Ağ Güvenlik Duvarı Çözümü Oluştururken Dikkat Edilmesi Gereken Hususlar

Enis Karaaslan, enis@bornova.ege.edu.tr
Ege Üniversitesi Network Güvenlik Grubu

ÖZET

Ağ güvenlik duvarı (network firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Bu çözümler yazılım veya donanımla yazılımın entegrasyonu şeklinde olabilir. Güvenlik duvarı çözümü açık sistemler üzerinde bedava dağıtılan modüllerle sağlanabileceği gibi, fiyatları sundukları servislerle orantılı olarak artan ticari ürünlerle de sağlanabilir. Bu bildiride bu tür çözümlerin tanımları yapılmış ve güvenlik duvarı çözümü seçerken dikkat edilmesi gerekenler belirtilmiştir.

1. SORUNLAR

Internet bağlantısında bir kurumun karşılaşabileceği sorunlar aşağıdaki gibidir [1]:

- Dış dünyadan kurum ağına (içeriye) yapılacak saldırılar.
- Internet'te dolaşırken kullanıcı bilgisayarına, bilgisayardan da sisteme virüs bulaşması.
- İmesh, edonkey, overnet gibi programlarla dosya paylaşımının yapılması ve bandgenişliğinin (internet veriyolu kapasitesinin) maksadı dışında kullanılması.
- Internet'te özellikle vakit kaybettirici bazı sitelere ulaşımın kurum içerisinde, kurum zamanında (mesai saatlerinde) yapılması.
- İçeriden yetkisiz kişilerin dışarıya bilgi göndermesi.
- Yetkisiz kullanıcıların Internet'te gezinmesi.

2. GÜVENLİK DUVARI ve BİLEŞENLERİ

Güvenlik duvarı, bir sistemin özel bölümlerini halka açık (public) bölümlerden ayıran, kullanıcıların ancak kendilerine tanınan haklar düzeyinde sistemden yararlanmasını sağlayan çözümlerdir. Güvenlik duvarı belirli bir makinayı denetlemek için o makina üzerine (host-based) kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir. Bu bildiride ağ güvenliğini sağlamak üzere kullanılan ağ güvenlik duvarı çözümleri üzerinde durulmuştur.

Ağ güvenlik duvarı, içeride birbirlerine güvenen, az korumalı makinaların olduğu bir kurum ağı ile dış ağlar (Internet) arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır. Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar. Yukarıda belirtilen sorunları çözmek için bir antivirüs sunucusu veya web adresi denetleyicisi sunucusu ile ortak olarak çalışabilirler. Ağ güvenlik duvarı, yazılım veya donanımla yazılımın entegre olduğu çözümler şeklinde olabilir.

Bir güvenlik duvarı çözümünde verilebilecek servislere örnek olarak aşağıdakiler sayılabilir:

