

Doküman Kodu: BGT-2002

GÜVENLİK DUVARI GÜVENLİĞİ KILAVUZU

SÜRÜM 1.00

16 TEMMUZ 2007

Hazırlayan: Cem BAŞKOCAGİL

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
<http://www.bilgiguvenligi.gov.tr>
teknikdok@bilgiguvenligi.gov.tr

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliği konusunda bilinçlendirmeyi hedeflemektedir. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda bahsi geçen belirli ticari marka isimleri kendi özgün sahiplerine aittir. Burada anlatılanlar tamamen tavsiye niteliğinde olup değişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen UEKAE Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Dr. Mehmet Kara'ya teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam	6
1.2 Hedeflenen Kitle	6
1.3 Tanımlar ve Kısaltmalar	6
1.4 Dokümanda Kullanılan Semboller	7
2. FİZİKSEL GÜVENLİK	8
3. İŞLETİM SİSTEMİ GÜVENLİĞİ.....	8
4. GÜNCELLİĞİN SAĞLANMASI.....	9
5. TOPOLOJİ İÇİNDE KONUMLANDIRMA.....	10
6. ERİŞİM KONTROLÜ POLİTİKASI	14
7. KURAL TABLOSU	14
8. AĞ ADRES ÇEVİRİMİ	18
9. UZAKTAN YÖNETİM	22
10. AĞ TRAFİĞİ KAYITLARI.....	23
11. SALDIRI ÖNLEME MEKANİZMASI.....	24

1. GİRİŞ

Güvenlik duvarları ağ güvenliğinin vazgeçilmez bir parçasıdır. Günümüzde güvenlik duvarları artık sadece ağ trafiğini denetlemekle kalmayıp bunun yanı sıra bazı saldırıların tespitini de yapabilmektedir. Güvenlik duvarı, internet bağlantısını güvenli hale getirmek için artık bir standart haline gelmiştir. İnternet ve İnternet kullanıcıları güvenlik duvarlarını kullanarak bağlantılarını güvenli hale getirmektedirler [2].

Güvenlik duvarları kurum ağını dış ağlardan gelebilecek tehditlere karşı korur. Sağladığı güvenlik seviyesine göre çeşitli güvenlik duvarları bulunmaktadır. En temel güvenliği paket filtreleyici güvenlik duvarları sağlar. Bu güvenlik duvarları sadece istenmeyen IP paketlerinin kurum ağına sızmasını engelleyebilmektedir. Durumsal paket filtreleme özelliğini barındıran güvenlik duvarları daha üst düzey bir koruma sağlamaktadır. En üst düzey güvenliği içerik kontrolü gerçekleştirebilen güvenlik duvarları sağlamaktadır. Bu güvenlik duvarları saldırı niteliği taşıyan ağ trafiğini doğrudan engelleyebilmektedir [1, 2].

Güvenlik duvarı seçiminde kurumdaki kullanıcı sayısı, ağ trafiği yoğunluğu, varlıkların ve verilerin kritiklik derecesi, kullanılan uygulamalar gibi bir takım faktörler göz önünde bulundurulmalıdır. Böylelikle ihtiyaç duyulan güvenlik seviyesi belirlenip bu seviyede korumayı sağlayacak bir güvenlik duvarı seçilmelidir. Genellikle standart bir güvenlik için kurumun dış ağa çıktığı noktada yönlendirici kullanılmakta ve güvenlik duvarı bu yönlendiricinin arkasında konumlandırılmaktadır [2].

Güvenlik duvarları, saldırı tespit sistemleri (STS), anti virüs sistemleri ve içerik kontrolcülerini gibi başka güvenlik mekanizmaları ile birlikte kullanılıp güvenlik daha da artırılabilir. Örneğin güvenlik duvarı, bir saldırı tespit sistemi ile entegre çalışabilir. İhtiyaç duyulan güvenlik seviyesine göre güvenlik duvarları için değişik ağ topolojileri kullanılabilir. Örneğin dışarıya hizmet veren sunucular için ayrı bir ağ segmenti oluşturulabilir. İstenen korumanın sağlanabilmesi için güvenlik duvarı doğru bir şekilde konumlandırılmalı ve dikkatlice yapılandırılmalıdır. Bu amaçla önceden uygun bir güvenlik politikasının yazılmış olması gerekmektedir.

Her güvenlik mekanizması gibi güvenlik duvarları da hatalı yapılandırmalar, güncel yama eksiklikleri ve sıkılaştırmaların yapılmaması gibi nedenlerden dolayı bir takım zafiyetler barındırmaktadır. Bunun dışında güvenlik duvarlarının her türlü saldırıya karşı koruma

sağlayamayacağı unutulmamalı ve kademeli güvenlik prensibi (**defense in depth**) uygulanıp ek güvenlik mekanizmaları kullanılmalıdır [2].

Bu doküman uygun güvenlik duvarının seçilmesi, güvenli olarak yapılandırılması ve sıkılaştırılması için tavsiyeler içermektedir.

1.1 Amaç ve Kapsam

Güvenlik duvarları artık her kurum ağının vazgeçilmez bir parçası haline gelmiştir. Güvenliğin sağlanmasında ve dışarıdan gelen saldırıların engellenmesinde büyük rol oynayan güvenlik duvarının güvenli bir şekilde yapılandırılması gerekmektedir. Aksi takdirde iç ağ, dışarıdan gelen saldırılara ve yetkisiz erişimlere karşı korunmasız kalabilir.

Bu dokümanda güvenlik duvarının yönetilmesinde dikkat edilmesi gereken hususlar üzerinde durulmuş ve güvenlik duvarının güvenli olarak yapılandırılması için gerekli işlemlerden bahsedilmiştir. Öncelikle genel güvenlik adımları anlatılmış daha sonra dokümanın ekler kısmında çeşitli güvenlik duvarı modelleri için daha özel güvenlik adımları ele alınmıştır.

1.2 Hedeflenen Kitle

Bu doküman güvenlik duvarının yönetilmesinden ve güvenli olarak yapılandırılmasından sorumlu kişiler tarafından kullanılabilir.

1.3 Tanımlar ve Kısaltmalar

UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
STS	: Saldırı Tespit Sistemi
DMZ	: DeMilitarized Zone (Yarı Güvenli Bölge)
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
ICMP	: Internet Control Message Protocol
SNMP	: Simple Network Management Protocol
IP	: Internet Protocol
SYN	: SYNchronization
ACK	: ACKnowledgement

FIN	: FINish
NAT	: Network Address Translation (Ağ Adres Çevrimi)
PAT	: Port Address Translation (Port Adres Çevrimi)
NTP	: Network Time Protocol
FTP	: File Transfer Protocol
DNS	: Domain Name System
SMTP	: Simple Mail Transfer Protocol
HTTP	: Hyper Text Transfer Protocol

1.4 Dokümanda Kullanılan Semboller

Sembol	Açıklaması
(yabancı terim)	İngilizce terimleri belirtmek içindir.
Komut	Kod parçalarını ve betikleri belirtmek içindir.
<u>Vurgu</u>	Vurgulanmak istenen kelimeler içindir.

