AĞ GÜVENLİĞİ

Talat Fırlar

***Özet*-Bu çalışmada IP ağlarındaki güvenlik sorunları incelenmiş ve bu sorunun çözümü için bir mekanizma önerilmiştir. Bu çerçevede, genel olarak ağ güvenliği kavramı üzerinde durulmuş, Internet, Ethernet Ağları ve IP Ağlarındaki güvenlik konusunda bilgiler verilmiştir. Bu çalışma, sadece IP Ağlarındaki güvenlik probleminin tanımını yapmak ve bir çözüm mekanizması ortaya çıkarmak için hazırlanmıştır. Gerçek uygulama geleceğe bırakılmış bunun yanında gerçek uygulama için öneriler sunulmuştur. Bu makale, insanların Internet'teki bilgi ve kaynaklarını korumak için kullandıkları farklı güvenlik modellerini tanımlayacağız**

Anahtar Kelimeler-Güvenlik, Doğruluğunu Onaylama, Yerel Alan Ağları, Internet, TCP/IP, Şifreleme, Paket Sürücü , Web güvenliği, Web tarayıcı güvenliği, Aktif içerik teknojilerinin güvenliği.

***Abstract*-In this study, the security problems in IP Networks is investigated and a mechanism for solving this problem is proposed. Within this scope, the general network security concept is explained, and some information about security problem in IP networks and Ethernet, Internet Networks are given. This study is prepared just for defining the security problem in IP networks and to obtain a solution mechanism. The real life implementation is postponed as a future work. But the proposals for the real life implementation are presented.we describe different models of security people have used to protect their data and resources on the Internet.**

***Keywords: Security*- Access Control, Authentication, Local Area Networks, Internet, TCP/IP, Encipherment, Packet Driver.**

I.GİRİŞ

Internet'in en büyük avantajını oluşturan, tüm dünyanın bağlı olduğu veri ağı olma özelliği, aynı zamanda en zayıf olduğu noktayı da oluşturur; GÜVENLİK!. Internet üzerinde hareket eden hiçbir veri gerekli önlemler alınmadığı takdirde güvenli değildir. Aynı zamanda İnternet'e bağlı bir ağın yine gerekli önlemler alınmadan güvenli olduğu söylenemez.

Internet ile beraber toplumların iletişim yapısı büyük bir değişikliğe uğramıştır. İletişim ve haberleşme, yüzyıllar önce başlayan posta sisteminden günümüz Internet'ine kadar büyük bir yolculuk geçirmiştir ve bu yolculuk hala devam etmektedir.Bu büyük yolculuk ve değişimin ana kaynağı Internet'tir. Internet, iki güçlü müttefik olan, bilişim ve iletişimi, öne sürmektedir. Telefon şebekeleri ya da radyo ağı gibi tek bir hizmet için işletilen iletişim ağları yerine, Internet bilişimin gücünü kullanarak, tek bir iletişim ağını birçok uygulama için kullanmaktadır. Bu sistem aynı anda mesajlaşma, genel yayınlama, ses ve video, gerçek zamanlı paylaşım ve daha birçok uzlaşma gerektiren uygulamayı desteklemektedir. İletişim ve bilişimin bu birlikteliği, iletişim dünyasında büyük bir değişime neden olmuştur ve bu kapsamda farklı iletişim hizmet sektörleri arasındaki sınırlar giderek belirginliğini yitirmeye başlamıştır.

Benzer bir şekilde bu birliktelik; bilişim dünyasına da değişiklikler getirmiştir. Genelde veri işleme cihazı olarak kabul edilen bilgisayar, yerini sayısal asistanlara, Web TV'lere, ağ kameralarına ve iletisim yeteneklerini kullanan diğer aygıtlara bırakmıştır. Bu gelişmeleri nasıl tanımlarsak tanımlayalım, karşı çıkamayacağımız tek bir konu vardır ki; o da iletişim ve bilişim endüstrisindeki büyük gelişme ve değişimdir. Bu değişimin en büyük itici gücü Internet bilgisayar ağı ve onunla berber gelen Intranet, elektronik ticaret, Internet servis sağlayıcı gibi yeni oluşumlardır. Bu da bize gelecekte, iletişim ve haberleşmenin giderek daha büyük bir hızla bilgisayar ağları üzerine kayacağını göstermektedir. Elektronik ticaret gibi gerçek zamanda yapılan ve para transferinin söz konusu olduğu işlerde; performansın, doğruluğun ve güvenliğin en üst düzeyde olması gerekir. Bu nedenle, bu tip uygulamaların yapılacağı Internet bağlantısı olan Intranet'lerin olduğu her kuruluşta konunun yani bilgisayar ağı yönetiminin öneminin en iyi şekilde anlaşılması ve kolay, hızlı, uygulanabilir olması gerekmektedir. Bunu sağlayabilmek için bilgisayar ağı yönetimi konusunun bileşenlerinin ve öneminin çok iyi anlaşılması gereklidir. Bilgisayar ağı yönetimi konusu, en genel biçimiyle; ağ mimarisi, performans yönetimi, hata yönetimi, kurulum yönetimi, kullanıcı hizmetleri yönetimi, güvenlik yönetimi gibi bir bilgisayar ağını en

T.Fırlar;İ.Ü.Teknik Bilimler M.Y.O,Avcılar İstanbul

etkin biçimde işletebilmek için gereken temel alanları içermektedir. Ayrıca, bilgisayar ağı hizmetlerinin kalitesi, kriptografi, sanal özel ağlar (virtual private networks), Internet hizmetleri mühendislik ve işletme stratejileri ile Internet ve toplum politikaları gibi konular da herhangi bir bilgisayar ağının yönetimini etkileyen faktörleri oluşturmaktadır. Bu çalışmada; bu konular daha detaylı bir biçimde incelenmekte ve ülkemizde de gerek akademik gerekse sanayi sektörlerinin bu gelişmelerin dışında ya da gerisinde kalmamaları için neler yapılması gerektiğine ilişkin önerilerde bulunulmaktadır.