- *NAT (Network Address Translation):* İç ağda internete çıkamayacak özel ip şemaları (10.0.0.0/8, 192.168.0.0/16 vb) tanımlanır ve dış bağlantılarda NAT sunucusunun reel ip'si kullanılarak iç ağ konusunda saldırganın bilgi sağlaması engellenir. Güvenlik için artıları olmakla beraber, NAT çoğunlukla adres yönetimi için kullanılmaktadır.
- *Paket Filtreleme:* En basit güvenlik duvarıdır. Router, modem gibi cihazlarla birlikte gelir. Erişim listelerinin (access list) kullandıkları yöntemdir. Bu yöntemle güvenlik duvarından geçen her üçüncü seviye (IP, IPX ..vb) paketine bakılır ve ancak belli şartlara uyarsa bu paketin geçişine izin verilir. Paket filtreleme, güvenlik duvarının her fiziksel bağlantısı üzerinde ayrı ayrı ve yöne bağlı (dışarıya çıkış, içeriye giriş) olarak uygulanabilir. Uygulamaların bağlantı için kullandıkları portlar (icq, imesh ..vb portları) baz alınarak hangi ağların veya kişilerin ne zaman bu uygulamalarla bağlantı kurabileceği belirlenebilir. Paket filtrelemede birim zamanda tek bir pakete bakıldığı ve önceki paketler hakkında bir bilgiye sahip olunmadığı için bu yöntemin çeşitli zayıflıkları bulunmaktadır [2].
- *Dinamik (Stateful) Filtreleme*: Paket filtrelemeden farkı, paketin sırf protokolüne bakarak karar verilmesi yerine, güvenlik duvarının bir bağlantıyı hangi tarafın başlattığını takip etmesi ve çift yönlü paket geçişlerine buna göre karar vermesidir. Her bağlantı için durum bilgisi tablolarda tutulduğu için paket filtrelemedeki zayıflıklar bulunmamaktadır. Dezavantajı ise dinamik filtrelemenin çok daha fazla işlemci gücüne ve belleğe ihtiyaç duymasıdır. Özellikle bağlantı(connection) sayısı arttıkça işlem ihtiyacı da artacaktır[2]. Paket filtreleme yerine dinamik filtreleme tercih edilmelidir.
- *DMZ (Silahtan Arındırılmış Bölge):* Dış dünyaya hizmet verecek sunucular buraya yerleştirilmektedir. Özellikle iç ağda NAT uygulaması yapılıyorsa dış dünyaya hizmet veren cihazlar reel ip'lerle burada konumlandırılacaklardır.
- *Proxy:* Proxy bir bağlantı uygulamasında araya giren ve bağlantıyı istemci (client) için kendisi gerçekleştiren bir servistir. Proxy'nin kullanımı, uygulama temelli (application-level) güvenlik duvarı olarak da adlandırılabilir. Bu tür bir uygulama aynı zamanda şu amaçlar için kullanılabilir:
  - Kimlerin bu servisleri kullanacağını belirlemek
  - Performans amaçlı olarak özellikle aynı isteklerin bir defaya indirgeyerek bağlantı sayısını azaltmak ve bandgenişliğinin daha etkin kullanılmasını sağlamak.
- *Anti-Virus çözümleri:* HTTP, FTP ve SMTP trafiğini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.
- *İçerik Filtreleme (content filtering):* Çeşitli yazılımlarla ulaşılmak istenen web sayfalarını, gelen e-posta'ları filtrelemeye yarayan sistemlerdir.
- *VPN:* Ortak kullanıma açık veri ağları (public data network) üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi esas olarak alınır. Public/Private anahtar kullanımı ile sağlanır.

- *Saldırı Tespiti (ID):* Şüpheli olayları ve saldırıları tespit etmeyi hedefleyen bir servistir. Saldırı tespit sistemleri(IDS), şüpheli durumlarda e-posta veya çağrı cihazı gibi yöntemlerle sistem yöneticisini haberdar edebilmektedir.
- *Loglama ve Raporlama:* Kayıtlama (log) ve etkinlik raporları birçok güvenlik duvarı tarafından sağlanmaktadır. Bu kayıtlar çok detaylı ve çok fazla veri içerebilmektedir. Bazı güvenlik duvarları bu logların incelenmesini kolaylaştırmak için çeşitli analiz ve raporlama servisleri sunmaktadır. Kayıtlar sistemlerin zayıflıklarının ve saldırıların belirlenmesinde işe yaramaktadır.

3. İHTİYAÇLARIN BELİRLENMESİ (ANALİZ)

Bir ağ için güvenlik duvarı çözümüne gidilirken ihtiyaçlar belirlenmeli ve ağdaki hangi alanların daha çok güvenliğinin sağlanılması gerektiği tespit edilmelidir. Ağ yöneticisi güvenlik duvarını seçmeden önce iç ağında bulunan (alt) ağları listelemeli, güvenlik matriksi (security matrix) oluşturarak hangi ağların hangi ağlara ve sunuculara ulaşacağını ve ne tür haklar tanınacağını belirlemelidir. Buna göre bir alt ağı güvenlik duvarının bir bacağına (ağ arabirimine) alıp almamaya da karar verilebilmektedir.

