T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AÇIK SİSTEMDEKİ GÜVENLİK DUVARINI KULLANARAK AĞDAKİ PAKETLERİN KONTROLÜ

Gürkan KARABATAK

Tez Yöneticisi:
Yrd. Doç. Dr. Ali KARCI

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ELAZIĞ, 2006

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AÇIK SİSTEMDEKİ GÜVENLİK DUVARINI KULLANARAK AĞDAKİ PAKETLERİN KONTROLÜ

Gürkan KARABATAK

Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı

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

Danışman: Yrd. Doç. Dr. Ali KARCI

Üye: Yrd. Doç. Dr. Burhan ERGEN

Üye: Yrd. Doç. Dr. İbrahim TÜRKOĞLU

Bu tezin kabulü, Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...../...../..... tarih ve ..... sayılı kararıyla onaylanmıştır.

TEŞEKKÜR

Bu tez çalışmam boyunca, ilgi ve yardımlarını esirgemeyen eski danışmanım Sayın Yrd. Doç. Dr. Hasan H. BALIK'a ve yeni danışmanım Sayın Yrd. Doç. Dr. Ali KARCI'ya ve çalışmam boyunca beni destekleyen ve yardımını esirgemeyen ailem ve tüm arkadaşlarıma sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

WAN	: Geniş Alan Ağları
MAN	: Büyük Şehir Alan Ağları
LAN	: Yerel Alan Ağları
TCP	: İletim Kontrol Protokolü
UDP	: Kullanıcı Datagram Protokolü
OSI	: Açık Sistem Bağlantıları
IP	: İnternet Kontrol Protokolü
FTP	: Dosya Transfer Protokolü
SMTP	: Basit Posta Aktarma Protokolü
SNMP	: Basit Ağ Yönetim Protokolü
SSH	: Güvenli Kabuk
PPP	: Noktadan Noktaya Bağlantı Protokolü
ISS	: İnternet Servis Sağlayıcı
NAT	: Ağ Adres Dönüşümü
SNAT	: Kaynak Ağ Adres Dönüşümü
DNAT	: Hedef Ağ Adres Dönüşümü
GPL	: Genel Kamu Lisansı
VPN	: Sanal Özel Ağ
IDS	: Saldırı Tespit Sistemi
DoS	: Servis Engelleme Saldırısı

ÖZET

Yüksek Lisans Tezi

AÇIK SİSTEMDEKİ GÜVENLİK DUVARINI KULLANARAK AĞDAKİ PAKETLERİN KONTROLÜ

Gürkan KARABATAK

Fırat Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

2006, Sayfa : 44

Bu çalışmada, günümüzde artık her alanda farklı çözümler sunan açık kaynak kodlu yazılımlar hakkında bilgiler verilmiş ve bu yazılımlara en çok ihtiyaç duyulan yerlerden biri olan ağ ortamları için donanımsal bir ağ aygıtı oluşturulmasından bahsedilmiştir. Bu amaçla tamamen web üzerinden yönetilebilecek ve istenildiği zaman seri port üzerinden konsol bağlantısı yapılarak da kullanılabilecek bir güvenlik duvarı tasarlanmıştır. Bunun dışında tasarlanacak güvenlik duvarı bağlantı takibi, trafik analizi ve benzeri yardımcı araçları da bünyesinde barındırmaktadır. Bu sayede günümüzde kullanılan ağ cihazlarına açık kaynak kodlu bir alternatif sunulmaya çalışılmıştır. Ayrıca bu güvenlik duvarının ileride farklı ihtiyaçlara cevap verebilmesi veya güvenlik duvarına yeni özellikler katılabilmesi için, Linux çekirdeği üzerindeki modüllerinde değişiklikler yapılabilineceği örnek bir çalışma ile gösterilmiştir.

Sonuç olarak oluşturulan güvenlik duvarının avantajları ve dezavantajları ortaya koyularak günümüzde var olan diğer sistemler ile karşılaştırması yapılmıştır.

Anahtar Kelimeler : Güvenlik duvarı, Linux, Netfilter, Iptables, açık kaynak kod.

ABSTRACT

MS Thesis

CONTROL OF THE PACKETS ON NETWORK BY USING FIREWALL ON OPEN SYSTEMS

Gürkan KARABATAK

Fırat University

Graduate School of Natural and Applied Sciences

Department of Computer Engineering

2006, Page : 44

In this study, open source code softwares, which present different solutions in every area, were introduced, and a hardware tool, which is needed very much in network, was mentioned about. At this aim, a firewall which is controlable on the web completely and can be used on the serial port by console connection on demand, was designed. It also contains connection tracking, traffic analyse, and similar tools in its structure. By the way, an open source code alternative to network tools was presented. To response to requirement in the future of this firewall or adding new features to this firewall; modules of this firewall on Linux kernel could be modify, was shown with an example application.

Finally, the advantages and disadvantages of this firewall was exposed and compared with other systems which are exist on today.

Keywords: Firewall, Linux, Netfilter, Iptables, open source.

1. GİRİŞ

Ağ (network), paylaşım amacıyla iki ya da daha fazla cihazın bir araya getirilmesiyle oluşturulan bir yapıdır. Yüzlerce iş istasyonu veya kişisel bilgisayardan oluşabileceği gibi, iki bilgisayarın birbirine bağlanmasıyla da elde edilebilir. Bir ağla amaçlananlar kısaca şu şekilde özetlenebilir[1].

- *Kaynak paylaşımı:* Cihazların (yazıcı, disk, teyp vs), uygulamaların ve bilginin paylaşımı.
- *Yüksek Güvenilirlik:* Verilerin ve cihazların yedeklenmesi.
- *Harcanacak Paradan Tasarruf :* PC'lerin her geçen gün daha cazip hale gelen fiyat/performans oranı, ağ lisansı ile yazılım maliyetinin düşmesi.
- *Ölçeklenebilirlik:* Daha fazla işlemci eklenerek sistem performansının artması, yedek hatlarla kapasitenin artırılması.
- *İletişim:* Çalışanların kendi aralarında ve dünya ile kurdukları iletişimin sağlanması.
- *Bilgi*: Gazetelerden tartışma gruplarına, e-posta'dan elektronik ticarete, video-konferans, web, ftp, eğlence gibi bilgi paylaşım ortamlarına ulaşabilmek mümkündür. Ağları da dört ana grupta toplayabiliriz. Bunlar;
- *Yerel Ağlar(LAN):* Bina veya ofis içi gibi sınırlı alanlar içinde kurulurlar. Diğer ağ tiplerine göre daha hızlı çalışırlar.
- *Kampüs Ağları:* Birbirine yakın olan binalar arasında bilgi ve kaynak paylaşımını sağlarlar.
- *Ulusal Ağlar:* Tüm ülkeye yayılmış olan organizasyonların birimleri arasında veri iletişimini sağlarlar. Bu tür ağlara Büyükşehir Alan Ağları (MAN), ya da geniş alan ağları (WAN) adları da verilebilir. Bunlar Telekom şirketleri (TT , AT&T vs.) tarafından sağlanan bir iletişim alt yapısını gerektirirler.
- *Uluslararası Ağlar:* Veri iletişim ihtiyacı ülke sınırlarını aşmaya başladığında devreye girerler. İletişim, okyanusları aşan kablolar aracılığıyla veya uydu sistemleriyle sağlanabilir. WAN (Wide Area Networks) genel adıyla anılırlar.

Veri Transfer (İletim) Hızı bir ağın iletim kapasitesini ölçmek için geliştirilmiş matematiksel bir modeldir. Birim olarak "bps" (bit per second) kullanılır[1]. Yerel ağların iletim hızları geçen yıllara kadar 1-100 Mbps (Mega bit per second) arasında değişirken, artık gigabit teknolojiler sayesinde günümüzde 1000 Mbps ve üstü hızlar kullanılmaya başlanmıştır.

Ağların olabildiğince sorunsuz çalışması, sorun olduğunda da en kısa sürede sorunun giderilmesi gerekir. Bu nedenle ağlar tasarlanırken ve kurulurken bazı standartlara uyulmalı Switch ve Router gibi iletişim cihazların da etkin kullanılabilmesi için düzgün olarak

ayarlanmaları gerekmektedir. Bu nedenlerle iletişim teknolojilerinin etkin bir şekilde kurulumu, yönetimi için bu konuda yetişmiş, kendini yetiştirmiş insanlara ihtiyaç duyulmaktadır. Yine kullanılan başka bir cihazda güvenlik duvarlarıdır. Bu cihazlarında kontrolü ve ayarlanması uzman kişiler tarafından yapılmalıdır. Bu cihazlar ağları dışarıdan ve içeriden gelebilecek tehditlere karşı koruyarak ağların sorunsuz şekilde işleyişini sağlamaktadır. Bu çalışmada bu cihazlar hakkında incelemeler yapılmıştır.

1.1. İnternet

İnternet, tüm dünyayı kapsayan, 171 milyonun üzerinde bilgisayarın birbirine bağlandığı binlerce bilgisayar ağının tümüdür. 2002 yılı sonunda İnternet kullanıcısı sayısı 665 milyona ulaşmıştır[2]. İnternet genel bilgiye erişimi desteklemekte ve elektronik posta (elektronik mail), konferans, bildiriler gibi konularda iletişim hizmetleri sağlamaktadır.

Bütün bilgi ve servisler, İnternet'i oluşturan çeşitli ağlara dağıtılmıştır ve geçerli bir İnternet adresi ve fiziksel bağlantısı olan herhangi bir yerden ulaşılabilir durumdadırlar. Kuruluşlar İnternet'e iki ana nedenden dolayı bağlanmaktadırlar. Birincisi, İnternet yararlı bilgilere dünya çapında bir bağlanabilirlik ve erişim sağlar. İkincisi, İnternet'e bağlanmak, kuruluşlara özel bir geniş bölge ağı kurmaktan daha ucuza mal olmaktadır.

Amerika Birleşik Devletleri'nde İnternet'in işletimi federal yönetimlerce vergi mükelleflerinin vergilerinden karşılanmaktadır. İnternet'in kullanımı bir zamanlar araştırma, eğitim ve devlet kuruluşlarının etkinlikleriyle sınırlandırıldıysa da, son zamanlarda ticari kullanımı büyük oranda artmıştır. Bu gelişmeler, bazı gözlemcileri İnternet'in yakın gelecekte tamamıyla özelleştirileceği yolunda spekülasyonlara itmektedir. Böyle bir durumda İnternet kaynaklarına ulaşım kullanım fiyatlarına göre belirlenebilecektir.

1.1.1. Tarihsel Gelişim

İnternet'in ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan Savunma İleri Düzey Araştırma Projeleri Kurumu'na (DARPA- Defence Advanced Research Project Agency) dayanır. 1969'da çeşitli bilgisayar birimleri ve askeri araştırma projelerini desteklemek için Savunma Bakanlığı ARPANET adında Paket Anahtarlamalı Ağ oluşturmaya başlanmıştır. Bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarlarını da içererek büyümüştür. 1973 yılında, ağ için bir protokol seti geliştirmek amacıyla Stanford Üniversitesi'nde daha sonra BBN'in ve University College, London'in da dahil olduğu bir İnternetworking projesi başlatılmıştır. 1978'e kadar 'İletim Kontrol Protokolünün (TCP - Transmission Control Protocol) dört uyarlaması

geliştirilmiş ve denenmiştir. 1980'de bu küme sabitleşmiş ve ARPANET'e bağlı bilgisayarlar arasındaki iletişimi kolaylaştırılmıştır. 1983'te tüm ARPANET kullanıcıları İletim Kontrol Protokolü/İnternet Protokolü (TCP/IP Transmission Control Protocol/İnternet Protocol) olarak bilinen yeni protokole geçiş yaptılar. O yıl TCP/IP, ARPANET'i de içeren Savunma Bakanlığı İnternetinde kullanılmak üzere standartlaştırıldı. ARPANET 1990 Haziranında kullanımdan kaldırıldı. Yerini ABD, Avrupa, Japonya ve Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalar (backbone) aldı. ARPANET'in kaldırılmasına rağmen, TCP/IP protokolü kullanılmaya devam etmiş ve gelişmiştir.

24 Ekim 1995'te FNC (Federal Networking Council) İnterneti tanıtan bir bildiri yayınlamıştır. FNC'ye göre İnternet'in tanımı aşağıdaki gibidir :

İnternet,

1. Birbirilerine IP protokolüne dayalı global bir adres uzayı ile lojik olarak bağlı bilgisayarlardan oluşan bir bilgi sistemidir.
2. TCP/IP veya benzeri IP uyumlu protokoller kullanarak haberleşmeyi sağlar.
3. Yüksek düzeyli servislere ulaşılmasını sağlar.

1.1.2. Kullanılan Standartlar

İnternet birbirine bağlı çok sayıda bağımsız bilgisayar ağından oluşur. İnternet'te TCP/IP grubu protokoller kullanılmaktadır. TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Birçoğu, IP datagramlarının alt katman protokollerine nasıl taşınacağını gösterir. Setteki anahtar protokoller İletim Kontrol Protokolü (TCP), İnternet Protokolü (IP) ve Kullanıcı Datagram Protokolüdür (UDP - User Datagram Protocol). Uygulama servisleri içinde uç temel protokol bulunmaktadır: Bunlar virtual terminal hizmeti veren TELNET protokolü, Dosya Aktarma Protokolü (FTP File Transfer Protocol) ve Basit Posta Aktarma Protokolüdür (SMTP-Simple Mail Transfer Protocol). Ağ yönetimi ise Basit Ağ Yönetim Protokolünce (SNMP-Simple Network Management Protocol) sağlanmaktadır[3].

TCP/IP basından beri Yerel Ağ bağlantısı (LAN-Local Area Network), Yerel ve Geniş Bölge Ağları (LAN-WAN) bağlantısı, bilgisayar ağı yönetimi, ve bilgi servisi sağlanması gibi yeni ortaya çıkan konulara da hitap etmektedir. Protokol kümesi akla gelebilecek her tip bilgisayara destek vermektedir. TCP/IP`nin kaynak kodu açık olup, kullanımı teşvik edilmektedir.

Ağ yönetimi açısından SNMP, İnternet'i oluşturan TCP/IP tabanlı ağların yönetiminde en önemli standart durumundadır. SNMP istemci/sunucu (client/server) mimarisini kullanarak çeşitli ağ aygıtlarını işletmekte ve denetlemektedir. 1988'de kullanılmaya başladığından beri

SNMP öylesine başarılı olmuştur ki birçok ticari ağ isletmeni kendi özel İnternet'leri üzerindeki çeşitli Yerel Bölge Ağ elemanları için SNMP'yi kullanmaya başlamışlardır. Pek çok endüstri çözümleyicisi ise SNMP'nin yaygın kullanımını, OSI-tabanlı ağ yönetim sistemlerinin yavaş ilerleme nedeni olarak görmektedir[3].

1.1.3. İşletmen ve Servis Sağlayıcı Kuruluşlar

Son zamanlara kadar Amerika'da internete erişmenin en kolay yolu ya bir üniversitenin ya da bir devlet kurulusunun şemsiyesi altında gerçekleşebilmekteydi. Kullanıcılar, ücretsiz veya küçük bir bedel karşılığında anlaşma yaparak, bir adres elde edip internete bağlanabilmekteydiler. İnternet'in ağırlığının araştırma ve devlet projelerinden daha geniş ilgi alanlarına kaymasıyla beraber ağ işletmenleri ve servis sağlayıcıları da ticari erişim de dahil olmak üzere İnternet servislerini sunmaya başlamışlardır.

Örneğin, IBM, MCI Communications Corp. ve Merit Network Inc.'in oluşturduğu Gelişmiş Ağlar ve Servisler (ANS, Advanced Network and Services) adındaki bir konsorsiyum, NSFNET omurgası aracılığı ile İnternet'e bağlanmayı da içeren çeşitli hizmetler sunmaktadır. ABD'deki İnternet üzerindeki ana omurga olan NSFNET, Ulusal Bilim Vakfı (National Science Foundation) tarafından kurulmuştur[1].

NSFNET'e bir geçit yoluyla (gateway) bağlanmak isteyen bölgesel ve devlet ağları, üniversitelerin veri tabanlarına erişmek isteyen bilgi sağlayıcıları ve firmalar ANS'nin müşterileri arasında yer alır.

Türkiye'de TR-NET, (Türkiye İnternet Çalışma Grubu) TUBITAK ve ODTU deki merkezlerinden İnternet servisini tüm Türkiye'ye vermektedir.

1.2. Tezin Amacı

Bu tezde, güvenlik duvarları üzerine bir çalışma gerçekleştirilmiştir. Genel olarak güvenlik duvarlarının amaçlarını yerine getirebilecek, aynı zamanda birçoğunda olan avantajları kullanıp dezavantajlarını ortadan kaldıracak bir güvenlik duvarı tasarlanmaya çalışılmıştır. Bu amaçlar doğrultusunda bu çalışma için en uygun yapı olan açık kaynak kod mimarisi seçilip, oluşturulacak güvenlik duvarının yazılım temelli kısımları Linux çekirdeği ve benzer açık kaynak kodlu yazılımlar üzerinde gerçekleştirilmiştir. Bu güvenlik duvarının genel olarak tüm güvenlik duvarlarında olduğu gibi paket filtreleme, yönlendirme, ağ adres dönüşümü, bağlantı takibi ve trafik analiz gibi fonksiyonları yerine getirmesi gerekmektedir. Tüm bunlar oluşturulurken de güvenlik duvarının yeterince performanslı çalışması ve yeterince güvenli olması amaçlanmıştır. Sonuç olarak istenildiğinde küçük veya orta büyüklükte bir ağ üzerinde

gerekli işlemleri yerine getirebilecek, performanslı ve güvenli bir güvenlik duvarının tasarımı amaçlanmıştır.

