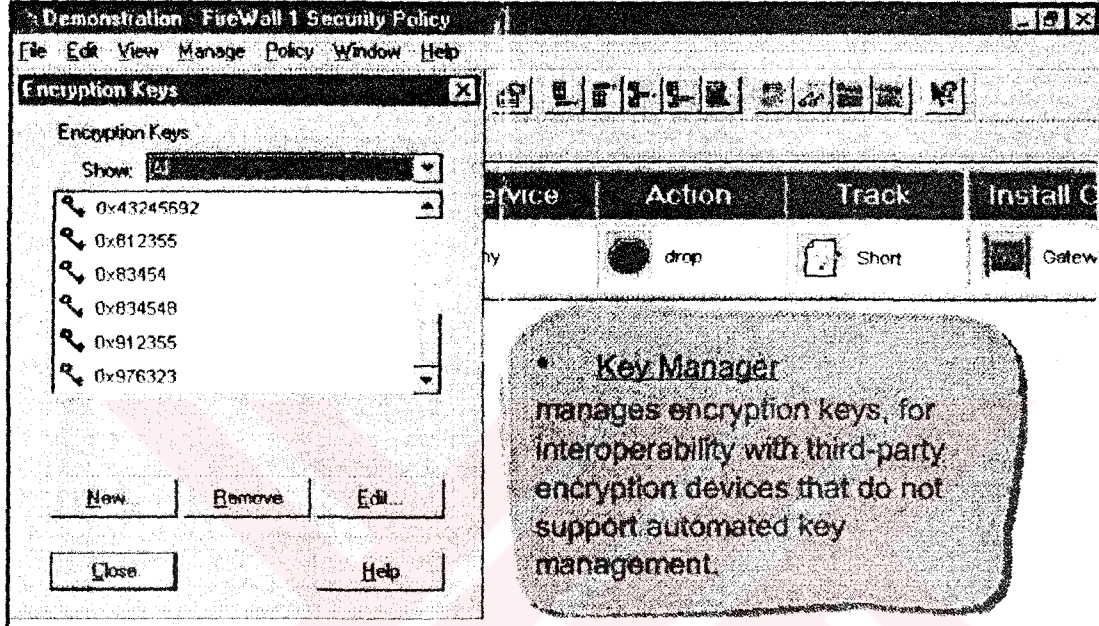
1. Sunucu Yöneticisi:



Şekil 5.11. Sunucu yöneticisi (Check Point FireWall-1, 1997).

UFP, CVP ve RADIUS itaatkar içerik elemesinin(screening) ve doğruluğu belgeleyici (authentication) sunucuların tanımlanmasını sağlar.

7. Anahtar Yöneticisi: Otomatik anahtar yönetimini desteklemeyen üçüncü parti şifreleme araçlarıyla uyumluluk için şifreleme anahtarlarını yönetir. (Şekil 5.12)



Şekil 5.12. Anahtar yöneticisi (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

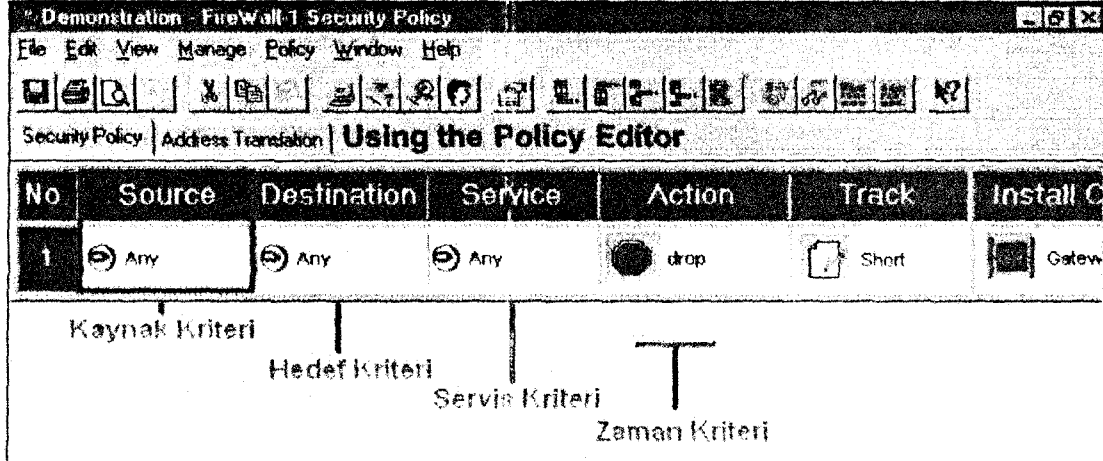
5.6. Güvenlik Politikalarını Ayarlamak

Check Point FireWall-1'in ödül kazanmış **Kural Tabanlı Politika Editörü** kullanılarak girişim çapında güvenlik politikası uygulanabilir.

FireWall-1, Firewall aracılığıyla olan tüm bağlantıları durdurur ve denetler. Daha sonra bunları güvenlik politikasındaki her kural ile karşılaştırır. Bu karşılaştırma sonucunda kurala uygun olmayan bir istek varsa durdurur ve sisteme, ağa geçmesini engeller.

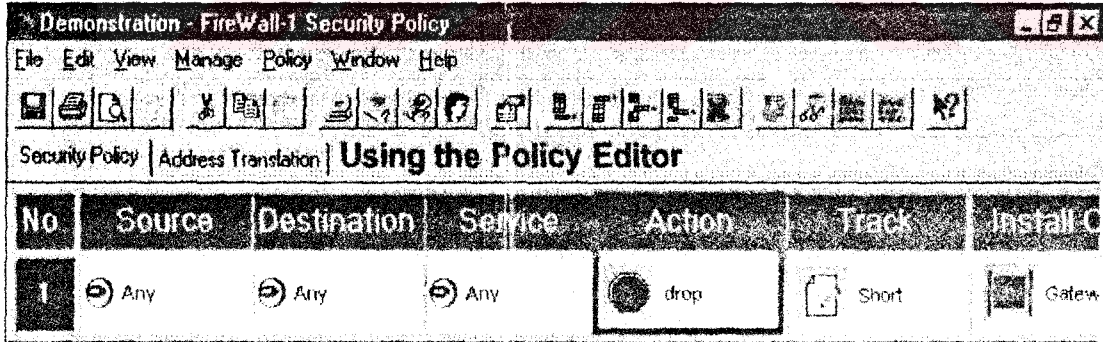
Bağlantı bu kuralların en az bir tanesine uymalıdır ki FireWall geçmesine izin versin. Aksi halde varsayılan olarak iletişimi koparır.

Eğer iletişim Şekil 5.13'teki kriterlerle karşılaştırılırsa; bunlar için daha önce belirlenmiş harekete uygulamaya geçer.



Şekil 5.13. Güvenlik politika kriterleri

Örnek; herhangi oluşan bir durum için drop(düşme) hareketi belirlenmişse bu durum oluştuğunda iletişim kopacaktır. (Şekil 5.14)

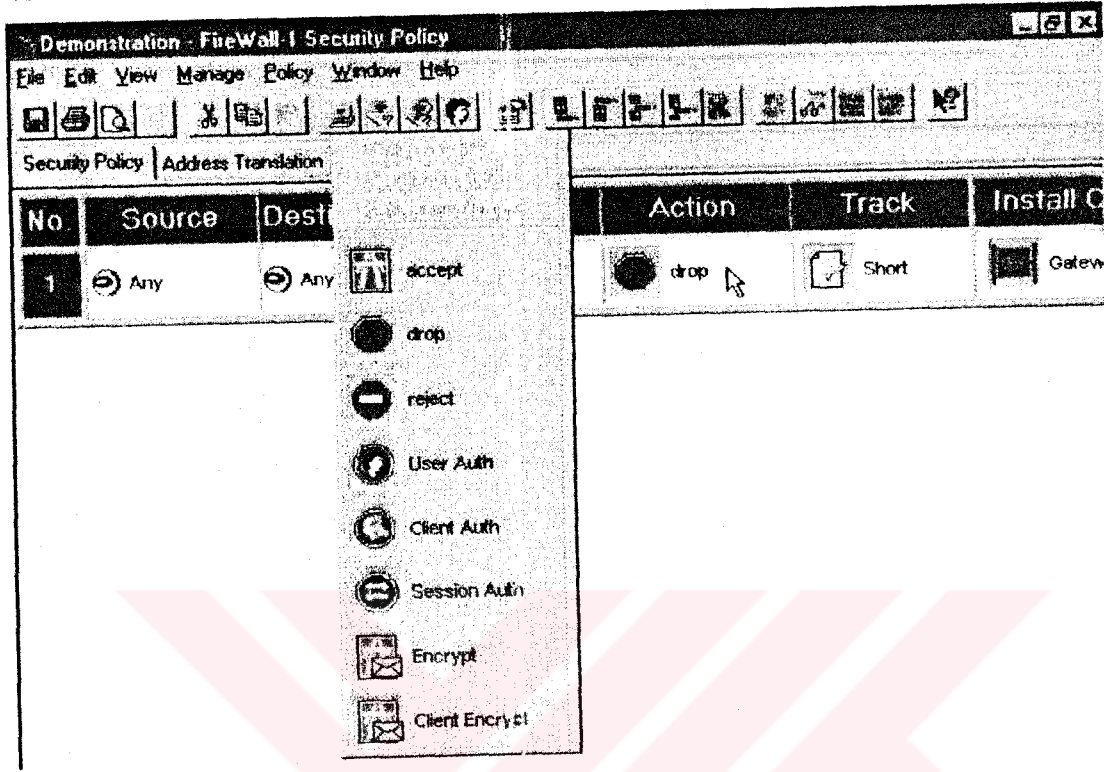


Şekil 5.14. Güvenlik politika kriterleri_servis engelleme

Ayrıca bu hareket durumu için izleme(tracking) mekanizması aktif hale gelecektir. İzah edilen durumlar için;

1. Öncelikle her kural için tanımlanmış nesneler kullanılarak kaynak, hedef, servis ve zaman kriterleri belirlenir.

2. Daha sonra ise bu kriterler olduğu zaman gerekli hareket belirlenir. (Şekil 5.15)



Şekil 5.15. Güvenlik politika hareketi belirleme

- **Accept:** Bağlantının yerine getirilmesine izin verir.
- **Drop:** Sessizce bağlantıyı düşürür.
- **Reject:** Kullanıcıya bağlantının reddedildiği konusunda haber verir.
- **User Auth/Client Auth/Session Auth (Authentication):**

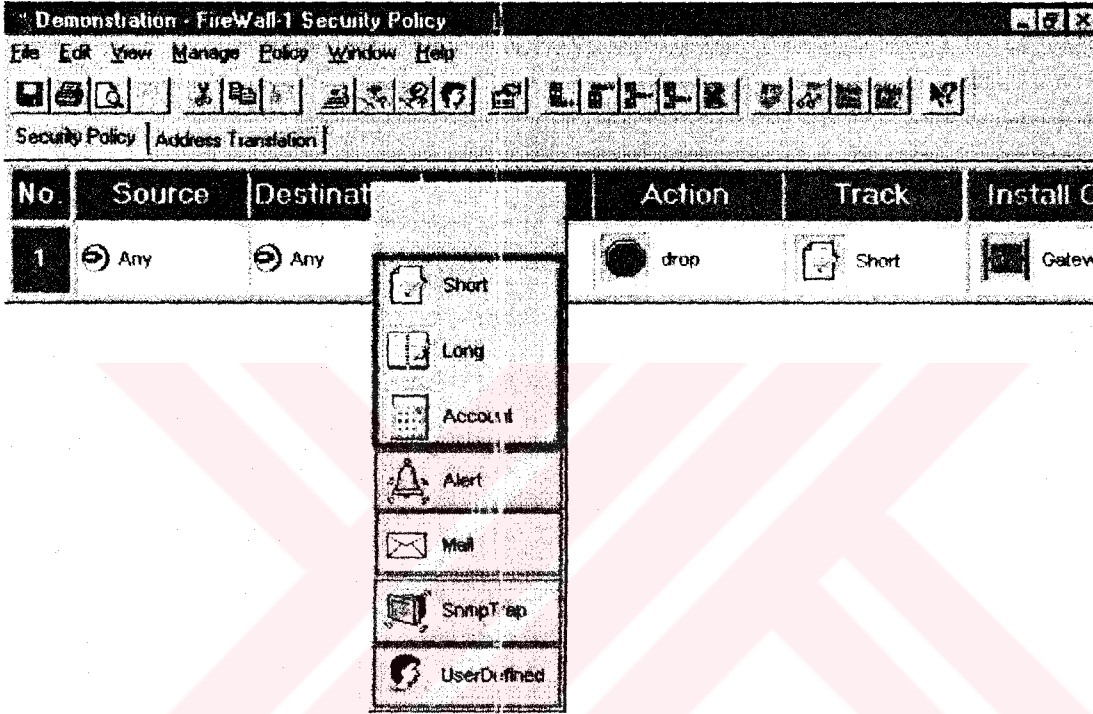
Kullanıcının geçerli olup olmadığını tasdik eder.

- **Encrypt/Client Encrypt (Encryption):** İletişimin özel olma durumunu korur.

3. Son olarak; uygun kayıt defteri ve izleme formatları belirlenir. (Şekil 4.16)

- **Short (Kısa):** Temel bağlantı bilgisini tutar.
- **Long (Uzun):** Bağlantı bilgisinin tamamını tutar.

- **Account (Hesap):** Bağlantı zamanını ve transfer edilen byte miktarını ekler.
- **Alert (Alarm):** Yönetim konsolunu harekete geçirir.
- **Mail (Posta) :** Elektronik posta bildirisi gönderir.
- **SNMP Trap:** Mevcut yönetim sistemleriyle entegrasyon kurar.
- **UserDefined:** Paging ve trouble ticketing gibi kullanıcı destekli uygulamalara bağlantı sağlar.



Şekil 5.16. Kayıt defteri ve izleme belirleme

Bir defa tanımlandığında, FireWall-1, tüm ya da belirli gateway'lerin ağın başından sonuna kadar güvenliğin dağıtıldığı şekliyle kontrol edilmesini sağlar.

5.7. Erişim Kontrolü (Access Control)

Erişim kontrolü, bir ağa giren ve çıkan bilgileri belirler. Aynı zamanda da bu bilgileri güvenlik tehlikelerine karşı korur.

