GÜVENLİK DUVARI ETKİNLİK ÖLÇÜMÜ

M. Fikret OTTEKİN
ICterra Bilgi ve İletişim Teknolojileri San. ve Tic. A.Ş.
Ankara, Türkiye
fikret.ottekin@icterra.com

ÖZET

Güvenlik Duvarı sistemleri tarafından uygulanan erişim kontrol kuralları sistem yöneticileri tarafından belirlenir. Bu kapsamda güvenlik duvarı üreticisi firmalarla yapılan bakım anlaşmaları sayesinde firmaların veritabanlarından otomatik olarak indirilen kurallar da kullanılmaktadır. Dolayısı ile güvenlik duvarının performansı, kısmen de olsa üretici firmanın zararlı IP alanları ile ilgili tercihleri ve bu adresleri belirleme konusundaki yetkinliği ile orantılı hale gelmektedir. Bu çalışmada, üretici firmadan bağımsız siber güvenlik firmaları tarafından yayınlanan kara listeleri kullanarak güvenlik duvarının etkinliğini ölçen bir metodoloji tanımlanmaktadır. Güvenliği sağlanacak ağı çok noktadan dinleyen bir Saldırı Tespit Sistemi tarafından çalıştırılması öngörülen metodolojinin başarı ile uygulanması, güvenlik duvarı sistemlerinin çok daha yüksek bir güvenle kullanılmasını sağlayacaktır.

Anahtar Kelimeler: Güvenlik Duvarı, kural listesi, ölçüm, Saldırı Tespit Sistemi.

FIREWALL EFFICIENCY MEASUREMENT

ABSTRACT

Filtering rules enforced by firewall systems are designated by system administrators. In that context, due to the maintenance agreements between the user and the firewall manufacturer, filtering rules automatically downloaded by the firewall from the manufacturer's database are employed as well. Hence, the overall performance of the firewalls become correlated with the malicious domain detection competence and preferences of the manufacturer company. In this article, a methodology to measure the efficiency of firewalls, utilizing blacklists published by cyber security companies independent from the firewall manufacturer is proposed. Method should be applied with an Intrusion Detection System listening to the target network from multiple points. Successful application of the proposed method would lead to the use of firewall systems within confidence.

Keywords: Firewall, filtering rules, measurement, Intrusion Detection System.

I. GİRİŞ (INTRODUCTION)

Güvenlik duvarları halen en çok kullanılan sınır güvenliği sistemleri arasında yer almaktadır [1]. Kurumsal ağlar ile Internet arasında konuşlandırılarak ağ erişim kontrolünü sağlayan güvenlik duvarlarının kural listelerinin yapılandırılması ile ilgili olarak iki yaklaşım olasıdır:

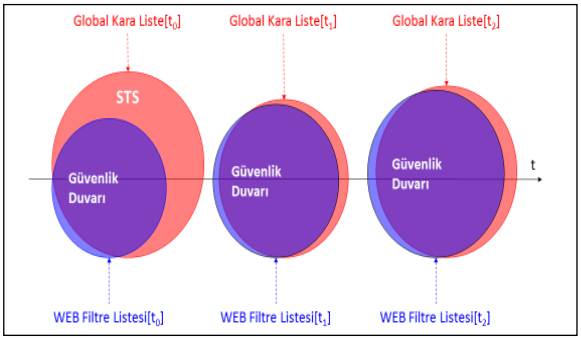
- Gevşek yaklaşım: "Yasaklanan trafiği tanımla ve engelle, kalan trafiği geçir",
- Sıkı yaklaşım: "İzin verilen trafiği tanımla ve geçir, kalan trafiği yasakla" [2].