2. FİZİKSEL GÜVENLİK

Güvenlik duvarının sürekliliği kurum açısından çok önemlidir. Çünkü kurum ağından çıkan ve kurum ağına giren tüm ağ trafiği güvenlik duvarı üzerinden geçmektedir. Güvenlik duvarının belirli bir süre hizmet verememesi ya da tamamen devre dışı kalması kurumun dış dünya ile olan iletişimini kesecektir. Bu nedenle güvenlik duvarının öncelikle fiziksel güvenliğinin sağlanması gerekmektedir. Böylelikle güvenlik duvarına yapılacak yetkisiz erişimler ve verilebilecek hasarlar önlenmiş olacaktır. Güvenlik duvarının fiziksel güvenliğinin sağlanması için aşağıdaki adımlar gerçekleştirilmelidir:

- Güvenlik duvarı kilitli kabinetlerin içinde bulundurulmalıdır.
- Güvenlik duvarının bulunduğu sistem odalarına sadece yetkili personelin erişimini sağlayacak kimlik doğrulama mekanizmaları (kilit, manyetik kart okuyucu, parmak izi okuyucu, vb...) konulmalıdır.
- Güvenlik duvarının, elektrik kesintisine karşı yedek bir güç kaynağı ile beslenmesi sağlanmalıdır [2].
- Güvenlik duvarının bulunduğu ortamdaki toz ve diğer yabancı maddelerden etkilenmemesi için uygun cihazlarla havalandırma ve filtreleme işlemlerinin yapılması sağlanmalıdır.
- Güvenlik duvarının yangın, sel, vb... gibi doğal etkenlerden korunması için gerekli önlemler alınmalıdır (örneğin yangın söndürme sistemleri)

3. İŞLETİM SİSTEMİ GÜVENLİĞİ

İster yazılımsal ister donanımsal güvenlik duvarı olsun, bütün güvenlik duvarları bir işletim sistemi üzerinde çalışır. Bu işletim sisteminden kaynaklanacak bir açıklık, güvenlik duvarının da bir açıklığı olarak kabul edilmektedir. Bu nedenle güvenlik duvarının üzerinde çalıştığı işletim sisteminin de güvenli hale getirilmesi gerekmektedir. İşletim sisteminin sıkılaştırılması için aşağıdaki adımlar gerçekleştirilmelidir:

- Güvenlik duvarı kurulmadan önce bir işletim sisteminin en son yamaları uygulanmalı ve bilinen açıklıkları kapatılmalıdır. Uygulanan yamalardan sonra işletim sisteminin kararlılığı test ortamında denenmelidir.

- Hem güvenlik duvarının çalışma hızını etkilemesi hem de potansiyel açıklıklar barındırması açısından işletim sisteminde kurulu gereksiz yazılımlar kaldırılmalıdır.
- Unutulmamalıdır ki işletim sistemi üzerinde çalışan her servis sistem için bir risk oluşturmaktadır. Çünkü herhangi bir saldırgan bu servislerdeki olası açıklıkları kullanarak sisteme saldırabilir. Ayrıca kullanılmayan servislerin çoğunun güvensiz varsayılan ayarlarda bulunması olasıdır. Bu nedenle işletim sistemi üzerinde gereksiz yere koşan servisler kapatılmalıdır.
- İşletim sistemi üzerine yüklü olan ve artık ihtiyaç duyulmayan ağ protokolleri kaldırılmalıdır. Böylelikle bu protokollerdeki zayıflıkları hedef alan saldırıların önüne geçilmiş olacaktır.
- Yetkisiz erişimlerin önüne geçilmesi amacıyla işletim sistemi üzerinde artık kullanılmayan kullanıcı/yönetici hesaplarının kaldırılması veya pasif hale getirilmesi gerekmektedir.
- Güvenlik duvarlarında kullanılmayan ağ ara yüzleri pasif hale getirilmeli veya donanımsal olarak sökülmelidir.
- İşletim sistemine özgü diğer sıkılaştırma adımları uygulanmalıdır. (UEKAE BGT-1001 Windows 2003/XP/2000 Güvenlik Kılavuzu, UEKAE BGT-3001 Rat Hat Enterprise Server Güvenlik Kılavuzu)

4. GÜNCELLİĞİN SAĞLANMASI

Her geçen gün yeni açıklıklar bulunmakta ve güvenlik mekanizmalarına saldırmak için kullanılmaktadır. Üreticiler de bu açıklıkları kapamak için yamalar çıkartmaktadır. Güvenlik duvarının da diğer güvenlik mekanizmaları gibi düzenli olarak güncellenmesi gerekmektedir. Güvenlik duvarına gerekli yamalar uygulanarak açıklıklar kapatılmalı ve güvenlik duvarının daha güvenli hale gelmesi sağlanmalıdır. Böylelikle en son çıkan güvenlik tehditlerine karşı güvenlik duvarı ayakta durmayı başarabilecektir. Bunun dışında uygulanan yamalar beraberinde ek güvenlik özellikleri de getirebilir. Bu güvenlik özelliklerinden yararlanılarak güvenlik duvarı daha güvenli bir şekilde yapılandırılabilir. Güvenlik duvarının güncellenmesinde aşağıdakilere dikkat edilmelidir:

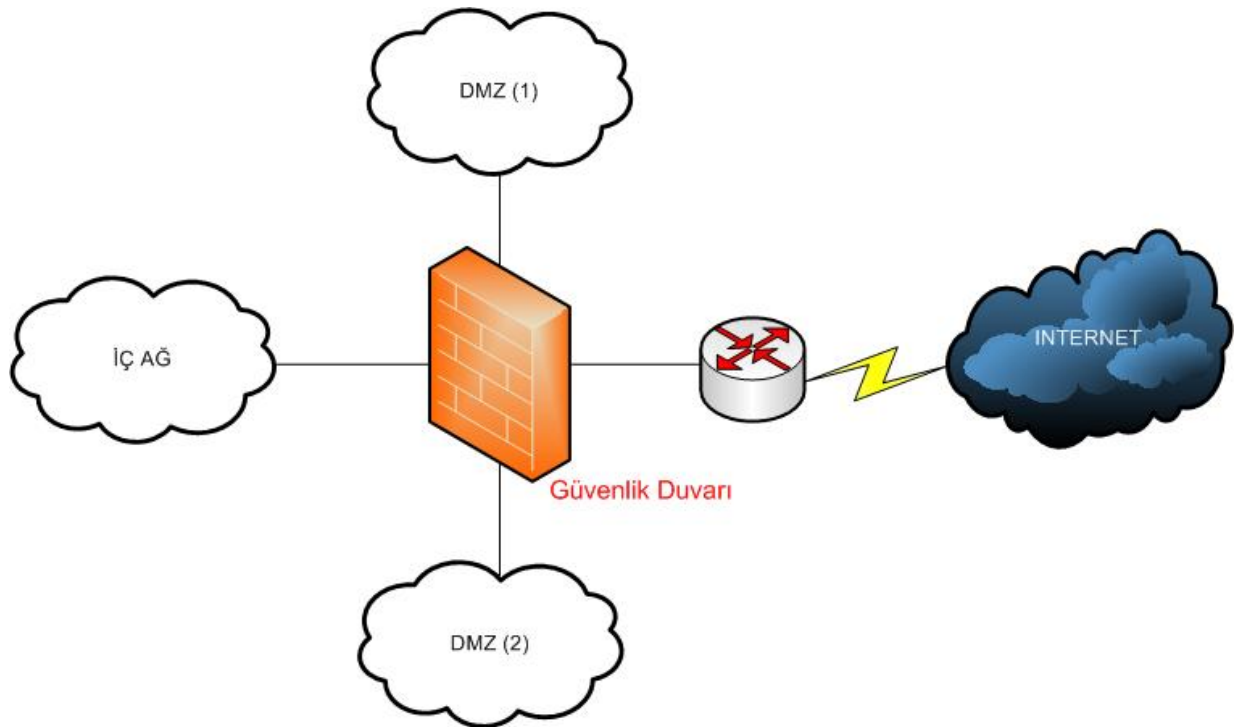
- Güvenlik duvarının güncellenmesi için üreticinin web sayfası düzenli olarak takip edilmeli ve ilgili yamalar indirildikten sonra güvenlik duvarına üreticinin tavsiye ettiği

şekilde uygulanmalıdır.

- Yama uygulanmadan önce iç ağın dış dünyayla olan bağlantısı geçici bir süreliğine kesilmelidir. Böylelikle güvenlik duvarı güncelleninceye kadar iç ağın dış ağdan gelebilecek yeni tehditlere karşı korunması sağlanmış olur.
- Herhangi bir yama uygulanmadan önce güvenlik duvarının yedeği alınmalı ve eğer mümkünse yamalar bir test ortamında uygulanıp denenmelidir. Böylelikle uygulanan yamaların sistemin sürekliliğini ve güvenliğini tehdit edecek herhangi bir etkiye neden olmadığından emin olunmalıdır.