Bu makalede, son yıllarda web'de sörf yapanları etkileyen web güvenliği problemlerinden sörf yapan kişinin mahremiyetini ihlal etmeye, kullandığı sistemin bütünlüğünü bozmaya, sistemin yararlı hizmet vermesini engellemeye veya sadece rahatsızlık vermeye yönelik yapılan saldırılar, sebepleri ile birlikte açıklanmaktadır. Güvenlik problemlerinin birçoğunun web tarayıcılarının kaynak kodunda yer alan hatalardan veya JavaScript, ActiveX ve Java gibi aktif içerik sağlayan teknolojilerin doğurduğu güvenlik boşluklarından istifade edilerek yapıldığı sonucu ortaya çıkmaktadır.Bazen de bu tür aktif içerik teknolojilerinin tarayıcılarla etkileşimi sırasında ortaya güvenlik boşlukları çıkabilmektedir
Internet bilgiye erişim sağlayan ve bilginin yayınlanmasında yeni yollar sunan muhteşem bir teknolojik gelişme. Fakat aynı zamanda bilginin kirletilmesi ve yok edilmesi için yeni yollar sunan büyük bir tehlike. Bu makale, insanların Internet'teki bilgi ve kaynaklarını korumak için kullandıkları farklı güvenlik modellerini tanımlayacağız. Makalede üzerinde durduğumuz nokta ağ güvenliği modeli ve genelde, Internet güvenlik duvarları kullanımı. Bir güvenlik duvarı bir ağın Internet'e bağlanmasını sağlarken güvenliği belirli seviyede tutan bir korunma biçimidir. Burada "Bir Internet Güvenlik Duvarı Nedir?" güvenlik duvarlarının ilkelerini ve sitenizi güvenli yapmak için neler yapıp yapamadıkları anlatılıyor. Bir güvenlik duvarı ile neler yapabileceğimizi tartışmadan önce neden bir güvenlik duvarına ihtiyacımız olduğu belirtilmelidir. Sistemlerimizde neleri koruyabiliriz. Günümüzde ne tip saldırı ve saldırganlar görebiliriz,sitemizi korumak için ne tip güvenlik çözümleri kullanabiliriz.

Bir güvenlik duvarı basitçe koruyucu bir cihazdır. Eğer bir güvenlik duvarı inşa ediyorsanız ilk düşünmemiz gereken neyi korumaya çalıştığımızdır. Internet'e bağlandığımızda üç şeyi riske atıyoruz:

Bilgilerimiz: bilgisayarlarımızda tuttuğumuz bilgiler

Kaynaklarımız: bilgisayarların kendileri

Ünümüz

Bilginin korunması gereken üç ayrı özelliği vardır [1]:

Gizlilik: diğer insanların onu bilmesini istemeyebilirsiniz.

Bütünlüğü: diğer insanların onu değiştirmesini istemezsiniz.

Mevcudiyeti: mutlaka kendiniz kullanmak isteyeceksiniz.

İnsanlar gizlilik ile ilgili risklere odaklanırlar ve bunların büyük risk olduğu doğrudur. Çoğu firma en önemli sırlarını - ürünlerinin dizaynı, finans kayıtları veya öğrenci kayıtları- bilgisayarlarında tutarlar. Diğer taraftan sitenizde bu tip gizli bilgiler içeren makineleri Internet'e bağlanan makinelerden ayırmanın çok kolay olduğunu fark edebilirsiniz.Bilgilerinizi bu yolla ayırdığınızı ve Internet'ten erişilebilen hiçbir bilginin gizlilik içermediğini varsayalım. Bu durumda neden güvenlik konusunda endişelenesiniz ki? Çünkü gizlilik tek korumanız gereken şey değil. Hala bütünlük ve mevcudiyet konusunu düşünmelisiniz. Sonuçta eğer bilgiler gizli değilse, değiştirilmesi umurunuzda değilse ve birilerinin ona erişip erişemediği de umurunuzda değilse, neden onun için yer harcıyorsunuz?.Bilgiler gizli olmasa da, o yok edildiğinde yada değiştirildiğinde oluşacak sonuçlar sizi etkileyebilir. Bu sonuçların bazıları hazır hesaplanabilir giderlerdir. eğer bilgi kaybederseniz, tekrar yapılandırılması için para ödemeniz gerekir, o bilgiyi herhangi bir şekilde satmayı planlıyorsanız, bilgi direk olarak sattığınız bir şey olmasa da satış kaybı olur. Ayrıca güvenlik problemleri ile ilgili gözle görülmeyen giderler de vardır. En önemlisi güven kaybıdır (kullanıcı güveni, müşteri güveni, yatırımcı güveni, ekip güveni, öğrenci güveni, halkın güveni).

Güvenlik suçları diğer suç tiplerinden farklıdır çünkü saptanması zordur. Bazen birinizin sitenize girdiğini bulmanız uzun zaman alabilir. Bazen de hiç bilmezsiniz. Birisi sisteminize girip sisteme yada bilgiye hiçbir şey yapmasa da, onların bir şey yapmadığını onaylayana kadar zaman (saatler veya günler) kaybedersiniz. Çoğu zaman her şeye-zarar ver saldırısı yapan birisi ile uğraşmak sisteminize girip zarar vermeyen biri ile uğraşmaktan daha kolaydır. Eğer her şeye zarar verirlerse üzerine bir bardak su içip yedeklerden açarsınız ve hayatınıza devam edersiniz. Fakat hiçbir şey yapmamış gibi görünüyorlarsa sisteminize yada bilgileriniz zarar vermediklerine emin olmak için uzun zaman inceleme yaparsınız.Bir saldırgan Internet'te sizin kimliğiniz ile bulunuyor. Yaptığı her şey sizden geliyor gibi görünüyor. Sonuçları nelerdir?.Çoğu zaman, sonuçlar diğer sitelerin - yada güvenlik güçlerinin - niye sistemlerine girmeye çalıştığınızı arayıp sormaya başlamasıdır. (Bu göründüğü kadar nadir bir durum değildir. Sıkça bu tip vakalarla karşılaşılır.)Bazen, bu sahtekarlar size zamandan fazlasını kaybettirirler. Sizden hoşlanmayan yada yabancılara hayatı zorlaştırmaktan zevk alan bir saldırgan haber gruplarına yada başka yerlere sizden geliyormuş gibi görünen mesajlar atabilirler. Genelde, bunu yapanlar inanılmasından çok nefreti hedeflerler fakat bu mesajlara çok az insan inansa da durumun temizlenmesi uzun ve zor olabilir. Bu tip

olaylar ününüze kalıcı zarar verebilir.Bir siteye erişim kazanmadan elektronik mesaj göndermek mümkün fakat eğer mesaj site dışından gönderilmişse sahte olduğunu göstermek daha kolaydır. Sitenize erişimi olan bir saldırganın gönderdiği sahte mesaj sizden geliyor gibi görünecektir, çünkü sizden gelmektedir. Ayrıca mesaj listeleriniz ve kimlere mesaj gönderdiğiniz gibi bilgilere erişen bir saldırganın sitenize erişimi olmadan sahte mesaj gönderen birinden çok daha fazla avantajı olacaktır.Bir saldırgan sizin kimliğinizi kullanmasa da sitenize izinsiz giriş ününüz için iyi değildir. İnsanların firmanıza olan güvenini sarsar. Ek olarak çoğu saldırgan bir bilgisayardan diğerine geçerler ve bir sonraki kurbanın sizin sitenizin bilgisayar suçluları için bir platform olduğunu düşünmesini sağlar. Çoğu saldırgan girdikleri sistemleri korsan yazılım ve pornografi dağıtımı için kullanırlar. Sizin hatanız olsa da olmasa da, isminizin diğer saldırılara, yazılım korsanlığına ve pornografiye karışması durumunda bunların sonuçlarından kurtulmak zordur.