Fiili uygulamada güvenlik duvarlarında genellikle bu iki yaklaşımın karmasından oluşan bir durumla karşılaşılmaktadır. Internet ile DMZ arasındaki trafiğin izlenmesi ve engellenmesi sıkı yaklaşımla yapılandırılırken, kullanıcı bilgisayarlarının bulunduğu kurumsal ağ ile Internet arasındaki trafik gevşek yaklaşımla yapılandırılmaktadır. Bu durum, kullanıcı bilgisayarlarına WEB'in engellenen alanlar haricinde her yerine bağlantı kurma olanağını vermekte, kullanıcıları pek çok farklı saldırı türüne açık hale getirmektedir. Dolayısı ile güvenlik duvarı tarafından engellenmesi gereken zararlı IP alanlarının devamlı olarak güncellenmesi gerekmektedir. Ancak pek çok kurum ve kuruluş bu işi hakkıyla yapacak insan kaynağına ve prosedüre sahip değildir. Internet ile kurumsal ağlar arasında akan trafiğin yönetilmesi kapsamında genellikle güvenlik duvarı ile birlikte alınan ve güvenlik duvarı platformunda çalışan "WEB filtreleme" modülü ve bakım hizmetinden faydalanılmaktadır. Güvenlik duvarı üreticisi firma tarafından belirlenen ve sistem yöneticisinin tercihi ile etkinleştirilen "Terör", "Kumar", "Ekstremizm", "Zararlı madde satışı", "Proxy" vb. kategorilerdeki kurallar aracılığı ile kurum içinden Internet'e yapılmaya çalışılan erişimler engellenmektedir.

Güvenlik duvarları periyodik olarak geliştirici firma veritabanına bağlanarak engellenecek kategorilere ait en güncel WEB filtreleme listelerini alıp kullanarak bu işlevi gerçekleştirmektedir. Böylece en önemli sınır güvenliği sistemlerinden biri olan güvenlik duvarlarının yönetilmesi konusunda yetki önemli ölçüde üretici firmaya geçmektedir.

Yukarıda sayılan kategorilerde siber uzayda faaliyet gösteren pek çok grup veya örgüt mevcut olduğundan bunların izlenmesi ve tespiti kurumsal siber güvenliğin kapsamını gerçekten aşan bir iştir. Ancak güvenlik duvarının izlenmesi, performansın ölçülmesi ve iyileştirme yollarının araştırılması kurumsal olanaklarla yapılabilir.

Güvenlik duvarlarının hızla yer ve yöntem değiştiren saldırganlara karşı ne kadar etkin koruma sağladığı belirsizdir. Esasen siber uzayda faaliyet gösteren saldırganların etkinliği de WEB filtreleme listesi de zaman içinde değişmektedir (**Şekil 1**). Herhangi bir t_0 anında saldırganları karşılama ve engelleme konusunda etkili olan filtreleme listesini üreten firmanın, iki hafta, iki ay veya iki yıl sonra da aynı başarıyı göstereceğinin garantisi yoktur. Dolayısı ile güvenlik duvarı etkinliğinin, filtreleme listesi bakımı hizmetini sağlayan firmadan *bağımsız* kuruluşlar tarafından üretilen saldırgan bilgileri kullanılarak izlenmesi son derece faydalı olacaktır.



Şekil 1. Güvenlik Duvarı WEB filtre listesinin ve STS kara listesinin zaman içinde değişimi.

Güvenlik duvarı performansından genellikle iletim hızı, desteklenen paralel oturum sayısı gibi ağa ilişkin parametreler anlaşılmaktadır [3], [4]. Güvenlik duvarı kural listesi uzunluğunu optimize ederek performansı yükseltmeyi hedefleyen çalışmalar da yapılmıştır [5]. Bu makaledeki çalışma ise güvenlik duvarı WEB filtreleme listesinin kapsayıcılığını ve etkinliğini izleyerek performansı ölçmeyi hedeflemektedir.

İzleyen bölümlerde çok portlu bir saldırı tespit sistemi ve üretici firmadan bağımsız siber güvenlik firmaları tarafından üretilen (makalenin bir sonraki bölümünde "Bağımsız kaynaklardan alınan IP kara listeleri" olarak adlandırılan) kara listeler kullanılarak ve güvenlik duvarından geçen ağ trafiği izlenerek güvenlik duvarı etkinliğinin ölçülmesi ve sınır güvenliğinin iyileştirilmesi için kullanılabilecek bir metod önerilmekte olup dört bölümde açıklanacaktır:

1. Bağımsız kaynaklardan IP kara listelerinin toplanması ve işlenmesi
2. Çok portlu saldırı tespit sisteminin kurum ağında konuşlandırılması
3. Etkinlik ölçümü
   a. Güvenlik Duvarını aşarak "bilinen saldırganlar" ile kurum bilgisayarları arasında akan trafiğin izlenmesi
   b. Güvenlik Duvarının istenmeyen trafiği engelleme etkinliğinin belirlenmesi
4. Güvenlik Duvarında ve kurum bilgisayarlarında yapılması gereken iyileştirmeler