MRTG[1] ve Saldırı Tespit Sistemleri (IDS) gibi çözümlerle ağ takip edilmeli ve ağın belirli noktalarından geçen tafik, trafiğin cinsi ve bağlantı sayısı ölçülmelidir. Kurum böylece ağdaki veri akışı hakkında bilgi edinebilecektir.

Analiz süreci tabii ki burada özetlendiği kadar basit değildir. Her türlü verinin analitik methodlarla incelenmesi ve irdelenmesi gerekmektedir. Mümkünse profesyonel bir destekten yararlanılmalıdır.

4. YAZILIM VE DONANIM ÇÖZÜMLERİ

Güvenlik duvarı çözümü yazılım veya donanımla yazılımın entegre olduğu sistemler şeklinde olabilmektedir. Bu tür çözümlerin birbirine çeşitli artıları ve eksileri bulunmaktadır.

İşletim Sistemi Üzerinde Çalışan Çözümler:
İşletim sistemi üzerinde çalışan çözümlerin artıları aşağıdaki gibidir:

- Çok detaylı raporlamalar alınabilir.
- İnce detaylara kadar kullanıcıları ayrıştırmak ve takip etmek mümkündür

Bu tür sistemlerin üzerinde çalıştığı işletim sisteminin açıkları en büyük eksiğidir. Burda şu da belirtilmelidir ki bu işletim sistemleri genelde öz (core) olarak kurulduklarından üzerlerindeki servisler kısıtlıdır. Güvenlik duvarları da üzerlerinde çalıştıkları işletim sistemlerinin bazı açıklarını kapatırlar. İşletim sistemi üzerinde çalışan sistemlerin eksileri olarak aşağıdakileri belirtmek mümkündür:

- *Bakım Problemleri:* Güvenlik duvarının üzerinde çalıştığı işletim sisteminin de ayrıca bakımı gerekecektir.

[1] Multi Router Traffic Grapher (MRTG), SNMP protokolü ile toplanan verileri grafiksel olarak görüntüleyen bir programdır [3].

- *Kurulum:* İşletim sisteminin doğru kurulması gereklidir. Gerekmeyen servislerin kaldırılması ve bazı yamaların (patch) uygulanması gerekmektedir. Kurulum süresi, kutu çözümlerine göre daha uzun sürmektedir.
- *İşletim Sisteminin Güvenliği:* Güvenlik duvarının üzerinde kurulduğu işletim sisteminin öncelikle güvenliği sağlanmalıdır. İşletim sistemini seçerken o sistemle birlikte gelen güvenlik açıkları ve zayıflıkları araştırılmalı ve çeşitli ayarlamalarla güvenliğin sağlanabileceği sistemler seçilmelidir.

Kutu (Donanım) Çözümleri:
Kutu çözümleri kullanıldıkları yerin özelliğine göre ikiye ayrılabilir:

- *Küçük kutu çözümleri:* Bunların üzerinde genellikle Ev/Küçük İşletmeler (Home/Small Bussiness) çözümleri çalışır ve bu sınıftaki ürünlerin üzerindeki yazılımlar işlev ve genişletilebilirlik açısından kısıtlı sürümlerdir. Genellikle donanımsal genişletilebilirlikleri yoktur.
- *Performans kutuları:* Bunların üzerinde (100+ kullanıcı) kurumsal sürümler çalışır ve bunlar İşletim Sistemi üzerinde çalışan sürümlerle aynıdır. Ana fark, bu donanımların sözkonusu yazılım için ayarlanmış (tune) edilmiş özerk (proprietary) donanımlar olmasıdır. Bu nedenle aynı koşullardaki işletim sistemi tabanlı versiyonlardan daha performanslı çalışmaktadırlar.