5. TOPOLOJİ İÇİNDE KONUMLANDIRMA

Güvenlik duvarının mimari topoloji içindeki konumu oldukça önemlidir. Hatalı bir konumlandırma yapıldığı takdirde güvenlik duvarı işlevini tam anlamıyla yerine getiremeyecektir. Bu amaçla güvenlik duvarı bütün ağ segmentleri arasındaki ağ trafiğini denetleyebilecek bir şekilde konumlandırılmalıdır [5]. Genellikle güvenlik duvarı, iç ağ(lar)ın dış ağa tam çıktığı noktada yönlendiriciden önce konumlandırılmaktadır. Ancak bu şekilde güvenlik duvarı tüm ağlar arasında akan ağ trafiğinin denetimini yapabilir. Böyle bir topoloji Şekil 5.1’de verilmiştir:



Şekil 5.1 Tipik bir güvenlik duvarı topolojisi

Aslında bu yapı sık olarak kullanılan “Yarı Güvenli Bölge Yapısı (DMZ)” olarak bilinmektedir. Güvenlik duvarı değişik ihtiyaçlar için topoloji içerisinde farklı şekillerde konumlandırılabilir. Aşağıda günümüzde yaygın olarak kullanılan güvenlik duvarı konumlandırma şekilleri verilmiştir:

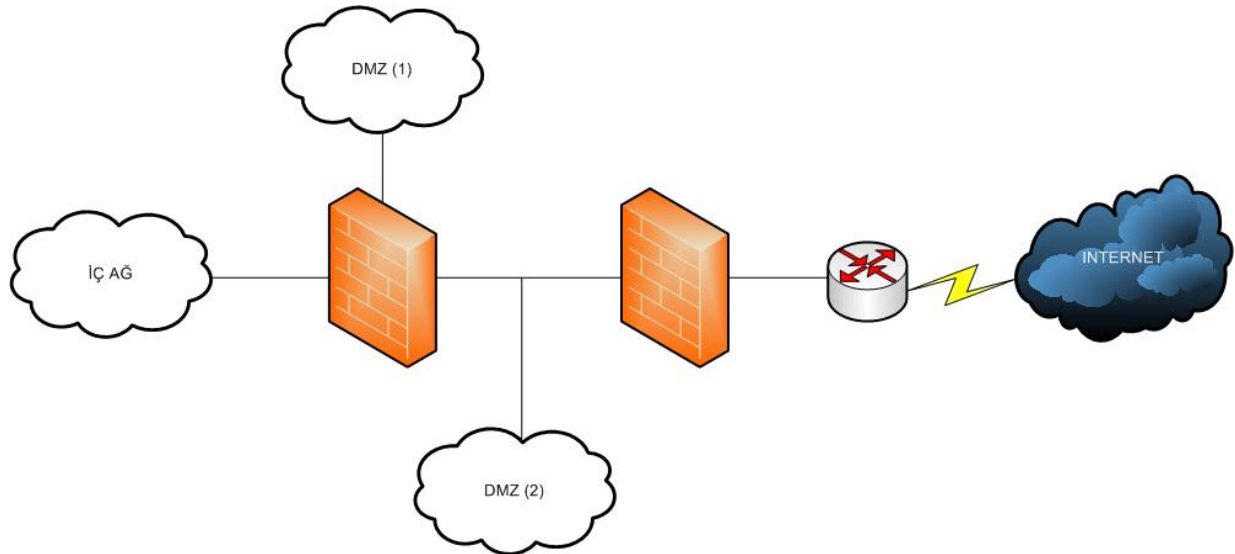
- Yarı Güvenli Bölge Yapısı (DMZ): Eğer iç ağ farklı güvenlik seviyesine sahip bölgelere ayrılmışsa ve bu bölgeler arasında akan trafiğin güvenlik duvarı tarafından denetlenmesi isteniyorsa bu yapı kullanılmalıdır [6]. Bu yapıda, iç ağ dışında kalan diğer ağ segmentleri DMZ ağları olarak tanımlanır. Bu ağ segmentleri, yarı güvenli bölge olarak da adlandırılır (Şekil 5.1).

Bu yapıda güvenlik duvarı bütün ağ segmentleri arasındaki ağ trafiğini denetleyebilecek şekilde konumlandırılmalıdır. Böylelikle iç ağdan ve dış ağdan, DMZ ağlarına yapılacak erişimlerin denetlenmesi sağlanmış olur.

- Kaskat (Sandviç) Yapı: Yapılan erişimlerin daha sıkı bir şekilde denetlenmesi isteniyorsa birden fazla güvenlik duvarı da kullanılabilir. Bu yapıda iki güvenlik duvarı arka arkaya konumlandırılır. Böylelikle güvenlik daha da artırılmış olur (Şekil 5.2).

Bu yapıda kullanılan güvenlik duvarları genellikle farklı marka olacak şekilde seçilmelidir. Çünkü aynı marka güvenlik duvarları aynı zayıflıklara sahip olacaktır. Bu nedenle dış ağdaki herhangi bir saldırgan dış güvenlik duvarının zayıflığını bulup bu güvenlik duvarını atlattığı zaman aynı zayıflığı kullanarak içteki güvenlik duvarını da atlabilecektir. Ancak farklı marka güvenlik duvarları kullanıldığında aynı saldırgan herhangi bir güvenlik duvarının zayıflığını bulsa bile bu zayıflığı diğer güvenlik duvarını atlatmak için kullanamayacaktır.

En dıştaki güvenlik duvarında ağ trafiği daha az kritere bakılarak (örneğin sadece hedef adrese göre) süzülmesi ve asıl denetim daha fazla kritere bakılarak iç güvenlik duvarı tarafından yapılmalıdır. Böyle bir yapı ile yetkisiz erişimlerin önü dış güvenlik duvarında büyük bir ölçüde kesilmiş olur ve iç güvenlik duvarının yükü hafifler. Ağ trafiğinin denetimi daha sıkı ve etkin bir şekilde yapılır.



Şekil 5.2 Kaskat yapı

- **Yedekli (Clustered) Yapı:** Bir tek güvenlik duvarının kullanılmasından kaynaklanabilecek performans sorunlarının aşılması ve sürekliliğin sağlanması için bu yapı kullanılmalıdır. Bu yapıda, birden fazla güvenlik duvarı (genellikle iki tane) paralel bir şekilde konumlandırılır ve bu güvenlik duvarlarının birlikte çalışması sağlanır. Böylelikle herhangi bir güvenlik duvarı çökse bile diğer güvenlik duvarı ağı korumaya devam eder (Şekil 5.3).