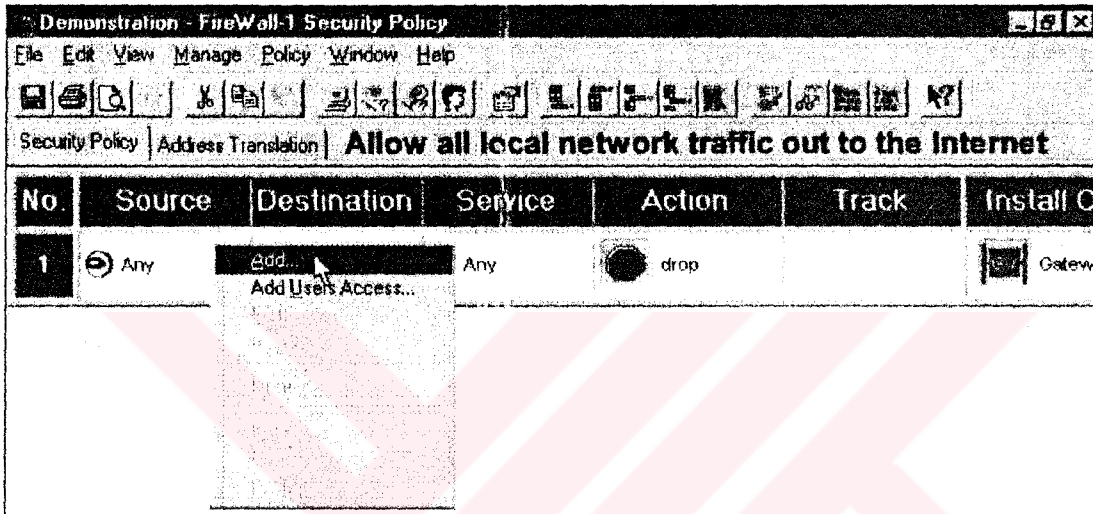
Örneğin :

- Bir site tüm yerel ağ trafiğinin internete çıkmasına izin verebilir.
- Sadece HTTP trafiğinin siteye girmesine izin verebilir.
- Süpheli hareketler için ALARM üretebilir.

Kural Editörü ile erişim kontrolü güvenlik politikası üretmek basittir.

Örnek 1: Şimdi örnek olarak yerel ağ trafiğinin tüm internete çıkmasını sağlayan bir kural tanımlanmaya çalışılırsa;

- Kaynak, şirket yerel alan ağı olacaktır.
- Hedef ise internet olacaktır.



Şekil 5.17. Yeni kural tanımlama

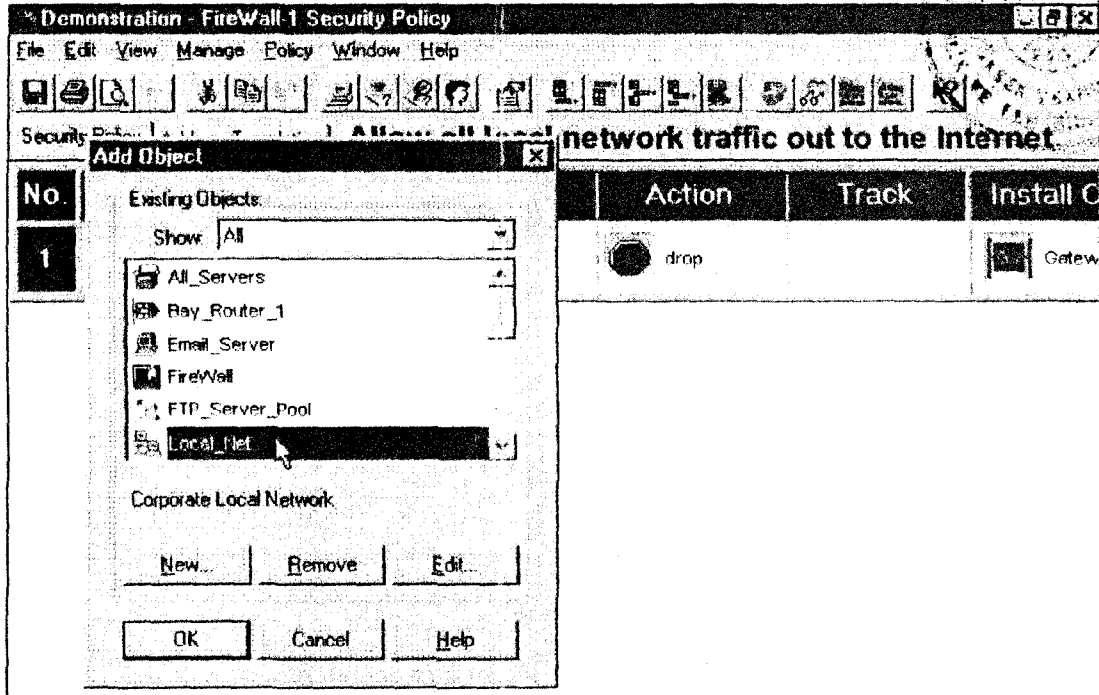
1. Kaynak yöneticisinde yeni bir nesne ekleme işlemi gerçekleştirilir.(Şekil 5.17) Çıkan nesne ekleme bölümünde Local_Net (yerel ağ) seçilir. (Şekil 5.18, 5.19)

2. Daha sonra ise hedef belirlenir. Bu kuralda seçilen hedef ise herhangi bir yerdir. Yani yer kısıtlaması yok. Herhangi bir hedef. (Şekil 5.20)

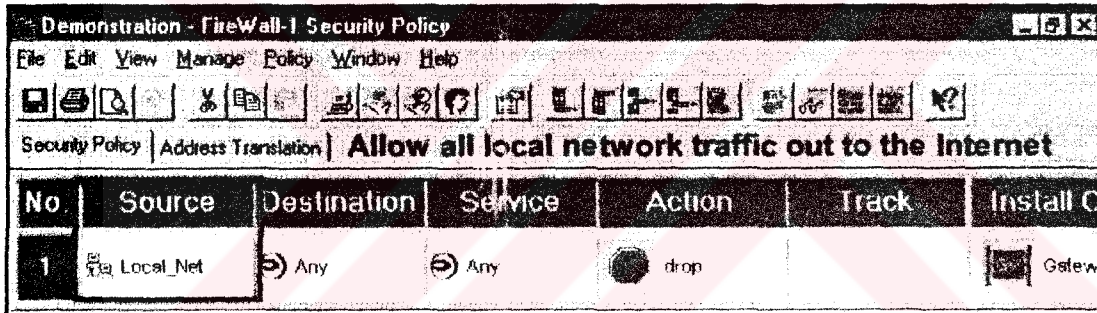
3. Servis olarak ise yine herhangi bir servis kullanılacaktır. (Şekil 5.21)

4. Kurala göre yerel alan ağından internete bilgi gönderildiğinde hareket tarzı olarak ise bu işlem kabul edilecektir. (Şekil 5.22)

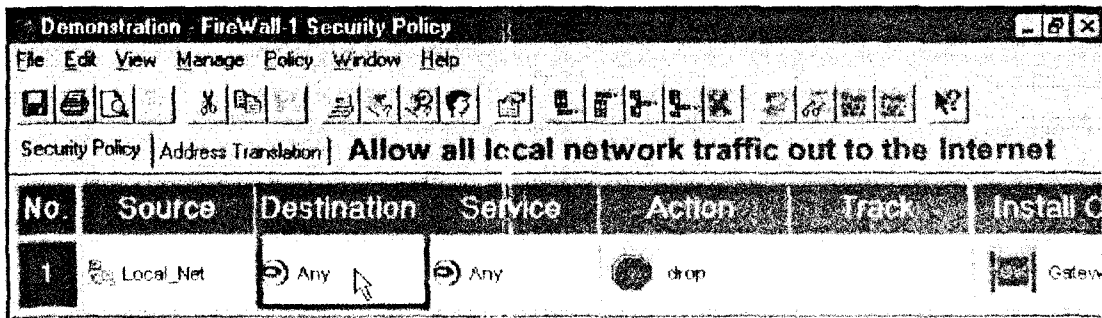
5. Kayıt defteri olarak ise sadece temel bağlantı bilgisi tutulsun.(Şekil 5.23)



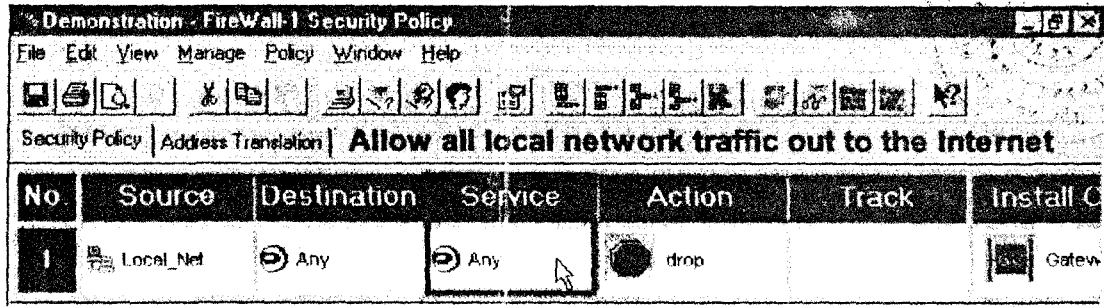
Şekil 5.18. Kaynak yöneticisine yeni nesne ekleme



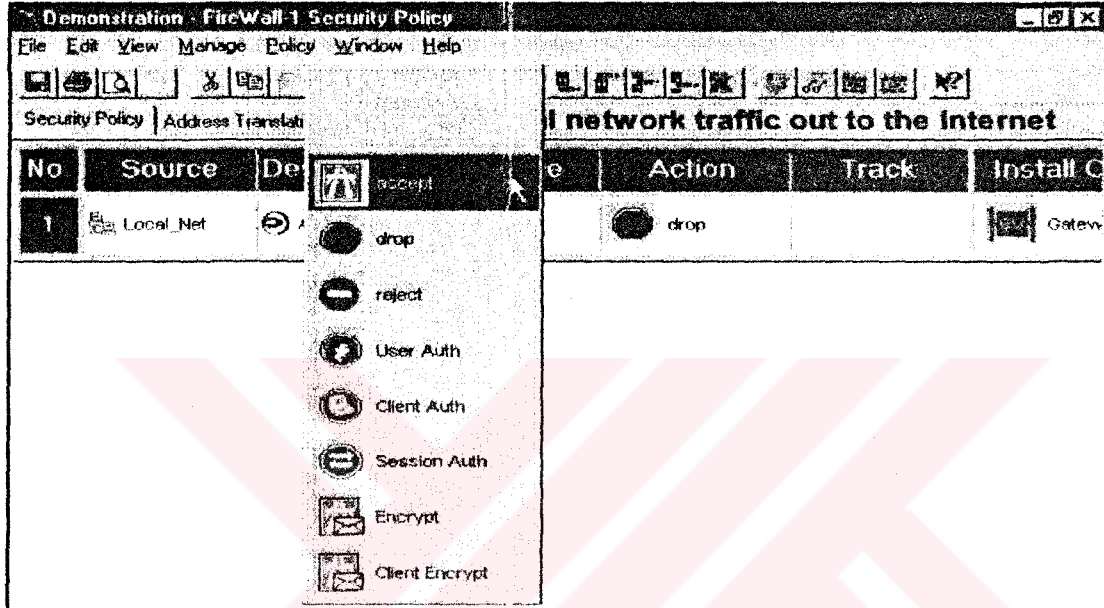
Şekil 5.19. Kaynak yöneticisine Yerel_Ağ ekleme



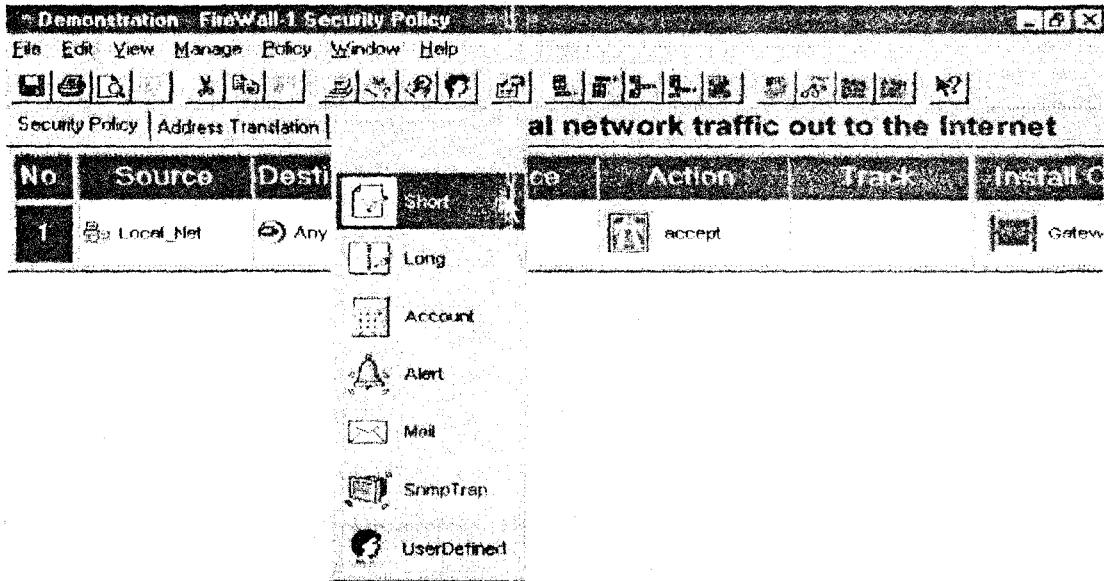
Şekil 5.20. Hedef belirleme



Şekil 5.21. Servis belirleme



Şekil 5.22. Hareket tarzı olarak işlemi kabul etme



Şekil 5.23. Kayıt defteri tutulması

Sonuçta tanımlanmış olan kural şöyle olacaktır: (Şekil 5.24)

No	Source	Destination	Service	Action	Track	Install On
1	Local_Net	Any	Any	accept	Short	Gateway

Şekil 5.24. Tanımlanmış kural

Örnek 2: Herhangi bir kaynaktan WEB sunucusuna gelen HTTP isteklerinin kabul edilmesinin kuralı: Kayıt defteri kısa tipte olacaktır.