Kutu çözümlerin artıları aşağıdaki gibidir:

- Uygulama için özel geliştirilmiş entegre devrelere (ASIC) sahip olduklarından daha yüksek performans elde edilebilmektedir.
- Genelde en kötü saldırılarda dahi cihazı kapatıp açınca yeniden çalışmaya devam ederler.
- Versiyon yükseltmeleri (upgrade) diğer sistemlere göre daha çabuk yapılır.
- Hizmet dışı kalma süreleri (downtime) azdır.
- İşletim sistemleri bilinmediğinden (Genelde UNIX türevleridir) ve az kullanıldığından açıkları fazla bilinmez.

Kutu çözümlerin eksileri aşağıdaki gibidir:

- Yazılabilecek kurallar cihazın versiyonu ve kapasitesi ile sınırlıdır.
- Küçük kutu çözümlerinin donanımsal genişletilebilirlik özellikleri yoktur. Daha güçlü bir cihaz için büyük olasılıkla bir üst versiyonun alınması gerekecektir. Performans kutularında ise işlemci ve bellek terfileri zor ve pahalıdır.
- Raporlamaları genelde çok sınırlıdır.
- Özellikle küçük kutu çözümlerinde, değişik saldırılara karşı yeni çözümler çok çabuk çıkmaz.
- Versiyon yükseltmeleri (upgrade) mutlaka açılıp kapanma gerektir.
- Performans kutuları işletim sistemi üzerinde çalışan çözümlerden daha pahalıya mal olabilmektedir.

5. ÜRÜNLER HAKKINDA BİLGİ TOPLAMA

Ürünler hakkında internet üzerinden bilgi alınabilecek kaynak grupları aşağıda sıralanmıştır [4]:

- *Haber Grupları:* Bu konudaki haber gruplarına http://groups.google.com adresinden ulaşıp gerekli aramalar yapılabilir. Ana haber grubu comp.security.firewalls ‘dır.
- *E-posta Grupları:* Güvenlik duvarlarının performanslarının ve güvenlik servislerinin tartışıldığı gruplara örnek olarak “firewalls-digest” verilebilir. Üye olmak için majordomo@greatcircle.com adresine mesaj kısmında “subscribe firewalls-digest” içeren bir e-posta göndermek yeterlidir. Örneğin firewall-wizards ve firewalls listelerine aşağıdaki adreslerden ulaşmak mümkündür:
  http://lists.insecure.org/lists/firewall-wizards/2003/Jan/
  http://www.isc.org/services/public/lists/firewalls.html
- *Web Sayfaları:* İnternet üzerinde birçok sitede güvenlik duvarları ile ilgili çalışmalar bulunmaktadır. Bunlara örnek olarak aşağıdakiler verilebilir:
  - *Test sonuçları yayınlayan siteler:* “Data Communications”, “InfoSecurity News” ve “Network World” gibi magazinler periyodik olarak güvenlik duvarlarını çeşitli kriterlere göre test etmektedirler. Güvenlik duvarı karşılaştırma tablosu örneği için bakınız [5].
  - Coast Araştırma Enstitüsünün güvenlik duvarı ile ilgili sayfaları için bakınız [6].
  - Çeşitli güvenlik duvarı ürünleri ve adresleri için bakınız [7].
  - Çokça sorulan sorular (FAQ) için bakınız [8].

Eğer ticari bir ürün alınacaksa mümkünse teknik bir yetkili tarafından ürünün sunumu yapılmalı ve ürünün yetenekleri hakkında daha detaylı bilgiye ulaşılmaya çalışılmalıdır.

6. SEÇİM SIRASINDA DİKKATE ALINMASI GEREKENLER

Güvenlik duvarı çözümünde kullanılacak ürünleri (yazılım veya donanım) seçerken dikkat edilmesi gereken hususlar aşağıda sıralanmıştır:

- Güvenlik Alanında Deneyim
- Verilecek Servisler
- Performans
- Ölçeklenebilirlik
- Kullanım ve Konfigürasyon Kolaylığı
- Maliyet
- Teknik Destek

Güvenlik Alanında Deneyim:
Ürünü geliştiren firmanın veya güvenlik çözümünü sunan firmanın ne kadar süredir bu konuyla uğraştığı ve bu konudaki deneyimi önemli bir kriter olarak karşımıza çıkmaktadır. Bu ürünün hangi kurumlarda kullanıldığı (bu gizli tutulması istenebilir) veya kaç değişik kurumda kullanıldığı da önemlidir.