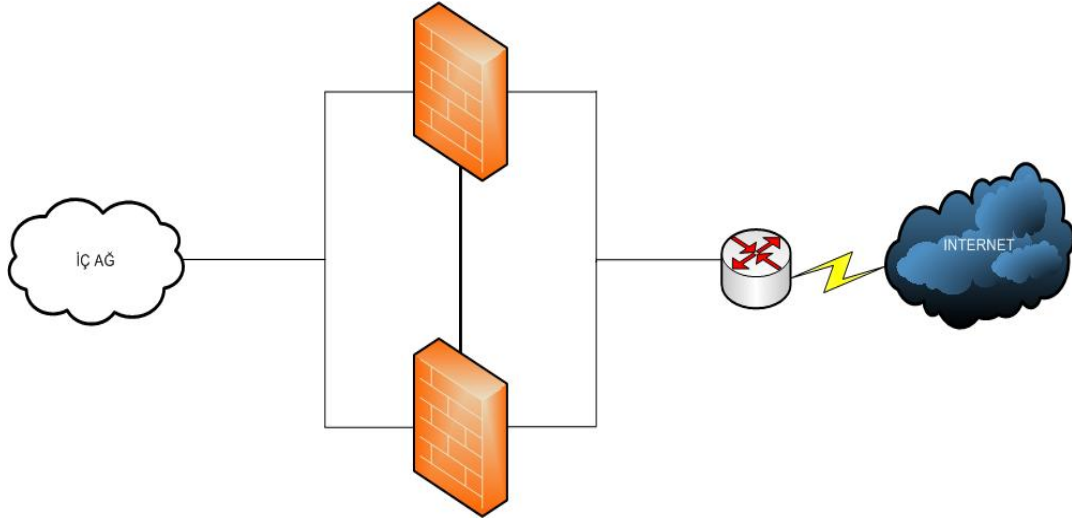
Böyle bir yapı, yapılan bağlantılara ilişkin durumların her iki güvenlik duvarında da tutulması ile sağlanır. Tutulan bu durumların iki güvenlik duvarında da aynı olması sağlanmalıdır. Bu nedenle yedekli yapı içerisinde bulunan güvenlik duvarlarının tuttukları durum bilgilerini birbirlerine göndermeleri gerekmektedir. Bu amaçla güvenlik duvarları diğer ağlardan izole bir ağ üzerinden birbirine bağlanır ve bu ağ üzerinden durum bilgilerini birbirleriyle paylaşır. Bu ağ, senkronizasyon ağı olarak bilinir. Güvenlik duvarları bu ağ üzerinden birbirlerinin durumları hakkında bilgi edinirler. Örneğin yedekli yapı içerisindeki bir güvenlik duvarı görevini yapamaz hale geldiğinde diğer güvenlik duvarı bu durumu senkronizasyon ağı üzerinden öğrenir. Eğer bu ağ bir nedenle işlevini yitirecek olursa yedekli yapı da işlevini yitirecektir. Bu nedenle yedekli yapının sağlanmasında senkronizasyon ağının önemi büyüktür. Yedekli yapıda iki tür çalışma şekli mevcuttur. Bunlar:

- **Yedekli çalışma (Aktif – Pasif):** Aynı anda sadece tek bir güvenlik duvarı aktif olarak çalışmaktadır. Diğer güvenlik duvarı pasif modda ancak her zaman çalışmaya hazır bir şekilde beklemektedir (**standby**). Eğer aktif olarak çalışan

güvenlik duvarı bir şekilde işlevini yapamaz hale gelirse, pasif moddaki güvenlik duvarı senkronizasyon ağı üzerinden bu durumu öğrenir ve aktif moda geçer. Bu çalışma şekli ile sadece süreklilik sağlanır.

- **Yük dengeleme (Aktif - Aktif):** Bu çalışma şeklinde her iki güvenlik duvarı da aktif olarak çalışmaktadır. Gelen ve giden ağ trafiği iki güvenlik duvarı arasında belirli bir oranda paylaştırılmaktadır. Örneğin ağ trafiğinin %40'lık kısmı seçilen bir güvenlik duvarı, %60'lık kısmı ise diğer güvenlik duvarı üzerinden geçecek şekilde bir ayar yapılabilir. Böylelikle her bir güvenlik duvarı üzerine düşen yük miktarı ayarlanabilir. Bu şekilde güvenlik duvarlarının her biri üzerine düşen yük normal çalışma şekline göre azaltılmaktadır. Eğer bu yapıdaki güvenlik duvarlarından biri görevini yapamaz hale gelirse bütün ağ trafiği diğer güvenlik duvarının üzerinden geçer. Bu çalışma şekli ile hem süreklilik sağlanır hem de performans artırılır.

Yedekli yapıda çalışan güvenlik duvarlarının konfigürasyonları birebir aynı olacak şekilde yapılmalıdır. Ancak bu şekilde yedekli çalışma ve yük dengeleme mümkün olabilir. Yedekli yapı kullanılarak hem süreklilik sağlanır hem de performans artırılır.



Şekil 5.3 Yedekli yapı

6. ERİŞİM KONTROLÜ POLİTİKASI

Güvenlik duvarının, kurumun güvenlik ihtiyaçlarına cevap verecek bir şekilde çalışması için öncelikle bir erişim kontrolü politikası oluşturulmalıdır. Erişim kontrolü politikası, basit anlamda kurumun erişim ihtiyaçlarını belirleyen bir dokümandır. Erişim kontrolü politikası hazırlanırken kurumun ağları arasındaki erişim ihtiyaçları dikkate alınmalıdır. Bu amaçla ağ segmentleri arasında ihtiyaç duyulan servisler tespit edilmelidir. Daha sonra ağ segmentleri arasında ihtiyaç duyulan servislere izin verilmesini, ancak bunun dışındaki tüm erişim isteklerinin engellenmesini belirten bir politika oluşturulup dokümante edilmelidir [7].

Esas olarak erişim kontrolü politikası bir takım kısıtlayıcı kurallardan oluşmaktadır. Her bir kural izin verilecek ya da engellenecek erişime ilişkin bilgiler içermektedir. Erişim kontrolü politikasındaki her bir kuralda en azından aşağıdaki üç kriter bulunmalıdır:

- Erişimi sağlayacak ağ(lar) / bilgisayar(lar)
- Erişilecek ağ(lar) / bilgisayar(lar)
- Erişim sağlanacak servis(ler)

Bazı güvenlik duvarlarında bu kriterlere ek olarak zamana göre de erişim kontrolü yapılabilmektedir. Bu nedenle bu tip güvenlik duvarları için erişim kontrolü politikasında zaman kriteri de bulundurulmalıdır.

Bir erişime ilişkin tüm kriterler belirlendikten sonra ilgili kuralda bu bilgilerle tanımlanmış erişime izin verilip verilmeyeceği belirlenmelidir. Erişim kontrolü politikasının kuralları bu şekilde sırayla oluşturulmalıdır. Son olarak erişim kontrolü politikasının güvenlik duvarına uygulanması sağlanmalıdır.

7. KURAL TABLOSU

Güvenlik duvarı ağ trafiğini kural tablosuna göre denetler. Başka bir deyişle güvenlik duvarının kural tablosu, hangi ağ trafiğine izin verilip hangi ağ trafiğinin engellenmesi gerektiği bilgisini içermektedir. Bu açıdan kural tablosunun dikkatli bir şekilde oluşturulması kurum açısından önem taşımaktadır. Kural tablosunun sistematik bir şekilde oluşturulması ve dokümante edilmesi gerekmektedir.

Güvenlik duvarının kural tablosu, önceden hazırlanmış bir erişim kontrolü politikası esas alınarak oluşturulmalıdır. Bu amaçla kurumun erişim kontrolü politikası öncelikle güvenlik duvarının anlayabileceği kurallar dizisine dönüştürülmeli ve daha sonra güvenlik duvarının

kural tablosuna yansıtılmalıdır. Bir kural tablosunda genellikle aşağıdaki alanlar bulunmaktadır:

- **Kaynak IP:** Erişimi başlatan bilgisayarın IP adresi (örneğin bir ftp istemcisi)
- **Hedef IP:** Erişim sağlanacak bilgisayarın IP adresi (örneğin bir ftp sunucusu)
- **Servis:** Erişim sağlanacak servis (örneğin ftp servisi)
- **Zaman:** Erişim sağlanacak zaman aralığı (örneğin mesai saatleri)
- **Davranış:** Söz konusu erişime izin verilip verilmeyeceği bilgisi (örneğin geçir veya düşür)
- **Kayıt:** Söz konusu erişimle ilgili kayıt tutulup tutulmayacağı bilgisi (örneğin kayıt tut veya e-posta gönder)

Kural tablosu, güvenlik duvarının temelini oluşturmaktadır. Hatalı oluşturulmuş bir kural tablosu, güvenlik duvarının istenmeyen bağlantıları geçirmesine neden olur. Bu nedenle kural tablosunun dikkatli bir şekilde oluşturulması ve erişim kontrolü politikasını en iyi şekilde yansıtması sağlanmalıdır. Ancak bu şekilde güvenlik duvarı istenen güvenliği sağlayabilir. Güvenlik duvarının kural tablosu oluşturulurken aşağıdakiler göz önünde bulundurulmalıdır:

- Kural tablosundaki kuralların sıralamasına dikkat edilmelidir. Bazı güvenlik duvarlarında ağ trafiğine uyan ilk kural uygulanırken bazı güvenlik duvarlarında ise ağ trafiğine uyan son kural uygulanmaktadır. Bu nedenle kurallar, kullanılan güvenlik duvarının davranışına uygun olarak sıralanmalıdır.