I.1-İzinsiz-Girme Saptamasından Önce: Geleneksel bilgisayar Ggüvenliği

Birçok insan bilgisayar güvenliğinin yanlış şeyler olmasını engellemek olarak düşünür. Yakın geçmişte bile, firewall`lara rağmen, bu yaklaşım başarılı olmadı. Farklı tipteki güvenlik ürünlerinin güçlü ve zayıf yanlarını bilmek izinsiz-girme saptamanın sitenize sağlayacağı getirileri daha iyi görmenizi sağlayacaktır. Bunu gerçekleştirebilmek için aşağıdakileri öğreneceksiniz:

- Ürünlerin stratejinize nasıl uyacağını kritik olarak düşünmede kullanılabilecek bir Standart Güvenlik Modeli
- Tanılama ve doğrulama ürünlerinin problemleri nasıl çözebildiğini yada çözemediğini
- İşletim sistemlerinin standart erişim kontrol yetenekleri ve bunların savunmanızı nasıl güçlendireceği
- Firewall`ların ve diğer tekniklerin ağ güvenliğinizi nasıl güçlendirdiği ve niye yeterli olmadığı
- Bütün bu savunma mekanizmalarına rağmen niye hala izinsiz-girme saptama`ya ihtiyacınız olduğu.

I.2. İzinsiz-Girme Saptama (IDS) ve Klasik Güvenlik Modeli

İzinsiz-giriş saptama sıcak bir konu. Geçtiğimiz aylarda, çeşitli izinsiz-giriş saptama şirketleri daha büyük güvenlik firmaları tarafından satın alındılar. Bütün firmalar güvenlik ürünlerinin rakiplerininkilerden farklı olmasını istiyordu ve ürünlerine izinsiz-giriş saptama sistemi eklemek yapılacak şeylerden biriydi. Fakat, niye IDS`e ihtiyaç duyulsun ki? Cevabı gerçekten anlamak için temele dönmelisiniz.Bilgisayar güvenliği karışık bir konu. Söylediklerinizin ve diğerlerinin söylediklerinin kesin olması için basit terimlerle düşünmek gerekiyor. Bilgisayarlarınız ve ağlarınız ne kadar karışık olursa olsun, her bir parçasına, özneler, nesneler ve erişim kontrolü terimleri ile yaklaşabilirsiniz.

I.3-Temele Dönüş: Klasik güvenlik modeli

Evren karışık bir canavar, fakat 'subatomic' seviyede bir kaç basit fiil ve sıfatlara indirgenebilir, ve işe gidebilmeniz için evreni bu seviyede anlamanıza gerek yoktur. Bilgisayar güvenlik çözümleri uygulamak için ve güvenlik açıklarından kaçınmak için sistemlerinizin her parçasının detaylarını düşünmek zorundasınız. Sitenizdeki parçaları anlamalı ve 'Bunun altında ne var?' gibi soruları kendinize sormalısınız. Eğer biri size gelirde yeni bir uygulama kurmak istediğini belirtirse her seferinde aynı sorularla başlamalısınız: Kimler kullanacak? Nesneler neler? Erişimler nasıl ayarlanıyor? Güvenliğinden kim sorumlu?

II.AĞ GÜVENLİĞİ

Bilgisayar ağından beklenen hizmet ürünleri ve hizmet kalitesi daha da artmıştır; dolayısıyla bilgisayar uygulamasında gereksinim duyulan her türlü sayısal iletişim ihtiyacının karşılanması bilgisayar ağlarından beklenmektedir.Bunu karşılamak amacıyla da kurumlar, firmalar hem kendi alt yapılarını güçlendirmekte hem de önceden var olan Internet gibi tüm dünyaya yayılmış global ağlardan olabildiğince yararlanmaya çalışmaktadır. Yani kendi özel bilgilerini herkese açık ortamdan geçirmek zorunda kalmakta ve kendi ağını herkesin kullandığı ağa fiziksel bağlanmak zorunda kalmaktadır. Bu durumda da kişiler, firmalar veya kurumlar için yaşamsal sayılabilecek özel bilgi ve diğer kaynakların gizliliği ve güvenliğinin nasıl sağlanacağı sorunu ortaya çıkmaktadır. Bu bölümde ağ güvenliğinin nasıl sağlanacağı sorunu ortaya çıkmaktadı

· Güvenilir Sistem
· Güvenli Sistem
  - Güvenlik düzeyleri
  - Özel sanal ağlar, VPN
  - Güvenlik duvarı, Fire Wall

. Kısıtlama – İzin Verme Yöntemi
. Güvenlik Duvarı Türleri
  -Paket süzmeli güvenlik duvarı
  - Devre düzeyli geçit yolu
  -Uygulama düzeyli geçit yolu

Internet'in genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir; bu gelişmeye paralel olarak ağ kurulup işletmeye alındıktan sonra, ağ yönetimi ve ağ güvenliği büyük önem kazanmış ve ağın güvenilir biçimde çalıştırılması anahtar sözcük konumuna gelmiştir. Çünkü komple bir ağ o günün teknolojisi ile en iyi biçimde projelendirilip kurulduktan sonra iş bitmemekte, ağ performanslı, güvenilir ve güvenliği sağlanmış olmalıdır.Güvenilir ve güvenli sözcükleri, aslında tamamen farklı anlamları olan, ancak birbiriyle sürekli karıştırılan iki sözcüktür. Güvenilir güçlü, güvenli denetimli anlamındadır.

II.1- Güvenilir Sistem

Güvenilir sistem güçlü sistem demektir; yoğun trafikte bile tüm sistem kendisinden beklenen performansı sergiler ve herhangi bir tıkanmaya, çökmeye sebep olmaz. Bunun için sistemde kullanılan aktif cihazların uygulamaya dönük dikkatli seçilmiş olması ve daha da önemlisi konfigürasyonunun iyi ve bilinçli bir şekilde yapılmış olması gerekir.