II. BAĞIMSIZ KAYNAKLARDAN ALINAN IP KARA LİSTELERİ (IP BLACK LIST OBTAINED FROM INDEPENDENT SOURCES)

Saldırı Tespit Sistemi (STS), güvenlik duvarı etkinliğini ölçmek için çalıştırılırken bağımsız kaynaklardan alınan IP kara listelerinden faydalanacaktır. USOM zararlı bağlantılar listesine [6] benzer şekilde, pek çok yabancı kaynak sık sık güncellenen IP kara listeleri yayınlamaktadır [7], [8]. STS düzenli aralıklarla bu kaynaklara bağlanacak ve kaynaklar tarafından yayınlanan listeleri kullanarak kendi IP kara listesini oluşturacaktır.

Farklı kaynaklardan alınan listeler değerlendirilirken çeşitli yöntemlerden biri tercih edilebilir. Örneğin, kara listeler hiç bir işleme tabii tutulmadan birleştirilebileceği gibi sadece kara listelerin tamamında veya birkaç tanesinde yer alan IP adreslerinden oluşan bir kara liste de üretilebilir.

Giriş bölümünde "Bilinen Saldırganlar" olarak atıf yapılan, üçüncü tarafların IP adreslerinden oluşan ve birleştirme işleminin ardından elde edilen IP adresleri seti, bu makalenin geri kalanında "Kara Liste" olarak adlandırılacaktır.

Kara Listenin asli özelliği saldırganlar tarafından kullanılma olasılığı yüksek olan bilgisayarların adreslerini içermesidir. Bu listeye bağımsız kaynaklardan alınan adreslere ilave adresler de eklenebilir. Örneğin, farklı ağlarda konuşlu STS'ler tarafından tespit edilen imza tabanlı saldırıların yapıldığı bilgisayarların adresleri de Kara Listeye eklenebilir.

Kara Liste, kurumsal ağ ile dış dünya arasında akan trafiğin değerlendirilmesi kapsamında referans olarak kullanılacaktır. Dolayısı ile Kara Liste'nin olabildiğince çok sayıda ve birbirinden bağımsız kaynaktan toplanan bilgilerden oluşturulması etkinlik ölçümü açısından önem arz etmektedir.

III. SALDIRI TESPİT SİSTEMİNİN KURUM AĞINDA KONUŞLANDIRILMASI (ESTABLISING IDS IN THE NETWORK)

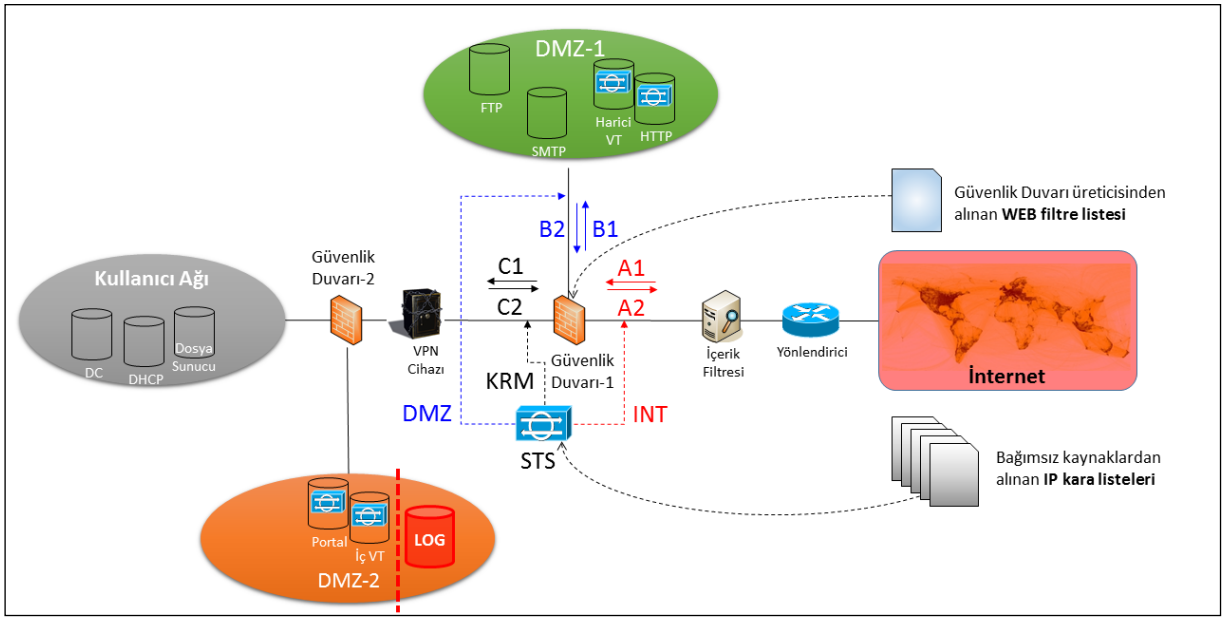
Sınır güvenliği sistemlerinin kurumsal ağlarda konuşlandırılması ile ilgili olarak bilinen pek çok topoloji mevcuttur [9]. Kurumsal ağın birden çok