Tablo 7.1 'de kural sıralaması yanlış yapılmış bir kural tablosuna örnek verilmiştir:

No:	Kaynak IP:	Hedef IP:	Servis:	Zaman:	Davranış:	Kayıt:
1	HERHANGİ	HERHANGİ	HERHANGİ	HER ZAMAN	DÜŞÜR	KAYIT TUT
2	DIŞ AĞ	WEB SUNUCU	WEB	HER ZAMAN	GEÇİR	-

Tablo 7.2 Kural sıralaması yanlış yapılmış bir kural tablosu

Örneğin kural sıralamasının önemli olduğu bu kural tablosunda “DIŞ AĞ”dan iç ağdaki “WEB SUNUCU”ya yapılan “WEB” erişimlerine izin verilmiş olmasına karşın “İZİN VERİLENLER DIŞINDAKİ TÜM AĞ TRAFİĞİNİ DÜŞÜREN” kural en başa konulduğu için öncelikle bu kurala bakılacak ve bütün ağ trafiği düşürülecektir. Bu örnekte kural sırasının önemi karşımıza çıkmaktadır. Kurallar doğru olduğu halde kuralların kural

tablosundaki sıralaması yanlış olduğundan kural tablosu istenen davranışı gösterememektedir. Örnekteki kural tablosunun istenen davranışı gösterebilmesi için ilk kural ile son kural yer değiştirmelidir. Böylelikle istenen erişime izin verilecek ve bu erişim dışında kalan diğer erişimler engellenecektir.

- Kural tablosunda sadece ihtiyaç duyulan ağ trafiğine izin verilmeli, bunun dışında kalan tüm ağ trafiğinin geçişi engellenmelidir. Bu amaçla kural tablosunun en sonuna, “İzin verilenler dışındaki tüm ağ trafiğini düşür” şeklinde bir kural (**Cleanup Rule**) girilmelidir. Böylelikle belirtilen ağ trafiği dışındaki bütün ağ trafiği güvenlik duvarı tarafından düşürülecektir. Zaten güvenlik açısından da bir güvenlik duvarından beklenen en uygun davranış bu şekilde olmalıdır.
- Bir ağda bazı erişim istekleri diğer erişim isteklerinden daha sık yapılıyor olabilir. Eğer durum böyleyse, bu erişim isteklerinin daha hızlı bir şekilde yerine getirilmesi gerekebilir. Bu amaçla kural tablosunda daha sık sağlanan erişimlere ilişkin kurallar diğer kurallardan daha önce konumlandırılmalıdır. Böylelikle sık sağlanan erişimlerin diğer erişimlere göre güvenlik duvarında daha önce kontrol edilmesi sağlanmış olur. Sık kullanılan kuralların kural tablosunun en başına konulması hem güvenlik duvarının performansını arttıracak hem de sık yapılan erişim isteklerine daha hızlı cevap verilmesini sağlayacaktır [1].
- Kural tablosu mümkün olduğunca sade tutulmalıdır. Bu amaçla sadece ihtiyaç duyulan kuralların kural tablosunda bulundurulmasına dikkat edilmelidir. Böylelikle hem kural tablosunun gereksiz yere büyümesi engellenir hem de güvenlik duvarının performansı artırılmış olur. Ayrıca sadece izin verilen ağ trafiğinin geçirilmesi sağlanacağından güvenlik tam anlamıyla sağlanmış olur.
- Güvenlik duvarının kendisinin de gelebilecek saldırılardan korunması gerekmektedir. Bunun için kural tablosunda, doğrudan güvenlik duvarını hedef alan yetkisiz erişim isteklerini engelleyen bir kural (**Stealth Rule**) bulunmalıdır. Bu kural, kural tablosunda mümkün olduğunca ilk sıralarda yer almalıdır [1].

- Kural tablosundaki mevcut kurallar mümkün olan en fazla kısıtlamayı getirecek şekilde sıkılaştırılmalıdır. Gevşek bırakılan kurallar istenmeyen erişimlere izin verilmesine neden olabilir. Ayrıca gereğinden fazla erişime olanak tanıyan kurallar sisteme yetkisiz erişim yapılma riskini de arttırmaktadır. Örneğin DMZ bölgesindeki bir web sunucuya iç ağdan sadece belirli bir kullanıcının erişim ihtiyacı olmasına karşın bütün iç ağın erişimine izin verilmesi yetkisiz erişimlere neden olacaktır. Bu nedenle sadece gerekli kullanıcıların gerekli sunuculardaki gerekli servislere erişimine izin verilmelidir. Başka bir deyişle kuralların kaynak adres, hedef adres ve servis alanlarına kısıtlama getirilmelidir. Bunun dışında, eğer mümkünse, kritik erişimlerde kimlik doğrulama uygulanmalıdır.

Tablo 7.3’de gereğinden fazla erişime olanak tanıyan bir kural tablosuna örnek verilmiştir:

No:	Kaynak IP:	Hedef IP:	Servis:	Zaman:	Davranış:	Kayıt:
1	DIŞ AĞ	WEB SUNUCU	HERHANGİ	HER ZAMAN	GEÇİR	-
2	HERHANGİ	HERHANGİ	HERHANGİ	HER ZAMAN	DÜŞÜR	KAYIT TUT

Tablo 7.3 Gereğinden fazla erişime olanak tanıyan bir kural tablosu

Bu kural tablosundaki ilk kurala dikkatli bakılacak olursa “DIŞ AĞ”dan, iç ağdaki “WEB SUNUCU”nun bütün portlarına yapılan erişim isteklerine izin verilmektedir. Böyle bir durumda “DIŞ AĞ”daki herhangi bir saldırgan iç ağdaki “WEB SUNUCU”da açık olan bir porttaki açıklıktan faydalanarak bu porta kötü niyetli erişim sağlayabilir. Çünkü “WEB SUNUCU”nun tüm portlarına olan erişime güvenlik duvarı tarafından izin verilmiş durumdadır. Bu durum güvenlik açısından uygun değildir. Bu nedenle “WEB SUNUCU”ya sadece “WEB” erişim isteklerinin yapılmasına izin verilmeli, bunun dışındaki erişimler engellenmelidir. Çünkü bir “WEB SUNUCU” ancak “WEB” hizmeti vermektedir. Bu durumda “WEB” hizmeti dışındaki erişimlere izin verilmesi mantıksız olacaktır. Bu nedenle ilk kuraldaki “Servis” alanındaki “HERHANGİ”, “WEB” olarak değiştirilmelidir. Bu şekilde “WEB SUNUCU”nun sadece http portuna olan erişime izin verilmesi sağlanmış olur.

- Kural tablosunda engellenen ağ trafiğine ilişkin geriye cevap döndürülmemeli, ağ paketlerinin sessizce düşürülmesi sağlanmalıdır. Aksi takdirde geriye döndürülen cevaplar uzaktan sisteme erişmeye çalışan bir saldırganın güvenlik duvarının varlığı hakkında bilgi verecektir. Unutulmamalıdır ki herhangi bir saldırganın sistem hakkında elde edindiği her bir bilgi sisteme saldırma olasılığını arttırmaktadır.

- Denetlenebilirliğin artırılması amacıyla sadece kritik ağ trafiğine ilişkin kayıtların tutulması ve bu kayıtların sonradan incelenmesi sağlanmalıdır. Böylelikle ağa yapılan olası saldırıların gözden kaçırılması engellenmiş olur ve yapılan erişimler hakkında detaylı bilgi elde edilir. Bunun için kritik olarak nitelendirilecek ağ trafiği önceden belirlenmelidir.
- Kural tablosundaki kuralların anlaşılabilirliğini arttırmak amacıyla her bir kurala ilişkin açıklama eklenmelidir. Açıklama kısmında hangi güvenlik duvarı yöneticisinin, hangi tarihte ve hangi amaçla bu kuralı eklediği bilgisi bulunmalıdır. Böylelikle kural tablosunda yapılan değişikliklerin takip altına alınması da sağlanmış olur.