Verilecek Servisler:
Verilecek servisler ve dikkat edilmesi gerekenler aşağıdaki gibidir:

- *Saldırı engelleme:* Ürünün hangi saldırıları nasıl engellediği de seçim aşamasında önemli bir kriter olarak karşımıza çıkmaktadır.
- *Dinamik (Stateful) Filtreleme:* Dinamik filtrelemede takip edilen verinin zenginliği ve ne kadar detaylı incelendiği güvenlik seviyesini belirlemektedir. Birçok firma dinamik filtrelemeyi uyguladığını iddia etmektedir ama bütün uygulamalar öne sürüldüğü kadar dinamik ve güvenli değildir. Detaylı bilgi için bakınız [9].
- *DMZ:* DMZ uygulamasında bu ağ için ayrı bir ağ arabirimi (bacak) gerekecektir.
- *VPN:* Birim zamanda yapılacak VPN bağlantı sayısı alınan cihazda desteklenip desteklenmediği kontrol edilmelidir. VPN ile bağlantıların çok olacağı ağlarda, ürünün VPN için kullanıcı sayısına göre ek ücret talep edip etmediği kontrol edilmeldir. Ayrıca VPN şifreleme kullandığından makinaya eksta yük getireceği de unutulmamalıdır.
- *NAT uygulaması:* NAT uygulamasının özellikle büyük ağlarda makinayı oldukça yoracağı düşünüldüğünde, NAT işlevini yürütmek için ayrı bir sunucu ayırmak daha iyi olabilecektir.
- *Üçüncü parti (Third party) Yazılımlarla İletişim:* Anti-virüs veya içerik filtreleme gibi servisleri sunan cihazlarla iletişimin nasıl sağlandığı, hangi protokolün kullanıldığı (CVP veya benzerleri) ve işleyişindeki performans incelenmelidir.
- *Saldırı Tespit Sistemleri(IDS):* Saldırı tespiti sistemi, güvenlik duvarı cihazından ayrı bir cihazda çalışabilir. Ayrı bir sistem olarak çalıştığında iki çözümün entegre çalışabiliyor olması önemli bir tercih nedeni olmalıdır. IDS'de sistem yöneticisini saldırılardan haberdar etmek için kullanılan alarm yöntemleri ve alarm durumları ayarlanabiliyor olmalıdır.
- *Log tutma ve raporlama:* Güvenlik duvarının, kayıtların analizini sağlayacak ve gereksiz kayıtları temizleyerek daha öz sonuçlar sunacak servisler sunup sunmadığı araştırılmalıdır.

Performans:

Güvenlik duvarı, kullanıcıların ağ üzerindeki iletişimini mümkün olduğunca az yavaşlatmalıdır. Bunun için sistemin hızlı çalışıyor olması gerekmektedir.

Çözümün uygulanacağı ağda ne kadar reel veri akışı (throughput) olacağı, birim zamanda kaç kullanıcının internete çıkacağı ve kaç bağlantının (connection) oluşacağı hesaplanmalı veya tahmin edilmelidir. Bağlantı sayısı kullanılan programlara göre değişmektedir. Örneğin icq, imesh gibi programların birden fazla bağlantı kurduğu unutulmamalıdır. Güvenlik duvarında yazılacak kurallar ve verilen servisler arttıkça gereken işlemci gücü artacaktır. Aynı zamanda sisteme olacak bağlantı sayısı da hem işlemci hem de bellek harcayacaktır. Bu hizmetleri karşılayabilecek işlemciye ve belleğe sahip çözümlere gidilmelidir.