No	Source	Destination	Service	Action	Track	Install On
1	Any	Web_Server	http	accept	Short	Gateway
2	Local_Net	Any	Any	accept	Short	Gateway

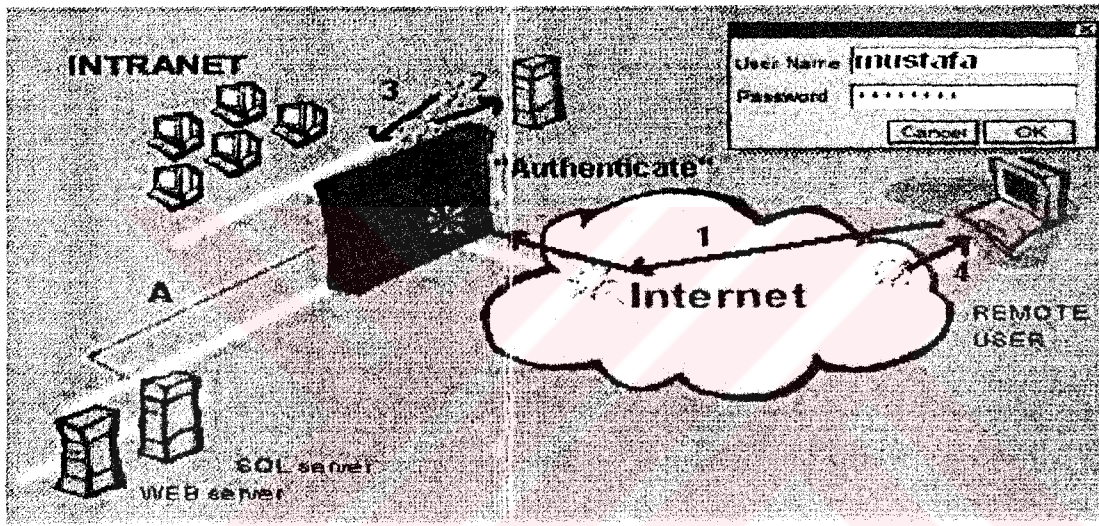
Şekil 5.25. HTTP kuralının tanımlanması

Örnek 3: Yukarıdaki kurallar haricindeki tüm trafiğe ise alarm durumu kuralı tanımlanırsa, firewall'a yukarıdaki kuralların haricinde bir istek geldiğinde iletişim kesilecek ve alarm sistemi devreye girecektir. (Şekil 5.26)

No	Source	Destination	Service	Action	Track	Install On
1	Any	Web_Server	http	accept	Short	Gateway
2	Local_Net	Any	Any	accept	Short	Gateway
3	Any	Any	Any	drop	Alert	Gateway

5.8. Kimlik Onaylama(Authentication)

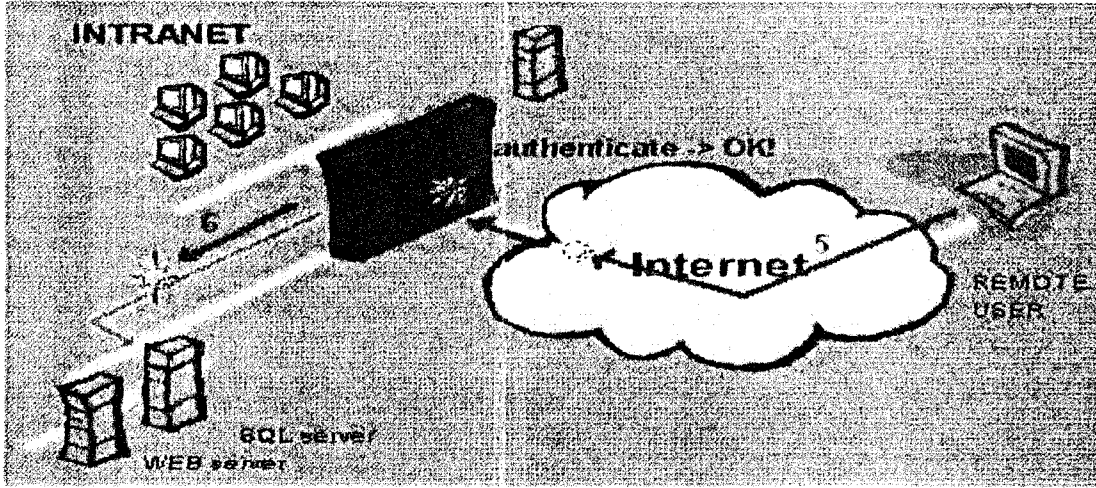
İnternet, uzaktan erişim sağlayan kullanıcılara ve iletişim yapan kişilere bir sitenin ağ kaynaklarına erişimi sağlar. Burada ise erişim sağlayan bu kişilerin gerçekte sistemde tanımlı kişiler olup olmadığı çok önemlidir. Bunun doğrulanması amacıyla, kimlik onaylama bir kişinin ağa bağlanmasına izin vermeden önce onun kimlik bilgilerini doğrulamayı sağlar. Böylece ağa, dolayısıyla sisteme erişim sağlayan kişinin sistem açısından yasal veya yasal olmayan birisi olduğu kontrol edilebilir. (Şekil 5.27)



Şekil 5.27. Kimlik onaylama (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

- Bu işlem için Firewall kullanılmayan bir ağda uzaktan erişim sağlayan bir kişi herhangi bir tanımlama hareketiyle karşılaşmadan ağ kaynaklarına erişebilir. (Şekil 5.27)
- FireWall-1 olan sistemde uzaktan erişim sağlayan bir kişi önce FireWall-1 ile iletişim kurmak durumunda kalır. (Şekil 5.27)
- FireWall-1 saydam olarak bu isteği yakalar ve erişim isteğini dahili veya harici kimlik onaylama sunucusuna gönderir. (Şekil 5.27)
- Bu doğrulama burada kullanıcı şifre diyalogudur. Bu diyalog kullanıcıya gönderilir. Kullanıcı bu sorgulamayı cevaplar. (Şekil 5.27)

▪ Kullanıcı ismi ve şifresi burada doğrulandıktan sonra yapılmış olan istekler gerekli sunuculara ulaştırılır. (Şekil 2:28)



Şekil 5.28. Kimlik onaylama işlemi başarılı (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

Şimdi ise bu olayları FireWall-1 üzerinde gerçekleyelim.

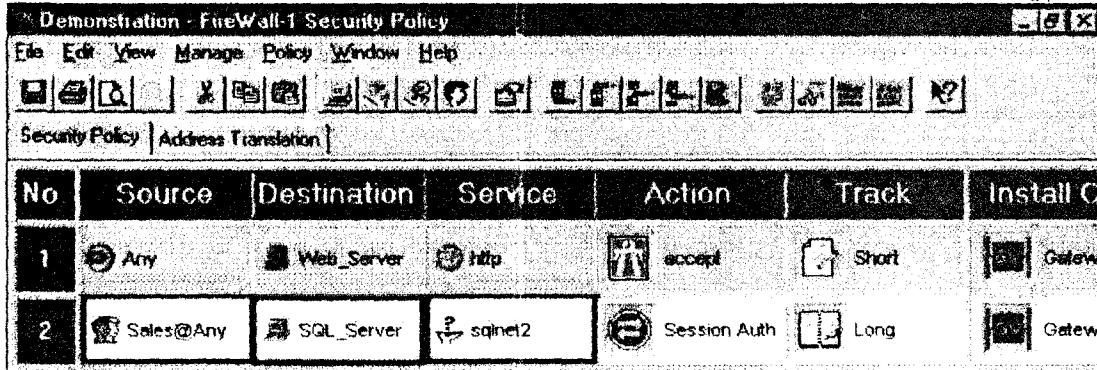
Örnek olarak; bir şirketin herhangi bir departmanı birtakım servis ya da servisler kullanarak bazı kaynaklara erişimi gerçekleştirmek istensin. Bu direkt dahili ağdan da olabileceği gibi uzaktan erişimle de olabilir. Örnek departman **satış departmanı** olsun. Bunun için önce;

1. Kaynak olarak satış departmanı seçilir.
2. Kullanılacak hedef olarak SQL sunucu olsun.
3. Servis olarak da sqlnet2 kullanılsın.

Demonstration - FireWall-1 Security Policy						
File Edit View Manage Policy Window Help						
Security Policy Address Translation						
No	Source	Destination	Service	Action	Track	Install C
1	Any	Web_Server	http	accept	Short	Gateway
2	Sales@Any	SQL_Server	sqlnet2	Session Auth	Long	Gateway
3	Local_Net	Burada authentication(dogrulama) eklenmiş güvenlik politikası görülmektedir.			Short	Gateway
4	Any				Alert	Gateway

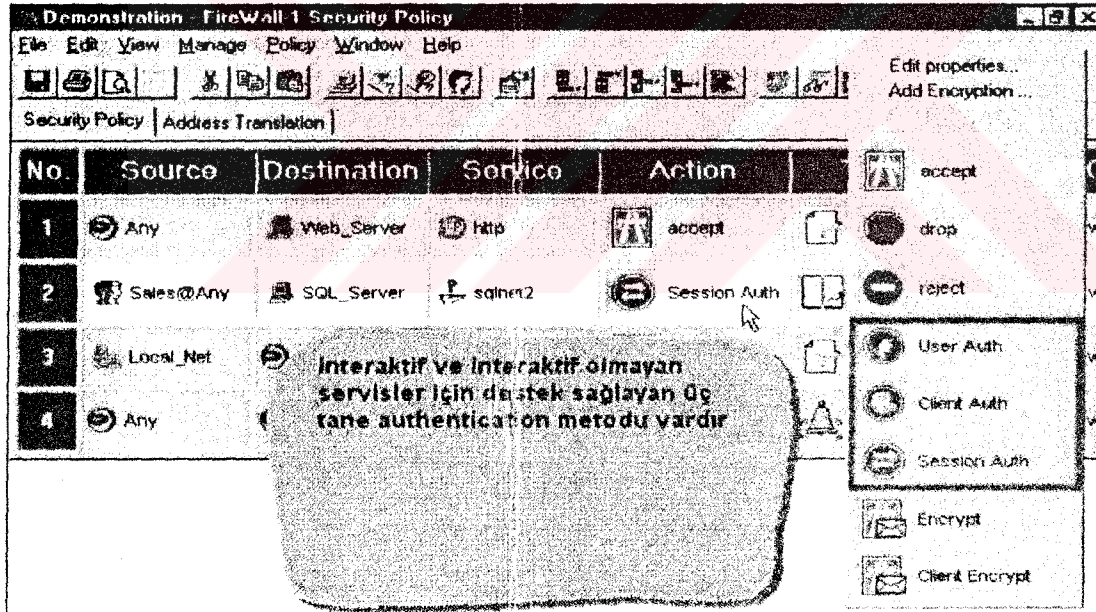
Şekil 5.29. Kimlik onaylama eklenmiş güvenlik politikası

Tanımlanan bu kuralda şirketin satış departmanındaki her kişi sqlnet2'yi kullanarak SQL sunucuya erişme hakkı tanınır. (Şekil 5.30)



Şekil 5.30. Sqlnet2'yi kullanarak SQL sunucuya erişime izin verme

Ayrıca interaktif olan ve olmayan servisler için destek sağlayan üç adet kimlik onaylama metodu mevcuttur. (Şekil 5.31)



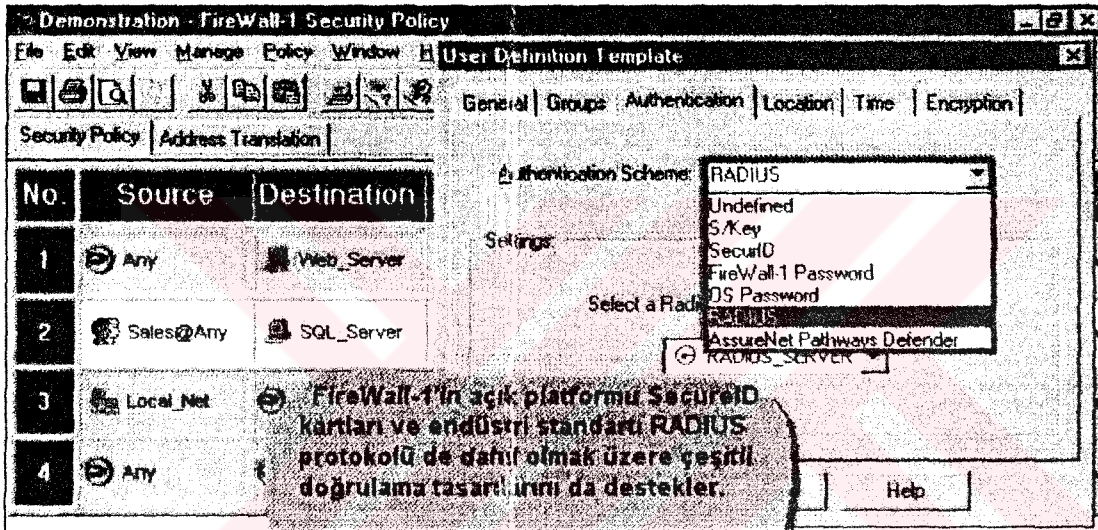
Şekil 5.31. Kimlik onaylama metotları

1. **Kullanıcı Kimlik Onaylama(User Authentication):** Gelişmiş bir login prosedürü kullanarak TELNET, FTP ve RLOGIN doğrulamalarını yapar.

2. **İstemci Doğrulama(Client Authentication):** Her bir makine temelinde TCP/UDP/RPC servis doğrulamasını gerçekleştirir.

3. Saydam Oturum Doğrulama (Transparent Session Authentication): Herhangi TCP/UDP/RPC servislerinin doğrulamasını destekler. Bu servisler başlangıç login prosedürünü sağlamasalar dahi bunu gerçekleştirir.

FireWall-1, kendisi endüstrinin standart özelliklerini bünyesinde barındırmakla beraber dış kaynakları kullanım bakımından açık bir platformdur. Güvenliğin bazı bölümlerini eğer istenirse 3.parti uygulamalarla sağlayabilir. Burada da bazı standart doğrulama tasarımlarını da içermektedir. (Şekil 5.32)



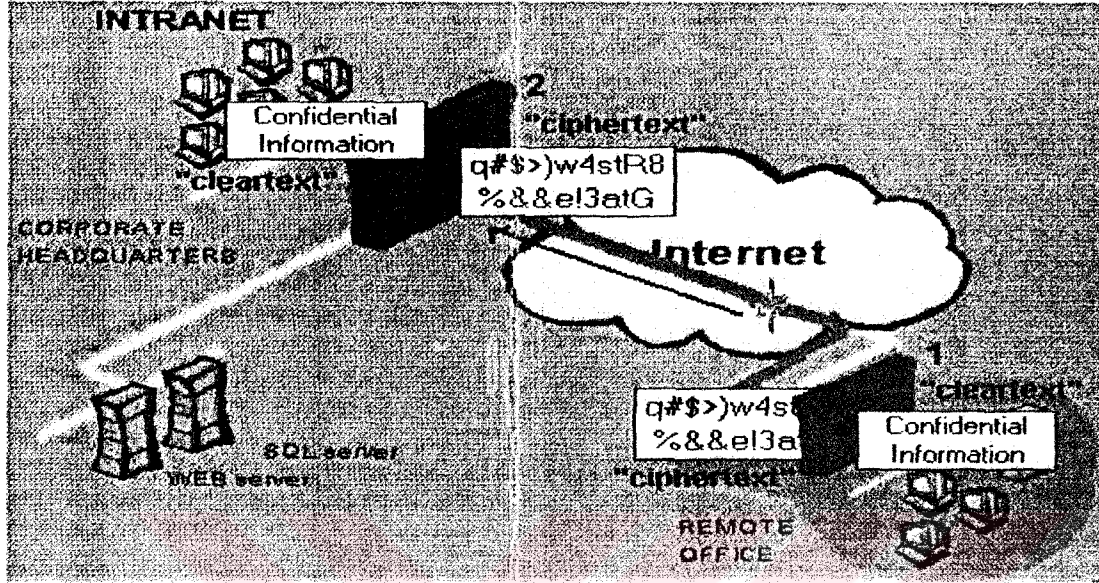
Şekil 5.32. Kimlik onaylama güvenlik metotları

Sonuç: Sadece doğruluğu tanımlanmış uzak kullanıcılar SQL sunucuya erişebilirler.

5.9. Şifreleme(Encryption)

İnternet, özel kiralık hatlara uzak mesafeli ağlar arası işlemler için esnek ve düşük fiyatlı bir alternatiftir. Bununla birlikte interneti bu yolla kullanmak şirketin özel iletişimini genel yani herkese açık hale getirir.