8. AĞ ADRES ÇEVİRİMİ

İç ağdaki bilgisayarların gerçek IP bilgilerinin dış dünyadan gizlenmesi ve gerçek IP adreslerinden tasarruf edilmesi amacıyla güvenlik duvarında ağ adres çevrimi (NAT) gerçekleştirilir. Ağ adres çevrimi basit anlamda bir IP adresini başka bir IP adresine dönüştürmek anlamına gelmektedir [4].

Gerçek IP adreslerinden tasarruf edilmesi amacıyla iç ağda özel IP adres aralıkları kullanılır. Bunlar:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Normalde bu IP adresleri kullanılarak dış dünya ile bağlantı sağlanamaz. Çünkü bu IP adresleri için yönlendirme yapılamaz. Bu nedenle bu IP adresleri için ağ adres çevrimi gerçekleştirilmelidir. Ağ adres çevrimi ile özel IP adresleri, dış dünya ile bağlantı kurmayı sağlayacak gerçek IP adreslerine dönüştürülür. Böylelikle iç ağdaki bilgisayarlarda gerçek IP adresi kullanılmadan dış dünya ile iletişim sağlanmış olur. Bu şekilde gerçek IP adreslerinden tasarruf edilir. Ayrıca iç ağdaki bilgisayarların gerçek IP adresleri dış dünyadan gizlenmiş olur. Bu da güvenliği artırır. Üç çeşit ağ adres çevrimi mevcuttur:

- Statik Ağ Adres Çevrimi: Statik ağ adres çevriminde her bir bilgisayarın IP'si ayrı bir gerçek IP adresine dönüştürülmektedir. Başka bir deyişle iç ağdaki bilgisayarlar dış dünyaya birbirinden farklı IP adresleri ile çıkmaktadır. Sadece belirli sayıdaki bilgisayarlar için statik ağ adres çevriminin yapılması daha uygun olmaktadır. Çünkü her bir bilgisayarın dışarı çıkması için ayrı bir gerçek IP adresi kullanılmakta ve bu da eldeki gerçek IP adreslerinin daha çabuk tükenmesine yol açmaktadır. Bu özelliğine rağmen statik ağ adres çevrimi güvenlik duvarına çok fazla yük getirmemektedir. Çünkü bilgisayarların dış dünyaya açılırken kullanacağı IP adresleri önceden belirlenmiştir. Bu nedenle yapılan ağ adres çevrimi “Statik” olarak adlandırılmaktadır [4].

Statik ağ adres çevrimi iki yönlü olarak yapılmaktadır. Yani hem iç ağdaki bilgisayarlar dış dünyaya erişirken hem de dış dünyadaki bilgisayarlar iç ağa erişirken statik ağ adres çevrimi gerçekleştirilmektedir. Bu anlamda bağlantıyı başlatan taraf hem iç ağ hem de dış dünya olabilir. Ancak bazı durumlarda güvenlik açısından dış dünyanın iç ağa erişmemesi istenebilir. Bu durumda statik ağ adres çevrimi yerine dinamik ağ adres çevrimi kullanılmalıdır.

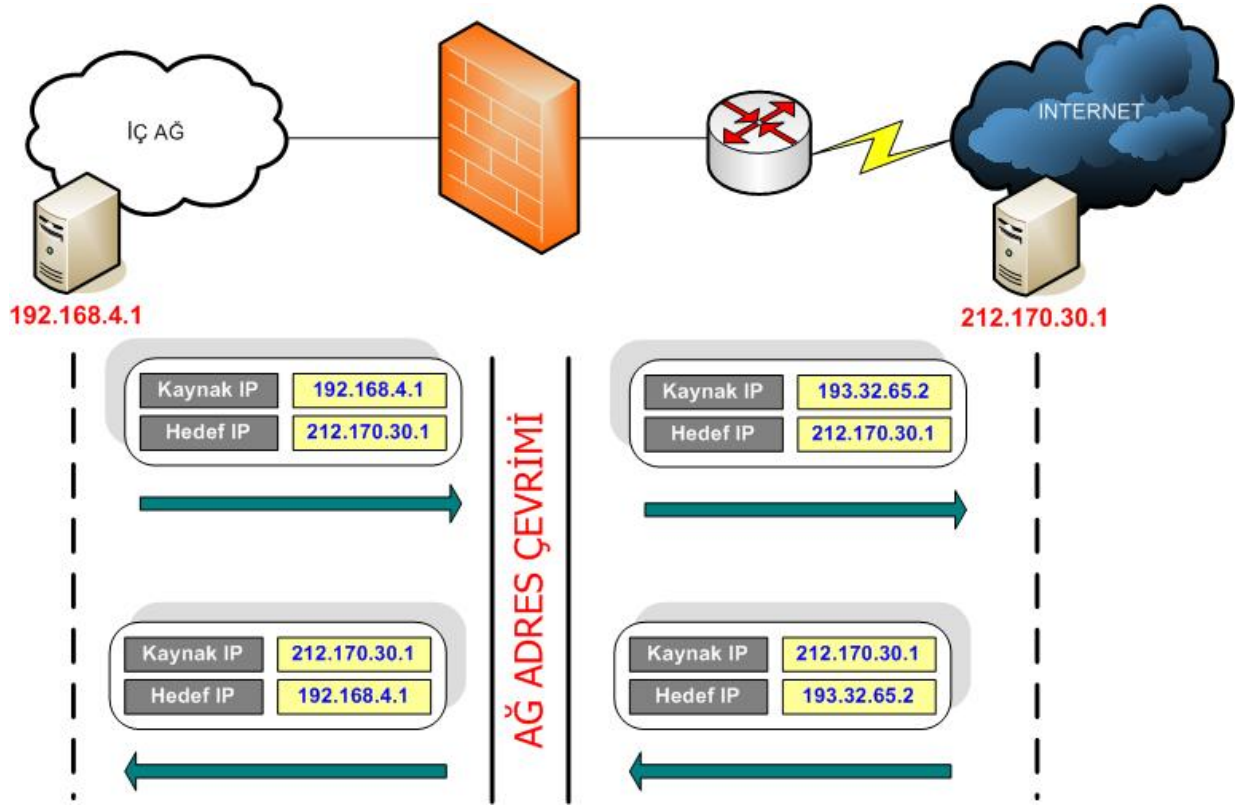
- Dinamik Ağ Adres Çevrimi: Dinamik ağ adres çevriminde iç ağdaki bilgisayarların IP adresleri tek bir IP adresine dönüştürülmektedir. Başka bir deyişle iç ağdaki bilgisayarlar aynı IP adresi ile dış dünyaya çıkmaktadır. Bunun yanında dinamik ağ adres çevrimi yapılırken port adres dönüşümü de (PAT) gerçekleştirilmektedir [4]. Yani iç ağdaki bilgisayarlar aynı IP adresi ile fakat farklı bir port numarası kullanarak dışarı çıkmaktadır. Böylelikle bağlantıların birbirinden ayırt edilmesi sağlanmaktadır. Dinamik ağ adres çevrimi iç ağdaki bilgisayarların tamamının ya da tamamına yakınının dış dünyaya çıkması için uygundur. Ancak dinamik ağ adres çevrimi, statik ağ adres çevrimine göre daha çok performans gerektirmektedir. Çünkü bilgisayarların dışarı çıkarken kullanacakları kaynak port numaraları dinamik olarak belirlenmektedir. Ancak buna rağmen dinamik ağ adres çevrimi bütün bir ağı tek bir IP adresinin arkasına gizleyebilmekte ve eldeki gerçek IP adres aralığından büyük miktarda tasarruf sağlamaktadır.