Her geçen gün kurumların bandgenişliği büyüklüğü artmaktadır. Aslında performans azalmasına yol açan faktörün, güvenlik duvarı üzerinden geçen trafikten çok, bağlantıların durum tablolarının yönetimidir. B Sınıfı adresi büyüklüğünde (65,535 ayrı IP adresi) bir yükün güvenlik duvarının çökmesine yol açabileceği gözlenmiştir [10].

Eğer işletim sistemi üzerinde çalışan bir çözüme gidilecekse; Sistem güçlü bir sunucu (server) üzerinde çalışmalı, mümkünse bu cihazın bir yedeği bulunmalıdır. Büyük bir kampüs ağı (>1000 bilgisayar) düşünüldüğünde en az iki işlemcili ve 2 Gigabyte belleğe sahip sunucu mimarisinde bir cihaz seçilmesi önümüzdeki birkaç sene için temel servislerin sunulmasını sağlayabilecektir. Bu cihazın yedeklemeli (redundant) birimleri olması sistemin daha güvenilir çalışmasını sağlayacaktır. Bu cihaz enerjiyi kesintisiz güç kaynağından (UPS) almalı, mümkün olduğu kadar bu cihaza fiziksel erişim kısıtlanmalıdır.

Ölçeklenebilirlik:
Artan ihtiyaçlar da göz önünde bulundurularak, sistemin bir kaç senelik plan içinde yeni koşullara ayak uydurabilmesi için genişletilebilirlik özelliklerini destekleyip desteklemediği de incelenmelidir.

Kullanım ve Konfigürasyon Kolaylığı:
Grafik arabirimlerle kuralların ve kuralların uygulanacağı objelerin tanımlanmasının kolaylığı, yapılacak işin daha hızlı olmasını sağlayacağından bir tercih konusu olabilmektedir.

Maliyet:
Çözüm için ister ticari bir ürün kullanılsın, isterse açık sistemler (open systems) kullanılsın kuruma bir maliyeti olacaktır. Maliyet her zaman tercih durumunda önemli bir kriterdir. Burada eldeki bütçenin alabileceği en iyi sistemin kurulması söz konusudur. Konulacak sistemin sadece bugünü kurtarması hedeflenmemeli, birkaç yıllık ağın genişleme durumu da dikkate alınarak buna göre bir seçim gerçekleştirilmelidir. Sahip olma maliyeti (cost of ownership) de dikkate alınmalı ve uzun vadede bu ürünün yıllık yenilemeleri, yama (patch) ücretleri de planlanmalıdır. Teknik destek ücreti de hesaba katılmalıdır.

Daha yüksek fiyatlar her zaman daha iyi güvenlik anlamına gelmemektedir. Kurum değer/maliyet analizi yaparken sağlıklı bir şüphecilik içinde olmalı ve ürünün hangi özelliği nedeniyle daha pahalı olduğunu firmadan öğrenmelidir [4].

Teknik Destek:
Güvenlik duvarı endüstrisi uzmanı olan Marcus Ranum'un da belirttiği gibi ticari bir güvenlik duvarı almanın en önemli nedenlerinden biri firmadan destek alabilmektir [4]. Bazı firmalar bu tür çözümlerin kurulumu, bakımı, eğitimi ve danışmanlık hizmetlerini de sunmaktadırlar. Bu tür hizmetlerin hangilerinin yapılan anlaşmada olduğuna dikkat edilmelidir. Terfi ve yama (patch) uygulamalarının nasıl sağlanacağı ve ne tür bir teknik desteğin ne kadar ücretle temin edilebileceği mutlaka incelenmelidir. Yazılımsal veya donanımsal ne tür garantilerin olduğu mutlaka belirlenmelidir. Hizmet alınan firmanın bu çözümü ne kadar süredir sunduğu, kaç firmaya bu hizmeti verdiği öğrenilmelidir. Firmanın tam gün çalışan kaç tane destek mühendisine sahip olduğu, bu kişilerin sertifikaları, bu kişilere hangi saatler arasında erişilebileceği gibi bilgiler de önem kazanmaktadır. Sınırsız e-posta desteği ve telefon desteğinin birçok durumda işe yaramayacağı ve yerinde müdahale için destek gerekebileceği de unutulmamalıdır.