noktadan, çok sayıda gerçek veya sanal sensör ile izlenmesi de halen bilinen bir uygulamadır [10].

Bu çalışmada, STS'nin kurumsal ağda konuşlandırılması konusunda Şekil 2'de gösterilen temel ağ topolojisi üstünde çalışılacaktır. Bu makalenin geri kalanında kullanılan "Güvenlik Duvarı" ifadesi ile kastedilen ve etkinliği ölçülen, Şekil 2'deki "Güvenlik Duvarı-1"dir.

STS'nin Şekil 2'de gösterilen topolojide üç port ile izleme yapması önerilmektedir.

- İlk portun Internet hattı ile Güvenlik Duvarı arasındaki trafiği,
- İkinci portun Güvenlik Duvarı ile DMZ-1 arasındaki trafiği,
- Üçüncü portun ise Güvenlik Duvarı ile Kullanıcı Ağı ve DMZ-2 arasındaki trafiği izleyecek şekilde konuşlandırılması gerekmektedir.



Şekil 2. Kurumsal Ağ Topolojisi ve Çok Portlu Saldırı Tespit Sistemi

Bu portlar sırası ile INT, DMZ ve KRM portları olarak adlandırılacaktır. Kurumun İnternet erişimine açık birden fazla DMZ kullanması halinde aynı metodoloji kullanılarak dört veya daha fazla noktadan da izleme yapılabilir.

Üç portun her birinden okunan trafiğin "kuruma gelen trafik" ve "kurumdan çıkan trafik" şeklinde ikiye ayrılarak incelenmesi, dolayısı ile altı farklı paket dizisi üstünde çalışılması gerekecektir.

Bu bağlamda STS portlarından okunan trafiğin Kaynak IP adresleri ve Hedef IP adreslerinde bulunan bilgi Tablo 1'de özetlenmiştir.

Şekil 2 ve Tablo 1 göz önünde bulundurularak aşağıdaki çıkarımlar yapılabilir:

1. Kuruma gelen trafikte (A1, B1 ve C1 dizileri) Kaynak IP adresleri, kurumdan çıkan trafikte ise (A2, B2, ve C2 dizileri) Hedef IP adresleri kurum bilgisayarlarının dış dünyada iletişim halinde olduğu bilgisayarların adreslerini vermektedir. Bu adresler Kara Liste ile karşılaştırılacaktır.
2. Hemen her kurum tarafından kullanılan NAT ("Network Address Translation") mekanizması, sadece A1 ve A2 dizilerindeki paketler incelenerek Internet ile bağlantı halinde olan kurumsal kullanıcı bilgisayarlarının belirlenmesini güçleştirmektedir [11].
3. A1, B2 ve C2 dizilerinde Kara Liste'de bulunan IP adreslerinin tespit edilmesi, kurumsal bilgisayarların Kara Liste'de bulunan bilgisayarlarla iletişim halinde olduğunu veya iletişime geçmeye çalıştığını gösterir. Bu trafik Güvenlik Duvarı tarafından engellenecek bile olsa, kurumsal bilgisayarlara kötücül yazılımların büyük olasılıkla yerleştiği anlamına gelmektedir.