II.2-Güvenli Sistem

Güvenli sistem denetimi sistem demektir; Internet gibi genele açık bir ağa bağlanan kurumsal ağların dışarıdan gelebilecek tehlikelere karşı korunması, kurumun sahip olduğu bilgi ve verilere izin verildiği ölçüde erişilmesi ve kurumun kendi elemanları tarafından yapılacak iç ve dış erişimlerin denetlenebilmesini belirtir. Bir ağ, Internet'e bağlandıktan sonra iç ve dış erişimler için koruma duvarı (fire wall) herhangi bir güvenlik sistemi içermiyorsa, sahip olunan bilgiler tehdit altındadır. Böyle bir koruma duvarı koymadan kendi ağımızı kamuya açık bir ağa eklersek, ardından birtakım sorunlar da kendiliğinden gelir. Nasıl olsa sistemlere girilirken sistemlerim kullanıcı adı ve şifre sorgulaması yapıyor dememeli, güvenlik konusunda ciddi önlemler alınmalıdır.

II.3 -Güvenlik Düzeyleri

Güvenlik düzeyi, özel bilginin saklı olduğu yerde hangi düzeyde korunacağını gösterir. Bilgi çeşitli düzeylerde koruma altında alınabilir. En alt düzeyi veri kaydı düzeyinde koruma altına almaktadır. Örneğin bir veritabanına ait veri kaydının belirli alanlar şifrelenerek, o bilgilere erişilmesi denetim altına alınabilir. Böylece, koruma altına alınmış olan alanlara yalnızca erişim hakkı olan veya oraya erişmek için şifre anahtarına sahip kullanıcılar erişebilir. Bu koruma düzeyinin bir üstü veri kaydının bir kısmını değil de tamanını korumaktır. Daha sonra diğer güvenlik düzeyleri gelir....

Kayıt alanı düzeyinde veya Veri kaydı düzeyinde koruma en sıkı korumayı sağlar; iyi bir şifreleme ve şifre anahtarı üretme algoritması kullanılır. Bilgisayara bağlanmayı veya uygulama programı düzeyinde sorgulama ise birbirine benzer biri ilgili uygulama programına girişi, diğeri bilgisayar sistemine girişi denetler. Ağ kaynaklarını hizmet türleri açısından veya ağa girişi sorgulama da ise genel olarak ağa dışarıdan bağlanmayı ve ağ üzerinde sunulan hizmetlere erişimi denetler; bu güvenlik düzeyleri genel olarak koruma duvarları (fire wall) tarafından sağlanır. Örneğin Internet'e eklenen LAN'ın ağa giriş sorgulama-bilgisayara bağlanmayı sorgulama ve ağ kaynakları hizmet türleri açısından korunması için bir güvenlik duvarı kullanılabilir.

II.4 Terminoloji

Göndericinin alıcıya bir mesaj göndermek istediğini varsayalım. Ve dahası bu gönderen mesajı güvenli olarak göndermek istiyor. Başka bir kimsenin bu mesaja göz atmadığından emin olmak istiyor.Bir mesaj düzyazı (plaintext/ cleartext) dır. Mesajın anlamını gizlemek için değiştirilmesi işlemine encryption (şifreleme) denir. Şifrelenmiş bir yazı şifreli yazı (ciphertext) dır. Şifreli yazı`yı tekrar düzyazıya çevirme işlemine deşifreleme/şifre çözme (decryption) denir [2]. (Eğer ISO 7498-2 standardını takip etmek istiyorsanız, 'encipher' ve 'decipher' terimlerini kullanın. Bazı kültürler 'encrypt' ve 'decrypt' kelimelerini ölü vücutlarıyla alakalı olduğundan rahatsız edici buluyorlar).Bu Mesajları güvenli saklama sanatı ve bilimi 'cryptography' ve bununla ilgilenen kişilere 'cryptographer' adı verilmektedir. Cryptanalyst`ler (şifre analizcileri) cryptanalysis ile yani şifreli yazı`ları kırma sanatı ve bilimi ile uğraşanlardır. Matematiğin bu her iki alanında (cryptography ve cryptanalysis) kapsayan dalında cryptology (kriptoloji) ve bu alanla ilgilenenlere de cryptologist denmektedir. Modern kriptolojisiler genelde teorik matematik eğitimi almaktadırlar.

Düzyazı mesaj için M ile normal düzyazı için ise P ile gösterilmektedir. Bit akışı, metin dosyası, bitmap, dijitize bir ses akışı, dijital bir video görüntüsü olabilir. Bilgisayar ile alakalı olduğu sürece , M basitçe ikili bilgidir. Düzyazı göndermek için yada depolama için kullanılabilir. Her durumda, M şifrelenecek mesajdır.Şifreli yazı C ile gösterilir. Ayrıca ikili bilgidir: bazen M ile aynı boyutta bazen de daha büyük. (şifrelemeyi sıkıştırma ile birleştirerek, C M den daha küçük olabilir. Fakat şifreleme bunu yapmaz.) M üzerine uygulanan şifreleme fonksiyonu E , C yi üretir. Yada matematiksel yazılımla[1]:

$$E(M) = C$$

Tersi işlemde, C üzerine uygulanan deşifreleme fonksiyonu D M yi üretir.

$$D(C) = M$$

Mesajı şifreledikten sonra deşifrelemenin tek amacı orijinal düzyazıyı bulmak olduğundan aşağıdaki yazılım doğru olmalıdır:

$$D(E(M)) = M$$

Kimlik-Doğrulama, Bütünlük, ve İnkar-edememe

Gizliliği sağlamaya ek olarak, cryptography`nin genellikle aşağıdakilerde sağlaması istenmektedir:

—Kimlik-Doğrulama (Authentication) Bir mesajın alıcısının mesajın kaynağından emin olması gerekir; kötü amaçlı bir kimse kendisini başkası gibi gösterememelidir.

—Bütünlük (Integrity). Bir mesajın alıcısının mesajın yolda değiştirilmediğinden emin olması gerekir; kötü amaçlı bir kimse orijinal mesajın içeriğini değiştirdikten sonra yollayamamalıdır.

—İnkar-edememe (Nonrepudiation). Mesajı gönderen daha sonra mesajı gönderdiğini inkar edememelidir.

Bunlar bilgisayarlardaki sosyal etkileşimler için hayati gereksinimlerdir ve yüz-yüze etkileşimlere benzerdir. Bir kişi olduğunu söylediği kişidir.. bir kişinin kimlik

belgeleri - sürücü belgesi, pasaport- geçerlidir. Bir kişiden gelen doküman gerçekten o kişiden gelmiştir.. Bunlar kimlik-doğrulama, bütünlük ve inkar-edememenin sağladıklarıdır.