İkinci olarak oluşturulan bu güvenlik duvarının sadece Linux çekirdeği üzerinde var olan özellikleri ile yetinmemek ve oluşturulacak güvenlik duvarına esneklik kazandırmak için Linux çekirdeği üzerinde de çeşitli değişiklikler yapılabilmesi için çalışmalar yapılmış ve çekirdeğe müdahale edilebilmesi sağlanmıştır. Bu amaç doğrultusunda çekirdek içerisine bazı kodlar eklenerek istenilen şeyin gerçekleştirilebildiği gözlemlenmiştir.

Tezin ilk bölümünde açık kaynak kod, Linux çekirdeği, Netfilter güvenlik duvarı alt sistemi ve kullanılan diğer açık kaynak kodlu yazılımlar hakkında bilgiler verilmiş ve oluşturulan güvenlik duvarı üzerinde ne şekilde kullanıldıkları açıklanmıştır. Bu yazılımlar ile oluşturulan güvenlik duvarı, güvenlik duvarının yönetimini sağlayan web arabirimi ve gerektiğinde kullanılabilecek konsol bağlantısı gibi diğer araçlar hakkında da bilgiler verilmiştir. İkinci kısımda ise oluşturulan güvenlik duvarının altyapısında kullanılan Linux çekirdeğinin güvenlik duvarı özelliklerini yerine getiren Netfilter güvenlik duvarı alt sisteminin üzerinde gerektiğinde değişiklikler yapılabileceği anlatılıp, yapılan bir örnek çalışma ile ilgili bilgiler verilmiştir. Son olarak sonuç bölümünde oluşturulan güvenlik duvarının avantajları ve dezavantajları hakkında bilgiler verilip çalışmanın sonuçları açıklanmıştır.

2. GÜVENLİK KAVRAMI VE GÜVENLİK DUVARLARI

2.1. Güvenlik

Ağ (network), paylaşım amacıyla iki ya da daha fazla cihazın bir araya getirilmesiyle oluşturulan bir yapıdır. Yüzlerce iş istasyonu veya kişisel bilgisayardan oluşabileceği gibi, iki bilgisayarın birbirine bağlanmasıyla da elde edilebilir. Bu ağ ortamıyla, iletişim, bilgiye ulaşım, kaynak paylaşımı, yedekleme ve ölçeklenebilirlik gibi servisler sağlanabilmektedir.

Ağı oluşturan sistemler tasarlanırken veya devreye alınırken güvenlik pek hesaba katılmadığı için, bu sistemlerin çeşitli zayıflıkları bulunmaktadır. Bu zayıflıklar kötü niyetli veya meraklı kişiler tarafından kullanıldığında, sistemler ve servisler kullanılmaz hale gelebilir, ya da kurumlar için çok önem taşıyan bilgilerin öğrenilmesi/değiştirilmesi mümkün olabilir.

Ağ güvenliği, yönetilen servislerin devamının sağlanmasını (availability), bilginin gizliliği (confidentiality) ve başka kişiler tarafından değiştirilmemesini (integrity) sağlamaya yönelik çalışmaların bütünü olarak özetlenebilir. Etkin risk yönetimi ile var olan güvenlik riskleri, azaltılarak kabul edilebilir bir seviyeye indirilebilir. Güvenlik kavramı için en temel prensipler şunlardır.

- Güvenlik bir ürün değil, bir süreçtir (Bruce Schneier).
- Bir zincir, ancak en zayıf halkası kadar güçlüdür.
- % 100 güvenlik yoktur.

2.1.1. Güvenlik İhtiyacı

Sürekli değişmekte olan küresel iletişim, pahalı olmayan İnternet bağlantıları, ve hızlı adımlarla ilerleyen yazılım gelişimi dünyasında, güvenlik gitgide daha fazla sorun haline gelmektedir. Şu anda güvenlik temel bir gereksinimdir, çünkü küresel bilişim doğal bir güvensizlik içinde bulunmaktadır. Örneğin, veriniz A noktasından B noktasına İnternet üzerinde giderken, yolu boyunca bir dizi başka noktalardan geçebilir, ve bu şekilde diğer kullanıcılara, gönderdiğiniz verinin yolunu kesebilmek, hatta veriyi değiştirebilmek için fırsatlar verebilir. Hatta sisteminizdeki diğer kullanıcılar, kötü niyetle, sizin isteğiniz dışında verinizi başka bir şekle sokabilir. "Korsan" da denilen bazı saldırganlar sisteminize izinsiz erişim sağlayabilir, ileri düzey bilgileri kullanarak sizmişsiniz gibi davranabilir, sizden bilgi çalabilir, hatta kendi kaynaklarınıza erişiminizi engelleyebilir.

2.1.2. Güvenliğin Ölçüsü

Öncelikle, hiçbir bilgisayar sisteminin tamamen güvenli olamayacağını aklımızdan çıkarmamamız gerekir. Bütün yapabileceğiniz, sisteminizi bozmaya çalışan birinin, bu işini gitgide daha zor bir hale getirmek olacaktır. Ortalama bir ev Linux kullanıcısı için "korsan"ları uzak tutmak fazla bir şey gerektirmez. Bununla birlikte, daha Büyük-Ölçek Linux kullanıcıları (bankalar, telekomünikasyon şirketleri vb.) için yapılması gereken çok çalışma vardır.

Değerlendirilmesi gereken bir diğer etken de, güvenlik önemleriniz arttıkça, bu güvenlik önlemlerinin kendisi sistemi kullanılmaz hale getirebilmektedir. Bu noktada dengeleri sağlayacak kararlar vermelisiniz, öyle ki sisteminiz kullanılabilirliğini yitirmeden amaçlarınıza uygun bir güvenlik içinde olmalı. Örneğin, sisteminize telefon yoluyla bağlanmak isteyen herkese modem tarafından geri-arama yapılması gibi bir güvenlik önleminiz olabilir. Bu daha güvenli olmakla birlikte evinde bulunmayan bir kişinin sisteme giriş yapmasını zorlaştırır. Ayrıca Linux sisteminizin ağ veya İnternet bağlantısı olmayacak şekilde de ayarlayabilirsiniz, fakat bu da sistemin yararlı kullanımını sınırlandırmak olacaktır.

Eğer orta büyüklükte veya büyük bir siteyseniz, bir güvenlik politikası oluşturmalı, ve bu politika sitenizin ne kadar güvenliğe gereksinimi olduğunu belirtiyor olmalıdır. Bu politikaya uygun olarak alınan önlemlerin ve yordamların uygulandığından emin olmak için bir izleme yordamı da olmalıdır. Yaygın olarak bilinen bir güvenlik politikası örneğini http://www.faqs.org/rfcs/rfc2196.html adresinde bulunabilir. Bu belge yakın zamanda güncellenmiştir, ve şirketinizin oluşturulacak güvenlik politikası için harika bir iskelet görevi görecek bilgiler içermektedir.

2.1.3. Korunması Gerekenler

Sistemimizi güvenli hale getirmeden önce, korunmamız gereken tehdidin düzeyine, hangi tehlikeleri dikkate almamak gerektiğine, ve sonuç olarak sisteminizin saldırıya ne kadar açık olduğuna karar verilmesi gerekmektedir. Koruduğumuz şeyin ne olduğunu, neden korumakta olduğumuzu, değerinin ne olduğunu, ve verimizin ve diğer "değerli"lerimizin sorumluluğunun kime ait olduğunu belirlemek amacıyla sistemimizi çözümlememiz gerekir.

Risk, bilgisayarınıza erişmeye çalışan bir saldırganın, bunu başarma olasılığıdır. Bir saldırgan, dosyaları okuyabilir veya değiştirebilir, veya zarara yol açacak programlar çalıştırabilir, önemli verileri silebilir. Bizim hesabımıza, veya sistemimize erişim sağlamış biri, bizim kişiliğimize bürünebilir.

Ek olarak, bir sistemde güvensiz bir hesap bulundurmak bütün ağın güvenliğinin bozulmasıyla sonuçlanabilmektedir. Eğer bir kullanıcıya .rhosts dosyasını kullanarak giriş yapma, veya tftp gibi güvensiz bir servisi çalıştırma izni verilirse, bir saldırganın "kapıdan içeri bir adım atması" riski göze almış olmaktadır. Saldırgan bir kez bizim veya bir başkasının sisteminde bir kullanıcı hesabı sahibi olduktan sonra, bu hesabı diğer bir hesaba, veya diğer bir sisteme erişim kazanmak için kullanabilmektedir.

Tehdit, genellikle tipik olarak ağınıza veya bilgisayarınıza izinsiz erişim sağlamak için güdülenmiş birinden gelmektedir. Sistemimize erişim için kimlere güveneceğimize, ve ne gibi tehditler ortaya çıkabileceğine karar verilmesi gerekir.

Biri sistemimize girerse tehlikede olan nedir? Çevirmeli ağ ile PPP bağlantısı sağlayan bir ev kullanıcısı ile makinelerini İnternete bağlayan bir şirketin, veya diğer büyük bir ağın ilgilendikleri farklı olacaktır.

Kaybolan herhangi bir veriyi yerine koymak/yeniden yaratmak için ne kadar zaman gerekeceği önemli bir konudur. İşin başında yapılan bir yatırım için harcanan zaman, daha sonra kaybolan veriyi yeniden yaratmak için harcanan zamandan on kat daha az olabilir. Yedekleme stratejileri gözden geçirilmeli ve veriler sık sık doğrulanmalıdır.

2.1.3.1. Bilgisayar Güvenliği

Belki de sistem yöneticilerinin en çok yoğunlaştığı güvenlik alanlarından biri bilgisayar bazında güvenliktir. Bu, tipik olarak, kendi bilgisayarınızın güvenli olduğundan emin olmanız, ve ağınızdaki bütün herkesin de emin olduğunu ümit etmenizdir. İyi parolaların seçilmesi, bilgisayarınızın yerel ağ servislerinin güvenli hale getirilmesi, hesap kayıtlarının iyi korunması, ve güvenlik açıkları olduğu bilinen yazılımın güncellenmesi, yerel güvenlik yöneticisinin sorumlu olduğu işler arasındadır. Bunu yapmak mutlak şekilde gereklidir, fakat ağınızdaki bilgisayar sayısı arttıkça, gerçekten yıldırıcı bir iş haline dönüşebilir.

2.1.3.2. Yerel Ağ Güvenliği

Ağ güvenliği, en az bilgisayarların güvenliği kadar gerekli olan bir kavramdır. Aynı ağ üzerindeki yüzlerce, binlerce, hatta daha fazla bilgisayarla, güvenlik her birinin tek tek güvenli oluşu üzerine kurulamaz. Bilgisayar ağını sadece izin verilen kullanıcıların kullandığını garanti altına almak, güvenlik duvarları oluşturmak, güçlü bir şifreleme kullanmak, ve ağınızda "yaramaz" (yani güvensiz) makineler bulunmadığından emin olmak, güvenlik yöneticisinin görevlerinin bir parçasıdır.

2.1.3.3. Karmaşıklaştırma Yoluyla Güvenlik

Tartışılması gereken güvenlik tiplerinden biri "karmaşıklaştırma yoluyla güvenliktir. Bunun anlamı, örneğin, güvenlik açıkları bulunan bir servisin standart olmayan bir porta (kapı) taşınmasıdır, saldırganların bu şekilde servisin nerde olduğunu fark etmeyerek bu açıktan yararlanamayacağı umulur. Diğerlerinin ise servisin nerede olduğunu bilmeleri, dolayısıyla yararlanabilmeleri gerekir. Sitenizin küçük, veya göreli olarak daha küçük ölçekli oluşu, saldırganların sahip olduklarınızla ilgilenmeyeceği anlamına gelmez.

2.2. Güvenlik Duvarları

Güvenlik duvarı özel ağ güvenlik sisteminizin önemli bir parçasıdır. Bir güvenlik duvarı özel ağınız ile İnternet gibi herkesin kullanımına açık ağ arasında güvenlik sağlar. Bu iki ağ arasındaki tüm trafik güvenlik duvarı tarafından incelenmelidir.

Güvenlik duvarı, sadece izin verilen trafiği geçirebileceğinden İnternet ile özel ağ arasındaki haberleşmenin serbestlik seviyesini kontrol etmede kullanılabilir. Örneğin, hangi servislerin ağınıza girişine ve hangilerinin çıkışına izin verileceğine karar verilebilir. Ayrıca dahili servislerinize kimlerin erişebileceği de belirlenebilir. Güvenlik duvarı ayarlanırken nelerin yasaklanacağı belirlenebilir ve geri kalan her şeye izin verilebilir. Bu ufak bir ağ için esnek ve uygundur. Fakat büyük bir ağı bu şekilde korumak zordur. Alternatif olarak, güvenlik duvarında hangi servislere izin verileceği belirlenip diğer her şey bloklanabilir. Bu kullanıcılara sınırlama getirse de çok daha güvenli bir metottur. İdeal olarak güvenlik duvarınız nelerin filtreleneceği konusundaki tanımlamalara ince ayar yapabilmeye izin vermelidir. Güvenlik duvarının kullanımı kolay olmalıdır, belki bir grafik kullanıcı ara yüzü ile (GUI) kullanım basitleştirilebilir. Ve basitçe yetkisiz istekleri durdurmak yerine, denemeleri de kayıt etmeli, tanımlamaya çalışmalı ve denemeyi hemen rapor etmelidir.

Bir güvenlik duvarının etkili olabilmesi için kendisine sızılmasına izin vermemelidir. Bununla beraber bir güvenlik duvarı tek başına özel ağınızı korumada tüm ihtiyacınız olan güvenliği sağlayamaz. Örneğin ağınızı veri kaynaklı (zararsız görünüp intranetinize girdikten sonra sisteminize içerden saldıran) saldırılardan koruyamaz.

Kullanıcıların bir güvenlik duvarını kullanmadan (bypass) etmesi mümkündür. Bunu basitçe ağdaki makinelerine bir modem takarak ISS`e (İnternet Servis Sağlayıcı) kendi bağlantılarını kurarak gerçekleştirebilirler. Fakat bu izlenmeyen bağlantılar aynı zamanda İnternet saldırganlarının içeri girebilmeleri içinde bir yol sağlar. Bazı güvenlik duvarları e-postaları virüs tehdidi için izler fakat virüs bulaşmış yazılımlara karşı bir koruma sağlamazlar.

Ve firma çalışanlarının önemli bilgileri dışarı göndermemesini garantileyemez. Bu sebeple güvenlik duvarı anti-virüs çözümü, kriptolama ve çalışanların eğitilmesi gibi güvenlik önlemleri ile birlikte kullanılmalıdır.

Bir güvenlik duvarı politikası uygularken harcamaları düşünülmelidir. Buna sadece başlangıçtaki donanım ve yazılımı almak değil sürecek olan bakımı, güncellemeler, yönetim ve eğitim harcamaları da dahil olmalıdır. Ve ağ trafiğini kontrol etmek zaman alacağından her güvenlik duvarı uygulanışı ile alakalı olarak bir performans harcaması da söz konusudur.

Haberleşmeyi yavaşlatmak İnternet`in amacına ters düşmektedir. Fakat bunun alternatifi de dışarıdakilere dahili ağınıza tam, izlenmeyen bir erişim izni vermektir. Veya İntranet`iniz ile İnternet arasında hiçbir bağ kurmamaktır.

Bir güvenlik duvarı firmanızın İnternet kullanımını izleyip kayıtlarını tutabilmenizi sağladığından İnternet bağlantısının geliştirilmesinde kullanılabilir. Kayıtlar incelenerek problemler ve yeni gereksinimler görülebilir.

Bir güvenlik duvarı, ağ adresi çevrimi (NAT - Network Address Translation) olarak da bilinen IP adres maskelemesi yapılabilmesini sağlar. IP adres maskelemesi ile ağınızdaki makinelerin adresleri harici kullanıcılar tarafından bilinemez. Bunun yerine harici kullanıcılar haberleşmeleri ağ-geçidinizin (gateway) IP adresine gönderirler ve oradan da doğru kişiye yönlendirilirler[3].

IP adres maskeleme sadece güvenlik sağlamakla kalmaz, aynı zamanda IP adreslerinin yetmediği durumlarda çözüm sağlar. Ayrıca başka bir İnternet Servis Sağlayıcısına geçildiğinde ağdaki tüm makinelerin IP adreslerinin değiştirilmesi gerekmez.

Güvenlik duvarları sadece intranet ile İnternet arasındaki haberleşmede kullanılmamaktadır. Aynı zamanda intranet içerisindeki trafiği kontrol etmede ve izlemede de kullanılabilir. Dahili güvenlik duvarları uygulamak intranet`inizi 'güvenlik alanları'na (security domains-bir güvenlik alanı aynı güvenlik seviyesine sahip makineler grubudur) ayırır. Eğer firmanızda tüm dahili bilgilere erişmemesi gereken kişiler varsa ağınızı güvenlik alanlarına bölünebilir. Örneğin, kullanıcı hesapları, pazarlama stratejisi veya ürün geliştirme hakkındaki önemli bilgilerin korunması gerekir. Bu özellikle çalışanların rakiplere bilgi sızdırmaya eğilimli oldukları durumlarda geçerlidir (FBI`ın bir anketine göre tüm bilgisayar suçlarının %80`i içerden gerçekleştirilmiştir).

Eğer sistemimizde sadece bir güvenlik duvarı varsa ve bir saldırgan onu geçmeyi başarırsa ağdaki tüm bilgilere erişebilir. Fakat dahili güvenlik duvarları varsa saldırgan ağınızın sadece bir bölümüne erişebilir. Bu sebeple saldırganın gerçekten istediği bilgilere erişebilmesi için çeşitli güvenlik duvarlarını aşması gerekecektir.