A2, B1 ve C1 dizilerinde Kara Liste'de bulunan IP adreslerinin tespit edilmesi, hem kurumsal bilgisayarların Kara Liste'de bulunan bilgisayarlarla iletişim halinde olduğunu, hem de Güvenlik Duvarı'nın bu trafiği engellemediğini gösterdiğinden kurumsal güvenlik açığının mevcut olduğu ve tehdit ajanları tarafından kötüye kullanıldığı anlamına gelmektedir. Kurum açısından en büyük riski arz eden durum budur.

III. ETKİNLİK ÖLÇÜMÜ (MEASURING EFFICIENCY)

Güvenlik Duvarı etkinliği, belli zaman aralıklarında akan trafiğin izlenmesi ve trafiği oluşturan paketlerin

incelenmesi sonucunda, zaman aralıklarının sonunda hesaplanacaktır.

TABLO I. STS TARAFINDAN İZLENEN PAKET DİZİLERİ VE IP ADRESLERİ

Port	**Paket Dizisi**	**Kaynak IP Adresi**	**Hedef IP Adresi**
INT	A1. Internet'ten gelen trafik	Saldırgana ait olabilecek kurum dışı bilgisayar adresi	Güvenlik Duvarı dış IP adresi *(NAT'lanmış* kullanıcı bilgisayarı adresi veya DMZ-1 sunucu adresi)
DMZ	B1. DMZ-1'e gelen trafik		DMZ-1'de bulunan sunucu adresi
KRM	C1. Kurumsal ağa gelen trafik		Kullanıcı bilgisayarı adresi
INT	A2. Internet'e giden trafik	Güvenlik Duvarı dış IP adresi (NAT'lanmış kullanıcı bilgisayarı adresi veya DMZ-1 sunucu adresi)	Saldırgana ait olabilecek kurum dışı bilgisayar adresi
DMZ	B2. DMZ-1'den giden trafik	DMZ-1'de bulunan sunucu adresi	
KRM	C2. Kurumsal ağdan giden trafik	Kullanıcı bilgisayarı adresi	

Etkinlik ölçümünün yapıldığı zaman aralıklarında STS, A1, B1 ve C1 paket dizilerinde yer alan her paketin kaynak IP adresini, A2, B2 ve C2 paket dizilerinde yer alan her paketin ise hedef IP adresini "Kara Liste"de arayacaktır.

A1n, B1n ve C1n parametreleri, sırası ile A1, B1 ve C1 dizilerindeki paketlerden, Kaynak IP adresi kara listede bulunduğu STS tarafından belirlenen paketlerin sayısını belirtir.

A2n, B2n ve C2n parametreleri ise, sırası ile A2, B2 ve C2 dizilerindeki paketlerden, Hedef IP adresi kara listede bulunduğu STS tarafından belirlenen paketlerin sayısını belirtir.

Bu durumda, gözlemin yapıldığı zaman aralığında Güvenlik Duvarına ait "Gelen Trafik Paket Engelleme Etkinliği" (GeTrEn), Giden Trafik Paket Engelleme Etkinliği" (GiTrEn) ve "Toplam Trafik Paket Engelleme Etkinliği" (ToTrEn) parametreleri şu şekilde hesaplanabilir:

$$GeTrEn = (A1n - (B1n + C1n)) / A1n, \quad (1)$$

$$GiTrEn = ((B2n + C2n) - A2n) / (B2n + C2n), \quad (2)$$

$$ToTrEn = ((A1n + B2n + C2n) - (A2n + B1n + C1n)) / (A1n + B2n + C2n) \quad (3)$$

Gelen trafik kapsamında A1n'in, giden trafik kapsamında (B2n + C2n)'in, toplam trafik kapsamında ise (A1n + B2n + C2n)'in gözlemin yapıldığı zaman aralığında "sıfır" olarak ölçülmesi mümkündür. Bu durumda Güvenlik Duvarının engellemesi gereken trafik tespit edilemediğinden, etkinlik ölçümünün yapılması da söz konusu olmayacaktır (Yukarıdaki formüllerde "sıfır ile bölme hatası" ortaya çıkacaktır).

Etkinlik ölçümü yapılırken paket sayısı yerine toplam veri uzunluğu da kullanılabilir. Bu durumda,

A1k, B1k ve C1k parametreleri, STS tarafından Kaynak IP adresi kara listede bulunduğu belirlenen paketlerin uygulama katmanı yüklerinin toplam uzunluğunu, yani kurum bilgisayarlarına iletilen toplam kötücül veri/dosya/komut uzunluğunu belirtir.