II.4.1-Algoritmalar ve Anahtarlar

Bir kripto grafik algoritma, (cipher da denir) şifreleme ve deşifreleme için kullanılan matematiksel fonksiyondur. (Genelde, iki ilgili fonksiyon olur, biri şifreleme için diğeri de deşifreleme için.).Eğer bir algoritmanın güvenliği o algoritmanın gizli olmasına bağlı ise bu bir sınırlı (restricted) algoritmadır. Sınırlı algoritmaların tarihi bir ilgisi vardır fakat bugünün standartları için uygun değillerdir. Geniş yada değişen bir kullanıcı kitlesi onları kullanamaz, çünkü bir kullanıcı gruptan ayrıldığında diğer herkes başka bir algoritmaya geçmek zorundadır. Eğer birisi kazara gizliliği bozarsa herkes algoritmasını değiştirmek zorundadır.Daha da kötüsü, sınırlı algoritmalar kalite kontrolü yada standartlaştırmaya izin vermezler. Her kullanıcı grubu kendi eşsiz algoritmalarını kullanmak zorundadır. Bu tip bir grup herkesin kullandığı cihaz ve yazılımları kullanmazlar, başka biriside aynı ürünü alıp algoritmayı öğrenebilir. Kendi algoritma ve uygulamalarını yazmak zorundadırlar. Eğer gruptaki hiç kimse iyi bir cryptographer değilse güvenli bir algoritmaya sahip olduklarını hiç bilemezler.

Bu büyük dezavantajlarına rağmen, sınırlı algoritmalar düşük-güvenlikli uygulamaları için büyük ölçüde popülerdirler. Kullanıcılar sistemlerindeki güvenlik problemlerini ya fark etmezler yada aldırış etmezler. Modern kriptoloji bu problemi (K ile gösterilen) bir anahtar ile çözüyor. Bu anahtar geniş ölçüdeki değerlerden herhangi birisi olabilir. Anahtarın muhtemel değerlerinin menziline anahtar-alanı (keyspace) adı verilir. Hem şifreleme hem de deşifreleme işlemleri bu anahtarı kullanır. (örneğin: her iki işlemde anahtara dayalıdır ve bu k alt-belirteci ile gösterilir.) fonksiyonlarımız ise şimdi aşağıdaki gibidir:

$$EK(M) = C,\ DK(C) = M,\ DK(EK(M)) = M$$

Bazı algoritmalar farklı bir şifreleme anahtarı ve deşifreleme anahtarı kullanırlar. Buda şifreleme anahtarı K1 buna karşılık gelen deşifrelenen anahtarı K2 den farklıdır. Bu durumda:

$$EK1(M) = C,\ DK2(C) = M,\ DK2(EK1(M)) = M$$

Bu algoritmalardaki bütün güvenlik anahtara (yada anahtarlara) dayalıdır; algoritmanın detaylarına bağlı değildir. Bu demektir ki algoritma yayınlanabilir ve analiz edilebilir. Algoritmayı kullanan ürünler topluca üretilebilirler. Kötü amaçlı birisinin algoritmanızı bilmesi önemli değildir; eğer anahtarınızı bilmiyorsa mesajlarınızı okuyamaz.Bir cryptosystem bütün mümkün düzyazıları, şifreli-yazıları, ve anahtarları içeren bir algoritmadır.

II.4.2-Simetrik Algoritmalar

T Anahtara dayalı algoritmaların iki genel çeşidi vardır: simetrik ve genel-anahtar. Simetrik algoritmalar, bazen geleneksel algoritmalar diye de adlandırılırlar, şifreleme anahtarının deşifreleme anahtarından hesaplanabileceği algoritmalardır. Birçok simetrik algoritmada şifreleme ve deşifreleme anahtarı aynıdır. Bu algoritmalar, (aynı zamanda gizli-anahtar algoritmaları, tek-anahtar algoritmaları yada bir-anahtar algoritmaları da denir) gönderen ve alıcının güvenli bir şekilde haberleşmeden önce bir anahtar üzerinde karar birliğine varmalarını gerektirir. Simetrik algoritmanın güvenliği anahtara bağlıdır, anahtarın bilinmesi mesajların şifrelenip deşifrelenmesine izin verir. Haberleşmenin gizli kalması gerektiği sürece anahtar gizli kalmalıdır.Simetrik algoritma ile şifreleme ve deşifreleme aşağıdaki gibi gösterilir: $EK(M) = C;\ DK(C) = M$

III -ÖZEL SANAL AĞ

Tüm dünyada yeni bir tür WAN (geniş alan ağı) çözümü hızla tanınıyor ve her geçen gün daha çok firma tarafından tercih ediliyor [3] ; VPN (Virtual Private Network/Özel Sanal Ağ). Bu yeni çözüm daha esnek ve en önemlisi çok daha düşük maliyetler ile geleneksel WAN çözümlerinin tüm işlevlerini yerine getiriyor. IP ağlarının gelişinden önce özellikle büyük ölçekli kuruluşlar, şube ve bayileri arasında veri iletişimini sağlamak için kendilerine ait geniş alan ağları kurarlardı. Bu yapıyı kurmak ve sürekli çalışır durumda olmasını sağlayabilmek için büyük zaman ve kaynak (ekipman, teknik personel, eğitim) ayırmak zorunda kalırlardı. Bugünkü eğilim ise daha mantıklı ve ekonomik olan entegre IP omurgasına doğru gidiyor. Firmalar dahili ağlar kurmak, ses/veri paketleri taşımak için bağımsız network'ler kurmak yerine, artık bu fonksiyonları intranet ve extranet, veya VOIP (voice over IP) formlarında IP network'leri üzerinde uygulamayı tercih ediyorlar [4].

Günümüzde sadece büyük kuruluşlar değil küçük ve orta boylu firmalar da ofislerini, bayilerini, iş ortaklarını kolayca ve ekonomik yoldan birbirine bağlayarak veri, hatta ses veya video iletişimi sağlama ihtiyacı duyuyor. Bu network yapısını firmaların kendi başına kurmaları son derece yüksek maliyetli ve zahmetli olduğundan firmalar, bağlantı ihtiyaçlarını VPN'ler sayesinde daha düşük maliyetler karşılığında, ülke geneline dağılmış erişim noktalarına ve yüksek performanslı bir ulusal omurgaya sahip İSS'ler aracılığı ile karşılamayı tercih ediyorlar.