Bir güvenlik duvarı çeşitli donanım ve yazılım parçalarından oluşur. Güvenlik duvarları bastion host`lar, paket-filtreleme yönlendiricileri, uygulama-seviyesi (application-level) ağ geçitleri ve devre-seviyesi (circuit-level) ağ geçitleri olabilir. Kombinasyon hangi ürünün alındığına bağlıdır.

'Bastion-host' dahili ağı harici bir ağa bağlayan bir ağ-geçidi makinesidir. İki ağ arabirim kartına sahip çift-evli (dual-homed) bir makine bastion-host`a örnek olarak verilebilir. Güvenli olması gerektiğinden bastion host`un yakından izlenmesi iyi bir fikirdir.

Ağ adres çevrimi (NAT) daha önce bahsettiğimiz gibi dahili IP`leri gizli tutarak güvenliği artırabilir. Ve tek bir kayıtlı IP adres olsa bile ağdaki farklı makineler İnternet ile bireysel olarak haberleşebilirler.

Sıradan bir yönlendirici IP paketlerini alıp adreslerine bağlı olarak en verimli yolu kullanarak yönlendirir. Her adresi inceler, en iyi yolun hangisi olduğuna karar verir ve sonrasında mesajı otomatik olarak yönlendirir. Karar hangi yolun en kısa olduğuna, en ucuz olduğuna bağlı olabilir veya ağ yöneticisi tarafından belirlenmiş olan önceliklere bağlı olabilir.

Bir paket-filtreleme yönlendiricisi her paketin yönlendirilip yönlendirilmeyeceğine karar vermek için inceler (paket-filtreleyiciye bazen izlenen yönlendirici (screened router da denir). Genelde paketin içeriğini incelemez, paket başlığı bilgilerine bakar. Paket filtreleyici, tarafınızdan sağlanan kabul edilebilirler listesine göre paketin kaynak ve hedef adresini, protokolü, servisi ve diğer bilgileri kontrol eder. Eğer politikanız pakete izin veriyorsa en uygun yola yönlendirilir. Aksi takdirde atılırlar.

Çoğu İnternet güvenlik duvarları tek başına paket-filtreleyen yönlendirici kullanmaktadır fakat, paket filtreleyici yönlendiriciler paketlerin içeriğini incelemediği için veriye-dayalı saldırılara karşı koruma sağlayamazlar. Paket filtrelemenin kullanımı kolaydır fakat aynı zamanda saldırılması da kolaydır. Ve hangi paketlere izin verilmeyeceğine siz karar verdiğinizden her hata güvenlik duvarını güçsüzleştirmektedir.

Bir uygulama-seviyesi ağ geçidi bir bastion-host üzerinde çalışabilmektedir ve e-posta gibi belirli uygulamalara olan trafikte kısıtlamalar yapabilir. Tüm ağ trafiği için genel amaçlı bir kod kullanımı yerine vekil sunucu (Proxy) servisi adı verilen özel bir kod kullanılmaktadır. Güvenlik duvarınızdan geçmesini istediğiniz her uygulama için ağ-geçidi üzerine bir Vekil sunucu servisi kurulabilir. Sadece, vekil sunucu kodu kurulan servisler uygulama ağ-geçidinden geçebilirler. Bir uygulama için vekil sunucu kodu uygulamanın sadece belirli özelliklerini destekleyecek şekilde ayarlanabilir.

Uygulama-seviyesi ağ-geçitleri katı bir güvenlik politikasını yürütmek için iyi bir seçimdir çünkü ağınızdan erişilen her servisi kontrol edebilmenize izin verir. Ayrıca kullanıcı

kimlik tanılamasını desteklerler ve detaylı kayıt (log) bilgisi sağlarlar. Ayarlanmaları bir paket-filtreleyici yönlendiriciden daha karmaşık olsa da bakımları daha kolaydır.

Paket filtreleyici yönlendiricilerin aksine uygulama ağ geçitlerinin kurulumu pahalıdır ve performansı düşürebilirler.

Vekil sunucu sunucusu bir uygulama-seviyesi ağ-geçidi tipidir. Bir uygulama ağ-geçidi gibi Vekil sunucu sunucusu transfer edilen verileri kontrol eder. Ayrıca kullanıcı ismi ve şifrelerin geçerliliğini de kontrol edebilir. Ve sık istek yapılan web sayfalarının kopyalarını saklayarak kullanıcıların daha hızlı erişmesini sağlayabilir.

Devre-seviyesi ağ-geçidi, bir bastion-host üzerinde uygulama-seviyesi ağ-geçidi veya bir Vekil sunucu sunucusu ile birlikte bulunan özelleştirilmiş bir fonksiyondur. Bir devre ağ-geçidi basitçe dahili makineleri harici TCP/IP portlarına bağlar. Transfer ettiği verileri veya servisleri incelemez. Devre-seviyesi bir ağ-geçidi İnternet`e direk erişim sağladığından sadece güvenilen dahili kişilerden dışarıya giden haberleşmelerde kullanırsınız. İçeri gelen bağlantılar için hala bir uygulama-seviyesi ağ-geçidi kullanırsınız. Bu yolla güvenilen kullanıcılardan dışarı giden bağlantıları hızlandırırken ağınızı harici saldırılardan koruyabilirsiniz.

2.2.1. Güvenlik Duvarı Tipleri

Güvenlik duvarlarını yazılım tabanlı ve donanım tabanlı olarak ikiye ayırabiliriz. Ancak unutulmamalıdır ki yazılım ve donanım bir bütündür. Her yazılımın çalışması için gerekli bir donanım ve her donanımın işleyişini sağlayan bir yazılım vardır. Bizim yazılım tabanlı ve donanım tabanlı olarak ayırtmamızın nedeni kullanıcı tercihini kolaylaştırmak ve kendi şartlarına göre uygun ürünü alabilmesini sağlamaktır.

Unutulmamalıdır ki yazılım tabanlı güvenlik duvarları üreticisi tarafından sadece yazılım olarak üretilip üzerinde çalışabileceği donanım belirtilir ve ürünü kullanmak isteyen kişi veya kuruluşun ilgili donanımı alıcının kendisinin temin etmesini bekler. Bu nedenle ilgili donanım olmadan kullanılamazlar[6].

Donanım tabanlı güvenlik duvarları ise üreticisi tarafından gerekli donanım ve bu donanımın işlevini sağlayacak ve kullanıcı arabirimini sağlayacak yazılım ile birlikte üretilir ve bu şekilde kullanıcı kişi ya da kuruluşa sunulur.

Aşağıda bu iki güvenlik duvarı türünün genel avantajları ve dezavantajları anlatılmaktadır.

2.2.1.1. Yazılım Tabanlı Güvenlik Duvarları

Bu tip güvenlik duvarları, genellikle kişisel ve sunucu bilgisayarları üzerine kurulabilen ve işletim sistemi ile bütünleşik olarak çalışan yazılımlardır. Genellikle yazılım şeklinde satılırlar ve hepsinin çalışabildiği belirli işletim sistemleri vardır. Bu yüzden bu tür güvenlik duvarları işletim sistemine bağımlıdır. Bir işletim sisteminde çalışan bir güvenlik duvarı diğerinde çalışmayacaktır.

Bu tip güvenlik duvarlarına örnek olarak birçok kişisel ve kurumsal güvenlik duvarı verilebilir. Kişisel ve ev kullanıcısı için güvenlik duvarı örnekleri olarak Symantec Norton Personal Firewall, Conseal PC Firewall, ZoneLabs Zone Alarm, Sygate Personal Firewall verilebilir. Hem kişisel hem de kurumsal olarak kullanılan birkaç güvenlik duvarı daha ayrıntılı olarak incelenecektir..

Bu tür güvenlik duvarları açık kaynak kodlu veya kapalı kaynak kodlu olabilir. Açık kaynak kodlu olanlar tamamen ücretsiz olup GPL (General Public License) lisansıyla dağıtılırlar. Kısaca, GPL, FSF tarafından geliştirilen ve kamunun kullanımına sunulan bir bilgisayar lisansıdır. GPL pek çok özgür yazılım tarafından kullanılmaktadır. GPL'in en fazla kullanıldığı platformlardan birisi Linux işletim sistemidir.

GPL altında yayınlanan bir yazılımla her istediğinizi yapamazsınız. Örneğin o yazılımı, beraberinde kaynak kodları olmaksızın dağıtamazsınız. Başka birisinin dağıtım haklarını kısıtlayamazsınız.

Bir yazılımı GPL altında yayınlamak, yazara telif hakkı güvencesi altında, yazılımının başkaları tarafından özgür yazılım felsefesine aykırı olarak dağıtılamayacağı güvencesini verir.

Kapalı kaynak kodlu ürünlerin tüm telif hakkı ise üretici firmaya ait olmakla beraber kullanmak isteyen kişi ve kuruluşun ilgili firmadan belirli bir ücret karşılığında ürünün lisansını alması gerekir. Alınan ürün hiçbir şekilde başka bir kişiye verilemez, üzerinde değişiklik yapılamaz ve sadece lisans sözleşmesinde yazan şekilde kullanılabilir. Her iki özellikteki güvenlik duvarlarının da kendine ait avantaj ve dezavantajları bulunmaktadır. Aşağıda her iki tipinde avantaj ve dezavantajları ayrı olarak incelenmiştir.

2.2.1.2. Donanım Tabanlı Güvenlik Duvarları

Bu tip güvenlik duvarları donanım şeklinde tasarlanmış ve üzerine bazı işlemleri gerçekleştirebilecek, kullanıcı arabirimi sunacak çeşitli yazılımlarla donatılmıştır. Genellikle hepsinde kendine özel bir işletim sistemi bulunmaktadır. Ancak genel olarak tüm işlemler çeşitli donanımlar tarafından yapılmaktadır. Bu tür güvenlik duvarlarına genellikle bir konsol portu

üzerinden veya genellikle http protokolü üzerinden bağlanılarak gerekli konfigürasyonlar yapılmaktadır. Bu tür güvenlik duvarları yönetim konsolları sayesinde işletim sistemlerinden bağımsız olarak kullanılabilirler. Bu sebepten dolayı genellikle tercih edilirler. Bu tür donanım üreten firmalara örnek olarak Cisco Systems, 3Com, Lucent, Hewlett Packard gibi firmalar verilebilir. Yine bu tür güvenlik duvarlarına örnek olarak da Cisco firmasının üretimi olan Pix ve Watchguard, Lucent firmasının üretimi olan Brick ve 3Com VPN firewallar verilebilir[6].

2.2.2. Güvenlik Duvarlarının Özellikleri

2.2.2.1. Yazılım Tabanlı Güvenlik Duvarlarının Özellikleri

Genel Avantajları:

- But tür güvenlik duvarları genellikle işletim sistemleriyle bütünleşik olarak çalıştıklarından çok daha ayrıntılı bir şekilde raporlama alınabilir.
- Uygulama yazılımları oldukları için gerekli donanım sağlanıldığı sürece rahatlıkla bir yerden başka bir yere aktarılabilirler.
- Yeni sürümleri veya eklentileri çıktığında kolaylıkla güncelleme işlemleri yapılabilir ve hataları giderilebilir.

Genel Dezavantajları:

- İşletim sistemine bağımlıdırlar, her yazılım her işletim sisteminde çalışmayabilir.
- İşletim sistemi üzerinde çalıştıkları için işletim sistemlerinin de bakımı söz konusudur.
- İşletim sistemlerinde bulunan hatalardan etkilenirler ve bu hatalardan performansları etkilenebilir.
- Tüm yazılımlarda olduğu gibi yazılım hatalarıyla sık sık karşılaşılır.
- Güvenlik duvarının kendisi yazılım olmasına rağmen işletim sisteminin üzerinde çalışacağı bilgisayarlara ihtiyaç duyarlar. Bu yüzden donanım bağımsız değillerdir. Herhangi bir donanım arızasından veya işletim sistemiyle donanım arasındaki uyuşmazlıktan etkilenirler.
- Kurulum süreleri donanımsal güvenlik duvarlarına oranla çok daha uzun sürmektedir.

Bu tür güvenlik duvarları açık veya kapalı kaynak kodlu olabilirler. Bunlarında kendi içlerinde avantajları ve dezavantajları mevcuttur[6].

Açık Kaynak Kodlu Güvenlik Duvarlarının Avantajları:

- Kaynak kodları açık olduğundan ve genellikle GPL lisansıyla dağıtıldığından herhangi bir lisans ücreti ödenmeden sahip olunabilir.
- Kaynak koduna gerektiğinde eklentiler yapılabilir hataları kolaylıkla bulunup arındırılabilir.
- Kullanılacak ortama göre istenildiği gibi değişiklik yapılarak maksimum performans elde edilmesi sağlanabilir ve gereksiz eklentilerden kurtulabilinir.
- Kaynak kodları açık olduğundan hataları çabuk tespit edilip kısa süre içinde kapatılır.

Açık Kaynak Kodlu Güvenlik Duvarlarının Dezavantajları:

- Kaynak kodları açık olduğundan kötü niyetli kişiler tarafından incelenerek hataları bulunarak diğer sistemlerin etkilenmesine sebep olunabilir.
- Genellikle gönüllü kişiler tarafından geliştirildiği için herhangi bir sorun karşısında başvurulacak 3. bir şahıs mevcut değildir. Oluşabilecek hatalardan kullanıcı sorumludur. Ancak bakım ve onarım için belirli bir maliyetle başkalarının desteği alınabilir.
- Belirli bir süre sonra geliştirici kişi tarafından geliştirilmesi durdurulabilir.

Kapalı Kaynak Kodlu Güvenlik Duvarlarının Avantajları:

- Kodları kapalı olduğu için kötü niyetli kişiler tarafından yazılımın sorunlarının bulunması çok daha zordur
- Genellikle üretici firmaya belirli bir lisans ücreti ödendiği için çeşitli anlaşmalar yapılarak üretici firma tarafından kurulum ve bakım garantisi ve oluşacak sorunların giderilmesi konusunda garanti alınabilir. Açık kaynak kodlu güvenlik duvarlarında ise bu genellikle yazılımla ilgisi olmayan kişi ve kuruluşlar tarafından istenebilir.
- Belirli bir firma tarafından geliştirildiği için uzun zaman geçtikten sonra bile geliştirilmesine devam edilir ve hataları giderilebilir.

Kapalı Kaynak Kodlu Güvenlik Duvarlarının Dezavantajları:

- Kapalı kodlu oldukları için geliştirilmesi hataların giderilmesi ve eklemelerin yapılması sadece üretici firma tarafından yapılabilir. Herhangi bir gereksinimde üretici firmanın beklenmesi gerekecektir.
- Kullanıcı tarafından karşılaşılacak herhangi bir sorunun sebebini tespit etmek çok daha zordur.

2.2.2.2. Donanım Tabanlı Güvenlik Duvarlarının Özellikleri

Genel Avantajları:

- En büyük avantajları uygulama için özel geliştirilmiş entegre devreler (ASIC) kullanılmış olmasıdır. Bu sayede daha yüksek performans sağlayabilirler.
- Genellikle en kötü saldırılarda bile cihaz kapatılıp tekrar açıldığında çalışmaya devam ederler.
- Minimum seviyede yazılım kullanıldığından ve bu yazılımların tam olarak ne oldukları bilinmediğinden yazılım açıklarından son derece az etkilenirler.
- Hizmet dışı kalma süreleri oldukça azdır.
- Yazılım oranı çok düşük olduğundan sürüm güncellemeleri diğer sistemlere göre çok daha hızlı yapılır.

Genel Dezavantajları:

- Yazılabilecek kurallar ve yapılabilecek işlemler cihazın kapasitesi (İşlemci gücü, Hafıza Miktarı vs..) ile sınırlıdır.
- Özellikle küçük yapıda olanların donanımsal olarak genişletilebilmek şansı düşüktür. Genellikle bir üst sürümlerinin alınması gerekir. Diğer tiptekilerde ise performans artırımı için gerekli güncellemeler hem pahalı hem de zordur.
- Raporlama işlemleri genellikle sınırlıdır.
- Değişik saldırılara karşı güncellenmeleri kolay değildir ve uzun bir zaman ister.
- Yazılımlarındaki sürüm güncellemeleri genellikle kapanıp tekrar açılma gerektirir.
- Özelleştirilmiş bir donanım yapısında olmalarından dolayı diğer sistemlere oranla pahalı sistemlerdir.