A2k, B2k ve C2k parametreleri ise STS tarafından Hedef IP adresi kara listede bulunduğu belirlenen paketlerin uygulama katmanı yüklerinin toplam uzunluğunu, yani kurum bilgisayarlarından gönderilmek üzere olan toplam veri/dosya/mesaj uzunluğunu (spam e-posta ve eki, sızdırılan veri, Botnet C/C merkezine gönderilen yanıtlar vb.) belirtir.

Bu durumda, gözlemin yapıldığı zaman aralığında Güvenlik Duvarına ait "Gelen Trafik Veri Engelleme Etkinliği" (GeTrEk), Giden Trafik Veri Engelleme Etkinliği" (GiTrEk) ve "Toplam Trafik Veri Engelleme Etkinliği" (ToTrEk) parametreleri şu şekilde hesaplanabilir:

$$GeTrEk = (A1k - (B1k + C1k)) / A1k \quad (4)$$

$$GiTrEk = (A1k - (B2k + C2k)) / A1k \quad (5)$$

$$ToTrEk = ((A1k + B2k + C2k) - (A2k + B1k + C1k)) / (A1k + B2k + C2k) \quad (6)$$

$$GeTrEn, GiTrEn, ToTrEn, GeTrEk, GiTrEk, ToTrEk \in [0,1]$$

Etkinlik parametreleri oran gösterdiğinden 0 ile 1 arasında gerçek sayılardır. Etkinliğin "sıfır" olarak ölçülmesi Güvenlik Duvarı'nın Kara Liste'den gelen trafiği engelleme konusunda tamamen etkisiz, "bir" olarak ölçülmesi ise tamamen etkili olduğunu gösterecektir.

Engelleme etkinliklerinin daha da çeşitlendirilmesi mümkündür. Örneğin, kara listede adresi yer alan (bilinen saldırganların kullandığı) bilgisayarlarla gerçekleşen iletişim yerine bilinen saldırı imzalarını içeren paketlerin ne kadarının engellendiği ölçülebilir.

Etkinlik ölçümünün doğru şekilde yapılması için dikkat edilmesi gereken en önemli husus, sensörler arası zaman senkronizasyonudur. Yukarıda tanımlanan A*, B* ve C* parametrelerinin aynı zaman aralığında hesaplanması, sonuçların doğruluğu açısından önem arz etmektedir. Zaman senkronizasyonunun tam olarak sağlanması halinde bile Güvenlik Duvarının işlem süresi dolayısı ile bazı paketlerin kaybolmuş gibi

gözükmesi ve Güvenlik Duvarı tarafından engellenmediği halde engellenmiş gibi gözükmesi olasıdır. Bu durumda etkinlik ölçümü, bazı zaman aralıklarında gerçek etkinlikten daha yüksek, takip eden zaman aralığında ise gerçek etkinlikten daha düşük hesaplanabilir. Zaman aralığının uzatılması halinde problem büyük ölçüde azalacaktır.

Güvenlik Duvarı etkinliğinin zaman içindeki seyri izlenerek, henüz Güvenlik Duvarı kural listesine girilmemiş saldırgan adreslerinden kurum ağına yapılan erişim denemelerinin yoğunluğundaki değişim gözlenebilir.

IV. İYİLEŞTİRME ÇALIŞMALARI (IMPROVEMENT STUDIES)

Bir önceki bölümde de belirtildiği gibi, A2, B1 ve C1 dizilerinde Kara Liste'de bulunan IP adreslerine raslanması, kurumsal güvenlik açığının mevcut olduğu, daha doğrusu Güvenlik Duvarında kural listesi ve WEB filtreleme listesinden oluşan bütünün güncel olmadığı anlamına gelmektedir.

Hem bu dizilerde, hem de "Kara Liste"de yer alan adresler, kurum bilgisayarları ile aralarında gerçekleşen trafikteki paket sayısı ve/veya toplam veri hacmi büyüklüğüne göre sıralanabilir. Gerçekleşen sıralama göz önünde bulundurularak belirlenen adreslerin Güvenlik Duvarı kural listesine eklenmesi ve engellenmesi yerinde olacaktır.

İkinci olarak, kara listedeki bilgisayarlarla iletişime geçen kurum bilgisayarlarının belirlenmesi ve bu bilgisayarlarla saldırganlar arasında gerçekleşen iletişimden kaynaklanan sorunların (AV taraması, formatlama vb. işlemlerle) düzeltilmesi gerekecektir.