Özel sanal ağ (Virtual Private Networks), kısaca VNP, kişiye veya kuruma ait özel bilgi ve verinin herkese açık şebekeler veya Internet gibi global ağlar üzerinden aktarılmasını sağlar. Internet gibi geniş bir alana yayılmış bir ağın, kurumsal bir işletmenin çok çok uzaktaki ofislerinin veya trafik yoğunluğu çok fazla olmayan şubelerinin güvenli bir iletişimi yapılacak biçimde Internet

üzerinden bağlanması sanal ağ oluşturulması anlamına gelir. Yanda ki şekilde bir kuruluşun merkezi ile şubeleri arasındaki bağlantının Internet üzerinden gerçekleştirilmesi görülmektedir; görüldüğü gibi merkez ve şubelerin Internet'e çıkışlarında birer güvenlik duvarı vardır. Güvenlik duvarlarının, böyle bir uygulamadaki işlevi, iletişim yapılacak noktalar arasında tünel oluşturmasıdır.Bu tünel üzerinden, özel bilgi ve veri Internet'e çıkarılmadan önce şifrelenir ve gelen şifrelenmiş paketlerden gerçek veri elde edilir. Dolayısıyla VNP uygulamasında en önemli konu, aktarılacak bilgi ve verinin şifrelenmesidir.

VPN (Özel Sanal Ağ) teknolojisi, firmaların şubeleri ve iş ortakları ile aralarında veri iletişimini güvenilir, kolay ve ekonomik biçimde sağlamasına olanak veren bir tünelleme teknolojisidir. VPN teknolojisinde, noktalar arası ekonomik ve güvenilir bağlantılar kurulurken iletişim maliyetini minimum seviyede tutabilmek için internet ortamı "iletişim omurgası" olarak kullanılır [4]. VPN'lerde kullanılan ağ kamuya açık bir ağdır, ancak ileti bir noktadan diğer noktaya kadar özel bir tünel aracılığı ile şifrelenerek ulaşır. Gerek Intranet/Extranet VPN'lerde gerekse remote Access/dial VPN çözümlerinde güvenlik, "tünelleme teknolojisi" ile garanti edilmektedir. Temel olarak, VPN trafiği ISS'nin İnternet omurgasında güvenli ve kapsüllenmiş/kapalı bir tünel içinde dolanır. Bu tünele giriş veya tünelden çıkış noktası sadece kurum tarafındaki güvenli router veya ağ güvenlik sunucusudur (firewall server).

Özel sanal ağ uygulamasında, temelde, biri kullanıcı/geçit yolu diğeri geçit yolu/geçit yolu olarak adlandırılan iki tür bağlantı yapılır. Kullanıcı/geçit yolu bağlantısında (ki daha çok gezici kullanıcılar için gereklidir) doğrudan kullanıcı bilgisayarı ile geçit yolu arsında bir şifrelenmiş tünel kurulur. Kullanıcı tarafından yüklü olan yazılım gönderme işleminden önce veriyi şifreler ve VPN üzerinden alıcı taraftaki geçit yoluna gönderir. Geçit yolu, önce kullanıcının geçerli biri olup olmadığını sınar ve gönderilen şifrelenmiş paketi çözerek içerde korunmuş alandaki alıcıya gönderir; alıcının verdiği yanıt ta yine önce geçit yoluna gider ve yine orada şifrelenerek kullanıcıya gönderilir. Geçit yolu/geçit yolu bağlantısında birbirleriyle iletişimde bulunacak sistemler, kendi tarafında bulunan geçit yoluna başvururlar; kullanıcı sistemleri verilerini geçit yoluna gönderir ve onlar kendi aralarında şifreli olarak iletişimde bulunurlar. Bu durum, farklı yerlerdeki LAN'ların Internet gibi herkese açık ağ üzerinden güvenli bir şekilde bağlanması için kullanılır [5].

IV-GÜVENLİK DUVARI

Herhangi bir noktası kamuya açık bir şebekeye bağlı olan bir ağın güvenliğinin sağlanması için ağın giriş çıkış noktasına güvenlik duvarı (Free wall) koyulması gerekir. Böylece ağa olan erişimler denetlene bilir, ağın iç yapısı dış gözlerden gizlene bilir. Güvenlik duvarı ağ yöneticisine tüm ağa olan erişimlerin bir noktadan denetlenmesi olanağını sağlar. Böylece dışarıdan gelebilecek saldırılar önlenebildiği gibi aynı zaman da sistemin işleyişi ile ilgili bilgilerin elde edilmesinde kullanılır.

Yazılım veya donanım tabanlı olarak geliştirilebilen güvenlik duvarları genel olarak aşağıdaki görevleri yerine getirir.

- Kullanıcı sınırlaması
  - İçeri erişim kısıtlaması
  - Dışarı erişim kısıtlaması
- Gözleme
  - -Dışarıdan yapılan erişimlerin gözlenmesi
  - -İçeriden yapılan erişimlerin gözlenmesi
- Şifreleme
  - Bilginin şifrelenmesi
  - Sanal özel ağ oluşturulması
- Adres Dönüşümü Yapılması
  - Kayıtsız kayıtlı adres dönüşümü yapılması
  - Ağın dışarıdan gizlenmesi

Güvenlik duvarı özel ağ ile Internet arasına konan ve istenmeyen erişimleri engelleyen bir sistemdir; bununla ağ güvenliği tam olarak sağlanır ve erişim hakları düzenlenebilir. Ancak güvenlik duvarı kurulurken dikkat edilmesi ve göz önüne alınması gereken bazı noktalar vardır. Bunların en önemlisi güvenlik duvarının belirli bir stratejiye göre hazırlanmasıdır; kurulmadan önce ne tür bilgilerin korunacağı, ne derece bir güvenlik uygulanacağı ve kullanılacak güvenlik algoritmaları önceden belirlenmelidir [6].

Güvenlik duvarının sistem üzerinde tam olarak etkili olabilmesi için, ağ ortamı ile Internet arasındaki tüm trafiğin güvenlik duvarı üzerinden geçirilmesi gerekir.

Güvenlik duvarlarının tercih edilmesi için en büyük nedenlerden biride adres dönüşüm (NAT, Network Address Translation) özelliğidir. Sadece tek bir IP adresi ile tüm ağ kullanıcıları Internet'e çıkabilir ve yerel ağ ortamındaki IP adresleri tamamen Internet ortamından yalıtılmış şekilde kullanılabilir. Böylece herhangi bir ISS (Internet Servis Sağlayıcı) değişikliğinde iç IP adresleri değişikliğine gerek kalmaz[7].

Bir güvenlik duvarı seçiminde ağ yöneticisinin göz önünde tutması gereken birkaç durum vardır.

- o Performans
- o Güvenlik Düzeyi ve İşlevsellik
- o Yönetim ve Raporlama Özellikleri
- o Karşılıklı Çalışabilirlik

IV.1-Kısıtlama – İzin Verme Yöntemi

Bir güvenlik duvarının getireceği kısıtlama, yapacağı denetleme tasarlanırken yerleştirileceği ağa göre düşünülmelidir. Kısıtlama koymak için bir çok yol vardır.