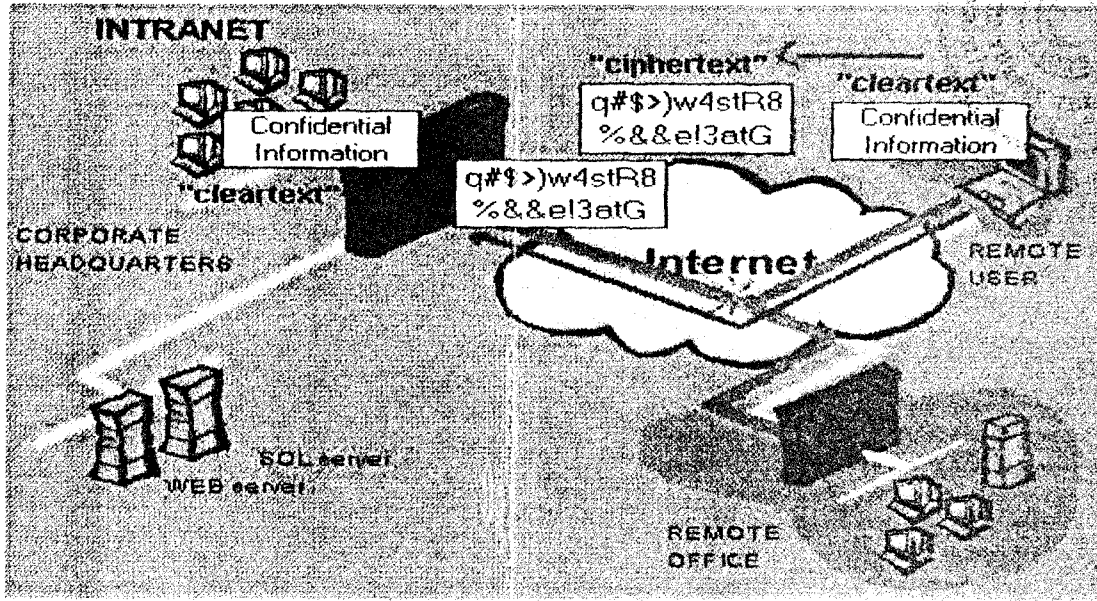
FireWall-1, VPN(Virtual Private Network, Özel Sanal Ağ) oluşturmak için internet vasıtasıyla bağlantı kuran siteler arası tüm veri iletişimini şifreleyebilir. Bu şifrelemeyle için uzak ofislerle intranet arasında özel sanal ağ oluşturur.



Şekil 5.33. Şifreleme (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite. 1997).

Uzaktan sistem kaynaklarını kullanmak için istemde bulunan tarafın bilgisi FireWall-1 tarafından şifreleme algoritmaları kullanılarak şifrelenir. (Şekil 5.33) Daha sonra şifrelenmiş olan bilgi diğer intranet FireWall-1'e ulaştığında bu bilgi gerekli anahtarlar kullanılarak ters işleminden geçer ve tekrar orijinal hale getirilir. (Şekil 5.33) Ve istek kaynaklara iletilir. Gelen şifreli bilginin bir şekilde orijinal hali değişmişse bu bunu şifreleme algoritması çözer ve bu durumda FireWall-1'e tanımlanmış kurallar ve direktifler doğrultusunda hareket eder.

Ayrıca FireWall-1 SecuRemote VPN'i uzaktan kullanıcılara da sağlar. (Şekil 5.34)



Şekil 5.34. Uzaktan erişimlerde koruma için şifreleme (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite. 1997).

Bu şifreleme metotları uygulama üzerinde gerçekleştirilirse:

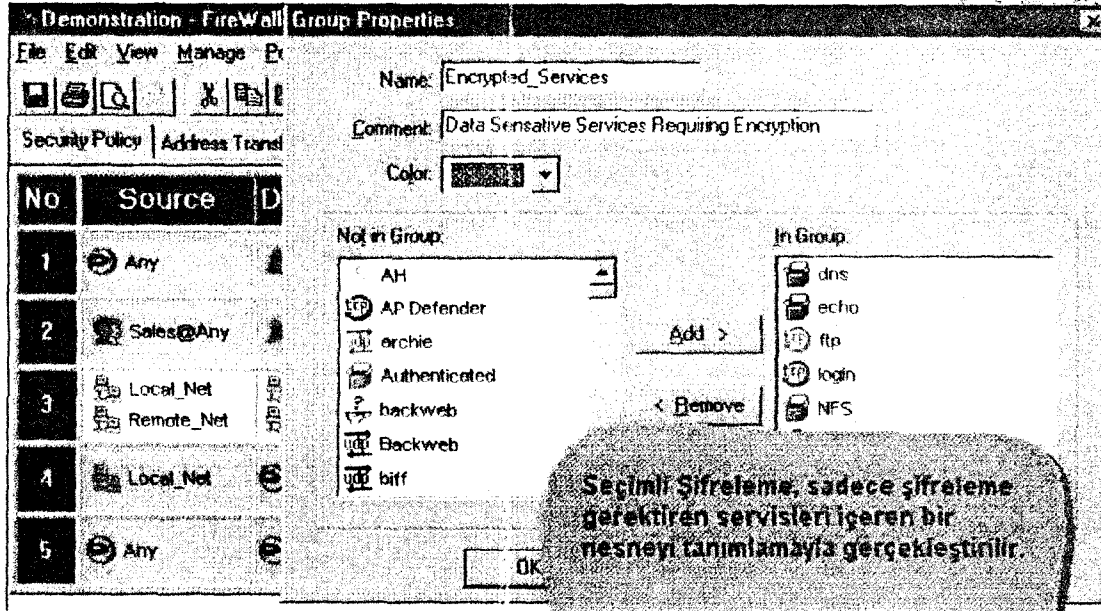
Demonstration - FireWall-1 Security Policy						
File Edit View Manage Policy Window Help						
Security Policy Address Translation						
No	Source	Destination	Service	Action	Track	Inst
1	Any	Web_Server	http	accept	Short	
2	Sales@Any	SQL_Server	sqlnet2	Session Auth	Long	
3	Local_Net Remote_Net	Remote_Net Local_Net	Encrypted_Services	Encrypt	Long	
4	Local_Net	Any	Any			
5	Any	Any	Any			

Şirket ve uzak ofis arasındaki VPN, yerel ve uzak ağı, kaynak ve hedef kriteri olarak ve şifreleme(encryption) hareketinin seçilmesiyle belirlenir.

Şekil 5.35. Hareket olarak şifreleme seçilmesi

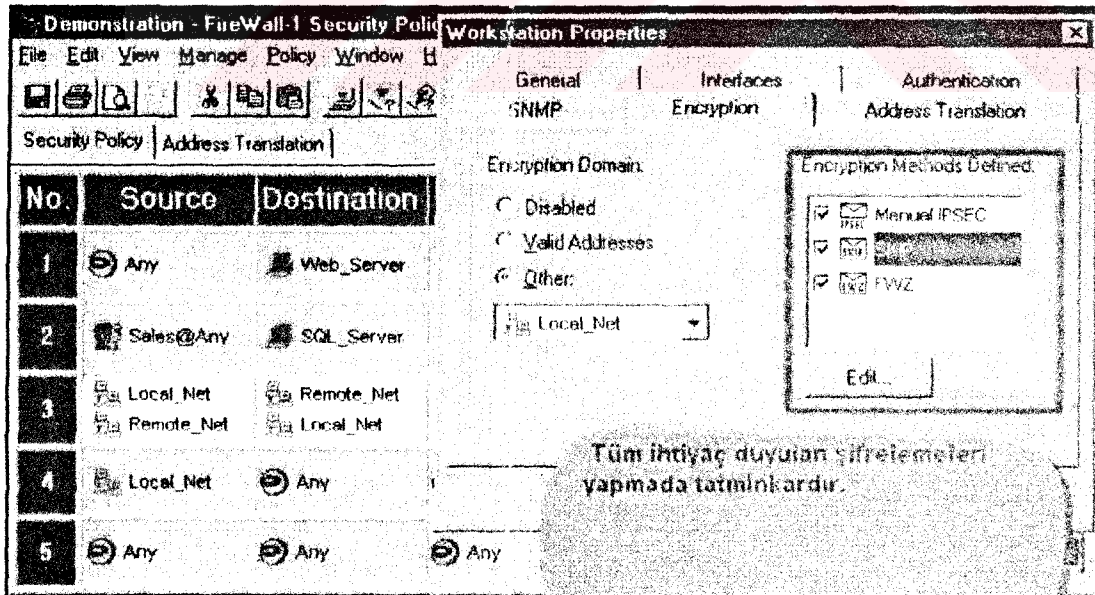
Bunun için kaynak olarak yerel ağ ve uzak ağ, hedef olarak uzak ağ, yerel ağ seçilir. (Şekil 5.35) Şifreleme için ise seçimlik şifreleme söz konusu

olduğunda ise sadece şifreleme gerektiren servisleri içeren nesne tanımlanmasıyla olur.(Şekil 5.36)



Şekil 5.36. Sadece şifreleme gerektiren servis tanımları

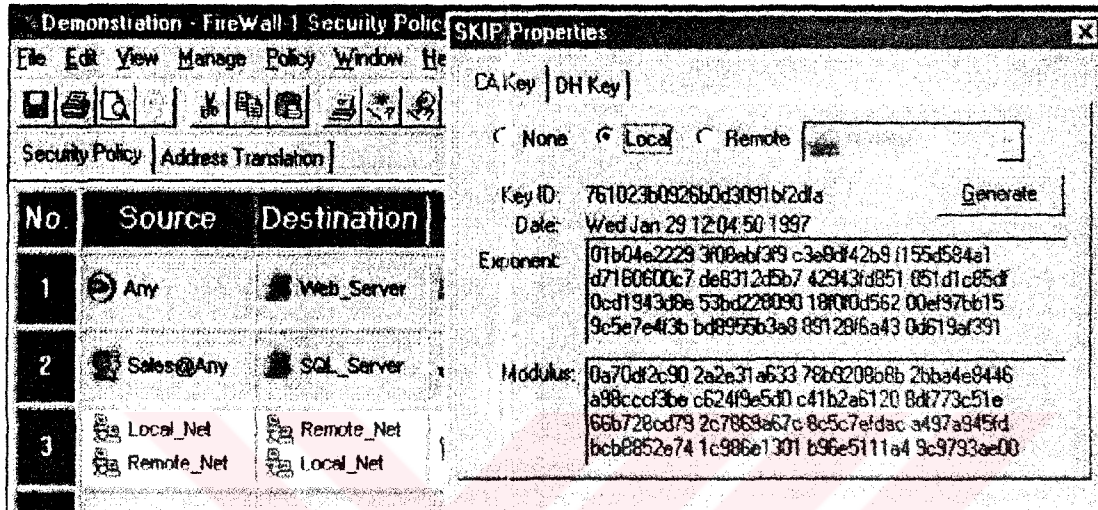
FireWall-1 seçmeli şifreleme gerçekleştiren firewall pazarındaki tek üründür. Diğer ürünler ise firewall'lar arasındaki tüm iletişimi şifreleyerek değerli sistem kaynaklarının harcanmasına neden olurlar.



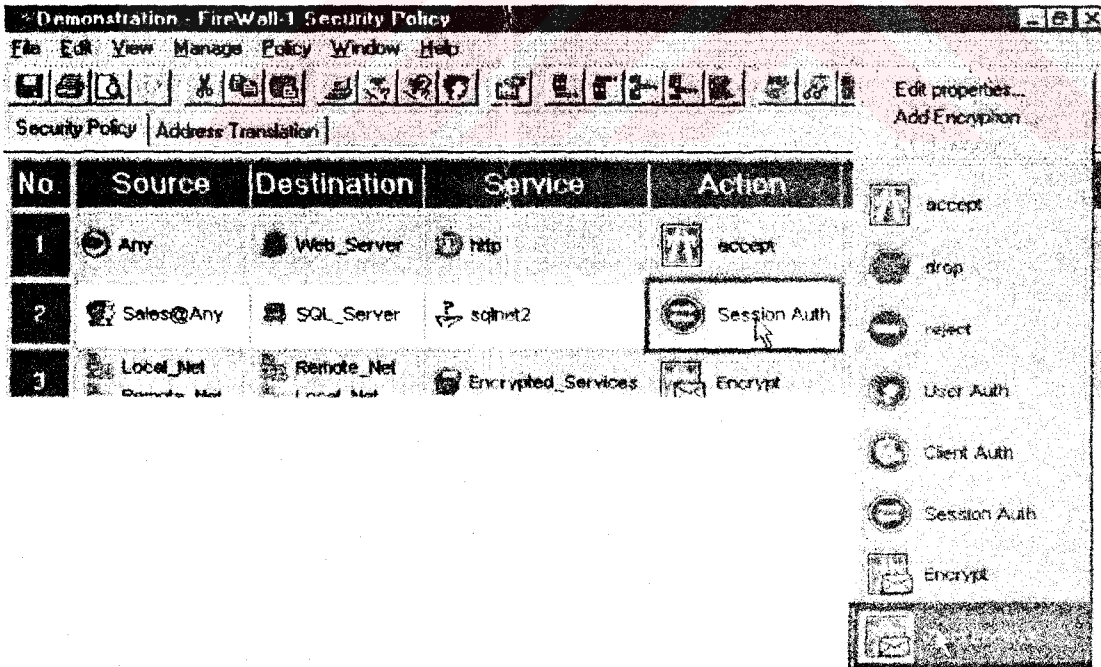
Şekil 5.37. FireWall-1 şifreleme teknikleri

Bunun yanında ise dünya çapında yayılan veya standart temelli şifreleme teknikleri kullanan iş ortakları gibi durumlarda bile FireWall-1 tüm şifreleme ihtiyaçlarına cevap verebilir. (Şekil 5.37)

FireWall-1'in dahili Certificate Authority(CA) anahtar yönetimi kabuslarını ortadan kaldırır. (Şekil 5.38)



Şekil 5.38. FireWall-1 Certificate Authority anahtar yönetimi



Şekil 5.39. Kimlik onaylamayı şifrelemeye çevirme

Şirket ağı ve uzaktan satış gücü arasındaki VPN, önceki kimlik onaylama kuralını istemci şifreleme kuralına çevirerek ve istemci sistem üzerine SecuRemote kurarak belirlenebilir. Bunun için ise Action kısmında açılan menüden Client Encrypt seçilir. (Şekil 5.39)

Artık şirket ağı, uzak ofis ve uzak satış gücü arasındaki tüm iletişim VPN kullanarak güvenli hale getirilmiştir. (Şekil 5.40)

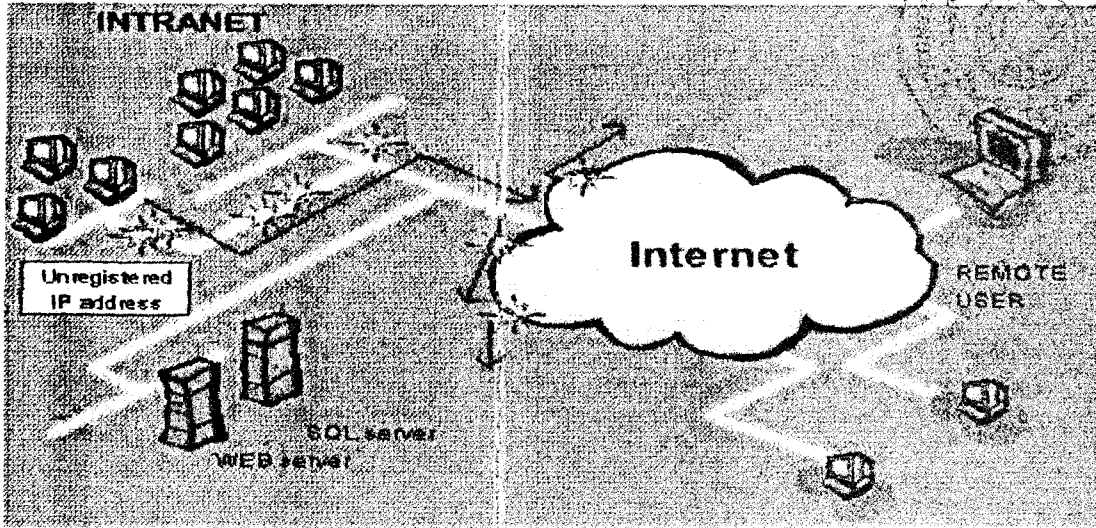
No	Source	Destination	Service	Action	Track	Inst
1	Any	Web_Server	http	accept	Short	
2	Sales@Any	SQL_Server	sqlnet2	Client Encrypt	Long	
3	Local_Net	Remote_Net	Encrypted_Services	Encrypt	Long	