Dinamik ağ adres çevrimi, statik ağ adres çevriminden farklı olarak tek yönlü olarak çalışmaktadır. Yani sadece iç ağdaki bilgisayarlar dış dünyaya erişim sağlayabilirken dış dünyadaki bilgisayarlar iç ağa erişim sağlayamamaktadır. Bu anlamda bağlantıyı başlatan taraf sadece iç ağdaki bilgisayarlar olabilir. Dış dünyadaki bilgisayarlar sadece bu bağlantı isteklerine cevap verebilir ama asla bağlantıyı başlatan taraf olamaz. Böylelikle iç ağdaki bilgisayarların dış dünyadan korunması sağlanmış olur.

- **Port Yönlendirme:** Statik ağ adres çevriminin özelleşmiş bir halidir. Dış dünyadan iç ağdaki web, ftp, e-posta gibi sunuculara erişim sağlanması amacıyla kullanılır. Port yönlendirmede erişim sağlanmak istenen sunucuya ilişkin gerçek IP adresi, güvenlik duvarının dış dünyaya açılan IP adresi olarak belirlenir. Dış dünyadaki herhangi bir kullanıcı söz konusu sunucuya ulaşmak için aslında güvenlik duvarının gerçek IP adresine erişim sağlar. Daha sonra güvenlik duvarı gelen bağlantı isteğini inceler ve kendisi için olup olmadığına bakar. Sonuç olarak bağlantı isteği eğer güvenlik duvarı için değilse ilgili sunucuya yönlendirilir. Böylelikle iç ağdaki sunucuya dış ağdan erişim sağlanmış olur. Bu tür erişimler için statik ağ adres çevrimi yerine port yönlendirmenin kullanılması daha güvenli olmaktadır.

Şekil 8.1’de statik ağ adres çevrimine bir örnek verilmiştir. Burada iç ağdaki “192.168.4.1” IP adresli bilgisayar dış dünyadaki “212.170.30.1” IP adresli bilgisayara erişim sağlamak istemektedir. Tanımlanmış ağ adres çevrimi kuralları ile iç ağdaki bilgisayarın dışarı çıkarken gönderdiği IP paketlerinin kaynak adresi “193.32.65.2” olarak değiştirilmektedir. Böylelikle iç ağdaki bilgisayarın dış dünyaya açılabilmesi sağlanmaktadır.

Dış dünyadaki bilgisayar gönderilen IP paketini alıp hedef IP adresi “193.32.65.2” olan bir cevap IP paketi oluşturur. Bu paket güvenlik duvarına geldiğinde öncelikle ağ adres çevrimi kuralları ile karşılaştırılır. Karşılaştırma sonucunda gelen paketin hedef IP adresi “192.168.4.1” olarak değiştirilir ve gelen IP paketi iç ağdaki ilgili bilgisayara yönlendirilir. Böylelikle gelen cevap IP paketinin orijinal hedefine ulaştırılması sağlanmış olur.



Şekil 8.1 Örnek bir ağ adres çevrimi

Dış dünya ile iletişim kurulduğunda geriye dönen cevapların iç ağdaki doğru bilgisayarlara yönlendirilmesi gerekmektedir. İletişimin devam etmesi ancak bu şekilde sağlanabilir. Bu amaçla yapılan her ağ adres çevrimine ilişkin bilgiler bir tabloda tutulur. Daha sonra bu tabloya bakılarak iç ağdaki hangi bilgisayarın dönüştürülen hangi IP'ye karşılık geldiği elde edilir. Geriye dönen cevaplardaki IP adresleri, ağ adres çevrimi ile tekrar orijinal IP adreslerine dönüştürülür ve iç ağdaki ilgili bilgisayarlara iletilir.

Güvenlik duvarı gelen ve giden ağ trafiği için öncelikle ağ adres çevrimi kurallarını uygulamakta, daha sonra kural tablosuna bakmaktadır. Dolayısıyla kural tablosu oluşturulurken iç ağdaki bilgisayarların daima orijinal IP adresi kullanılmalıdır. Ağ adres çevrimi sağladığı güvenliğin yanında belirli bir performans maliyeti de getirmektedir.

9. UZAKTAN YÖNETİM

Güvenlik duvarının uzaktan yönetilmesi ve yapılandırılması için yönetim konsolu kullanılır. Yönetim konsolu, küçük bir program parçası olabileceği gibi basit bir web arabirimi de olabilir. Yönetim konsolu, güvenlik duvarının bulunduğu bilgisayardan farklı bir bilgisayar üzerinde bulundurulmalıdır. Böyle bir çalışma şekli ile güvenlik duvarının yönetimi merkezileştirilir ve güvenlik duvarına yapılabilecek yetkisiz erişimler engellenir. Yönetim konsolunda güvenlik duvarına erişmeye yetkili yönetici veya kullanıcılar tanımlıdır. Bu yönetici veya kullanıcılara belirli haklar verilmiştir. Yönetim konsolu her yönetici veya kullanıcının güvenlik duvarına, verilen haklar dâhilinde erişimine izin verir. Örneğin güvenlik duvarının yapılandırma bilgilerini sadece okumaya yetkili bir kullanıcı olsun. Yönetim konsolu bu kullanıcının, güvenlik duvarının yapılandırma bilgilerini değiştirmesine izin vermez, sadece bu bilgileri okumasına izin verir. Ayrıca yönetim konsolu güvenlik duvarına yapılan erişimleri kayıt altına alarak hangi yönetici veya kullanıcının güvenlik duvarı üzerinde nasıl bir yönetim işlemi yaptığının da takip edilmesini sağlar.

Güvenlik duvarının yönetiminde bu kadar büyük rol oynayan yönetim konsolunun da güvenliğinin sağlanması gerekmektedir. Çünkü yönetim konsolu yetkisiz biri tarafından ele geçirildiğinde güvenlik duvarı için büyük bir tehdit oluşturabilir. Yönetim konsolunun güvenli hale getirilmesi için aşağıdaki adımlar gerçekleştirilmelidir:

- Bir güvenlik duvarı ancak yöneticisinin sağlayabildiği kadar güvenlidir. Bu nedenle yönetim konsolunun konusunda tecrübeli ve eğitimli bir yönetici tarafından yönetilmesi tercih edilmelidir. Böylelikle güvenlik duvarının yönetiminden kaynaklanacak hatalar en aza indirgenebilir.
- Yönetim konsolu güvenli bir ağda konumlandırılmalı ve işletim sistemi üzerinde güvenlik sıkılaştırmaları yapılarak güvenli hale getirilmelidir.
- Yönetim konsolu üzerinde sadece ihtiyaç duyulan yöneticiler tanımlanmalı ve bu yöneticilere sadece ihtiyaç duydukları kadar hak verilmelidir. Unutulmamalıdır ki gereğinden fazla verilen her hak güvenlik duvarına yetkisiz erişim riskini arttırmaktadır [2].
- Yönetim konsolu ile güvenlik duvarı arasındaki iletişimin şifreli olarak yapılması sağlanmalıdır.

- Yönetim konsolu, belirli bir süre boyunca işlem yapılmadığı takdirde, güvenlik duvarı ile bağlantısını koparacak şekilde yapılandırılmalıdır (eğer uygulanabiliyorsa). Böylelikle kullanımda olup başında herhangi bir yönetici bulunmayan bir yönetim konsoluna yetkisiz kişiler tarafından erişim yapılması engellenebilir.
- Güvenlik duvarının sadece belirtilen yönetim konsolları aracılığıyla yönetilebilmesi için kaynak IP adresi bazında erişim kısıtlanması uygulanmalıdır. Böylelikle yetkisiz bilgisayarların güvenlik duvarının yönetim ara yüzüne erişimi engellenmiş olur.