2.2.3. Linux Netfilter Güvenlik Duvarı Sistemi

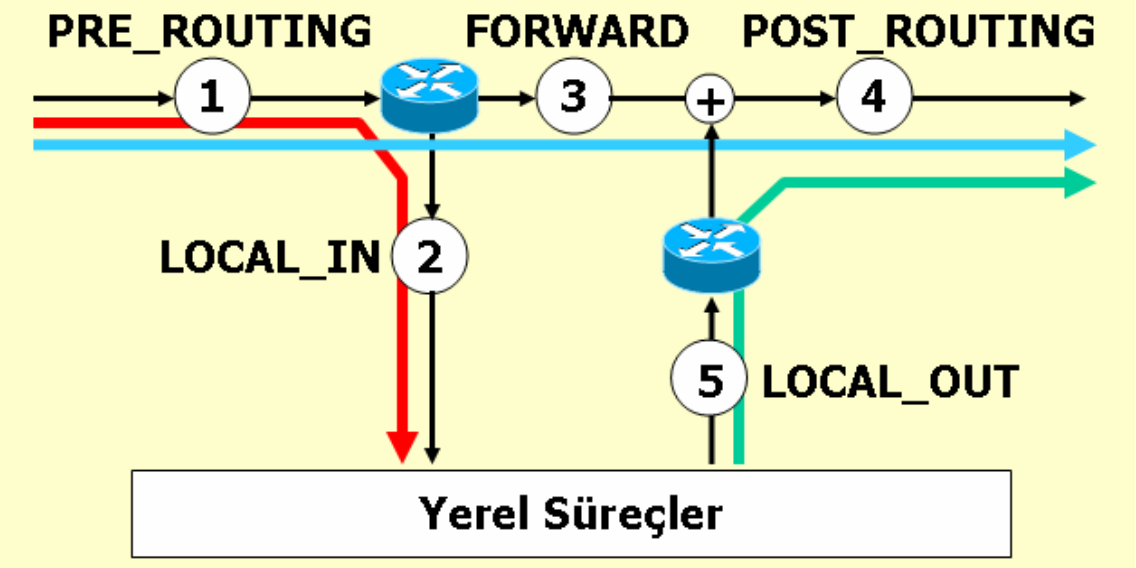
Linux çekirdeği içerisinde gömülü olarak çalışan GPL lisanslı bir güvenlik duvarı sistemidir. Linux 2.0 sürümünde kullanılan ipfadwm ve 2.2 sürümünde kullanılan ipchains güvenlik duvarı sisteminin geliştirilmiş bir sürümüdür. Linux 2.4 ve 2.6 çekirdek sürümlerinde kullanıma sunulmuştur. Iptables genel tablolama yazılımı ile kural kümeleri tanımlanmaktadır. Temeli bir çekirdek grup tarafından oluşturulmasına rağmen modüler bir yapısı olduğundan ve açık kaynak kodlu olduğundan tüm dünyada geliştirilme çalışmaları yapılmaktadır. Yine bu özelliğinden dolayı güvenlik duvarının kullanılacağı sisteme göre istenilen servislerin kurulması veya istenilmeyenlerin kaldırılması sağlanarak özelleştirilmiş bir halde de kullanılabilir. Genel özellikleri şu şekildedir[5].

- Farklı protokol kümelerine göre paket filtreleme yapılabilir.
- Tüm adres ve port dönüştürme işlemlerini desteklemektedir.
- QoS destekler ve karmaşık yönlendirme politikaları oluşturulabilir.
- Ip başlıklarındaki bitleri (TOS, DSCP, EPN) değiştirerek istenilen şekilde paket iletimine izin verir.
- Bant genişliği üzerinde kısıtlamalar veya dengelemeler yapabilir.
- Linux işletim sistemi sayesinde HTTP, SSH, Telnet vb.. gibi protokollerle uzaktan yönetim yapılabilir.
- Uygulama bazında FTP, SMTP, HTTP, H.323 protokolleri üzerinde filtreleme yapabilir. Dinamik filtrelemeyi destekler.
- Dinamik filtreleme sayesinde TCP bayraklarını kontrol ederek sadece güvenilen bağlantılara gelen cevapların geçişine izin verilerek diğerleri iptal edilebilir. Bu sayede farklı saldırıların önüne geçilebilir.
- PPTP,H.323, FTP gibi protokoller üzerinde bağlantı takibi yapabilir.
- Bulanık Mantık kullanılarak gelen paket sayısına göre dinamik bir filtreleme yapılabilir. Bu sayede saldırı özelliği gösteren trafiğin önüne geçilebilir.
- Paket büyüklüklerine göre denetim yapılarak bazı DoS saldırılarının önüne geçilebilir.
- Çeşitli uygulama protokolleri için bant genişliği limiti koyulabilir.

Netfilter çekirdekte bulunan ve IPv4, IPv6, DECnet gibi protokollerin denetlenebildiği bir mekanizmadır. Netfilter kullanabilmek için 2.3.15 veya üzeri bir Linux çekirdeğine sahip olmak ve çekirdek ayarlarında CONFIG_NETFILTER kısmının yüklenmiş olması

gerekmektedir. IPv4 'de bir paketin Netfilter sistemini nasıl dolaşabileceği Şekil 2.1'de basitçe belirtilmiştir.

IPv4'de, Şekil 2.1'de de görüldüğü üzere toplam 5 adet nokta mevcuttur. Her noktada paketler Netfilter tarafından, ayrı politikalara göre değerlendirilir. Bu yapıda bir paket yapısal olarak kontrol edildikten sonra(bozuk mu?, IP paketi mi?) sol taraftan Netfilter sistemine gelir. Sayılarla belirtilen yerler Netfilter'in kontrol noktalarıdır. "ROUTE" ile belirtilen yerler çekirdek tarafından yapılan yönlendirme işlemleridir. Her paketin ilk uğrayacağı yer (1) yani PREROUTING diye adlandırılan noktadır. Bir sonraki ROUTE noktasında çekirdek, paketin yerel sistem içindeki bir sürece mi, yoksa başka bir sistemdeki sürece mi giden bir paket olduğuna karar verir. Eğer yerel sistemdeki bir sürece ise paket (2) yani INPUT noktasına, değilse (3) yani FORWARD noktasına gönderilir. Eğer paketin gideceği yer sistemin yönlendirme tablosunda tanımlı değilse paket yok edilir. Yönlendirme işlemleri Netfilter'i ilgilendirmez. Lokal olarak üretilen paketler (5) yani OUTPUT noktasına, akabinde yönlendirmeye tabii tutulur. Şekil 2.1'de de görüldüğü gibi yerelde üretilen paketler ve FORWARD'dan gelen paketler (4) yani POSTROUTING noktasından sonra sistemi terk eder[6].



Şekil 2.1 Netfilter Güvenlik Duvarı Sisteminin Yapısı.

3. OLUŞTURULAN WEB TABANLI GÜVENLİK DUVARI

Günümüzde bilgisayar ağları ve internet alanındaki uygulamalar hızla artmaktadır. Bununla birlikte bu ağlardaki uygulamalar ve kullanıcıların güvenliği ise önemli bir sorun teşkil etmektedir. Bu sorun günümüzde çeşitli güvenlik duvarı yazılım ve donanım araçlarının çeşitli türlerde konfigürasyonu ile çözülmeye çalışılmaktadır[2,3].

Buradaki düşünce, hem kullanıcılara bilgisayarları başından erişebilecekleri hizmetler sunabilmek hem de bu hizmetlerin kesintisiz olmasını sağlamak ve hizmeti aksatıp suiistimal edebilecek herhangi bir kötü emelli girişime karşı önlemler alabilmektir. Bu nedenle bu araçların kullanımı bilgisayar ağları ve internet üzerindeki uygulamalarla doğru orantılı olarak artmaktadır. Yukarıda bahsettiğimiz avantajları kullanıp dezavantajları kaldırmak için pek çok çalışma yapılmış ve bu nedenle açık kaynak kodlu yazılımlar bu çalışmaların en önemli odak noktalarından biri olmuştur.

Bu amaçlarla günümüzde ticari olarak yapılmış pek çok çalışma mevcuttur. Bunlara güncel olarak verilecek en güzel örnekler 3COM firmasının Office Connect VPN Firewall'u , Astaro firmasının Security Gateway'i ve CyberGuard/SnapGear firmasının ucLinux tabanlı güvenlik duvarları ve yönlendiricileridir. Tüm bu ürünlerin ortak özellikleri ticari olmaları ve Linux çekirdeği kullanmalarıdır. Bu ürünleri ve bu amaçla üretilmiş birçok ticari ürünü ve özelliklerini internet üzerinden bulmak mümkündür[7]. Aynı şekilde günümüzde başta Cisco, Linksys, Belkin, Netgear ve D-Link gibi dünya üzerinde bilinen firmalar, ağ geçidi, yönlendirici, erişim noktası gibi birçok ürünlerinde yazılım olarak Linux çekirdeği kullanmaktadırlar. Özellikle Linksys firması kendi sitesinde bu ürünlerin Linux tabanlı kaynak kodunu da açık olarak sunmaktadır.

Bu konuda PC ler için yazılım tabanlı güvenlik duvarları örnekleri de mevcuttur. Bu tür yazılımlara örnek olarak da IPCop, Sentry Firewall, OpenWRT ve Teknowall verilebilir.

Tipik bir güvenlik duvarının yerine getirmesi gereken temel bazı işlevler bulunmaktadır. Bunların en temeli yönlendirme işlevi ve yönlendirme esnasında paket filtreleme işlemidir. Bunun dışında genellikle bağlantı takibi ve trafik analizi gibi ekstra özelliklerinin de bulunması gerekmektedir.

Güvenlik duvarı sisteminde Genel Ayarlar, Güvenlik Duvarı Ayarları, Yönlendirme Ayarları, Bağlantı Takibi ve Trafik Analiz kısımları bulunmaktadır.

Genel Ayarlar kısmında bulunan Ethernet ara yüz ayarları kısmı ile tüm ara yüzlere IP adresleri atanabilir ve var olan IP adresleri değiştirilebilir. Şifreleme kısmında Web sayfasına erişim için kullanıcı adı ve şifre atanabilir ve Reset kısmından ise Sistem resetleme işlemi yapılabilir. Tüm bu işlemlerin güvenli olarak yapılabilmesi için web sunucu SSL desteği

vermektedir ve https protokolü kullanılarak ta web arabirimine erişim yapılabilmektedir. Bu sayede yapılacak şifre tanımlamaları veya herhangi bir işlem ağ üzerinden dinleme yardımıyla kesinlikle tespit edilememektedir[8].

Güvenlik duvarı Ayarları kısmında Netfilter alt sistemi için gerekli kural ve politika işlemleri yapılır. Zincirler için politikalar belirlenip istenilen erişim kuralları eklenip, kaldırılıp, değiştirilebilir veya listelenerek basit ve hızlı bir şekilde yer değiştirilebilir. Özellikle erişim listeleri yukarıdan aşağıda doğru adım adım işlemekte olduğundan kurallar arasındaki yer değiştirme işlemi tek tıklama ile yapıldığından kullanıcı açısından büyük kolaylık sağlamaktadır.

Yönlendirme ayarları kısmında ağ için gerekli yönlendirme işlemleri yapılabilir. Bu yönlendirme işlemleri ağ veya host bazında olabilir ve Ağ geçidi tanımlama işlemleri yapılabilir. Ağ bazında istenilen ağ üzerine gelecek paketler farklı bir arabirime veya 3. bir yönlendiriciye yönlendirilebilir. Host bazında ise gerektiği zaman sadece belirli hostlar için trafik değişik adreslere yönlendirilebilir.

Bağlantı Takibi kısmında ise port ve IP bazlı olarak bağlantı takibi yapılabilir. Bu sayede belirli bir port veya IP bazında anlık bağlantılar takip edilebilir.

Güvenlik duvarı üzerinden gerektiğinde seri port kullanılarak seri bağlantı yapılabilir. Bu sayede web erişimi kesilse bile güvenlik duvarı seri bağlantı yoluyla Linux konsolu üzerinden yapılandırılabilir. Bu şekilde normal bir PC ye bağlantı yapmak için sadece bir adet Null-Modem kablosu yeterlidir.

Trafik Takibi kısmında ise saatlik, günlük, haftalık ve aylık olarak tüm ethernet arayüzleri hakkında bilgi toplanabilir ve bant genişliği kullanımları grafiksel olarak görülebilir.
Sistem herhangi bir Linux dağıtımı ve bilgisayar donanımı üzerine yapılandırılabilir. Sistem Linux-Netfilter-Iptables güvenlik duvarı sistemi, Kabuk programlama, Apache Web sunucusu ve PHP betik dili kullanılarak tasarlanmıştır.

Güvenlik duvarı tasarımında kullanılan Netfilter güvenlik duvarı alt sistemi genel olarak birçok güvenlik duvarından istenen özellikleri barındırmaktadır. Bununla birlikte oluşturulan güvenlik duvarı yeterince esnek olmalı ve gerektiğinde Linux çekirdeğindeki değişiklikler ile bu güvenlik duvarında istenen değişiklikler yapılabilmeli, sisteme ve ağa uygun hale getirilebilmeli, yeni teknolojiler eklenebilmeli; kısacası yeterince esnek olmalı ve her türlü ihtiyacı karşılamalıdır. Bu yüzden bu tezde oluşturulan güvenlik duvarı ile yetinilmeyip bu güvenlik duvarına temel olan ve Linux çekirdeği içerisinde bulunan Netfilter güvenlik duvarı alt sistemi üzerinde de gerekli değişiklikler yapılabilineceği örnek bir uygulama ile gösterilmiştir.

3.1. Güvenlik Duvarı Web Arabirimi

Güvenlik duvarının tamamen donanımsal bir yapı olmasından dolayı web arabirimi oldukça büyük bir önem arz etmektedir. Bu arabirimin oluşturulmasında ve çalışmasında bahsedilen yapılar dışında yardımcı araçlar, veritabanı veya ekstra eklentiler kullanılmamıştır. Bunun amacı oluşturulan yapının Linux çekirdeği üzerine rahatlıkla oturtulması ve bu çekirdeği kullanan herhangi bir işletim sisteminin bu güvenlik duvarı içerisinde kullanılabilmesini sağlamaktır.

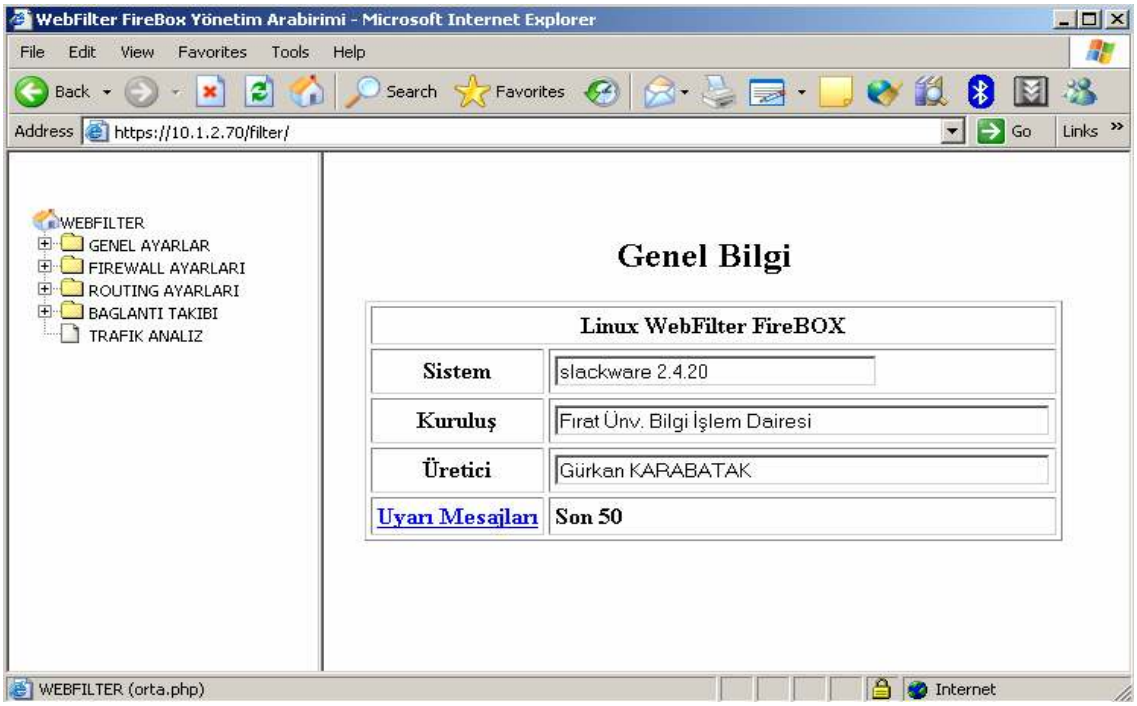
3.1.1. Genel Ayarlar Modülü

İlk olarak güvenlik duvarının web yönetim kısmındaki bu modül tasarlanmıştır. Bu modülde güvenlik duvarına web üzerinden bağlanıldıktan sonra. Interface Ayarları, Şifreleme ve Reset kısımları oluşturulmuştur.

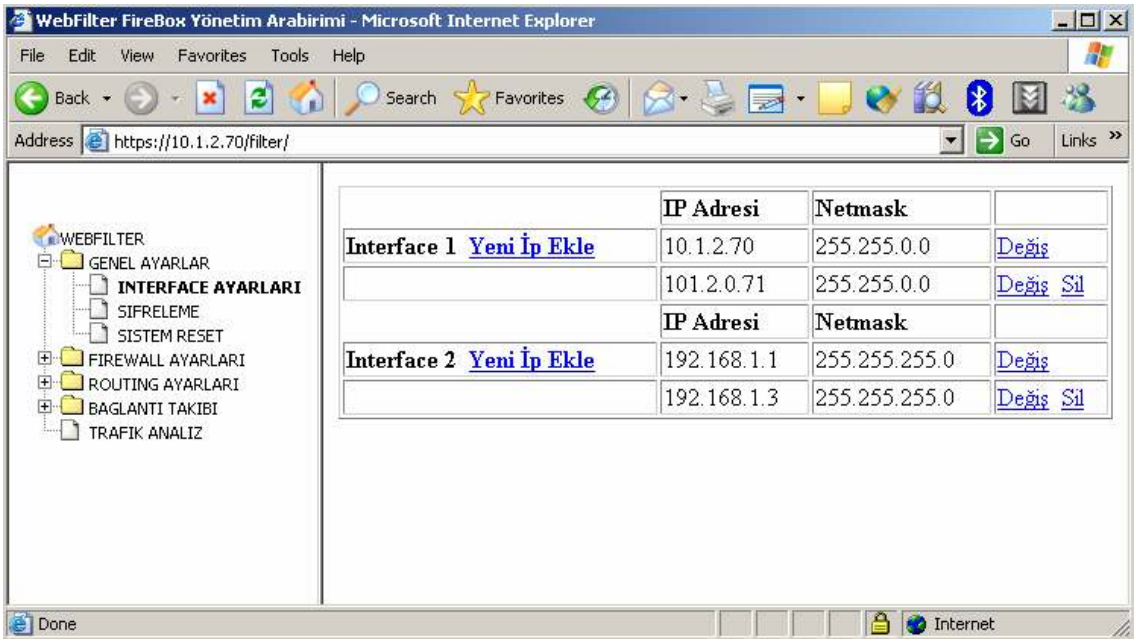
Interface ayarları için PHP betik dili ile Linux üzerinde kabuk programlama yapılmış ve gerekli komutlar kullanılarak web yönetim konsolu üzerinden güvenlik duvarı interfacelerine müdahale edilebilmesi sağlanmıştır. Web üzerinden tüm interfaceler otomatik olarak görüntülenip gerekli ip adresleri değişimlerinin yapılabilmesi sağlanmıştır.