Ancak aşağıdaki iki durum çok kullanılır ve başlangıç noktasını tarif eder.

o Engelleme (Belirli hizmetler dışında tüm sistem erişiminin engellenmesi)

o Serbest Bırakma (Belirli hizmetler dışında tüm sistem erişimin serbest olması)

IV.2- Güvenlik Duvarı Türleri

Güvenlik duvarı tasarımı için çeşitli teknikler vardır; kullanılan teknik doğrudan güvenlik duvarının türünü gösteriri Örneğin paket süzme tekniğine dayana bir güvenlik duvarı paket süzmeli güvenlik duvarı (packet-filtering fire wall) olarak adlandırılır. Güvenlik duvarı türleri:

- o Paket Süzmeli Güvenlik Duvarı
- o Devre Düzeli Geçit yolu
- o Uygulama Düzenli Geçit yolu

IV.3-Paket Süzmeli Güvenlik Duvarı (PFFW)

Paket süzme, güvenlik duvarı oluşturmanın en kolay yoludur. Paketlerin başlık alanı içindeki bilgilere bakılarak istenmeyen paketler karşı tarafa geçirilmez. Bu amaçla bir kurallar tablosu oluşturulur. Bu tabloda belirtilen kurallara uymayan paketler karşı tarafa geçirilmeyip süzülür. Belirli bir düzeyde koruma sağlar, ancak çok sıkı bir koruma sağlamaya bilir.

Paket süzmeli güvenlik duvarı oluşturmanın OSI başvuru modeline göre 3. seviye güvenlik duvarı olarak da anılırlar (yetenekleri bu katmana atanmış olan işlevlerle sınırlıdır) Dolayısıyla bu tür güvenlik duvarı oluşturmanın en kolay yolu konfigüre edilebilir bir yönlendirici kullanılmaktadır. Bilindiği gibi yönlerine bakarak, ağlar arası ortam içinde gelen paketlerin alıcı ve gönderici adreslerine bakarak, yönlendirmeyi ona göre yaparlar. Paket süzmeli güvenlik duvarları da benzer yapıda çalışırlar; gelen paketler, başlık alanı içerisindeki bilgilere bakılarak analiz edilir ve ona göre geçirilir veya atılır; veya göndericiye bir mesaj gönderilir. Başlık alanı içerisindeki bilgiler genel olarak aşağıda listelendiği gibidir[8].

- o Alıcı ve Gönderici IP Adresleri
- o Taraflardaki Port Numaraları
- o Paket Türleri (UDP-TCP-...)
- o Hizmet Protokolleri (TelNet-http-SMTP-IP Tunnel..)

Uygulamada hemen hemen tüm IP yönlendiriciler paket süzmeli güvenlik duvarı yeteneğini desteklemektedir. Bu yetenek ya yönlendiriciyle beraber hazır olarak gelmekte ya da daha sonra yazılım güncellemesi yapılarak yönlendiriciye yüklenir.

IV.3.1-Belirli Servise Bağlı PFFW

Normalde PFFW'de kullanılan algoritmaya göre çalışırlar; ancak sadece belirli bir hizmet portu üzerinden işlem yaparlar. Örneğin TelNet sunucu sistemi uzak bağlantıları 23.TCP portundan, SMTP sunucu sistemi ise 25.TCP portu üzerinden dinleme işlemi yaparlar. Bu sistemde izin verilmiş olan ana makine (host) listesi bulunur. Yalnızca, bu listede bulunan ana makinelere uygun port numarasıyla gelen paketlere geçiş izni verilir. Diğerlerinin geçişi engellenir.

IV.3.2-PFFW için Değerlendirme

Eğer karmaşık bir süzgeçleme kullanılırsa konfigürasyon işlemi gittikçe zorlaşır. Genellikle süzgeçleme arttıkça, yönlendirici üzerinden geçen paket sayısı azalır. Yönlendirici güvenlik duvarı işlevini yerine getirirken kendi görevi yanında, yani paketin başlık bilgisini yönlendirme tablosunda arama işlemi yanında, süzme işlemlerini de o pakete uygulamalıdır. Bu durumda süzme yapmak için yönlendiricinin CPU'yu kullanması gerekir. Bu da performansta bir düşüklüğe yol açabilir.

PFWR kullanımında IP paketleri seviyesinde erişim denetimi yapıldığından ve uygulama seviyesine çıkılamadığından bazı uygulamalar için yetersiz kalabilir.

IV.3.3-Devre Düzenli Geçit yolu

Devre düzeyli geçit yolları, OSI başvuru modelinin 4. katmanı olan oturum katmanı (session layer) düzeyinde çalışır; özel ağın güvenliği için arada vekil (proxy) sistem kullanılır. Devre düzenli geçit yolunda, oturum bir kez kabul edilip kurulduktan sonra, her paket için denetim yapılmaz; paketler kurulan sanal devre üzerinden akar.

Paket süzmeli güvenlik duvarına göre daha sıkı koruma sağlar. Oturum kurulurken ilgili port sınamaları yapılır ve oturum kurulduktan sonra o portu, oturumun kurulmasını başlatan taraf sonlarına kadar sürekli açık tutarEn önemli özelliği iç kullanıcı ile dış bir sunucu arasında doğrudan bağlantı olmamasıdır. Özel ağın yapısını dışarıya karşı iyi gizler.

IV.3.4-Uygulama Düzeyli Geçit yolu

Uygulama düzeyli geçit yolları en sıkı koruma yapan güvenlik duvarı tekniğidir.OSI başvuru modeline göre uygulama katmanı düzeyinde çalışır; dolayısıyla tam denetim yapma imkanı sunar. Uygulama düzeyinde denetim yapılabilir. Genel olarak güçlü bir iş istasyonu üzerine yüklenen yazılımla gerçekleştirilir. Bu tür geçit yolları devre düzeyli geçit yollarına benzer; ancak oturum kurulduktan sonra bile paketlerin sınaması yapılır. Bu da beklenmedik saldırılara karşı korumayı kuvvetlendirir.

Bu yöntem,ağ yöneticisine, paket süzmeli ve devre düzeyli geçit yoluna göre daha güvenli, daha sıkı bir koruma sağlama imkanı verir. İstenen programların çalışmasına izin verirken, yasak olanlar ise engellenir. Bu tür güvenlik Duvarı kullanılması durumunda ağ

yöneticisine büyük bir sorumluluk düşer; gerekli olan konfigürasyonu kendisi yapmalıdır.
Uygulama düzeyli geçit yolunda, kabul edilecek veya kabul edilmeyecek kuralları içeren bir tablo oluşturur. Bu tablo üzerindeki bir kurala uyan ve geçme hakka elde eden paketler karşı tarafa geçirilir.Aksi durumda engellenir.