Kara listedeki bilgisayarlarla iletişime geçen kurum bilgisayarları şunlardır:

1. B1 ve C1 paket dizilerinde, Kaynak IP Adresi Kara Liste'de bulunan paketlerin, Hedef IP adresini kullanan kurum bilgisayarları (sunucular ve kullanıcı bilgisayarları).
2. A2 paket dizisinde, Hedef IP Adresi Kara Liste'de bulunan paketlerin, Kaynak IP adresini kullanan kurum bilgisayarları. Güvenlik duvarında muhtemelen çalıştırılmakta olan NAT mekanizması dolayısı ile hangi kurum bilgisayarı olduğu doğrudan anlaşılamayacaktır. Kullanıcı bilgisayarını tam olarak tespit etmek için NAT kayıtları veya gözlemin yapıldığı zaman aralığında kaydedilen B2 ve C2 paket dizileri ile korelasyon sağlanması gerekecektir.

Yukarıda tanımlanan metodoloji kullanılarak yapılan izleme sonucunda Tablo 2'de gösterilene benzer bir sonuç oluşabilir:

Yukarıdaki tablodaki parametrelerden ToTrEn ana gösterge olmakla birlikte, bu parametrenin Güvenlik Duvarına gelen Kara Liste paket sayısı (A1n + B2n + C2n) ile birlikte değerlendirilmesi gerektiği unutulmamalıdır. ToTrEn, toplam paket sayısının çok düşük olduğu durumlarda, yüksek olduğu durumlardaki kadar anlamlı olmayacaktır.

TABLO II. GÜVENLİK DUVARI ETKİNLİĞİ İZLEME BULGULARI

Sıra no.	İç (Kurumsal IP) Adresi	Dış (Kara Liste) IP Adresi	Güvenlik Duvarı Kural Listesinde ve/veya WEB filtreleme listesinde	Engellenen Paket Sayısı	Geçen Paket Sayısı
1	148.15.62.11	81.88.178.14	VAR	32345	0
2	148.15.62.13	81.88.178.14	VAR	31876	0
3	172.25.65.76	199.23.65.11	VAR	1455	0
4	172.25.65.93	204.15.77.23	YOK	0	2208
5	172.25.65.95	213.44.18.2	YOK	0	11452
-	Güvenlik Duvarından geçen Kara Liste paket sayısı *(A2n + B1n + C1n)*			-	13660
-	Güvenlik Duvarına gelen Kara Liste paket sayısı *(A1n + B2n + C2n)*			79336	
-	Engellenen Kara Liste paket sayısı *((A1n + B2n+C2n)-(A2n+B1n+C1n))*			65676	-
-	**ToTrEn ("*Toplam Trafik Paket Engelleme Etkinliği*")**			**0,82782 (%82,8)**	

Kaynak kısıtı vb. nedenlerle STS ile üç portlu izlemenin mümkün olmadığı, ancak iki portlu izlemenin yapılabileceği durumlarda, bu makaledeki topolojide etkinlik ölçümü yapılamayacaktır (Güvenlik Duvarının iki portlu olarak kulanıldığı durumda etkinlik ölçümü yapılabilir). Güvenlik Duvarı etkinlik ölçümü yapılamasa da, STS B* ve C* paket dizilerinin izlenebileceği DMZ ve KRM portlarına bağlanabilir. Bu durumda, Kara Liste ile konuşmaya çalışan kurum bilgisayarlarının hangileri olduğu, herhangi bir korelasyon çalışması yapılmadan bu paket dizilerinden belirlenebilecek ve bu bilgisayarlarla ilgili düzeltici önlemler devreye sokulabilecektir.

V. SONUÇ (CONCLUSION)

Güvenlik Duvarı sisteminin zaman zaman kurum ağına yapılan kötü niyetli erişimleri engelleme konusunda düşük performans göstermesi mümkündür. Bu çalışmada tarif edilen etkinlik ölçüm metodolojisi aracılığı ile çok portlu bir STS kullanılarak kurumsal Güvenlik Duvarı'nın Kara Liste trafiğini engelleme etkinliği ölçülmektedir. Ölçüm metodolojisinin merkezinde, Güvenlik Duvarı üreticisinden bağımsız kuruluşlar tarafından üretilen verilerden oluşturulan Kara Liste yer almaktadır.