Şifreleme kısmında web yönetim konsolu için kullanılan Apache web sunucu üzerinde ayarlar yapılarak web sayfasının istenildiğinde kullanıcı adı ve şifre verilerek güvenlik sorgulaması yapılması sağlanmıştır. Web sunucu dosyalarının bulunduğu dizinlerde gerekli dosyalar oluşturulması ve Apache konfigürasyon dosyalarında gerekli değişikliklerin yapılabilmesi için gerekli PHP kodları yazılarak işletim sistemi üzerinde bash kabuğu ile gerekli komutların çalıştırılabilmesi sağlanmıştır. Şifreleme işleminin iptalinde de yapılan işlemlerin geri alınması için gerekli kodlar yazılmıştır. Bu işlem için Apache web sunucu üzerinde .htaccess yapısı kullanılmıştır. Aynı şekilde yine Apache Web sunucu üzerinde SSL şifreleme için OpenSSL kriptografi yapısı ve Apache modülü olan ModSSL paketi kullanılmıştır.

Reset kısmında ise sistemi yönetim konsolu üzerinden resetleyebilmek için gerekli kodlamalar yapılmıştır. Aynı şekilde resetleme işleminden sonra sistemin doğru şekilde açılabilmesi için düzenlemeler yapılması sağlanmıştır. Şekil 3.1 ve 3.2'de Genel Ayarlar modülünden görüntüler görülmektedir.



Şekil 3.1 Güvenlik Duvarı Web Yönetim Ekranı Genel Görünümü.



Şekil 3.2 Güvenlik Duvarı Genel Ayarlar Modülü Interface Ayarları Sayfası.

3.1.2. Güvenlik Duvarı Ayarları Modülü

Bu kısım ile tamamen web üzerinden Linux işletim sistemine erişip güvenlik duvarı kurallarının oluşturulması sağlanmıştır. Bu kısımda güvenlik duvarında kullanılabilecek tüm

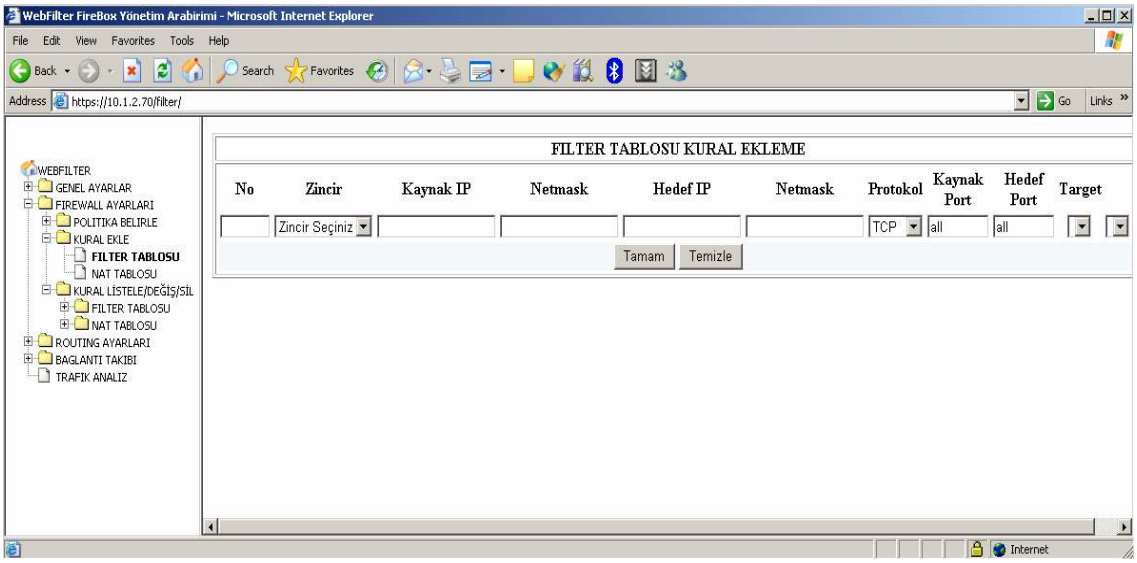
yapılandırma işlemleri (NAT,MASQ,ACCEPT,DROP) için tanımlamalar yapılmıştır. Bu kuralların sol tarafındaki butonlar sırayla: kuralı sil, kuralı değiştir, kuralı bir yukarı taşı ve kuralı bir aşağı taşı butonlarıdır. Bu sayede var olan kuralların düzenlenmesi son derece basitleştirilmiştir.

Bu sistemi oluşturmak için Apache web sunucu üzerinden Netfilter güvenlik duvarı yapısına müdahale edilebilmesi sağlanmıştır. Oluşturulan formlarla güvenlik duvarı için girilen parametreler Web sunucu üzerinden Linux çekirdeğindeki Netfilter alt sistemine iletilmiş ve gerekli kuralların işlenmesi sağlanmıştır. Tüm bu kuralların düzenli şekilde oluşturulması, düzenlenmesi, kaydedilmesi, gerektiğinde geri yüklenmesi ve yer değiştirilmesi gibi işlemler yine Nefilter sistemine müdahale edilerek ve web sunucu üzerinden çekirdek üzerindeki bash kabuğu ile komutlar çalıştırılarak sağlanmıştır.

Bu kısım üç bölümden oluşmaktadır. Bunlar Politika Belirleme, Kural Ekle ve Kural Listele/Değiş/Sil bölümleridir. Bu bölümler kısaca şu amaçlar için kullanılabilir.

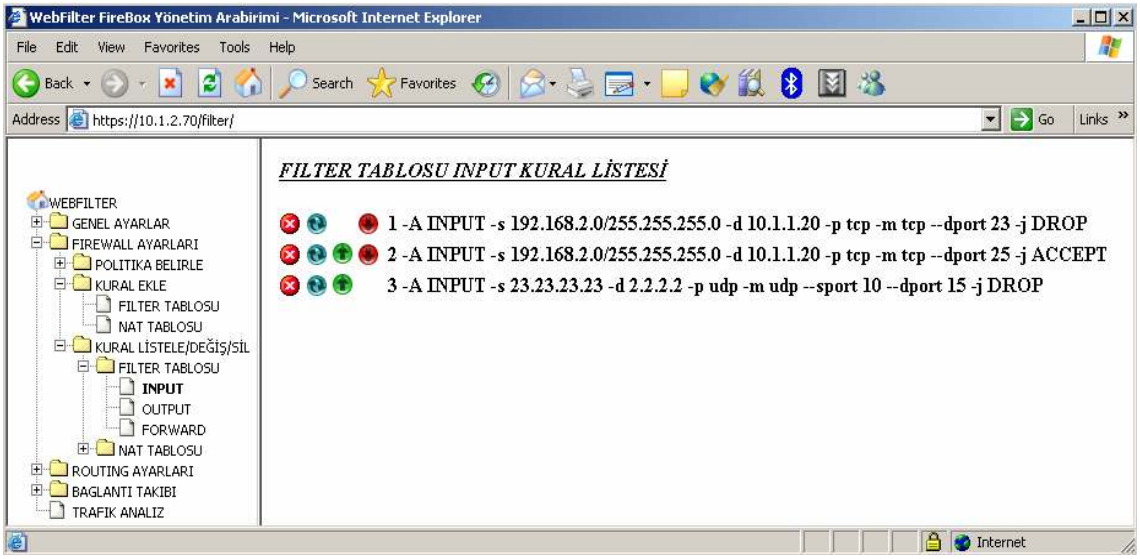
Politika Belirle bölümü genel olarak bir güvenlik politikası belirlemek amacıyla kullanılmaktadır. Bu kısma girildiğinde Filter tablosu ve Nat tablosu gibi iki seçenek karşımıza çıkmaktadır. Burada yapılacak olan işlem bu iki tablo ve içerisinde bulunan yönlendirme aşamaları için politika belirlemektir. Politika Accept veya Drop olarak iki şekilde belirlenebilir. Gelen paketler eğer erişim listesindeki hiçbir kural ile uyuşmuyorsa sonuç olarak o zincirin politikasına bakılır ve politika Accept ise paket kabul edilir, eğer politika Drop ise paket tamamen yok edilir.

Kural Ekle bölümü oluşturulan erişim listelerinin güvenlik duvarına girilmesi için tasarlanmış bir modüldür. Bu modülde iki farklı amaç için erişim listesi oluşturulabilir. Gerektiğinde ağ üzerinde NAT işlemi için, gerektiğinde ise filtreleme işlemi için erişim listeleri oluşturulabilir. Bu aşamalardan seçilen kısım için kullanıcı karşısına bir bölüm gelmektedir ve bu bölümde kullanıcı, güvenlik duvarı sisteminin yapısına göre Filter tablosu için INPUT, OUTPUT ve FORWARD, NAT tablosu için ise PREROUTING ve POSTROUTING zincirlerine kurallar ekleyebilmektedir. Kullanıcı karşısına gelen forumda bu erişim listelerinin oluşturulması için gereken kural numarası, zincir, Kaynak IP adresi ve Netmask bilgisi, Hedef IP adresi ve Netmask bilgisi, TCP protokolü ve port bilgileri ve son olarak da yapılması gereken işlem bilgisi girilebilmektedir. Şekil 3.3'te kural ekleme ekranı görülmektedir.



Şekil 3.3 Güvenlik Duvarı Kural Ekleme Modülü Filter Tablosu Sayfası.

Kural Listele/Değiş/Sil bölümü güvenlik duvarına eklenen erişim listelerinin görülebildiği, gerektiğinde her kuralın sol tarafındaki butonlara basarak istenilen kısmın değiştirilebileceği veya sil butonuna basılarak istenilen kuralın silinebilindiği kısımdır. Bununla birlikte yine aynı yerdeki yukarı ve aşağı butonlarıyla kurallar yukarıdan aşağıya doğru tek hamlede hareket ettirilebilmektedir. Bu işlemin önemi büyüktür çünkü bütün güvenlik duvarı sistemlerinde paketler ilk kuraldan başlayarak aşağıya doğru tüm kurallar ile karşılaştırılır. Bu yüzden herhangi bir kuralın bir kural yukarıda veya bir kural aşağıda olması gelen paketlere yapılan işlemin farklı olmasına neden olabilir.



Şekil 3.4 Güvenlik Duvarı Kural Listele Modülü Filter Tablosu Sayfası.

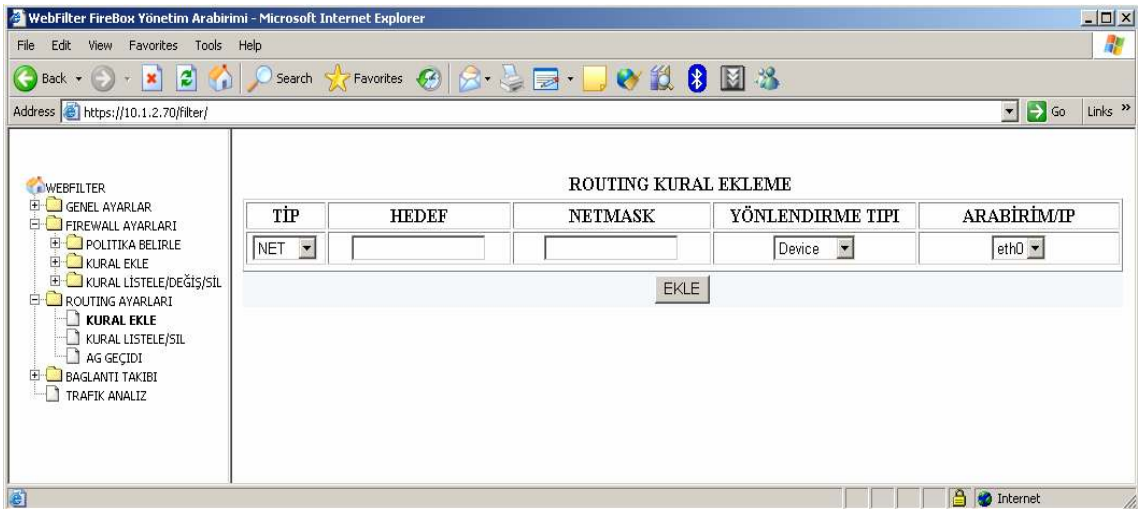
Şekil 3.4'te INPUT zinciri için kural listesi görüntülenmektedir. Bu alanda kurallar numaraları ile birlikte aşağıya doğru sıralı olarak gösterilmektedir. Kural numaralarının solunda görülen butonlar ise sırasıyla sil, değiş, bir yukarı kaydır, bir aşağı kaydır butonlarıdır.

3.1.3. Yönlendirme Ayarları Modülü

Bu modül tamamen yönlendiricilerin yaptığı işlemleri yapabilecek kabiliyette tanımlanmıştır. Bu sayede güvenlik duvarı ağ üzerinde yönlendirme işlemleri yapabilecek ve yönlendirici yerine kullanılabilecek hale getirilmiştir. Tüm güvenlik duvarlarında yönlendirme yapısı bulunmak zorundadır, çünkü paket filtreleme işlemleri, istenilen paketlerin yönlendirilmesi ve istenmeyenlerin engellenmesi mantığı ile çalışmaktadır. Bu kısımda yapılan işlemlerin gerçekleşmesi için web üzerinden Linux çekirdeğine route komutu ile yönlendirme listelerinin iletilmesi sağlanmıştır. Linux çekirdeği bu komut ile aldığı parametreleri işleyerek gerekli yönlendirme işlemlerini yapmaktadır. Yine tüm host ve ağ bazındaki yönlendirme listelerinin çekirdeğe gönderilebilmesi için web üzerinde formlar oluşturulmuştur.

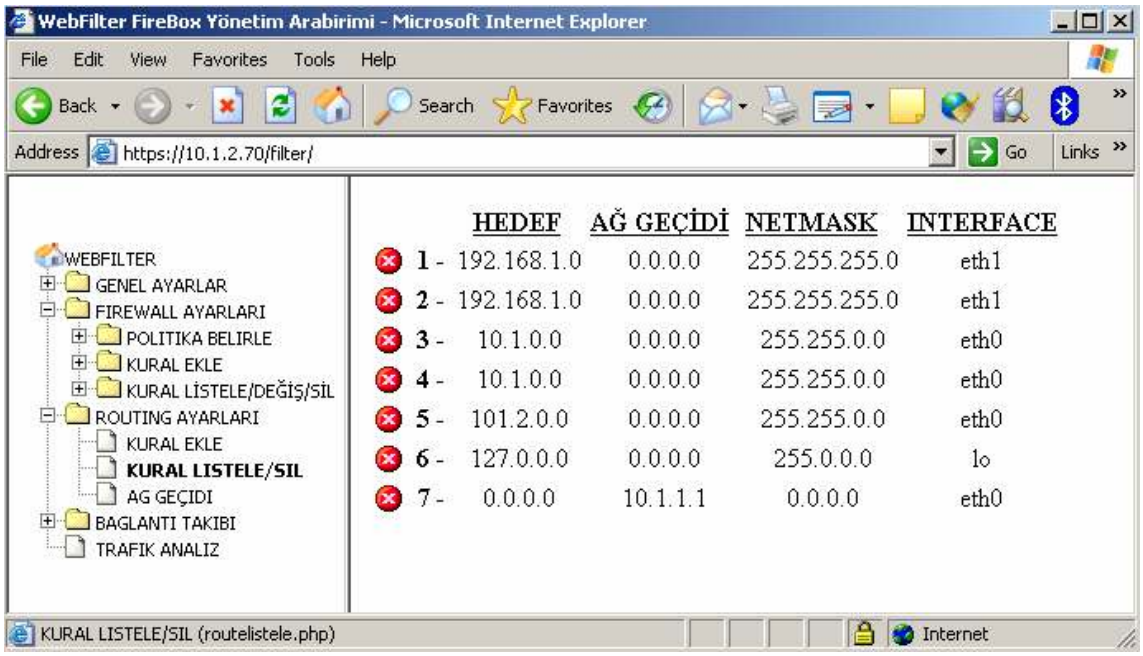
Yönlendirme ayarları bölümü üç farklı kısımdan oluşmaktadır. Bu bölümler Kural ekle, Kural Listele/Sil ve Ağ geçidi bölümleridir.

Kural ekle bölümünde kullanıcının host ve ağ bazında yönlendirme yapabildiği kısımdır. Bu bölüme girdikten sonra yönlendirme tipini seçip ip veya ağ adreslerini girdikten sonra isterse belli bir ağ arabirimine, isterse de herhangi bir ip adresine yönlendirme yapılabilir. Erişim listelerinde olduğu gibi bu bölümde de kural numaraları vardır ve gelen paketlerin yönlendirme işlemi bu kural numaralarına göre küçükten büyüğe doğru sırayla işletilir. Şekil 3.5'te yönlendirme kuralı ekleme ekranı görülmektedir.