Şekil 5.40. Uzaktan erişim için şifrelemenin tamamlanmış hali

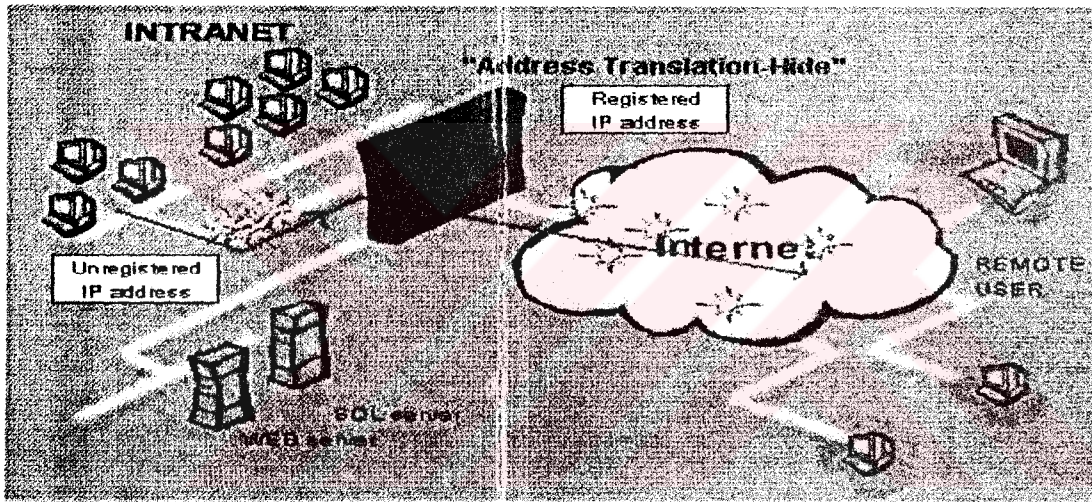
5.10. Adres Çevirme(Address Translation)

Bir ağı gün geçtikçe yeni iş istasyonları eklenir ve bunların da internete erişimleri gerekir. Kayıtlı olmayan bir IP adresi ile bu iş istasyonları bilgi otoyolundan yararlanamazlar. (Şekil 5.41)

Bu problemin giderilmesi ve eklenen istasyonların da internete erişim sağlaması için FireWall-1 Ağ Adres Çevirici fonksiyonu kullanılarak kayıt dışı olan IP adresleri kayıtlı IP adreslerine dönüştürülür. Böylece yeni iş istasyonları da kayıtlı olanlar gibi internete erişim sağlayabilirler. (Şekil 5.42)



Şekil 5.41. Ağa yeni kayıtlı olmayan istasyonların eklenmesi



Şekil 5.42. IP adreslerinin dönüştürülmesi

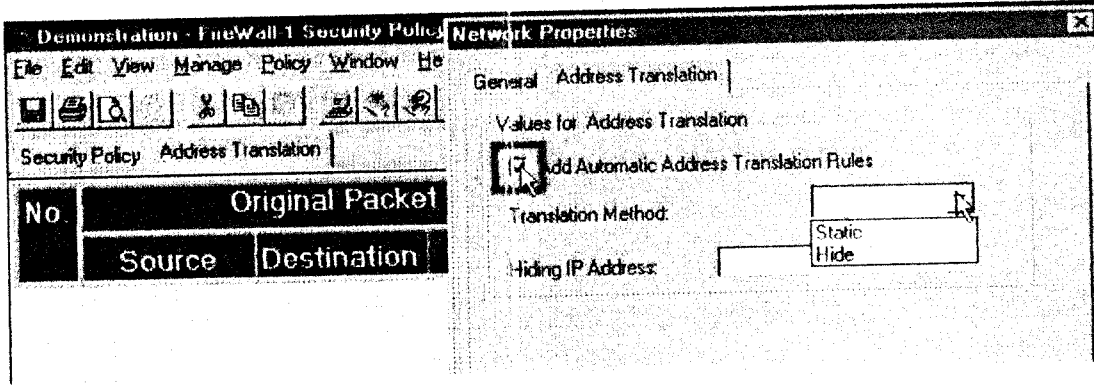
Adres çevirme işlemini FireWall-1 üzerinde ayarlanması:

Adres çevirme işlemi FireWall-1'de nesne tanımlama sürecinin bir parçasıdır. (Şekil 5.43)

Demonstration - FireWall-1 Security Policy					
File Edit View Manage Policy Window Help					
Security Policy Address Translation					
No	Original Packet			Translated Packet	
	Source	Destination	Service	Source	Destination

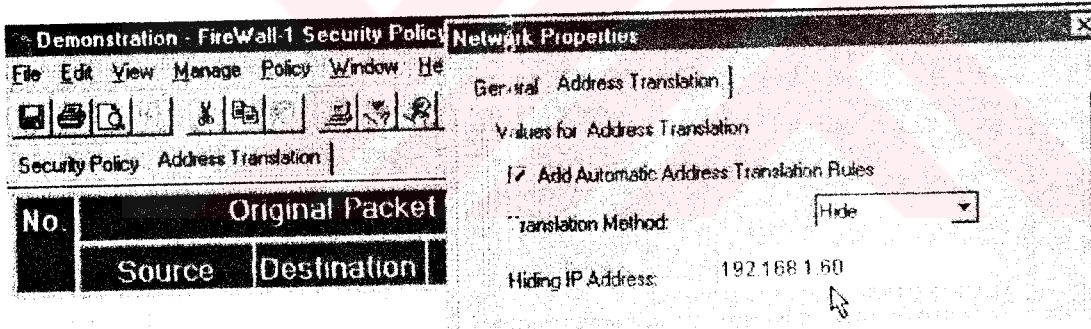
Şekil 5.43. Adres çevirme

- Basit olarak adres çevirimi seçilir.(Şekil 5.44)
- İstenilen çevirme metodu seçilir. Desteklenen metotlar **Static**(one-to-one, bire-bir) ve **Hide** yani dinamik(many-to-one, bire-çok) metotlarıdır. Dinamik seçilmiştir.(Şekil 5.44)



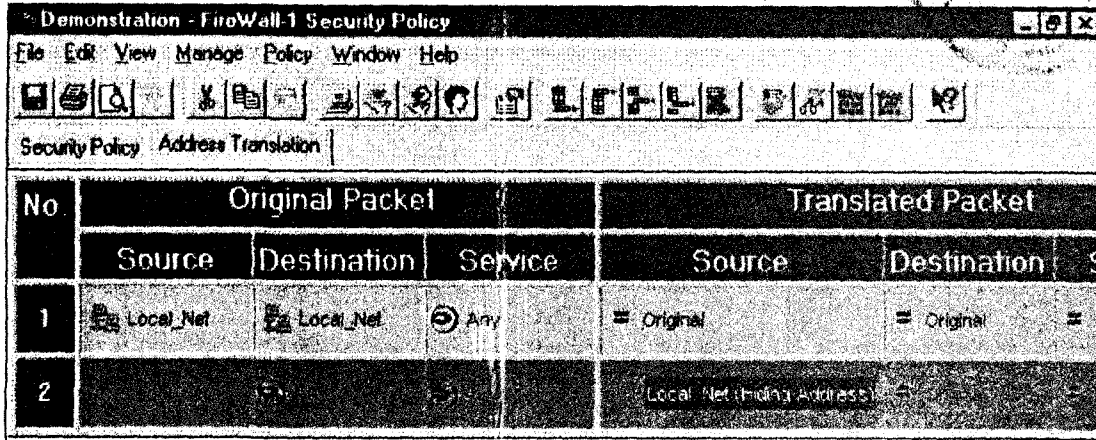
Şekil 5.44. Adres dönüştürme metodu

- Son olarak ise IP adresi seçilir. Burada 192.168.1.60 seçilmiştir.(Şekil 5.45)



Şekil 5.45. Adres çevirmede IP adresi seçilmesi

FireWall-1 otomatik olarak adres çevirme kuralını üretir. (Şekil 5.46)



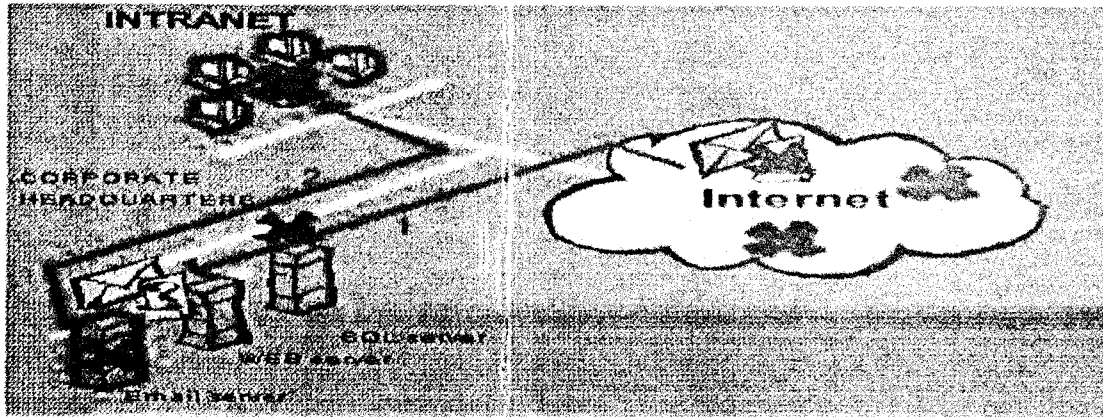
No	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	Local_Net	Local_Net	Any	Original	Original	Any
2	Local_Net	Local_Net	Any	Local_Net (holding Address)	Local_Net (holding Address)	Any

Şekil 5.46. FireWall-1 adres çevirme kuralını üretmesi

5.11. İçerik Güvenliği(Content Security)

Günümüzde internette yeni uğraştırıcı nesneler çıkmaktadır. Yeni nesil virüsler, JAVA ve ActiveX gibi çalıştırılabilir içerik taşıyan uygulamalar, uygunsuz URL siteleri... Bu liste günden güne artmaktadır.

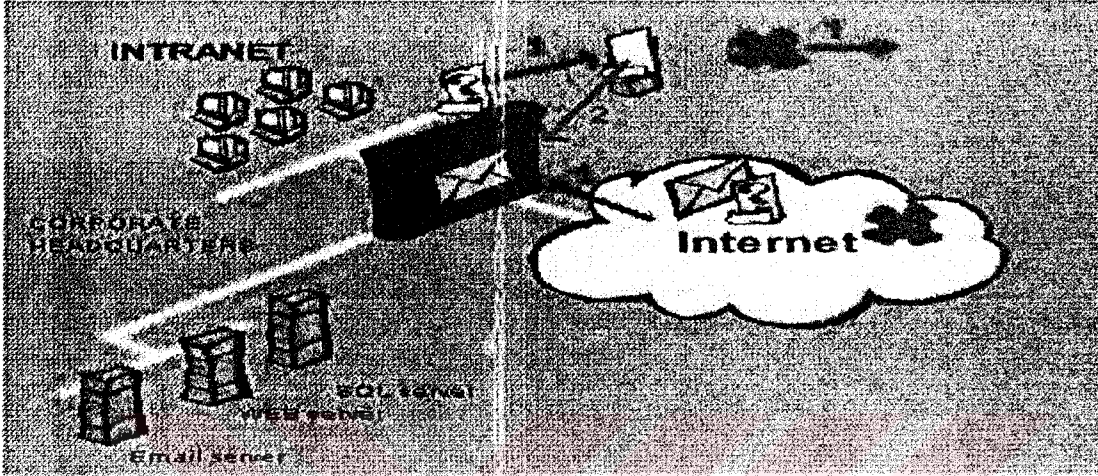
FireWall-1 tüm bu zararlı yeniliklere karşı ağ içerik güvenliği sağlamaktadır. Örneğin FireWall-1'in içerik güvenlik yetenekleri bir sisteme entegre olmadan, o sistem posta eklerine saklanmış virüs tehlikesiyle karşı karşıyadır. Virüs postayla e-posta sunucusuna gelebilir ve buradan da tüm ağa yayılabilir. (Şekil 5.47)



Şekil 5.47. İçerik güvenliği olmaması durumu

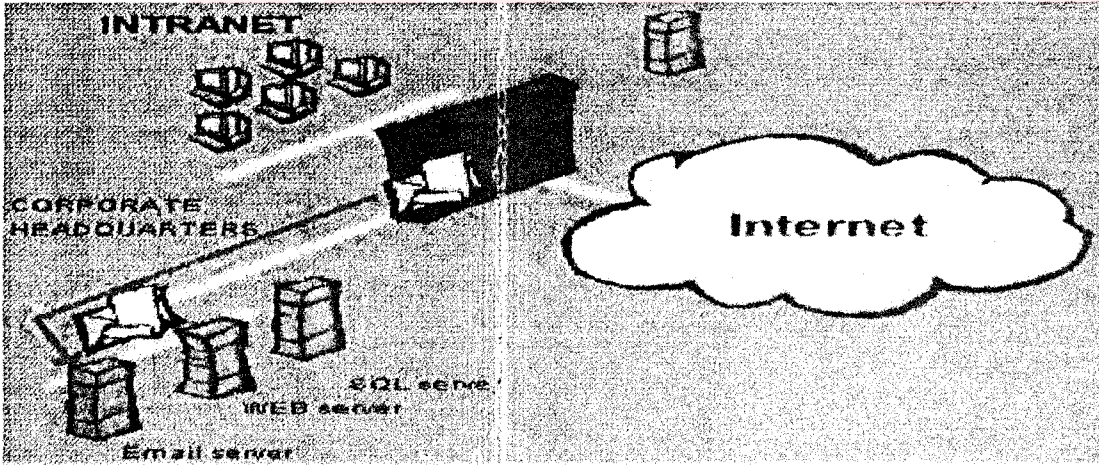
FireWall-1'in otomatik anti-virüs denetleme sistemi saldırıyı firewall geçidinde(gateway) durdurabilir.