V-SONUÇ

Ağ güvenliği; Internet ve özel sanal ağ (VNP) uygulamalarının yaygınlaşmasıyla oldukça önem kazanmıştır. Firma iç işleri için hazırlanmış bir LAN'ın Internet gibi herkese açık bir ağa bağlanması, özel bilgilerin korunması konusunu gündeme getirmiştir; aynı ağ ile hem firma içi iletişim korunması konusunu gündeme getirmiştir; aynı ağ ile hem firma içi iletişim kurulsun, hem de dış kaynaklardan yararlanılsın istenilmektedir. Güvenlik duvarı (firewall) ağ güvenliğini sağlamak için kullanılan cihazın genel adıdır. Hem dışarıdan gelecek tehlikeleri önlemeye çalışır hem de özel ağın iç yapısını dışarıdan gizler; en önemli unsurlarından iki tanesi şifreleme yeteneği ve adres dönüşüm (NAT) özelliğidir.

Her site bilginin nasıl kullanılacağını anlatan iyi tanımlanmış bir güvenlik politikası`na sahip olmalı. Bu güvenlik politikası farklı güvenlik modellerinden oluşturulmuş olabilir, çünkü bir güvenlik modeli çeşitli yollar ile uygulanabilen genel bir modeldir. Bir güvenlik modelini gerçekleştiren bir ürün güvenlik politikasını uygulamanıza yarayan bir araç sunar. Aynı güvenlik modeli diğer güvenlik politikalarını da destekleyebilir. Sitenizin güvenliğini arttırmak için kullandığınız her ürün kendi güvenlik modelini sunmalı. Birçok model, ürünler sitede birleştirildiğinde birbirini etkiler. Örneğin bir firewall ve işletim sistemi beraber çalışarak şirketiniz için güvenli bir internet bağlantısı sunarlar. Firewall ve işletim sistemi toplam çözümü sunmada farklı rollere ve sorumluluklara sahiptirler. Firewall, kendisinin güvenli bir ortamda çalışması için işletim sistemine bağımlıdır. Eğer işletim sisteminde güvenlik açığı varsa firewall`un güvenliği sağlamasına güvenilemez. Bu tip etkiler yüzünden, bir genel güvenlik modelinin nelerden oluştuğunu ve nasıl uygulayabileceğinizi bilmeniz gerekir.Kısaca, bir güvenlik modeli bireyleri ve bu bireylerin birbirleriyle nasıl etkileştiğini ve yardımlaştığını belirler. Ağlarımızdaki birçok bireyi zaten biliyorsunuz - kullanıcılar, gruplar, dosyalar, router`lar, workstation`lar, yazıcılar, disk sürücüleri, uygulama programları, istemciler, sunucular ve ağ adaptörleri. Bu bireyler bilgisayar ağlarında birbirleriyle çok farklı yollarda birbirleriyle etkileşirler. Sık rastladığınız bir erişim kontrol kuralı, bir bilgisayardaki dosyayı hangi kullanıcıların okuyabileceği olabilir. Daha başka örneklerde aklınıza gelebilir, ki buda güvenlik modeli fikrini zaten bildiğinizi gösterir. Genel güvenlik modelini araştırmadan önce, güvenliğe niye birinci derecede ihtiyaç duyulduğunu düşünün. Bir veya daha fazla ürün tarafından uygulanan bir güvenlik modeli, 3 ana amaca hizmet etmelidir.
Bilgisayar güvenliğinin amaçları; İzinsiz-giriş saptama ürünlerinin güvenliği arttırmada niye kullanılmaya başladığını anlamak için güvenlik ürünlerinin sağlamaya çalıştığı amaçları bilmelisiniz. Bu amaçlar geleneksel ürünlerle sağlanamadığı için kuruluşlar izinsiz-giriş saptama çözümlerine eğiliyorlar

Internet'e bağlanmak isteyen her şirket için, Internet üzerinde geçerli olan IP adreslerine ihtiyaç vardır. Bu adresler iç network'te kullanılması durumunda, Internet üzerinden bu network'e giriş daha kolay bir hale gelmektedir. Bunun engellenmesi için iç network'te Internet'te kayıtlı olmayan IP adresleri (unregistered IP's) kullanılır. Bu yüzden içerinden Internet'e giden trafiğin IP adreslerinin bir noktada değiştirilmesi gerekmektedir. Bu tür bir IP değişimi router veya firewall üzerinde yapılabilir. Firewall, İnternet'e açık ağların İnternet üzerinden gelebilecek saldırıları veya izinsiz yerel ağa girişleri engellemek amacı ile kurulan yerel ağ (LAN) ve İnternet arasında yer alan sunucuya yüklenen güvenlik yazılımlarına verilen genel isimdir. Firewall yazılımları İnternet güvenliğinin en üst düzeye çıkarılmasını sağlar. Diğer güvenlik hizmetleri ; E-mail virüs tarama sistemleri , Proxy , Microsoft Proxy Server 2.0. Proxy'ler firewall'lara benzer fakat genel güvenlik kurallarını desteklerler ve firewall 'lar kadar kapsamlı değildirler. Proxy'ler çift network kart ile desteklendikleri takdirde önemli ölçüde ağ güvenliğini sağlarlar.

KAYNAKLAR

[1]- Schneier, Bruce (Çeviri: Ertan Kurt) ;Applied Cryptography (Güvenlik-Şifreleme),2001.
[2]- Escamilla, Terry (Çeviri: Ertan Kurt); Intrusion Detection (Firewall un ötesinde ağ güvenliği),2001.
[3]- Braun,H.W., Chinoy,B., Claffy, K.C., Polyzos, G.C., Analysis and Modelling of Wide Area Networks:Annual Status Report. Technical Report.Applied Network Research.San Diego Supercomputer Center and Computer System Laboratory UCSD.February 1993.
[4]- Kosiur, David (Çeviri :Tansel Akyüz); Özel Sanal Ağlar [VPN} inşa etme ve yönetme,2001.
[5]- IBM Document number GG24-3178-03."Local Area Network Concept and Products". January,1994.
[6]- Chapman, D.Brent & Zwicky, Elizabeth D. (Çeviri:Ertan Kurt) ;ISBN 1-56592-124-0,Güvenlik Duvarı inşa Etmek (Building Internet Firewalls),2001.
[7]- IBM Document number GG24-3816-01."High-Speed Networking Technology : An Introductory Survey".June 1993.
[8]- ŞENTÜRK, Muzaffer;" IP ağlarında güvenlik ve doğruluk onaylayıcı hizmet birimi tasarımı",Yüksek Lisans tezi, B.Ü. Elektrik ve Elektronik Mühendisliği Bölümü,Eylül 1995.