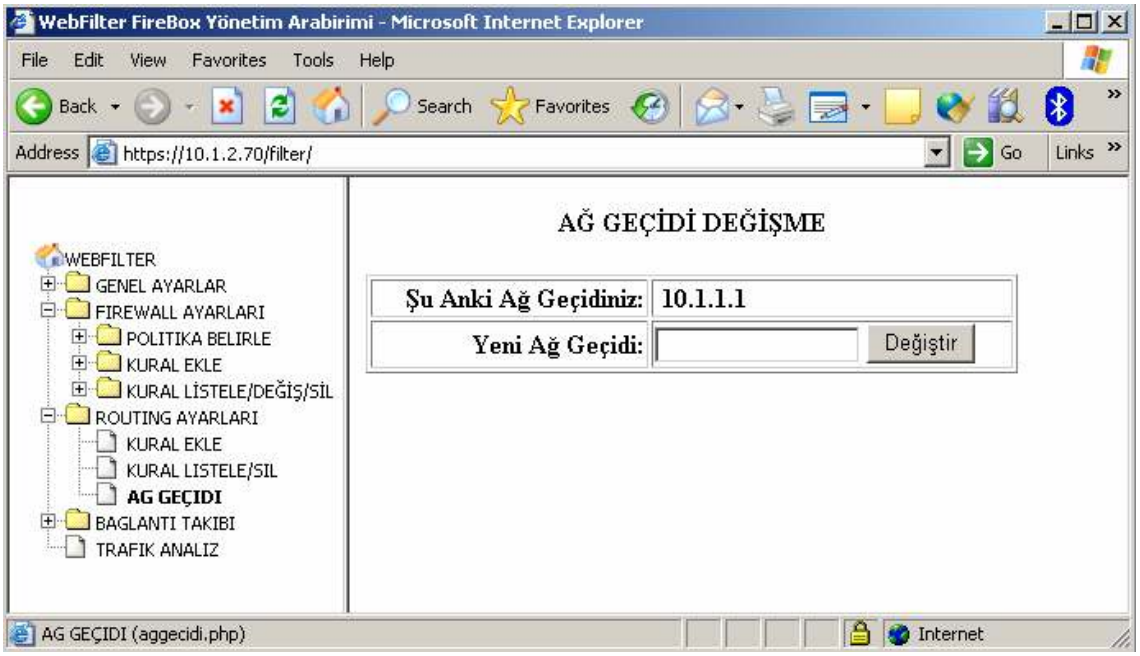
Şekil 3.5 Yönlendirme Ayarları Modülü Kural Ekleme Sayfası Görünümü.

Yönlendirme bölümündeki diğer bir kısım Kural Listele/Sil bölümüdür. Bu bölümde daha önceden girilmiş yönlendirme kuralları görülebilir. Her bir kuralın sol tarafındaki butona tıklanarak istenildiğinde silinebilir. Şekil 3.6'da bu ekran görülebilir.



Şekil 3.6 Yönlendirme Ayarları Modülü Kural Listele Sayfası.

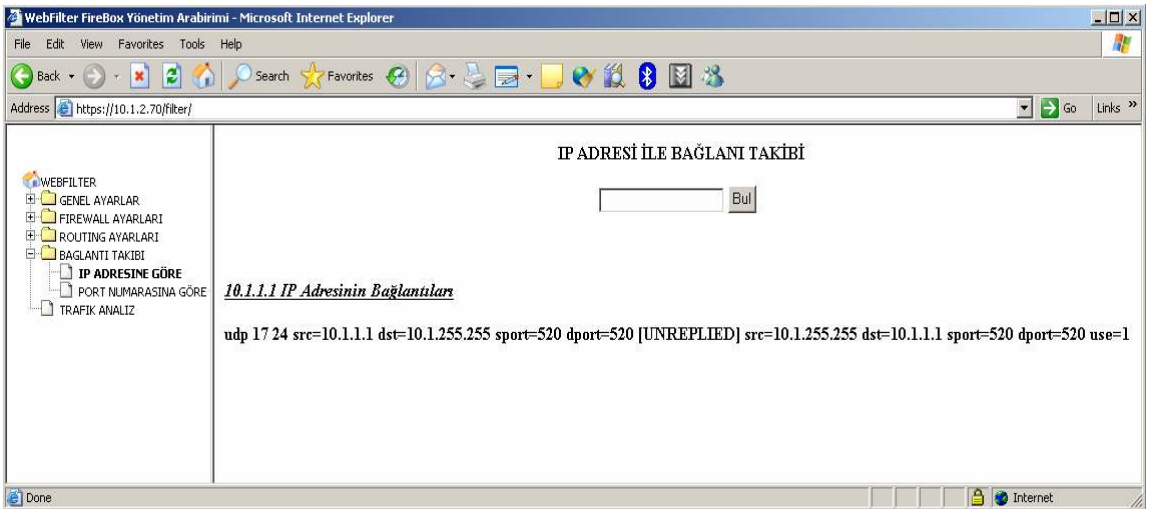
Yönlendirme bölümündeki son kısım ise Ağ Geçidi bölümüdür. Ağ geçidi bir ağ için varsayılan yönlendirme kuralı olarak belirtilebilir. Bu bölümde yönlendirme listelerinden herhangi birine uymayan bir paketin ne şekilde işlem göreceğini belirten Ağ geçidi tanımlanır. Ağ geçidi bir ağ için varsayılan yönlendirme kuralı olarak belirtilebilir. Tanımlanan ağ geçidi yine Kural Listele/Sil ekranında da görülebilir ve silinebilir. Ağ Geçidi bölümü Şekil 3.7'de görülebilmektedir.



Şekil 3.7 Yönlendirme Ayarları Modülü Ağ Geçidi Sayfası.

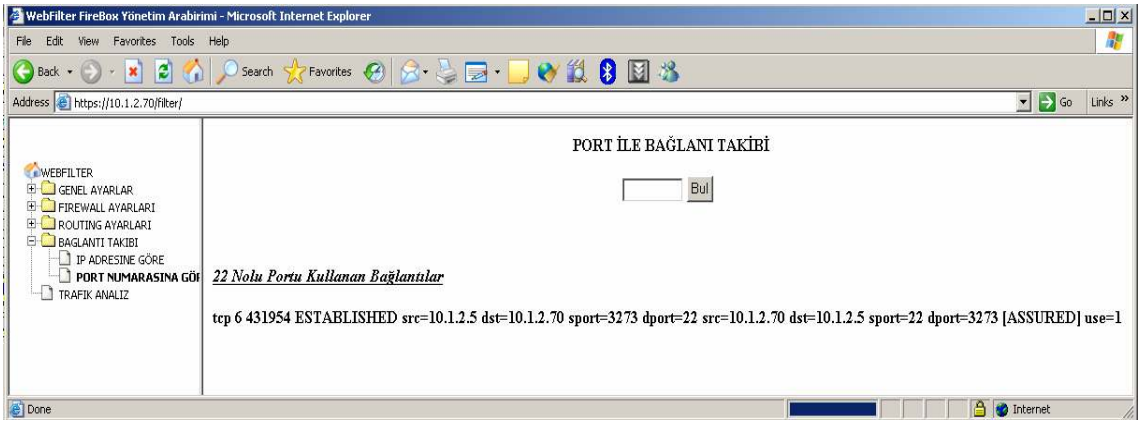
3.1.4. Bağlantı Takibi Modülü

Bu kısımda güvenlik duvarının kullanıldığı durumlarda gerekli bağlantı takibi işlemlerinin yapılabilmesi için tasarlanmıştır. Bunun için gerekli düzenli ifade yapıları kullanılıp bağlantı aşamasında port bazlı ve IP bazlı kontrollerin yapılması sağlanmıştır. Linux işletim sistemi kendi yapısında yönlendirme veya adres dönüşümü yaptığı durumlarda yapılan bu işlemleri belirli bir süre TCP/IP protokol kümesi gereği ip_conntrack isimli bir dosyada tutmaktadır. Bunun yapılmasının amacı yönlendirme ve adres dönüşümlerinde bağlantıların sürekliliğini sağlamaktır. Web arabirimin bu kısmında bu dosya içerisindeki tüm bilgiler alınıp bash kabuğu üzerindeki komutlar yardımıyla irdelenerek kullanıcıya aktarılması sağlanmıştır. IP bazlı izleme ekranının bir örneği Şekil 3.8' de görüldüğü gibidir.



Şekil 3.8 Bağlantı Takibi Modülü IP Adresine Göre Takip Sayfası.

Şekil 3.8'de görülen tipik bir udp bağlantısının bilgileridir. Bu bağlantıda 10.1.1.1 nolu kaynak IP adresinin 520 numaralı portundan, 10.1.255.255 nolu yayın (broadcast) adresinin 520 nolu portuna bir udp bağlantısı yapıldığı görülmektedir. Aynı şekilde paketin cevaplanıp cevaplanmadığı, kullanımda olup olmadığı veya sonlanıp sonlanmadığı gibi bilgiler de görüntülenebilmektedir. Şekil 3.9'da ise port bazlı bir arama ekranı görüntüsü bulunmaktadır.

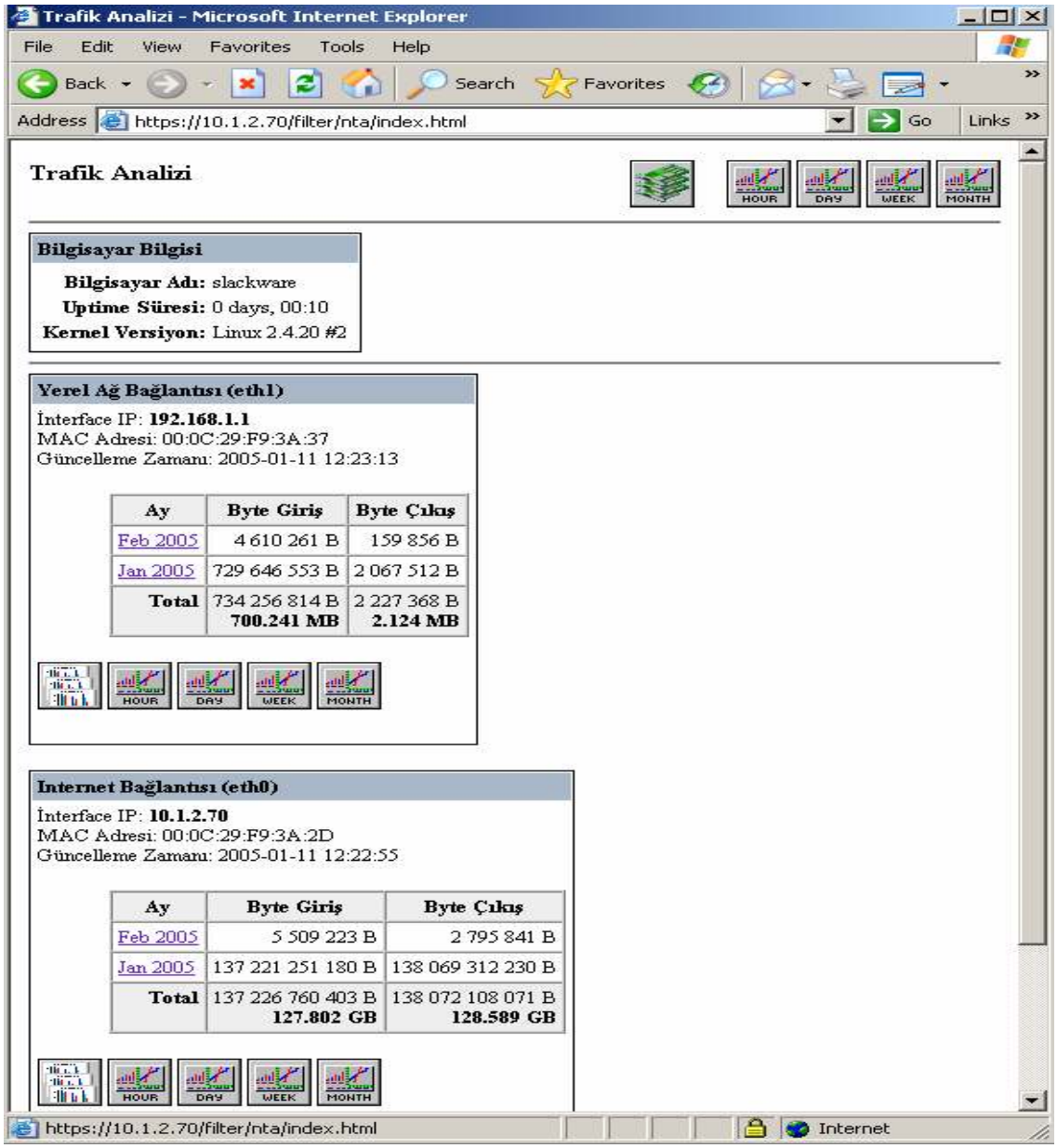


Şekil 3.9 Bağlantı Takibi Modülü Port Numarasına Göre Takip Sayfası.

Şekil 3.9'da tıpkı IP bazlı arama da olduğu gibi belli bir port numarasına yapılan tüm TCP ve UDP bağlantıları görüntülenebilmektedir. Bu sayede istenildiği anda güvenlik duvarı üzerinden geçen trafik kontrol edilip istenilen yasaklama işlemleri yapılabilir veya yasaklanıp yasaklanmadığı görülebilir.

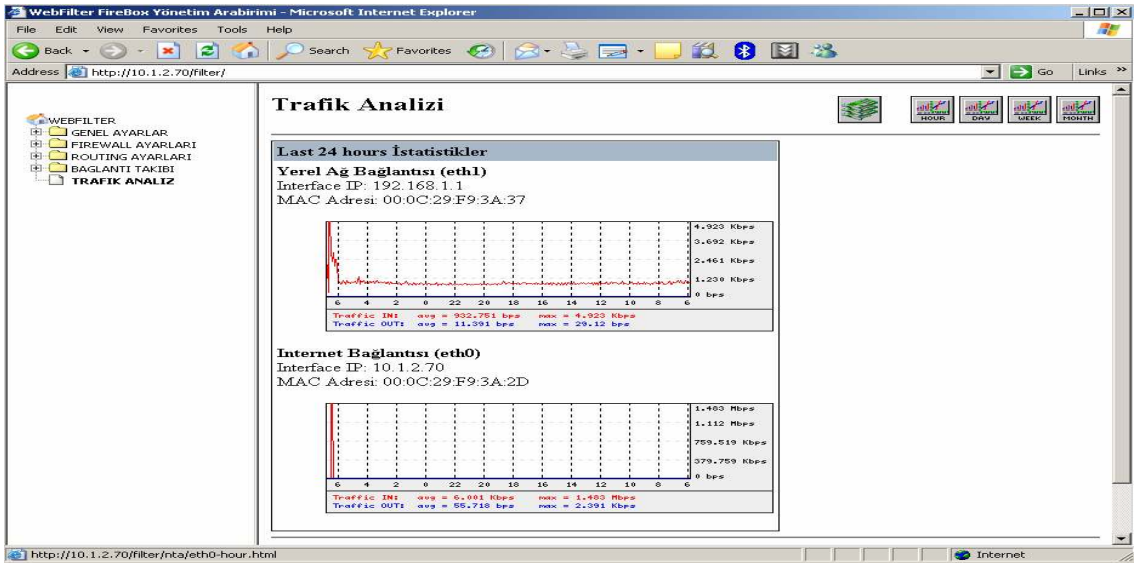
3.1.5. Trafik Analiz Modülü

Bu modülde güvenlik duvarı üzerinden geçen trafiği günlük, aylık, haftalık ve yıllık olarak takip etmek mümkündür. Bu sayede ağ üzerinde kullanılan ve her bir ethernet arayüzü üzerinden geçen trafiği grafiksel olarak takip edilebilir. Gerektiğinde yine bu zaman aralıkları için kullanılan toplam yapılan transfer miktarları her bir ethernet ara yüzü için ayrı ayrı görüntülenebilmektedir. Şekil 3.10' da Trafik Analiz Modülü ana ekranı görülmektedir.



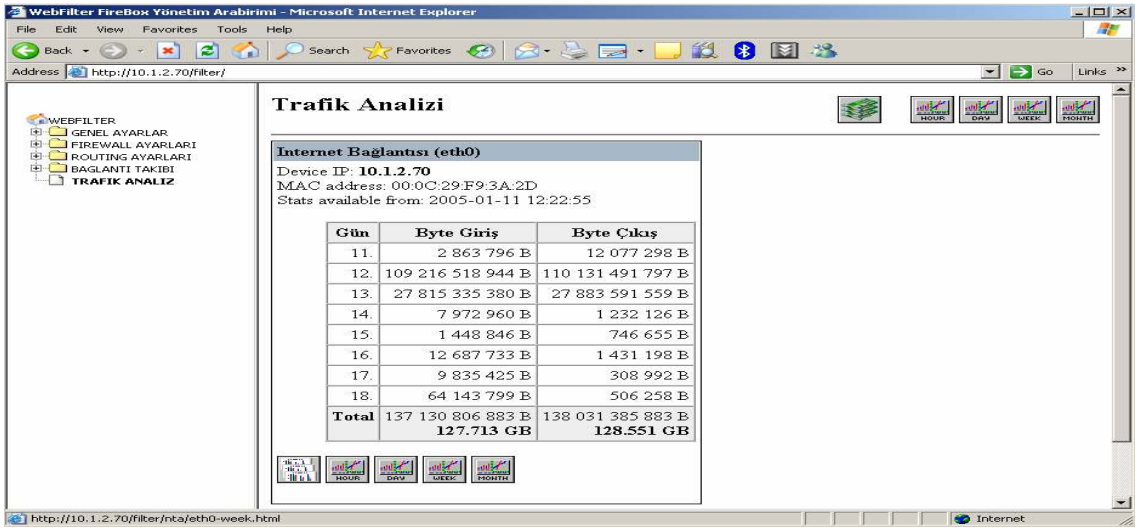
Şekil 3.10 Trafik Analiz Modülü Ana Ekranı.