İnternette gelen postayı ilk önce FireWall-1 karşılar. (Şekil 5.48) Kendisinde tanımlı harici bir anti-virüs programlarıyla posta içeriği taranır.(Şekil 5.48)



Şekil 5.48. FireWall-1 içerik güvenliği denetimi

Varsa problem ortadan kaldırıldıktan sonra posta tekrar firewall tarafından ilgili e-posta sunucuya gönderilir. (Şekil 5.49)



Şekil 5.49. İçerik güvenliğinin denetimden geçmesi (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

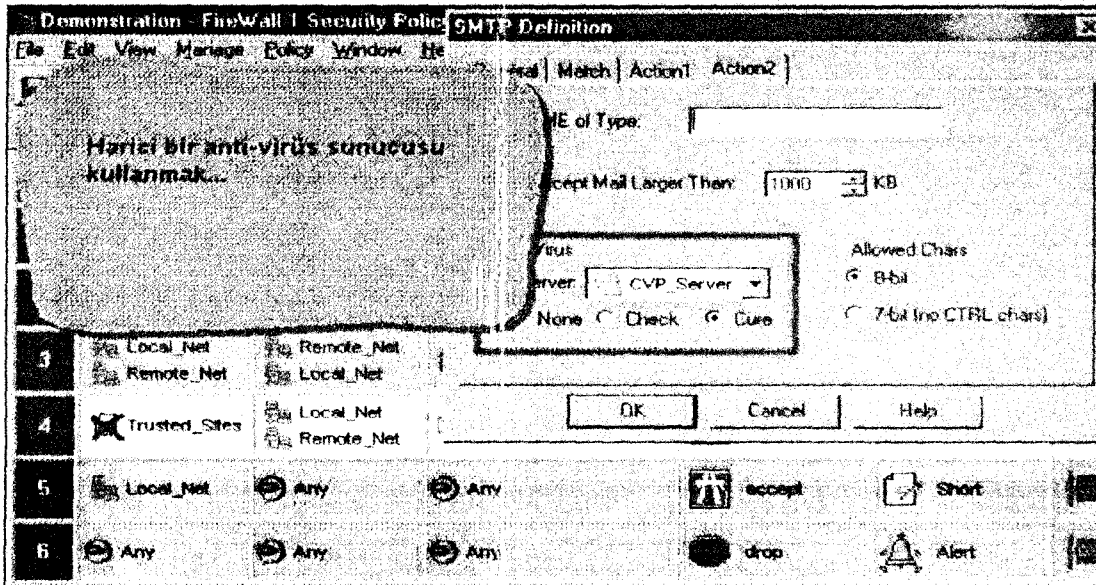
Fakat burada üçüncü parti anti-virüs programının güncel olması çok önem arz eder. Sonuçta firewall'ın kendisi bir virüs tarama programı değildir. Öyle olsa dahi piyasadaki son virüsleri desteklemesi gerekir. Aksi takdirde virüs taraması zaman ve para kaybindan başka bir şey değildir. Tabi eğer sisteme zarar veren bir durum olmuşsa bu da işin çabasıını oluşturur.

Harici bir anti-virüs programının sisteme entegre edilmesi:

- Kaynak olarak; e-postanın güvenilir olmayan sitelerden geldiği belirlenir.
- Hedef olarak; bu postanın Yerel Ağ(Local_Net) ve Uzak Ağ(Remote_Net) gittiği belirlenir.
- Daha sonra hareket tarzı olarak ise; bu posta sisteme kabul edilecektir. (Şekil 5.50)

3	Local_Net Remote_Net	Remote_Net Local_Net	Encrypted_Services	Encrypt	Long
4	Trusted_Sites	Local_Net Remote_Net	smtp->Mail_Virus_Scan	accept	Short
5	Local_Net	Any	Any	accept	Short
6	Any	Any	Any	drop	Alert

Şekil 5.50. İçerik güvenliğinin FireWall-1 de tanımı



Şekil 5.51. İçerik güvenliği için harici anti-virüs programı seçimi

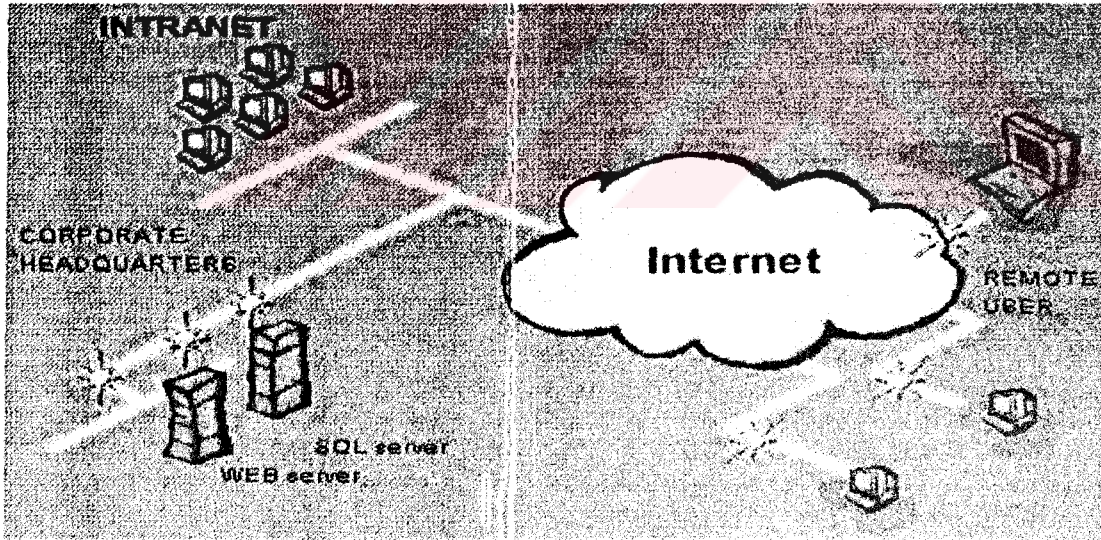
- Servis olarak ise; bu posta harici anti-virüs sunucularla taranacak ve problem varsa düzeltilecektir. (Şekil 5.51)

URL eleme, JAVA ve ActiveX eleme gibi içerik eleme fonksiyonları aynı yöntemle tanımlanabilir.

5.12. Bağlantı Kontrolü (Connection Control)

Bağlantı kontrolü, optimal ağ performans bakımı yaparken güvenlik sağlama olanağıdır. Bağlantı kontrolüne bir örnek; istemci isteklerini mantıksal bir sunucu grubuna cevap zamanlarını geliştirerek dengeli yüklemektir.

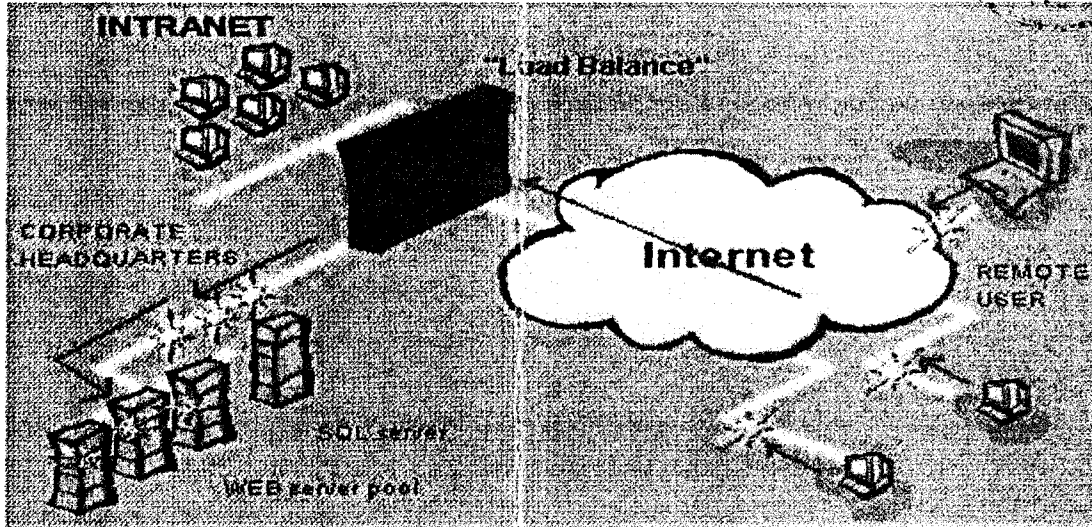
Sunucu dengeli yükleme olmadan bir web sunucusu gelen tüm istemci isteklerini karşılar. (Şekil 5.52)



Şekil 5.52. Tüm istekleri dengesiz yükleme (Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite, 1997).

FireWall-1'in bağlantı kontrol fonksiyonu mantıksal bir sunucu oluşturarak, tek sunucuyu sunucu grubuyla değiştirir. Böylelikle tüm sonradan

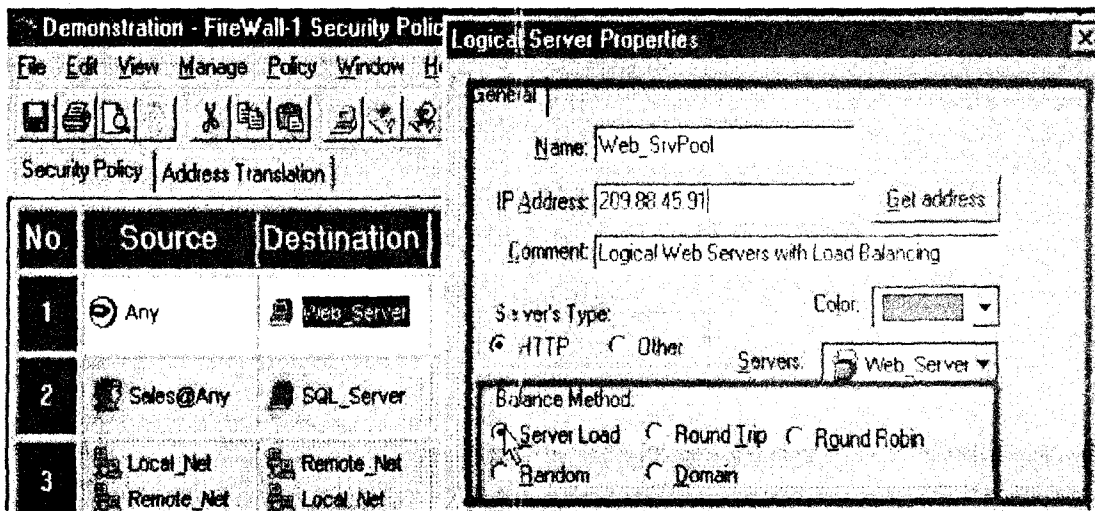
oluşan web istekleri kullanıcı cevap zamanları optimize edilerek mantıksal sunucu grubundaki uygun sunucuya dengeli yüklenecektir. (Şekil 5.53)



Şekil 5.53. FireWall-1'in gelen istekleri dengeli yüklemesi

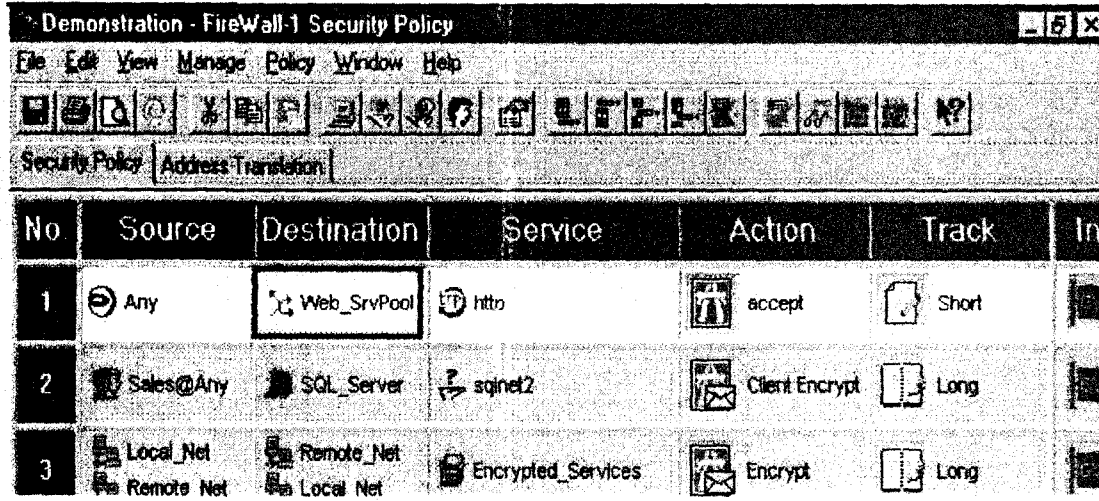
FireWall-1'i kullanarak bu kuralları tanımlama:

- FireWall-1 nesne yöneticisi kullanılarak mantıksal sunucu tanımlanır.
- FireWall-1, kendisinde daha önce tanımlanmış beş adet yük dengeleme algoritmasından birini kullanarak istemci isteklerini dağıtabilir. Bu beş algorithmadan Server Load(Sunucu Yükleme) seçilerek gruptaki en yüksek performanslı sunucuya istekler dağıtılır.(Şekil 5.54)



Şekil 5.54. FireWall-1'in yük dengeleme algoritmaları

■ Nesne tanımlandıktan sonra kuralı tamamlamak için kuraldaki Web_Server, mantıksal web sunucusuyla değiştirilir.(Şeki-5.55).



No	Source	Destination	Service	Action	Track	In
1	Any	Web_SrvPool	http	accept	Short	
2	Sales@Any	SQL_Server	sqlnet2	Client Encrypt	Long	
3	Local_Net	Remote_Net	Encrypted_Services	Encrypt	Long	

Şekil 5.55. FireWall-1'in yük dengeleme için hedefinin değiştirilmesi

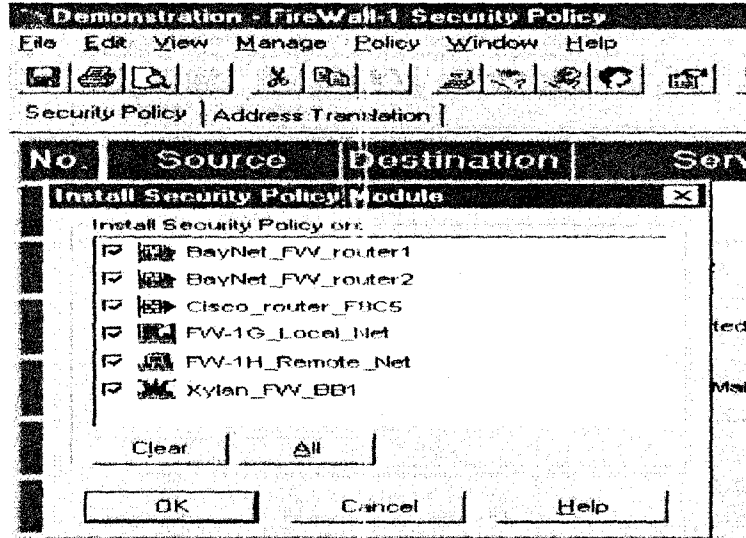
Böylelikle web sunucuya olan tüm istekler dengeli yüklenecektir.