Mümkünse güvenlik sistemi kuruma hizmeti sunan firma tarafından kurulmalı, ilk ayarlar yapılmalı ve kurum personeli konfigürasyon ve bakım işleri hakkında

bilgilendirilmelidir. Teknik bir sorundan dolayı güvenlik duvarının çalışamaması durumunda en geç bir hafta içinde bu sorunun halledilmesini içeren bir madde de anlaşmaya koyulmalı ve maddi yaptırımlar da belirtilmelidir.

7. YENİ TEKNOLOJİLER ve YENİ İHTİYAÇLAR

Kurumun kritik bilgilerini korumak için sadece bir güvenlik duvarı kurmak yerine daha karmaşık(complex) çözümlere gidebilir. Eğer böyle bir sistem kurulması planlanıyorsa, alınacak güvenlik duvarının da bunu desteklemesi gerekecektir. Örneğin saldırganın işini zorlaştırmak için ağda çoklu bariyer kullanarak derinine savunma (defense in depth) yapılabilir. Ayrıntılı bilgi için bakınız [11]. Bir donanımla sanal çoklu güvenlik duvarı oluşturmak üzerine de çalışmalar yapılmaktadır. Çoklu kiracılı (multitenant) sistemlerle farklı müşterilere farklı konfigürasyon ve kurallar uygulanabilmektedir. Ayrıntılı bilgi için bakınız [10].

SONUÇ

Güvenlik duvarları, sistemin ve ağın devamlılığını sağlamak için vazgeçilmez bir hale gelmektedir. Bu bildiride güvenlik duvarı çözümüne gidilirken dikkat edilmesi gereken hususlar belirtilmiştir. Kurumun sistemden beklentilerine ve elindeki bütçeye göre kurulabilecek sistemler değişebilmektedir. Aslında kurulacak sistemden çok, onun nasıl kurulduğu ve nasıl yönetildiği önemlidir. Ticari bir ürün almanın en önemli nedenlerinden birinin firmadan destek almak olduğu unutulmamalıdır. Ticari bir ürün alındığında, ürünün alındığı firmayla bakım anlaşmasının şartları detaylı olarak konuşulmalıdır.
Güvenlik duvarı çözümlerinin, sistem güvenliğinin elemanlarından sadece biri olduğu unutulmamalıdır. Ege Üniversitesi Network Güvenlik Grubu'nun güvenlik çözümleri ile ilgili çalışmalarına ve bu dökümanın güncellenmiş son versiyonuna http://security.ege.edu.tr/enisk adresinden ulaşılabilinir.

KAYNAKÇA

[1] Internet'e Bağlanırken Gerekenler: Proxy ve Firewall, Deniz Akkuş
http://www.arayan.com/da/yazi/proxy.html

[2] A Rookie's Guide to Defensive Blocks, 2002, Mike DeMaria
http://www.networkcomputing.com/1313/1313ws1.html

[3] Multi Router Traffic Grapher,
http://people.ee.ethz.ch/~oetiker/webtools/mrtg

[4] Smoking Out The Facts on Firewalls, Amy Thompson
http://www.securitymanagement.com/library/000296.html

[5] Firewall Evaluation Checklist
http://www.fortified.com/html/free_checklist.html

[6] Internet Firewalls - Resources
http://www.cerias.purdue.edu/coast/firewalls/

[7] Firewall Product Overview
http://www.thegild.com/firewall/index.html

[8] Internet Firewalls: Frequently Asked Questions, Matt Curtin and Marcus J. Ranum, http://www.ranum.com/pubs/fwfaq/
[9] Why all stateful Firewalls are not Created Equal http://www.sapphire.net/docs/stateful inspection comp white paper.pdf
[10] Defense Mechansims, 2001, Mike Frotto http://www.networkcomputing.com/1223/1223f1.html
[11] Building an In-Depth Defense, 2001, Brooke Paul http://www.networkcomputing.com/1214/1214ws1.html