Şekil 3.10'da da görüldüğü gibi bağlantı istatistikleri ay bazında tutulmakta ve her bir ağ arabirimi üzerinden gelen ve giden paket miktarları görüntülenmektedir. Ağ arabirimleri için IP ve MAC adresi bilgileri de görüntülenmektedir. İstenildiği zaman her bir arabirim için saatlik, günlük, haftalık ve aylık butonlarına tıklanarak yapılan paket trafiği miktarı görüntülenebilir. Bu paket trafikleri istenilirse grafiksel olarak istenilirse sayısal olarak izlenebilir. Şekil 3.11'de günlük bir paket trafiği grafiksel olarak görülebilir.



Şekil 3.11 Trafik Analiz Modülü Grafiksel Görünüm Sayfası.

Şekil 3.12'de de rakamsal olarak her bir gün için oluşan paket trafiği görülebilir.

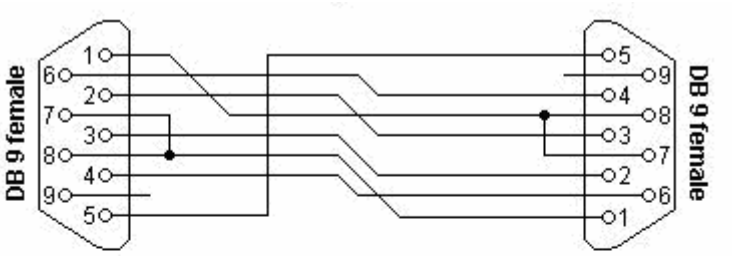


Gün	Byte Giriş	Byte Çıkış
11.	2 863 796 B	12 077 298 B
12.	109 216 518 944 B	110 131 491 797 B
13.	27 815 335 380 B	27 883 591 559 B
14.	7 972 960 B	1 232 126 B
15.	1 448 846 B	746 655 B
16.	12 687 733 B	1 431 198 B
17.	9 835 425 B	308 992 B
18.	64 143 799 B	506 258 B
Total	137 130 806 883 B **127.713 GB**	138 031 385 883 B **128.551 GB**

Şekil 3.12 Trafik Analiz Modülü Günlük Transfer Sayfası.

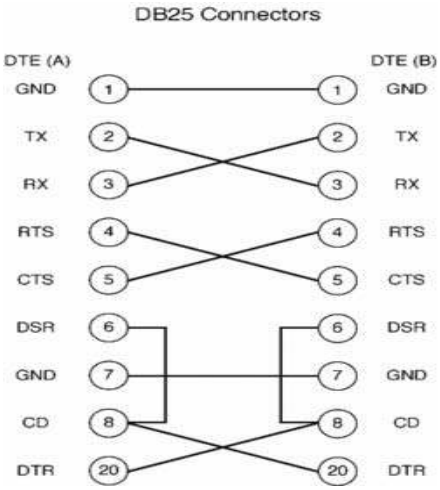
3.2. Konsol Port (Seri) Bağlantı Modülü

Bu kısım web yönetim arabiriminden tamamen bağımsızdır. Web yönetim kısmında sorun olduğunda veya TCP bağlantısının yapılamadığı durumlarda işletim sistemine ve güvenlik duvarına Seri port ve null modem kablosu kullanılarak bağlantı yapılabilmektedir. Bu sayede her durumda kullanıcının sisteme müdahale edebilmesi sağlanmıştır. Bu amaçla Linux çekirdeği üzerinde inittab yapısı kullanılmış ve gerekli seri bağlantının yapılabilmesi için Linux agetty yapısı kullanılarak ttyS0, ttyS2 gibi portlar belirtilip hızları 9600bps olarak ayarlanmıştır. Ağ cihazlarında genellikle bu bağlantı yapısı standart olarak kullanılmaktadır. Bu bağlantı için Hyper Terminal veya Putty isimli küçük programcıklar kullanılabilir. Yine bu bağlantı için kullanılması gereken 9 pinlik ve 25 pinlik Null-Modem kablosunun içyapıları ve genel görüntüsü Şekil 3.13, 3.14 ve 3.15'de görülebilir.

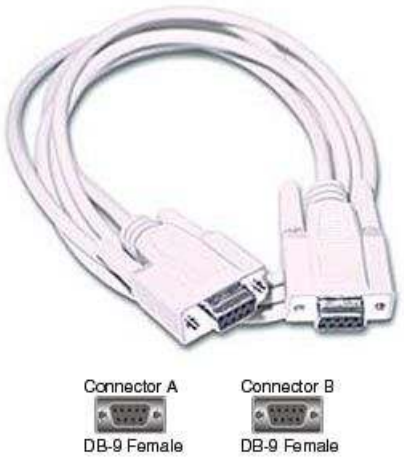


Connector 1	Connector 2	Function
1	7 + 8	$RTS_2 \rightarrow CTS_2 + CD_1$
2	3	Rx ← Tx
3	2	Tx → Rx
4	6	DTR → DSR
5	5	Signal ground
6	4	DSR ← DTR
7 + 8	1	$RTS_1 \rightarrow CTS_1 + CD_2$

Şekil 3.13 DB 9 Null-Modem Kablo Yapısı.



Şekil 3.14 DB-25 Null-Modem Kablo Yapısı.



Şekil 3.15 DB-9 Null-Modem Kablo Görünümü.

4. OLUŞTURULAN GÜVENLİK DUVARI İÇİN ÇEKİRDEK UYGULAMASI

4.1. Linux Çekirdeği Yapısı ve Netfilter Güvenlik Duvarı

Firewall çözümlerinin sistem geneline eklenmesi eskiye dayanmaktadır. Alan Cox, BSD işletim sistemlerinde yer alan ipfw uygulamasını 1.1 çekirdeğine ekleyerek ilk firewall çözümünü uygulamaya koymuştur. İzleyen süreçte ise ipfwadmin geliştirilerek ipfw uygulaması ortaya çıkmıştır. İlerleyen zamanda ise ipchains uygulaması geliştirilmiş ve sistemdeki yerini almıştır. Ipchains daha sonraları iptables adlı ayar dosyası ve bir dizi komut ile geliştirilmiştir [5,13]. Uzun yıllar iptables ve ipchains GNU/Linux dağıtımları için standart firewall çözümü olarak kullanılmıştır.

Genel ağ trafiğin yönetmek için iptables yeterli olmaktadır. iptables ile kapatılacak olan ve açık bırakılacak olan portlar sistem yöneticisi tarafından tanımlanmaktadır. Bu tanımlama uyarınca belirli portlar açık bırakılmakta ve kapatılmaktadır. Iptables ile dışarıdan gelen ve dışarıya gönderilen paketler incelenmekte ve sistem yöneticisi tarafından tanımlanmış kurallar çerçevesinde değerlendirerek gerekeni yapmaktadır. Kuralar tanımlanırken kullanılan ölçüler, kaynak ve hedef bilgisayarlar, port, paketlerin başlık dosyalarının özellikleri veya bunların farklı birleşimleri olabilmektedir. iptables ile paketler teker teker ele alınmaktadır. Bu düzenleme genel ağ trafiğini düzenlemek için yeterli olmaktadır.

Birçok durumda genel bir ağ trafiği düzenlemesi yeterli olmaktadır. Bu tür bir düzenleme basit ve kolayca yapılabilirken işlevsel özellikler eklemek ise olanaksız hale gelmektedir. Kabaca anlatacak olursak, evinizin pencerelerini, kapılarını kilitleyip sadece bir kapıyı açık bırakmak ve bu kapıya da güvenilir nöbetçiler koyarsanız bu genel bir düzenlemedir. Ancak güvendiğiniz birisi varsa, ona ikinci bir anahtar vererek başka bir kapıyı kullanmasına izin vermek ise genel bir uygulama değildir. Burada özel bir uygulamaya gidilmektedir. Özel yaklaşımlar genel çözümlerden daha fazlasına gereksinim duyar.

Çekirdeğe eklenen yeni kuşak kod ile firewall çözümlerinde genelden özele doğru geçilebiliyor. Netfilter, geliştirilen kod ile çekirdeğe gereksinim duyulan modülleri yükleyerek oturum tabanlı ağ trafiği düzenlemelerinin yapılmasına olanak vermektedir. Önemli bir nokta da ağ ve sistem yönetiminden sorumlu olan personelin çekirdek derlemek ve ayarlarını düzenlemek konusunda yeterli bilgi ve deneyime sahip olması gerekliliğidir. Çekirdek ile modül bazında çalışmak, çekirdeğin bir bütün olarak yeniden düzenlenmesini gerektirmez.

Netfilter "yeni" olarak nitelendirebilir. 2.4 Çekirdek ile Ocak 2001'de kullanılmaya başlanmıştır. Dolayısıyla da Netfilter tabanlı firewall düzenleme yazılımlarının da yeni olduğu söylenebilir. Netfilter ipchains ve iptables ile geriye doğru uyumlu olduğu için, bu düzenleyici yazılımlarda temel de iptables ve ipchains uyumlu olmaktadır. Netfilter güvenlik duvarı alt sistemini kullanmak için iptables ve ipchains isimli bu yazılımlar oldukça kolaylıklar sağlamakta ve kuralların yönetilmesini çok basitleştirmektedir[9,10,13].

4.2. Iptables

Iptables Netfilter için yazılmış birçok modulden birisidir. Netfilter için kullanıcıya bir arabirim sağlar. Iptables ile paket filtreleme işlemleri yapılabilmektedir. Bu işlem, çekirdekteki paket filtreleme tablosuna kural ekleyerek veya çıkartarak gerçekleştirilir. Bu tabloya eklenen kurallar sistem tekrar başlatıldığında kaybolur. Bu nedenle kuralların bir betik halinde hazırlanıp sistem başlangıç betiklerine dahil edilmesi gerekmektedir[10].

4.2.1. Paket Filtreleme

Filter tablosunda gerçekleştirilen işlemdir. Netfilter şemasından da görebileceğimiz gibi INPUT, FORWARD ve OUTPUT noktalarında gerçekleştirilir. Genellikle bu kısımlar zincir olarak adlandırılmaktadır. Sisteme gelen paket, filtreleme işlemine INPUT, FORWARD veya OUTPUT zincirlerinde tabii tutulabilir. Zincir bir dizi kural serisinden oluşur. Paket zincirdeki kurallar ile sıra ile eşleştirilir. Eğer paket bilgisi kuralda tanımlanan kriterlere uyuyorsa, pakete kuralda tanımlanan yaptırım uygulanır, yaptırım DROP ise paketin yaşamı sona erer, ACCEPT ise paket zincirden çıkar ve yolculuğuna devam eder. Eğer paket, zincirdeki hiçbir kural ile eşleşmiyorsa, bu paket için zincirde tanımlı olan politika uygulanır(ACCEPT, DROP, ...) Paket filtreleme için hali hazırda var olan ve silinemez zincirler olan INPUT, OUTPUT ve FORWARD'ın dışında kendi tanımlayacağımız zincirler de kullanılabilmektedir. Bu işlem için aşağıda birkaç örnek bulmak mümkündür.

Örnek 1:

Iptables –t filter –A INPUT –s 192.168.1.0/255.255.255.0 –p tcp –dport 80 –j DROP

Bu örnekte kaynak 192.168.1.0 ağından yerel makineye gelen 80 nolu web istekleri engellenmiştir.

Örnek 2:

Iptables –t filter –A FORWARD –s 192.168.1.1 –d 10.1.1.0/255.255.255.0 –p udp –dport 53 –j ACCEPT

Bu örnekte ise kaynak 192.168.1.1 makinesinden gelen ve hedef 10.1.1.0 ağına giden DNS isteklerine yerel makine üzerinden geçiş izni verilmiştir.

4.2.2. NAT (Network Address Translation)

Adından da anlaşılacağı üzere NAT işlemi ile paketlerdeki adresler üzerinde oynama yapılabilmektedir. Böylece paketler farklı bir yerden geliyormuş gibi gösterilebilir veya farklı bir ip'ye yönlendirilebilir. NAT işlemine tabii tutulan paketler, dönüşte NAT işleminin gerçekleştiği sistem tarafından ters NAT uygulanır. Bu işlem ile yapılan adres dönüşümü tersine çevrilerek paketin doğru yere gönderilmesi sağlanır. NAT işlemi SNAT (kaynak NAT) ve DNAT (Hedef Nat) olarak ikiye ayrılır. SNAT işleminde paketin kaynak IP adresi değiştirilir. DNAT işleminde ise paketin gideceği hedef IP adresi değiştirilir. NAT işlemi ile genel olarak aşağıdaki işlemler yapılabilir.

4.2.2.1. İnternet Paylaşımı

Çoğu zaman isp veya kablonet'in sağladığı tek ip'yi kullanarak birden çok bilgisayar internete taşınmak istenebilir. Bu işleme 'masquerading' adı verilir. Lokalden gelen paketlere SNAT yani kaynak adresi değişimi uygulanır. Lokalden gelen bütün paketlerin kaynak adresi internete bakan makinenin ip'si olarak değiştirilir çünkü özel IP'ler ile internete request gönderilemez. İnternete SNAT işlemi uygulanarak gönderilen paketler dönüşte ters SNAT işlemi uygulanır, böylece paket doğru hedefe yönlendirilir. Aşağıdaki örneklerde belirtilen kurallar ile ağ üzerindeki bir makineden diğer istemcilere internet paylaşımı yapmak mümkündür.

Örnek 1:

Iptables -t nat -A POSTROUTING -s 10.1.0.0/16 -j MASQUERADE

Bu örnekte 10.1.0.0 ağındaki tüm istemciler ağ geçidi üzerinde bulunan gerçek ip yi alarak internete çıkabileceklerdir. Buradaki *MASQUERADE* ifadesi ağ geçidinde internet üzerinde bulunan ağ arabiriminin IP sini otomatik olarak alınıp SNAT uygulanmasını sağlar.

Özellikle dialup bağlantılar veya gerçek IP adresi sürekli değişen DSL bağlantılar için uygundur.

Örnek 2:

Iptables –t nat –A POSTROUTING –s 10.1.0.0/16 –j SNAT –to 193.255.124.1

Bu tanımlama ise 10.1.0.0 ağından gelen tüm isteklerin kaynak IP adresini 193.255.124.1 yaparak internete iletilmesini sağlar.

4.2.2.2. Sunucu Kümeleme

Sunucu sistemlerinde dışarıdan bir ip gözükmesine rağmen arkada birden çok sunucudan oluşan bir kümeleme sistemi olabilir. Bu gibi sistemlerde istekler NAT işlemi yardımıyla arkadaki sunuculara sistem dinamiği çerçevesinde istenilen şekilde dağıtılabilir ve yük dengeleme yapılabilir. Şu şekilde bir örnek verilebilir.

Örnek:

iptables -t nat -A PREROUTING -s 0.0.0.1/0.0.0.1 -p tcp --dport 80 -j DNAT --to 10.1.1.1

Ağımızda 10.1.1.1 ve 10.1.1.2 IP lerine sahip 2 web sunucu olduğunu düşünürsek, bu tanımlama IP adresinin son biti 1 olan istemcileri 10.1.1.1 IP nolu web sunucuya, 0 olanları ise 10.1.1.2 IP nolu web sunucuya iletecektir. Bu işlem basit bir kümeleme işlemidir.

4.2.2.3. Transparan Vekil Sunucu

Bazı durumlarda belirli paketleri bir programa yönlendirilmek istenebilir. Mesela web paketleri herhangi bir sunucudaki vekil sunucu programına yönlendirilmek istenebilir, böylece yerel ağ için bu işlem transparan bir şekilde gerçekleşebilir, istekler web portuna gidiyor gibi gözükse de, aslında vekil sunucu üzerinden geçer. Bu işlem için şöyle bir örnek verilebilir.

Örnek:

iptables -t nat -A PREROUTING -s 10.1.0.0/16 -p tcp --dport 80 -j DNAT --to 10.1.1.5:8080

Bu işlem ile 10.1.0.0 ağından gelen tüm web istekleri, istemcilerin haberi olmadan 10.1.1.5 nolu transparan vekil sunucu üzerine iletilir.

.

4.3. Netfilter Modülleri ve Reject Modülünde Yapılan Değişiklik

Linux çekirdeğindeki Netfilter güvenlik duvarı sisteminde farklı işlemler gerçekleştiren pek çok modül bulunmaktadır. Bizim bu çalışma içerisinde yaptığımız bir uygulama Netfilter güvenlik duvarındaki bazı modüller üzerinde değişiklikler yapılabileceğini ve gerektiğinde güvenlik duvarına yeni modüller ve özellikler katılabileceğini göstermektir. Bu yüzden Netfilter güvenlik duvarı sisteminin modüllerinden biri alınarak üzerinde çeşitli değişiklikler yapılması sağlanmıştır. Bunun için modül üzerine yeni fonksiyonlar eklenerek yapılan değişiklikler gözlemlenmiştir. Yapılan bu işlemle oluşturulan güvenlik duvarına gerektiğinde farklı özellikler eklenebileceği gösterilmiştir. Bu sayede güvenlik duvarı çok esnek bir yapıya kavuşmaktadır. Benzer şekilde eklenecek yeni fonksiyonlar ile güvenlik duvarına yeni özellikler eklenebilecektir.