5.13. Yaygın Yönetim(Enterprise Management)

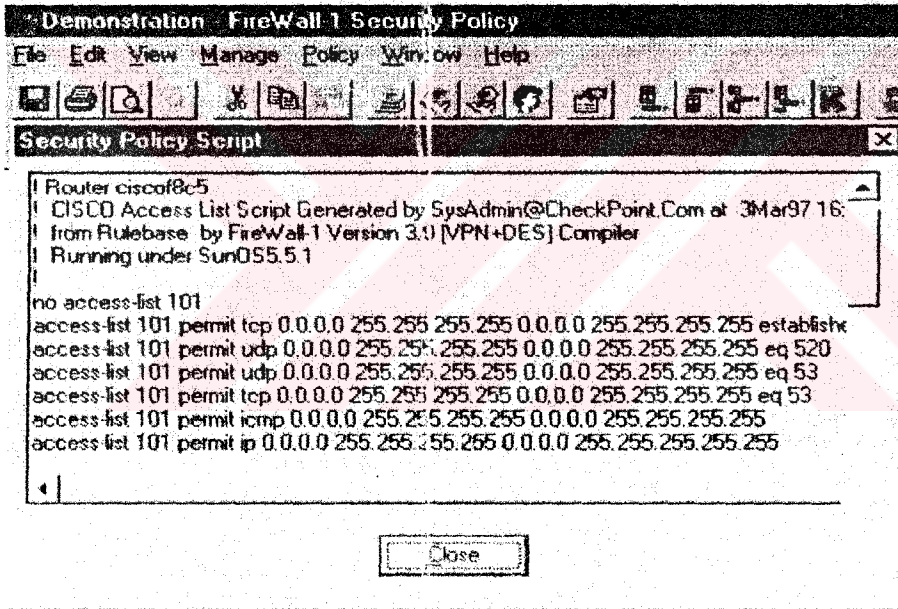
FireWall-1, güçlü yönetim araçları seti sağlar. Kural Editörü(Rules Editor) sektör çapında güvenlik politikası tanımlamak için kullanılır ve güvenlik, ağlarda baştan başa çok çeşitli yürütme noktalarına kadar dağıtılır. NT, UNIX sunucularda, Bay Networks routers, Xylan switch'leri ve çeşitli ağlararası cihazlarda kullanılır.(Şekil 5.56)

Kural Editörü aynı zamanda router konfigürasyonunu ve yönetimini basitleştirerek Access Control Lists(Erişim Kontrol Listeleri)'i yönetmek için de kullanılabilir.(Şekil 5.57)

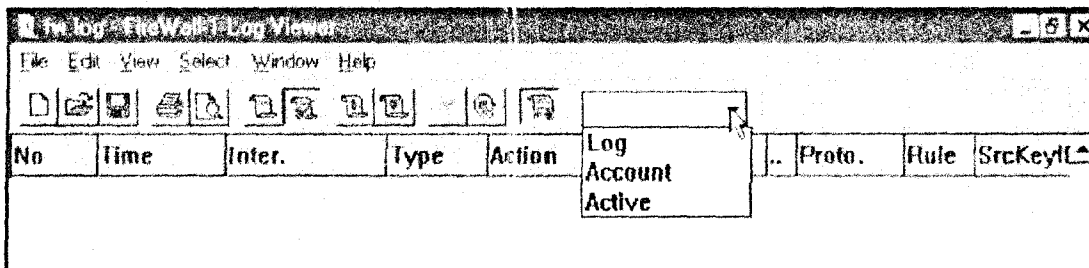
Log Viewer(Kayıt Göstericisi) birkaç gösterme ve veri toplama modu sağlar.(Şekil 5.58)



Şekil 5.56. FireWall-1 yönetimi seti

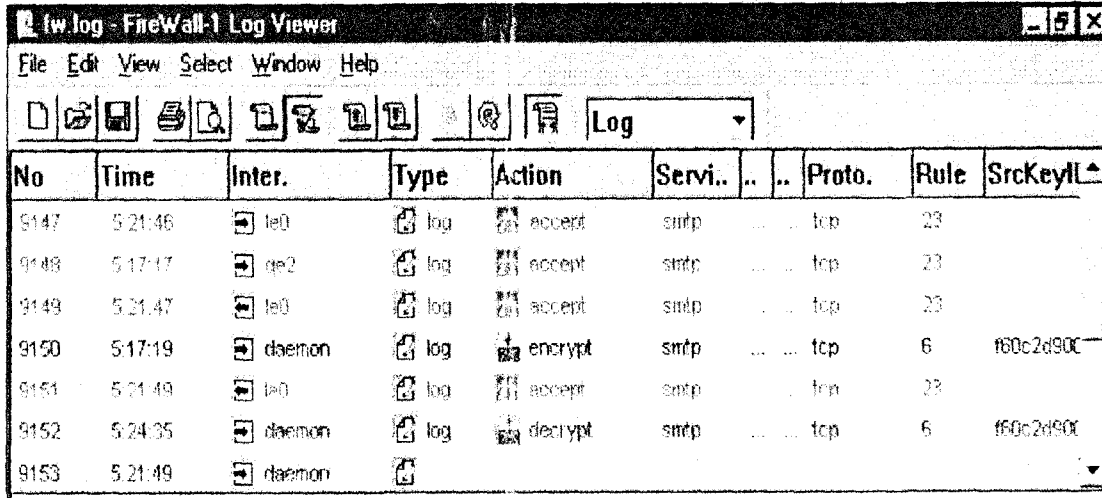


Şekil 5.57. FireWall-1 kural editörü



Şekil 5.58. FireWall-1 kayıt göstericisi

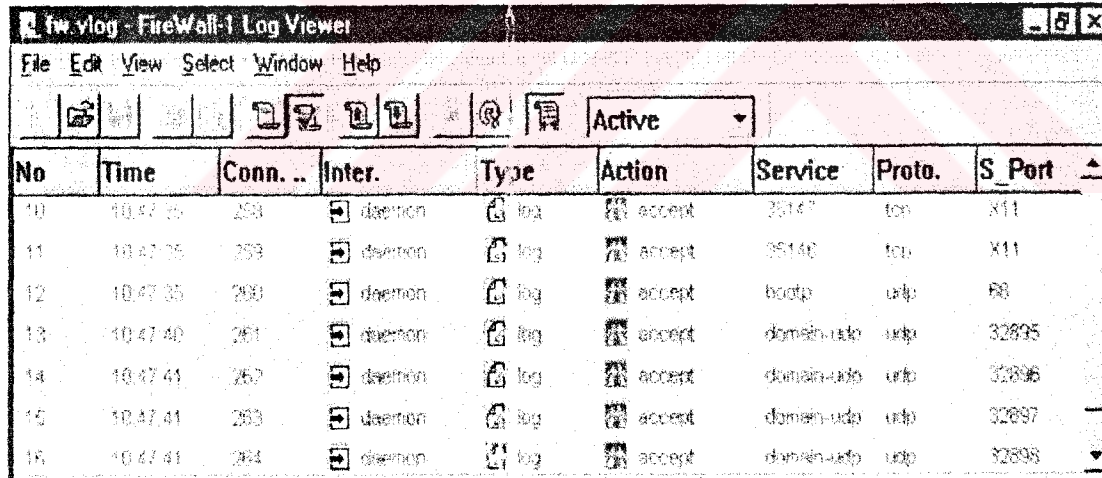
Bu seçeneklerden Log, firewall'un tutmuş olduğu kayıt defterinin tamamını gösterir.(Şekil 5.59)



No	Time	Inter.	Type	Action	Servi..	Proto.	Rule	SrcKeyID
9147	5:21:46	le0	log	accept	smtp	tcp	23	
9148	5:17:17	qe2	log	accept	smtp	tcp	23	
9149	5:21:47	le0	log	accept	smtp	tcp	23	
9150	5:17:19	daemon	log	encrypt	smtp	tcp	6	160c2d90c
9151	5:21:49	le0	log	accept	smtp	tcp	23	
9152	5:24:35	daemon	log	decrypt	smtp	tcp	6	160c2d90c
9153	5:21:49	daemon	log					

Şekil 5.59. FireWall-1 kayıt defteri

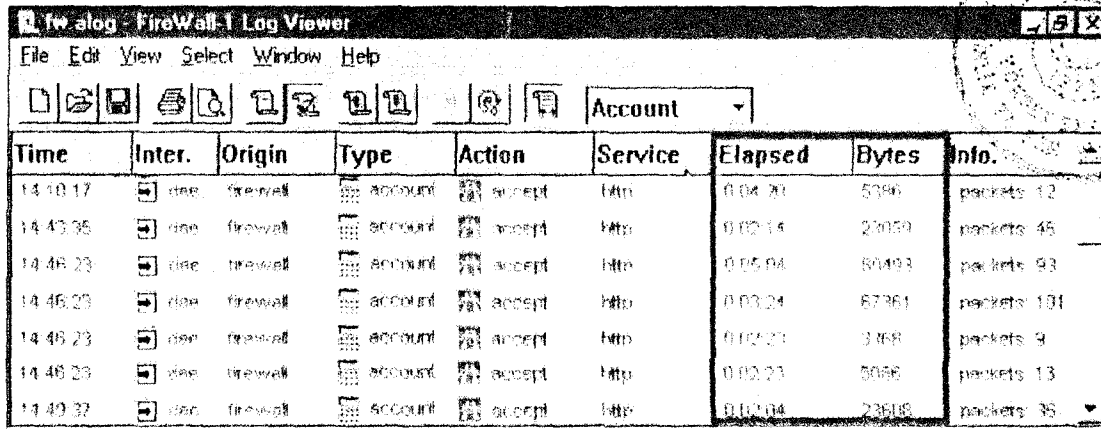
Aktif bağlantılar, FireWall-1 vasıtasıyla açık olan bağlantıların gerçek zamanlı gösterilmesini sağlar.(Şekil 5.60)



No	Time	Conn. ...	Inter.	Type	Action	Service	Proto.	S_Port
10	10:47:35	253	daemon	log	accept	25147	tcp	X11
11	10:47:35	253	daemon	log	accept	25148	tcp	X11
12	10:47:35	290	daemon	log	accept	bootp	udp	68
13	10:47:40	261	daemon	log	accept	domain-udp	udp	32895
14	10:47:41	262	daemon	log	accept	domain-udp	udp	32896
15	10:47:41	263	daemon	log	accept	domain-udp	udp	32897
16	10:47:41	264	daemon	log	accept	domain-udp	udp	32898

Şekil 5.60. FireWall-1 gerçek zamanlı kayıt defteri kontrolü

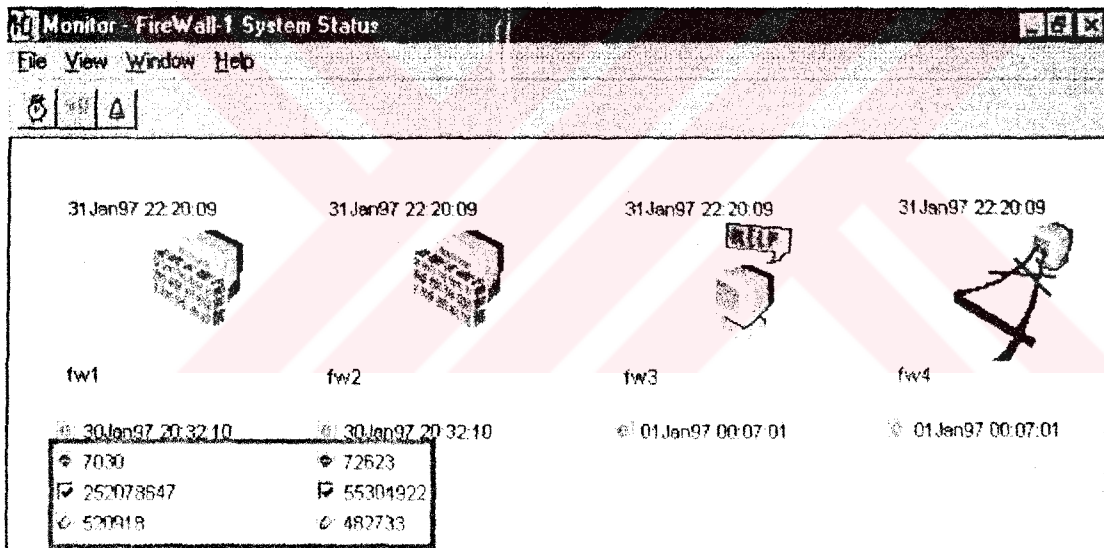
Hesap kayıtları ise, geri besleme raporlarının ve maliyetin temellerini oluşturur.(Şekil 5.61) Tüm kayıt verileri, hesap tabloları ve problem etiketleyen sistemler gibi üçüncü parti raporlama uygulamalarına ihraç (export) edilebilir.



Time	Inter.	Origin	Type	Action	Service	Elapsed	Bytes	Info.
14:40:17	die	firewall	account	accept	http	0:04:20	5796	packets: 12
14:43:35	die	firewall	account	accept	http	0:02:14	27059	packets: 45
14:46:23	die	firewall	Account	accept	http	0:05:04	60493	packets: 93
14:46:23	die	firewall	account	accept	http	0:03:24	67361	packets: 101
14:46:23	die	firewall	account	accept	http	0:02:23	3768	packets: 9
14:46:23	die	firewall	account	accept	http	0:02:23	5056	packets: 13
14:49:32	die	firewall	Account	accept	http	0:03:04	23608	packets: 35

Şekil 5.61. FireWall-1 gerçek zamanlı kayıt defteri göstericisi

Sistem Durum Göstericisi(System Status Viewer), her firewall gateway'inin durumunu gösterir. (Şekil 5.62) İstatistiksel sayaçlar denetlenmiş, reddedilmiş ve kabul edilmiş paketleri izlerler.



fw1	fw2	fw3	fw4
31 Jan 97 22:20:09	31 Jan 97 22:20:09	31 Jan 97 22:20:09	31 Jan 97 22:20:09
30 Jan 97 20:32:10	30 Jan 97 20:32:10	01 Jan 97 00:07:01	01 Jan 97 00:07:01
7030	72623		
252078647	55304922		
520918	482733		

Şekil 5.62. FireWall-1 sistem durum göstericisi

SONUÇ

Bu çalışmada yerel bir bilgisayar ağının internete açılması durumunda neyle karşı karşıya olduğu anlattım. Veriler, kaynaklar ve ünvan gibi tehlikeye maruz kalabilecek kavramlara açıklık getirdim.

Sistemlere zorla girmek, bilgi casusluğu, servisleri devre dışı bırakan saldırı tiplerini analiz ettim. Zararlılar, casuslar, hackerlar vs. gibi saldırgan çeşitlerini inceledim. Yine saldırı yöntemleri; port bombalama, IP sahtekarlığı(spoofing), ölümcül ping, SYN, FYN, UDP sahtekarlığı, koklamak(sniffing) ve IP parçalama gibi iletim protokollerini kullanan ataklar; kullanıcı parolası atakları gibi kimlik onaylama atakları; uzaktan saldırı, DNS, SMTP, MIME, NFS, URL, CGI gibi uygulama katmanı atakları olarak sınıflandırılma işlemini yaptım.

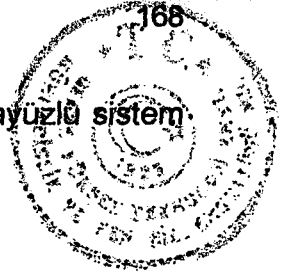
Ağa gelebilecek saldırılara karşı, karışık güvenlik, host güvenliği, ağ güvenliği gibi güvenlik yöntemlerini inceledim. En az yetki, derin savunma, boğum noktası, zayıf bağlantı, güvenli başarısızlık durumu, yaygın katılım gibi güvenlik stratejilerini inceledim.