10. AĞ TRAFİĞİ KAYITLARI

Ağ trafiğine ilişkin kayıtların tutulması hemen hemen bütün güvenlik mekanizmalarında bulunan bir özelliktir. Güvenlik duvarında da, istenen ağ trafiğine ilişkin kayıtların tutulması sağlanabilir. Gelen ve giden ağ trafiğine ilişkin olarak tutulan kayıtlar denetim kayıtları (audit trail) olarak da adlandırılmaktadır. Tutulan denetim kayıtlarının sonradan incelenmesi, ağlar arasında akan trafik hakkında bilgi verir. Böylelikle ağın izlenebilirliği ve dolayısıyla güvenliği artırılmış olur. Örneğin kurum ağına yapılan ve gözden kaçmış bir saldırı, sonradan denetim kayıtları incelenerek tespit edilebilir. Ya da ağdaki bir sunucuya yapılan erişim istekleri ile ilgili detay bilgiler (erişimi yapan bilgisayar, erişimin tarihi, erişimin sıklığı, vb...) elde edilebilir. Ayrıca denetim kayıtları belirli kriterlere göre sorgulanarak (kaynak bilgisayar, hedef bilgisayar, erişim sağlanan servis, vb...) istenen kayıtlara daha çabuk erişim sağlanabilir. Bu nedenle bir ağ yöneticisi için denetim kayıtlarının önemi büyüktür. Denetim kayıtlarından periyodik (haftalık, aylık, vb...) raporlar çıkartılarak ağa yapılan erişimlerin profili çizilebilir. Güvenlik duvarında denetim kayıtları ile ilgili olarak aşağıdakilere dikkat edilmelidir:

- Denetim kayıtlarından tam anlamıyla yarar sağlanabilmesi açısından güvenlik duvarının tarih ve saat bilgisinin doğru olarak ayarlanmış olması gerekmektedir. Bu amaçla bir NTP sunucu kullanılabilir.
- Sadece gerek görülen ve kritik olarak nitelendirilen ağ trafiklerine ilişkin kayıtların tutulması sağlanarak kayıtların gereksiz yere büyümesi engellenmelidir. Böylelikle daha küçük boyutlu kayıtlar oluşturulacağından bu kayıtların sonradan incelenmesi daha kolay olacaktır. Ayrıca güvenlik duvarında aşırı miktarda kayıt tutulması engellenerek performansın en az şekilde etkilenmesi sağlanmış olur. Çünkü kayıt tutma işlemi güvenlik duvarının performansını düşüren bir işlemdir ve gereksiz yere tutulan her bir kayıt performans düşüşlerine neden olacaktır.

- Denetim kayıtları yapılan erişimlerin kanıtları niteliğindedir. Denetim kayıtlarının kötü niyetli birinin eline geçmesi, sisteme yapılan erişimlere ait kanıtların yok olması anlamına gelmektedir. Bu nedenle, pratik olmamasına karşın, denetim kayıtlarının bir kopyası sadece okunabilir bir ortamda (örneğin bir kere yazılabilir CD) saklanmalıdır.
- Denetim kayıtları güvenlik duvarından ayrı bir bilgisayarda (örneğin yönetim konsolu üzerinde) tutulmalı ve yetkisiz erişimlerden korunmalıdır [2].
- Herhangi bir güvenlik olayının gerçekleşme aşamasında tespit edilebilme şansını arttırmak için denetim kayıtlarının düzenli aralıklarla incelenmesi gerekmektedir. Böylelikle gerçekleşen güvenlik olayının erken aşamalarda durdurulması sağlanabilir. Bu amaçla denetim kayıtlarının, en azından haftalık periyotlarla, incelenmesi ve raporlanması gerekmektedir. Bu şekilde güvenlikle ilgili olarak gerçekleşen olayların gözden kaçırılması engellenmiş olur.
- Ağ yöneticilerinin gerçekleşen kritik olaylarla ilgili anında bilgilendirilmesi için alarm mekanizması kullanılmalıdır. Örneğin alarm mekanizması aracılığıyla gerçekleşmekte olan bir saldırıya ilişkin bilgiler ağ yöneticilerine e-posta yoluyla gönderilebilir. Bu şekilde ağ yöneticilerinin gerçekleşen kritik olaylara daha çabuk müdahale etmesi sağlanır.
- Denetim kayıtlarının, eğer uygulanabiliyorsa, geriye dönük olarak yedeklenmesi büyük yararlar sağlayacaktır.

11. SALDIRI ÖNLEME MEKANİZMASI

Günümüzde saldırı önleme özelliği güvenlik duvarlarında da karşımıza çıkan bir özellik haline gelmeye başlamıştır. Normalde saldırı tespit ve engelleme sistemlerine ait olan bu güvenlik özelliği, güvenlik duvarlarına da kısıtlı olarak entegre edilmeye başlanmıştır. Saldırı tespit ve engelleme sistemleri kadar olmasa da bu özellik sayesinde güvenlik duvarları olası saldırıları tespit edip durdurabilmektedir.

Bu özellik genellikle uygulama tabanlı güvenlik duvarlarında bulunmaktadır. Bu tip güvenlik duvarları gelen paketlerin içeriğini kontrol edebilmektedir. Böylelikle zararlı içerik taşıyan paketler tespit edilip bloklanabilmektedir. Bununla birlikte tespit edilip engellenen saldırılara ilişkin kayıtlar tutulabilmektedir. Daha sonradan bu kayıtlar incelenip saldırıların niteliği hakkında fikir edinilebilir. Örneğin saldırıyı yapan bilgisayarın IP adresi tespit edilip bu IP

adresinden bundan sonra gelen bütün paketlerin bloklanması sağlanabilir. TCP – SYN seli gibi birçok servis dışı bırakma saldırısı engellenebilir. Bozuk paketlerin iç ağa sızması engellenebilir. Ya da uygulama tabanlı saldırılar durdurulabilir.

Ancak güvenlik duvarlarındaki bu özellik sınırlıdır ve sadece saldırı imzaları dâhilindeki saldırılar tespit edilip durdurulabilmektedir. Bu nedenle iç ağa gelen saldırıların tespit edilmesi ve engellenmesi için sadece bu amaç için özelleşmiş olan saldırı tespit ve engelleme sistemleri kullanılmalıdır. Bununla birlikte saldırı önleme özelliğine sahip bir güvenlik duvarının kullanılması gözden kaçabilecek saldırıların bloke edilmesini sağlayıp güvenliği arttıracaktır. Güvenlik duvarının saldırı önleme mekanizmasına ilişkin aşağıdaki adımlar gerçekleştirilmelidir:

- En son çıkan güvenlik tehditlerine karşı koruma sağlanabilmesi açısından saldırı imzaları periyodik olarak güncellenmelidir.
- Hem güvenlik duvarının yükünü hafifletmek hem de yanlış alarmların (**false positive**) sayısını azaltmak amacıyla gerek duyulmayan imzalar pasif hale getirilmelidir.
- Denetlenebilirliğin artırılması amacıyla kritik saldırılara ilişkin kayıtların tutulması sağlanmalıdır (eğer uygulanabiliyorsa).

KAYNAKÇA

- [1] Chris Brenton, Lance Spitzner, *Security 502 – Firewalls, Perimeter Protection & Virtual Private Networks*, SANS INSTITUTE, 2005
- [2] John Wack, Ken Cutler, Jamie Pole, *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology (NIST), January 2002
- [3] Dr. Thomas W. Shinder, Debra Littlejohn Shinder, Robert J. Shimonski, *Best Damn Firewall Book Period*, SYNGRESS, 2003
- [4] Chris Brenton, Cameron Hunt, *Active Defense - A Comprehensive Guide to Network Security*, SYBEX, 2001
- [5] Matthew Strebe, Charles Perkins, *Firewalls 24Seven*, SYBEX, 2002
- [6] Jason Albanese, Wes Sonnenreich, *Network Security Illustrated*, MCGRAW-HILL, 2004
- [7] Robert Stephens, Baryy J. Stiefel, Stephen Watkins, *Configuring Check Point NGX VPN-1/Firewall-1*, SYNGRESS, 2005
- [8] Rob Cameron, Brad Woodberg, Mike Swarm, Neil R. Wyler, Matthew Albers, *Configuring Juniper Networks NetScreen & SSG Firewalls*, SYNGRESS, 2007
- [9] Dr. Thomas W. Shinder, Debra Littlejohn Shinder, Martin Grasdal, *Configuring ISA Server 2004*, SYNGRESS, August 2004