Güvenlik Duvarı etkinliği, Güvenlik Duvarı'na tüm portlardan giren ve çıkan trafiğin Kara Liste göz önünde bulundurularak ve bu makalede tarif edilen metodoloji kullanılarak değerlendirilmesi sonucunda ölçülmektedir. Kara Listede bulunan adreslerle iletişime izin vermesi Güvenlik Duvarı etkinliğinin düşük, izin vermemesi ise etkinliğin yüksek olduğunu göstermektedir. Bu parametrenin sistem yöneticileri tarafından izlenmesi, Güvenlik Duvarı etkinliğinde

gerçekleşen düşüş ve yükselişlerin algılanmasını sağlayarak kuruma bu sorunla ilgili düzeltici/önleyici faaliyetlerin gerçekleştirilmesi gerektiğini anımsatabilir.

Dolayısı ile çok portlu bir STS'nin bu metodolojiyi çalıştıracak uygulama yazılımı ile donatılması, yapılandırılması ve kurum ağında konuşlandırılması, WEB filtreleme hizmeti veren firmanın performansı ve Güvenlik Duvarının etkinliği ile ilgili fikir vererek, sistemin çok daha bilinçli bir şekilde kullanılmasını sağlayacaktır.

TEŞEKKÜR

Yazar, bildirinin hazırlanmasını destekleyen ICterra Bilgi ve İletişim Teknolojileri A.Ş.'ye teşekkürlerini sunar.

Yazar, bildiriye konu olan "Güvenlik Duvarı Etkinlik Ölçümü" metodu ile çözümlenmeye çalışılan ihtiyacın belirlenmesine ve Global Kara Listelerle ilgili çalışmaların başlamasına vesile olan "Yeni Nesil Akıllı Tehdit Algılama ve Engelleme Siber Güvenlik Sistemi (ATES)" projesini destekleyen TÜBİTAK Sanayi Ar-Ge Projeleri Destekleme Programı'na teşekkürlerini sunar.

KAYNAKLAR

[1] T. Grudziecki, P. Jacewicz ve J. Łukasz, «Proactive Detection of Security Incidents,» ENISA, Heraklion, 2012.

[2] R. Contreras, «Best practices for firewall rules configuration,» 20 06 2016. [Çevrimiçi]. https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration/. [Erişildi: 23 6 2017].

[3] D. Newman, «RFC 2647 Benchmarking Terminology for Firewall Performance,» 8 1999. [Çevrimiçi]. Available: https://tools.ietf.org/html/rfc2647. [Erişildi: 23 6 2017].

[4] B. Hickman, D. Newman, S. Tadjudin ve T. Martin, «RFC 3511 Benchmarking Methodology for Firewall Performance,» 4 2003. [Çevrimiçi]. Available: https://tools.ietf.org/html/rfc3511. [Erişildi: 23 6 2017].

[5] E. W. Fulp ve S. J. Tarsa, «Methods, Systems and Computer Program Products for Network Firewall Policy Optimization». Patent: EP 1 864 226 B1, 15 5 2013.

[6] «Zararlı Bağlantılar,» USOM, TR-CERT, [Çevrimiçi]. https://www.usom.gov.tr/zararli-baglantilar/1.html. [Erişildi: 2017 6 15].

[7] «abuse.ch SSL IPBL for Suricata / Snort,» [Çevrimiçi]. https://sslbl.abuse.ch/blacklist/sslipblacklist.rules. [Erişildi: 19 6 2017].

[8] «DShield.org Recommended Block List,» [Çevrimiçi]. Available: https://www.dshield.org/block.txt. [Erişildi: 17 6 2017].

[9] K. Stouffer, V. Pillitteri ve S. Lightman, «5.5 Network Segregation,» *Guide to ICS Security*, Gaithersburg, National Institute of Standards and Technology, 2015, sf. 55-61.

[10] «Decide where to deploy Sensors and in what operating mode,» *McAfee Network Security Platform 8.3, IPS Administration Guide Revision H*, Intel Security, 2017, sf. 48-49.

[11] «Firewalls and Network Address Translation (NAT),» [Çevrimiçi]. Available: https://notes.shichao.io/tcpv1/ch7/. [Erişildi: 23 6 2017].