Yine Ftp, Tftp, Fsp, UUCP gibi dosya transfer protokolleri, Telnet, Rlogin, Rsh, On gibi uzaktan erişim servisleri, E-posta, WWW, HTTP protokolleri, DNS, Usenet haber servisleri, IRC, talk gibi gerçek zamanlı servisler, Ping, SNMP, Tracerout gibi ağ yönetim servisleri, NFS, AFS gibi dosya sistemleri, finger, gopher, archie, Wais gibi bilgi servisleri ve yazdırma servisleri olarak sınıflandırılacak internet servislerini tanıttım.

Güvenlik duvarı tasarımı konusunda perdelenmiş sistem mimarisi, perdelenmiş alt-ağ mimarisi, çift arayüzlü sistem mimarisi gibi yaklaşımları inceledikten sonra bunların çeşitlerini anlattım. Savunma hostları, paket filtreleme, proxy sistemleri gibi güvenlik duvarı bileşenlerini inceldim. Mevcut

168

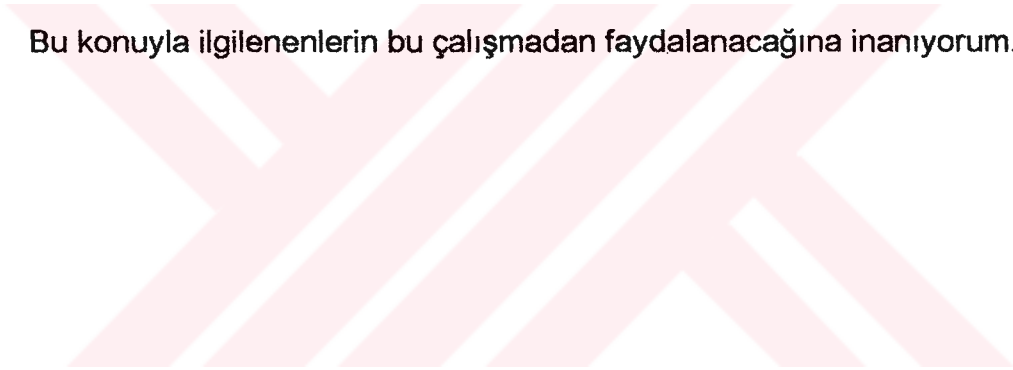
sistem için gerekli güvenlik kriterlerinin tespitinden sonra çift arayüzlü sistem mimarisinin yeterli olduğuna karar verdim.



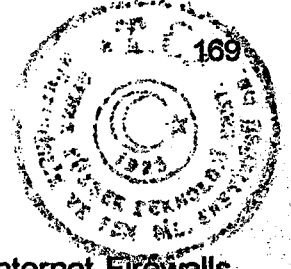
Orta ölçekli bir şirketin yerel ve geniş ağ yapısını inceledim. Ağ güvenliği için gerekli kriterler göz önüne alınarak ağ güvenliğinde çok önemli etken olan Check Point FireWall-1, CyberGuard Firewall, NetGuard Guardian güvenlik duvarı ürünlerini incelerdim. Yapılan değerlendirmeler sonucunda güvenlik yazılımı olarak Check Point Firewall-1 seçtim.

Bu şirketin; bundan sonra güvenlik alanında her zaman istediği verimi alabilmesi için, bu ürünle ilgili gelişen teknolojileri ve değişen şartları güncel takip etmesi gerekmektedir.

Bu konuyla ilgilenenlerin bu çalışmadan faydalanacağına inanıyorum.



KAYNAKLAR



1. Chapman, D. Brent and Zwicky, Elizabeth D., Building Internet Firewalls, O'REILLY 1995.
2. Check Point Software Technologies Ltd., Check Point FireWall-1 Product Suite 1997.
3. Check Point Software Technologies Ltd., Check Point FireWall-1 White Paper 1997.
4. Manas, Prof. Dr. Oğuz, Güvenlik Duvarları, BT/Haber 1998.
5. Akgül, Mustafa, İnternet ve İnternet; Araçlar ve Olanaklar 1997.
6. Wack, John P. and Carnahan, Lisa J., Keeping Your Site Comfortable Secure: An Introduction to Internet Firewalls, NIST Special Publication 800-10
7. Semeria, Chuck, Internet Firewalls and Security.
8. Sheldon, Tom, General Firewall White Paper, Nov. 1996
9. Gralla, Preston, How Intranets Work.
10. Brooks, Talley, Internet Security-Seven Firewalls That Keep Your Network Safe, Feb. 1997.
11. Ranum, Marcus J., Thinking About Firewalls, Trusted Information Systems, Inc. Glenwood, Maryland.

ÖZGEÇMİŞ

Mustafa UZUN 13.03.1973 tarihinde Remscheid(Köln)-Almanya'da doğdu. İlk öğrenimine 1980 yılında Akçaköy Merkez İlkokulu'nda başladı. Orta öğrenimini Akçaköy Lisesi orta kısmında tamamladı. 1988 yılında Trabzon Anadolu Teknik Lisesi Bilgisayar bölümüne girdi. Lise öğrenimini normal süresinden bir yıl önce, Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü'nü kazanmasından dolayı, tercihi olarak elektronik bölümünden mezun olarak tamamlayarak, bu üniversiteye girdi. 1996 yılında üniversite öğrenimini bölüm birincisi olarak tamamladı. Yine aynı yıl Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans hakkı kazandı. Halen bir sigorta şirketinin bilgi işlem merkezinde çalışmaktadır.

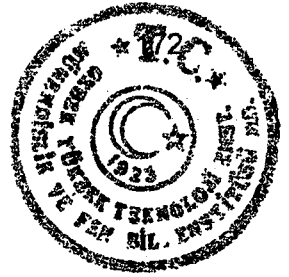


EK-1

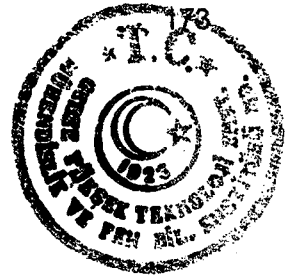
Güvenlik Duvarı Ürünleri

Burada verilen firma ve ürün bilgileri, ticari güvenlik duvarı ürünleri ve başvuru servislerini içermektedir. Fakat bu liste, ilgili tüm firma ve ürün bilgilerini içermeyebilir.

- 3Com : NETBuilder FireWall Service
- Actane : Actane Controller
- Advanced Network & Services, Inc. (ANS) : InterLock
- Artigiani Virtuali : Spaghetti
- Ascend : Secure Access Firewall
- Atlantic Computing Technology Corp. : Firewall Solutions
- Atlantic Systems Group (ASG) : TurnStyle Firewall System (TFS)
- BBN : Site Patrol
- BRAK Systems Inc. : Firewall-1
- Bull : NetWall
- Checkpoint Software Technologies Ltd. : Firewall-1
- Cisco Systems Inc. : Cisco IOS Security Architecture, Cisco Centri Firewall, Cisco PIX Firewall
- ComNet Solutions : Firewall Software Mediator One
- Compatible Systems Corp. : IntraGuard Firewall
- Computer Software Manufaktur GmbH : CSM Proxy PLUS
- CYCON Technologies : CYCON Labyrinth Firewall
- Data General : SECURELINE
- Deerfield Communications Company : Instant Internet, WinGate
- Digital Equipment (DEC) : DEC Firewall Services, AltaVista Firewall
- Digital Secured Networks Technology : NetFortress
- easynet DV GmbH : FireWall/Plus



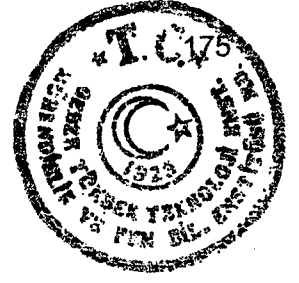
- Elron : Firewall
- enterWorks : NetSeer
- Equivalence : FireDoor (NT tabanlı)
- ExNet : ExFilter
- Firewall Security Corp. (Firewalls R us)
- Galea : Avertis
- Gemini Computers, Inc. : Gemini Trusted Security Firewall
- Global Technology Associates, Inc. : GFX Internet Firewall System
- GreatCircle Inc.: Consulting and Firewalls Tutorial
- Harris Computer Systems Corp. (HCSC) : CyberGuard
- HP : Checkpoint Firewall-1, Eagle
- Hughes Electronics Corp. : NetLOCK
- IBM : IBM Firewall
- Integralis: FireWall-1 (Checkpoint)
- Internet SmartWare: SmartWall
- Internode Systems: OpenVMS based FW
- James River Group, Inc. : ICE.Block
- KarlNet : KarlBridge
- The Knowledge Group : VCS FIREWALL
- KryptoKom : KryptoWall
- LanOptics : Guardian
- Livermore Software Laboratories, Inc. : Portus
- Livingston Inc.: FireWall IRX Router
- Lucent: Lucent Managed Firewall
- LUCIDATA: LuciGate
- Matranet : M>Wall
- MIDnet : SecurIt
- Milkyway Networks Corp. : Black Hole
- NEC : PrivateNet
- NetCS Informationstechnik GmbH : netGW
- NetGuard Ltd. : Guardian



- NetPartners : Firewall Reseller
- NetScreen : NetScreen
- Network Engineering Technologies, Inc. : NET Firewall
- Network-1 Software and Technology : FireWall/Plus
- Network Translation, Inc.: Private Internet Exchange (PIX)
- NodeWarrior Networks: Firewall and Security Services
- Norman: The Norman Firewall
- Obtuse Systems Corp.: Juniper Firewall Toolkit
- ON Technology: ONGuard
- Peapod: Borderware, Firewall for NT, Centri NT Firewall, SmartWall
- Qualix : Firewall-1
- Quarterdeck : IWareConnect
- Radguard : PyroWall
- Raptor Systems Inc. : Eagle, Eagle NT, The Wall
- Sea Change : BorderWare 4.0
- Secure Computing Corp. : Sidewinder (3.0), BorderWare Firewall Server, Firewall for NT
- Security On-Line Software (Solsoft) : Net SecurityMaster
- Siemens Nixdorf : NetSafe
- SmallWorks : NetGate
- SOS Corporation : Brimstone, Freestone
- StorageTek Network Systems Group : ATLAS, BoarderGuard
- Sun Microsystems : Sunscreen SPF-100, Solstice Firewall-1
- Technologic, Inc. : Interceptor
- TimeStep : PERMIT Security Gateway
- Trident Data Systems : Open System Security and Information Protection
- Trusted Information Systems (TIS) : Gauntlet, DMS Firewall Plus, TIS Firewall Toolkit
- Ukiah Software : NetRoad FireWALL, IpWALL and FireWARE
- Virtual Open Network Environment (V-ONE) Corporation : SmartWall

- WatchGuard Technologies, Inc. : WatchGuard
- WheelGroup Corp. : NetRanger
- Windsor Software Corp. : Win:isor Internet Connection Services
- Workgroup Technology : iWay-One
- ZapNet! : IPRoute/Secure





EK-2

Güvenlikle İlgili Bazı Kaynaklar

▪ WWW Sayfaları

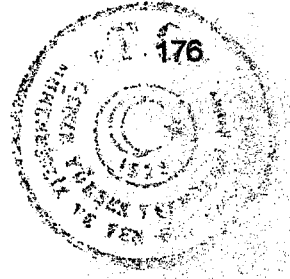
- Telstra** : Telstra Corporation – Telecom Australia
<http://www.telstra.com.au/info/security.html>
- COAST** : Computer Operations, Audit, and Security Technology
<http://www.cs.purdue.edu/coast/coast.html>

▪ FTP Siteleri

- COAST** : <ftp://coast.cs.purdue.edu/>
- CERT** : <ftp://info.cert.org/>

▪ Posta Listeleri

- Firewalls** : <ftp://ftp.greatcircle.com/pub/firewalls>
<http://www.greatcircle.com/firewalls>
- FWALL-** : Fwall-users@
Users
- Academic-** : Academic-Firewalls
Firewalls : <ftp://net.tamu.edu/pub/security/lists/academic-firewalls/>
- BugTrag** : Bugtrag-request@fo.net
- CERT-** : Cert-advisory-request@cert.org
- Advisory** : <ftp://info.cert.org/>



▪ Riskler

RISKS : <ftp://crwax.sri.com/risks/>
WWW- : majordomo@nsmx.rutgers.edu
Security

▪ Haber Grupları

comp.security.announce	Bilgisayar güvenlik ilanları
comp.security.unix	UNIX güvenliği
comp.security.misc	Karışık bilgisayar ve ağ güvenliği
comp.security.firewalls	Firewall'larda haber grupları.
alt.security	Alternatif bilgisayar ve ağ tartışma
comp.admin.policy	Güvenlikli bilgisayar yönetim politikası
comp.protocol.tcp-ip	TCP/IP güvenliği
comp.unix.admin	UNIX işletim sistem yönetimi
comp.unix.wizards	UNIX çekirdek içerikleri

▪ Cevap Grupları ve Diğer Organizasyonlar

CERT- : Computer Emergency Response Team / Coordination Center
CC : ftp://www.cert.org/pub/cert_faq
FIRST : Forum of Incident Response and Security Teams
<http://www.first.org/first/>
DARPA : Defense Advanced Research Projects Agency
SCC : Security Coordination Center
NIST : National Institute of Standards and Technology
CSRC : <http://csrc.ncsl.nist.gov/>
USENIX : USENIX Association



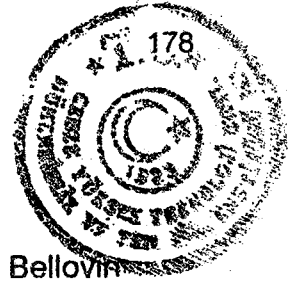
<http://www.usenix.org/>
SAGE : System Administrators Guild
<http://www.sage.usenix.org>
MIT : Massachusetts Institute of Technology
NIC : Network Information Center
CIAC : Computer Incident Advisory Capability
CNSRT : Computer Network Security Response Team
DCA : Defense Communications Agency
DDN : Defense Data Network

▪ Konferanslar

LISA : USENIX System Administration Conference
SANS : UNIX System Administration, Networking, and Security
SNDSS : Internet Society Symposium on Network and Distributed System Security

▪ Makaleler

<ftp://ftp.research.att.com/dist/smb/packets.ps>
ftp://ftp.research.att.com/dist/internet_security/dragon.ps.Z
ftp://ftp.research.att.com/dist/internet_security/berferd.ps.Z
<ftp://athena-dist.mit.edu/pub/virus/mit.ps>
<ftp://ftp.win.tue.nl/pub/security/admin-guide-to-cracking.101.Z>
<ftp://ftp.net.tamu.edu/pub/security/TAMU/NIS-paper.ps.Z>
<http://www.clark.net/pub/mjr/pubs/fwfaq>
<http://www.greatcircle.com/firewalls/FAQ>
<ftp://ftp.greatcircle.com/pub/firewalls/FAQ>



▪ Kitaplar

Firewalls and Internet Security

Internetworking with TCP/IP

Pretty Good Privacy

Practical UNIX and Internet Security

TCP/IP Network Administration

**Managing Internet Information
Services**

Network and Internetwork Security

Applied Cryptography

The Cuckoo's Egg

Cheswilk, Bill ve Steve Bellovin

Comer, Douglas E.

Garfinkel, Simson

Garfinkel, Simson ve Gene Spafford

Hunt, Craig

Liu, Cricket, Jerry Peek, Russ

Jones, Bryan Buus ve Adrian Nye

Stallings, William

Scheiner, Bruce

Stoll, Clif