Bu uygulamada Netfilter güvenlik duvarı sisteminin çekirdek modüllerinden biri olan Reject modülü üzerine fonksiyonlar eklenmiştir. Reject modülünün görevi TCP/IP paketlerinin reddedilmesi ve geriye bir cevap dönderilmesini sağlamaktır. Eklenen fonksiyonlar ile Reject modülü kullanıldığı anda sistem üzerinden bir dosya okunması sağlanmış ve bu dosyanın içeriğine göre Reject modülünün ne şekilde davranış göstereceği düzenlenmiştir. Bu şekilde Linux çekirdeği üzerinde herhangi bir değişiklik yapılabilmesi için öncelikle çekirdek kaynak kodunun sistem üzerinde bulunuyor olması gerekir. Çekirdek içerisindeki modüllerde yapılan değişikliklerden sonra ise aşağıdaki komutların çalıştırılması gerekmektedir. Bu sayede değişiklik yapılan modül derlenip istenildiği anda çekirdeğe eklenebilecektir.

make modules: Bu komut çekirdek modüllerinin derlenmesi ve obje kodlarının oluşturulmasını sağlar.

make modules install: Bu komut ise derlenen modüllerin uygun yerlere kopyalanmasını ve sistem başlangıcında yüklenebilecek hale getirilebilmesini sağlar.

insmod: Bu komut derlenen çekirdek modüllerinden herhangi birinin istenildiği anda çekirdeğe eklenip kullanılmasını sağlar

rmmod: Çekirdeğe eklenmiş modüllerden herhangi birinin sistemden çıkarılmasını sağlar.

Linux çekirdeği içindeki Reject modülüne eklenen fonksiyonlar şu şekildedir.

Dosya açma fonksiyonu:

```
static int dosyaac_init(void)
{
        char * file_to_read = kmalloc(20, GFP_KERNEL);
        file_to_read = "/webfilter/saat";
        dosya_oku(file_to_read);
```

```
        return;
}
```

Bu fonksiyon, Reject modülü içerisine eklenip, sistem üzerinden hangi dosyanın okunacağını belirtmektedir. File_to_read değişkenine atanan değer sistem üzerinden okunacak dosyadır. Bu değer dosya_oku fonksiyonuna gönderilerek dosyanın okunması sağlanmaktadır. Bu kısımda yapılacak değişiklik ile sistemde hangi dosyanın çağırılıp içeriğinin kontrol edileceği belirlenebilir. Ancak bu işlemden sonra, daha önce bahsedilen komutlar kullanılarak çekirdek modülü tekrar derlenmeli ve sisteme tekrar eklenmelidir.

Açılan dosyanın içeriğinin okunması için yazılan fonksiyon:

```
void dosya_oku(const char * fwrite) {
        int length_read, length_write;
        char buffer[4];
        struct file * f = NULL;
        mm_segment_t orig_fs;

        f = filp_open(fread, O_RDONLY, 00);

        if (!f || !f->f_op || !f->f_op->read)
          {
          printk("WARNING: File (read) nesnesinin içeriği boş!!!\n");
          }

        f->f_pos = 0;

        orig_fs = get_fs();
        set_fs(KERNEL_DS);

        length_read = f->f_op->read(f, buffer, sizeof(buffer), &f->f_pos);

        fput(f);

        return;
}
```

Bu fonksiyon ise dosya_ac fonksiyonundan hangi dosyanın okunacağı bilgisini alarak, dosyayı açıp içeriğini okuma görevi yapmaktadır. Açılan dosyanın içeriğindeki bilgiler buffer adı diziye atılmaktadır. Daha sonra bu değerler kullanılarak Reject modülünün içerisindeki reject fonksiyonunda bu kurala uyan paketlerin dosya içeriğine göre ne işlem göreceği ayarlanabilmektedir. Buna göre değiştirilmiş Reject fonksiyonu şu şekildedir.

```
static unsigned int reject(struct sk_buff **pskb,
                           unsigned int hooknum,
                           const struct net_device *in,
                           const struct net_device *out,
                           const void *targinfo,
                           void *userinfo)
{
int saat,bassaat,bitsaat;
saat=strftime ("%H", localtime(time()));

dosyaac_init();
bassaat=(buffer[0]*10)+buffer[1];
bitsaat=(buffer[2]*10)+buffer[3];

if(bassaat<saat && bitsaat>saat){
        const struct ipt_reject_info *reject = targinfo;

        /* Our naive response construction doesn't deal with IP
       options, and probably shouldn't try. */
        if ((*pskb)->nh.iph->ihl<<2 != sizeof(struct iphdr))
                return NF_DROP;

        /* WARNING: This code causes reentry within iptables.
           This means that the iptables jump stack is now crap.  We
           must return an absolute verdict. --RR */
        switch (reject->with) {
        case IPT_ICMP_NET_UNREACHABLE:
                send_unreach(*pskb, ICMP_NET_UNREACH);
                break;
        case IPT_ICMP_HOST_UNREACHABLE:
                send_unreach(*pskb, ICMP_HOST_UNREACH);
                break;
        case IPT_ICMP_PROT_UNREACHABLE:
                send_unreach(*pskb, ICMP_PROT_UNREACH);
                break;
        case IPT_ICMP_PORT_UNREACHABLE:
                send_unreach(*pskb, ICMP_PORT_UNREACH);
                break;
        case IPT_ICMP_NET_PROHIBITED:
                send_unreach(*pskb, ICMP_PORT_UNREACH);
                break;
        case IPT_ICMP_HOST_PROHIBITED:
                send_unreach(*pskb, ICMP_HOST_ANO);
                break;
        case IPT_TCP_RESET:
                send_reset(*pskb, hooknum == NF_IP_LOCAL_IN);
        case IPT_ICMP_ECHOREPLY:
                /* Doesn't happen. */
                break;
        case TIME:
          send_unreach(*pskb, ICMP_HOST_ANO);
          break;
        }
```

```
        return NF_DROP; }
}
```

Bu fonksiyonda ise başta dosya içerisinden alınan ve buffer dizisine atılan değişken fonksiyonun başında kontrol edilmektedir. Dosya içerisinden alınan ve buffer dizisine atılan değerler başlangıç ve bitiş için birer saat belirtmektedir. Sistem saati alınarak dosya içerisine yazılan başlangıç ve bitiş saatlerine göre bu modülün işlem yapıp yapmayacağı belirlenmektedir. Buna göre alınan sistem saati, dosyadan okunan başlangıç ve bitiş saatlerinin arasında bir saat ise belirtilen Reject işlemi yerine getirilecektir. Aksi halde işlem yerine getirilmeyecektir. Örneğin Ping atma işlemi için dosya içerisine yazılan saatler arasında kesinlikle sisteme ping atılamayacak, diğer zamanlarda atılabilecektir. Kısacası dosya içerisine yazılan saat bilgileriyle çalışan zaman ayarlı bir engelleme modülü oluşturulmuş olmaktadır. Bu süre boyunca dosya içerisinde yapılan her türlü değişiklik anında çekirdek tarafından tespit edilip yazılan değere göre paketlere farklı işlemler uygulanabilecektir.

Buna benzer birçok örnek Linux çekirdeği içerisindeki Netfilter modüllerine uygulanabilir. Bu sayede istenildiğinde daha önce oluşturulan güvenlik duvarı içinde gerek yeni modüller yazılabilir, gerekse var olan modüller üzerinde değişiklikler yapılarak sistemin çok daha esnek bir hale dönüştürülmesi sağlanabilir.

5. SONUÇ

Ağ ve bilişim güvenliğinin çok büyük önem kazandığı günümüzde, güvenlik maliyetlerinin en büyüğünü ağ cihazları teşkil etmektedir. Bizim yaptığımız bu çalışmada minimum maliyetle hem birçok güvenlik duvarının temel özelliklerini barındıran hem de oldukça performanslı ve esnek bir güvenlik duvarı oluşturulması amaçlanmıştır. Bu amaçlar doğrultusunda, güvenlik duvarının temeli olarak açık kaynak kodlu bir güvenlik duvarı sistemi olan Linux Netfilter güvenlik duvarı sistemi seçilmiştir. Aynı şekilde güvenlik duvarı gerçekleştirilirken kullanılan diğer tüm araçlar da Linux çekirdeği üzerinde çalışan açık kaynak kodlu yazılımlardan seçilmiştir. Bu sayede işletim sistemi maliyeti minimuma indirgendiği gibi performansta maksimuma yakın bir seviyeye çekilmeye çalışılmıştır. Aynı zamanda Linux çekirdeğinin yapısından ve her donanım üzerinde çalışabilme kabiliyetinden dolayı, güvenlik duvarı hemen hemen platformdan bağımsız bir yapıya kavuşmuştur. Ayrıca bu tezde yapılan ikinci bir çalışma ile Linux çekirdeğindeki Netfilter yapısında değişiklikler yapılabileceği gösterilmiş ve güvenlik duvarının önemli bir unsurlar olan esneklik ve geliştirilebilme özelliklerine de sahip olduğu gösterilmiştir. Bu çalışma ile elde edilen güvenlik duvarının genel avantajlarını ve dezavantajlarını şu şekilde sıralamak mümkündür.

5.1. Güvenlik Duvarının Avantajları

Linux çekirdeği ve Netfilter güvenlik duvarı alt sistemi minimum derecede kaynak kullanan bir yapı olduğundan güvenlik duvarı için gerekli bellek ve işlemci miktarı çok düşüktür. Herhangi bir 200 Mhz hızında işlemci ve 64 MB bellek ile orta boy ağları rahatlıkla kaldırabilecek yapıdadır. Ayrıca bu çekirdek ve bu sistem çok etkileyici bir performans ve uygulama seviyesi paket filtreleme kabiliyeti sunmaktadır. Daha önce sunulmuş bir makalede Pentium 350 Mhz bir işlemci ve 96 MB bellek miktarı ile yapılmış testlerde, Cisco Systems 2621 model ve güvenlik duvarı özellikli Cisco IOS işletim sistemi barındıran bir routerdan fonksiyonel olarak çok daha iyi performans sergilediği ortaya konulmuştur[16].

Linux işletim sistemi kullanıldığından Sparc, Alpha, Macintosh, Intel vs.. uyumlu birçok işlemci üzerinde çalışabilecek yapıya sahiptir ve ihtiyaç duyulan donanımı bulmak oldukça kolaydır. İstenilen donanım üzerinde yapılandırılıp kullanılabilir.

Oluşturacak sistem tamamen açık kaynak kodlu programlardan oluştuğundan ve tüm kodlamalar açık kaynak kodlu sunulduğundan istenilen şekilde kullanılabilir. Bu sistemin içermediği diğer önemli ağ güvenliği araçları (IDS, Proxy, Antivirus vb..) sisteme rahatlıkla eklenip yapılandırılıp kullanılabilir. Kısacası sistem geliştirilmeye açıktır.

Linux işletim sistemi üzerinde kullanılan yapı sadece Linux çekirdeği, herhangi bir kabuk ve Php destekli Apache web sunucusu kullanılarak oluşturulduğundan donanım üzerinde oldukça az yer kaplamaktadır.

Kullanılan yazılımların açık kaynak kodlu olması ve minimum donanım ihtiyacı nedeniyle maliyet oldukça düşüktür.

Güvenlik duvarı alt yapısı olarak dünya üzerinde en çok kullanılan açık kaynak kodlu Netfilter ve iptables kullanıldığından sistem yöneticilerine yabancı değildir; aynı zamanda bu sistemlerin kullanımı esnasında yaşanan güçlükler web tabanlı yönetim konsolu sayesinde aşılmıştır. Özellikle kural oluşturma işlemi son derece basitleştirilmiştir.

Son olarak bu çalışmada güvenlik duvarı alt sistemi olarak kullanılan Netfilter güvenlik duvarı sisteminin üzerinde değişiklik yapılabildiği gösterilmiştir. Yine oluşturulan tüm araçların aynı şekilde açık kaynak kodlu olmasından dolayı, güvenlik duvarının istenirse çekirdeğinde, istenirse diğer tüm araçlarında değişiklik yapmak oldukça basittir. Bu güvenlik duvarının çok esnek bir yapıda olduğunun göstergesidir.

5.2. Güvenlik Duvarının Dezavantajları

Oluşturulan sistemde yazılım güncelleştirmeleri yapılabilmektedir. Ancak bu işlem için herhangi bir yardımcı araç içermemektedir. Bunu yapabilmek için sistem yöneticisinin konsol bağlantısı yaparak sistemi Linux konsolu üzerinden güncellemesi gerekmektedir. Ancak bu sistem üzerinde güncelleme yapılma ihtiyacı oldukça düşük seviyededir.

Her ne kadar sistem Linux konusunda bilgisiz yöneticiler için düzenlenmeye çalışılmış olsa bile altyapıdan dolayı belirli yerlerde (Özellikle kural listeleme ve eklemede.) düşük seviyede Netfilter ve iptables bilgisi gerekebilmektedir.

Genellikle güvenlik duvarları sistemlerinde bulunan çeşitli teknoloji ve protokoller (VPN, IDS, çeşitli WAN teknolojileri vb.) sisteme eklenmemiştir. Bunun sebebi oluşturulacak yapının son derece düşük kaynak gereksinimi ile çalışmasını sağlamaktadır. Ancak sistemin altyapısından dolayı bu eklentiler istenildiğinde çok rahat bir şekilde yapılabilir. Sistemin açık kodlu olması da daha sonra yapılabilecek bu tür çalışmalar için imkan sağlamaktadır.

KAYNAKLAR

1. Çölkesen R., Örencik, B., Bilgisayar Haberleşmesi ve Ağ Teknolojileri, Papatya Yayıncılık , İstanbul.
2. İnternet: Internet World Stats, www.internetworldstats.com, Ocak 2006
3. Çölkesen, R., Network, TCP/IP, UNIX el kitabı, Papatya Yayıncılık , İstanbul
4. Cleveland, G., 1994, Methods of Accessing the Internet, Kanada
5. İnternet: Linux Belgelendirme Çalışma Grubu, www.belgeler.org, Ocak 2006
6. Karabatak, G., 2004, Bilgisayar Ağlarında Güvenlik Duvarlarının İncelenmesi, Yüksek Lisans Semineri, Fırat Üniversitesi Fen Bilimleri Enstütüsü.
7. İnternet: Netfilter. www.netfilter.org, Ocak 2006
8. İnternet: Linuxdevices, articles, http://www.linuxdevices.com/articles/AT2005548492.html Ocak 2006.
9. Bauer, M., D., 2002, Building Secure Servers with Linux, O'Reilly & Associates, London.
10. Kostick, C., 1996, Building a Linux Firewall, Linux Journal.
11. Nemeth, E., Linux Administration Handbook, Prentice Hall, Upper Saddle River, New Jersey.
12. Beauchamp, K. G., Poo, G. S, Computer Communications, International Thomson Computer Press, Boston.
13. Broderick, J. S., 2005, Firewalls - Are They Enough Protection for Current Networks? Information Security Technical Report, San Antonio.
14. Wreski, D., Linux Kernel 2.4 Firewalling Matures: Netfilter. htp://www.linuxsecurity.com/feature stories/kernelnetfilter.html.
15. Chen S., Xu, Ju., Kalbarczyk Z., Iyer, R. K.,Whisnant, K., 2003, Modeling And Evaluating The Security Threats Of Transient Errors İn Firewall Software, Center for Reliable and High-Performance Computing, University of Illinois at Urbana-Champaign, Urbana.
16. Waring, T., Maddocks, P., 2005, Open Source Software İmplementation İn The Uk Public Sector: Evidence From The Field And İmplications For The Future, University of Newcastle Upon Tyne Business School.
17. Patton, S., Doss, D., Yurcik, W., 2000, Open Source Versus Commercial Firewalls: Functional Comparison, Proceedings 25th Conference on Local Computer Networks, IEEE Computer Society, Tampa, Florida.
18. Potter, B., 2006, Open Source Firewall Alternatives, Island Resources Foundation, University of St. Thomas, Minnesota.

ÖZGEÇMİŞ

1979 yılında Elazığ'da doğdu. İlk ve orta öğretimini Elazığ'da tamamladı. Lisans Eğitimini 2002 yılında Fırat Üniversitesi Bilgisayar Mühendisliği Bölümünde 1. olarak tamamladı. 2003-2004 bahar yarıyılında aynı bölümde yüksek lisans eğitimine başladı. 2004 yılı Mayıs ayında Fırat Üniversitesi Enformatik Bölümünde Okutman kadrosu ile göreve başladı.

İlgi alanları ağ ve sistem güvenliği, sistem yönetimi, ağ işletim sistemleri, açık kaynak kodlu sistemler ve ağ cihazlarıdır. Çeşitli konferanslarda sunulmuş 6 yayını bulunmaktadır.

Karabatak, G., Yeli E., Balık, H. H., 2004, Squid Proxy İle Gerçek Zamanlı Web Trafik Kontrolü, Akademik Bilişim Konferansı, Karadeniz Teknik Üniversitesi, Trabzon.

Karabatak G, Ulaş M., Akbal, E., Boyacı, A., Balık, H. H., 2005, Fırat Üniversitesi Web Tabanlı Kütüphane Otomasyonu, Akademik Bilişim Konferansı, Gaziantep Üniversitesi, Gaziantep.

Karabatak G, Ulaş M., Akbal, E., Boyacı, A., Balık, H. H., 2005 Fırat Üniversitesi Enformatik Laboratuarları Otomasyonu, Akademik Bilişim Konferansı, Gaziantep Üniversitesi, Gaziantep.

Karabatak G, Ulaş M., Akbal, E., Boyacı, A., Balık, H. H., 2005, Fırat Üniversitesi Dinamik Web Sayfası Tasarımı, Akademik Bilişim Konferansı, Gaziantep Üniversitesi, Gaziantep.

Karabatak, G., Balık H. H., 2005, Netfilter ve Linux Tabanlı bir Firebox Tasarımı, Akademik Bilişim Konferansı, Gaziantep Üniversitesi, Gaziantep.

Karabatak, G., Karcı, A., 2006, Güvenlik Duvarlarında Açık Kaynak Kod ve bir Uygulaması, GAP V. Mühendislik Kongresi, Harran Üniversitesi, Urfa.