T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GÜVENLİK DUVARI KURALLARINA AİT ANOMALİLERİN TESPİTİ VE OPTİMİZASYONU

YÜKSEK LİSANS TEZİ

Abdu Endris MOHAMMED

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Doç. Dr. İbrahim ÖZÇELİK**

Ekim 2018

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GÜVENLİK DUVARI KURALLARINIA AİT ANOMALİLERİN TESPİTİ VE OPTİMİZASYONU

YÜKSEK LİSANS TEZİ

Abdu Endris MOHAMMED

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞM MÜHENDİSLİĞİ

Bu tez 30.10.2018 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr. Resul KARA Jüri Başkanı	Doç. Dr. İbrahim ÖZÇELİK Üye	Dr.Öğr. Üyesi Murat İSKEFİYELİ Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Abdu Endris MOHAMMED

30.10.2018

TEŞEKKÜR

Yüksek lisans ögrenimim sırasında ve tez çalısmalarım boyunca gösterdigi her türlü destek ve paylastıgı görüslerinden dolayı çok degerli hocam Doç. Dr. İbrahim ÖZÇELİK'e en içten dileklerimle çok tesekkür ederim. Sakarya Üniversitesi Bilgisayar ve Bilişim Fakültesinin tüm çalışanlarına da teşekkürlerimi sunuyorum.

Ayrıca Türkiye Cumhuriyeti Yurtdışı Türkler ve Akraba Topluluklar Başkanlığı eğitimi desteklediği için teşekkür ederim.

Son olarak, bu çabada ve tüm eğitim kariyerimde sevginizi ve desteğinizi veren herkese çok minnettarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

ARP	: Address Resolution Protocol
ASCII	: American Standard Code for Information Interchange
DHCP	: Dynamic Host Configuration Protocol
DNS	: Domain Name System
EBCDIC	: Extended Binary Coded Decimal Interchange Code
FDDI	: Fiber Distributed Data Interface
FTP	: File Transfer Protocol
HTTP	: Hyper Text Transfer Protocol
HTTPS	: Secure Hyper Text Transfer Protocol
ICMP	: Internet Conrol Message Protocol
IDS	: Intrusion Detection System
IPsec	: Internet Protocol Security
P2P	: Peer Two Peer
POP3	: Post Office Protocol
SMTP	: Simple Mail Transfer Protocol
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
–	: Range of IP or port numbers
*	: All IP addresses or port numbers

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Güvenlik duvarı, anomali sezme, sıkılaştırma, güvenlik duvarı kural optimizasyonu, siber güvenlik

Güvenlik duvarları, bir ağa gelen veya çıkan her bir paketi inceleyerek bir kuruluşun güvenlik politikasını güçlendirmeye yardımcı olan ağ cihazlarıdır. Günümüzde ağa bağlı sistemlerde güvenlik ve ağ performansı giderek daha kritik hale gelmekte ve güvenlik duvarının verimliliğine büyük ölçüde bağlı olmaktadır. Bu paket eşleştirme işlemi, ilk eşleşme bulunana kadar kuralları gelen bir paketin başlığı ile sıralı olarak karşılaştırarak gerçekleştirilir. Paket eşleştirme kuralında belirtilen eyleme bağlı olarak daha sonra ağa erişim izni verilecek veya yasaklanacaktır. Paket eşlemede kurallar genişledikçe ve karmaşıklaştıkça daha fazla zaman almaktadır. Bu nedenle, gelen paketler için uygun eylemin belirlenmesi mümkün olduğunca çabuk yapılmalıdır.

Bu tez çalışmasında, öncelikle raining 2D kutu model yapısal analiz yöntemini kullanarak güvenlik duvarı kural analizi yapılmaktadır. Sonrasında güvenlik duvarı kurallarını optimize etmek için Fazlalık Kural Anomalisi Tespiti ve Çözümü Algoritması ve Gölge Kural Anomalisi Tespiti ve Çözümü Algoritmasını kullanarak güvenliği artırmak ve paket eşleştirme süresini azaltmak için yeni bir bütünsel bir yaklaşım sunulmaktadır. Optimizasyon işlemi, çakışan kuralları otomatik olarak algılayıp kaldırarak ve ardından paket eşleştirme sıklıklarına göre yeniden sıralayarak yapılır. Son olarak çatışmasız bir kural seti elde edildikten sonra, güvenlik duvarı tarafından sürekli kontrol edilen baskın kuralların, tabloda mümkün olduğu kadar üstte olacağı ve güvenlik duvarı tarafından kontrol edilmeyen veya daha az kontrol edilen kuralların ise tabloda altta olacağı bir Eşleştirme Zaman Optimizasyonu algoritması ile paket eşleştirme süresi azaltılmaktadır.

OPTIMIZATION AND RESOLUTION OF ANOMALIES IN FIREWALL RULES

SUMMARY

Keywords: Firewall, anomaly detection, hardening, firewall rule optimization, cyber security

Security and network performance are becoming increasingly critical in network systems and are highly dependent on efficiency of the firewall. For each packet which enters or leaves the network, a decision has to be made by the güvenlik duvarı. Firewalls are network devices that help enforce an organizations' security policy by inspecting every packet arriving or departing a network. This packet matching process is accomplished by sequentially comparing the rules with the header of an arriving packet until the first match is found. The packet will then be allowed or banned access to the network depending on the action specified in the matching rule. Packet matching becomes more tedious and time consuming as rules become large and more complex. Therefore determining the appropriate action for arriving packets must be done as quickly as possible.

In this resarch we have addressed this problem using raining 2D-box model structural analyzing method and present a new holistic approach to improve the security and packet matching cost of a firewall by optimizing the firewall ruleset. The optimization process is done by automatically detecting and removing conflicting rules using anomaly detection and resolution algorithms for redundancy and shadowing anomalies. After getting the conflict free rules an optimize packet matching time algorithm is used to reordering them based on their packet matching frequency. A web based application called FADRO (Firewall Anomalies Detection, Resolution and Optimization) is developed to show how the proposed method detect and resolve all those conflicting rules and get anomaly free ruleset. After getting a conflict-free ruleset a reordering technique is done to identify a set of few dominant and decaying rules within a given specific period of time. Then the dominant rules which are continuously checked by the güvenlik duvarı will be as top in the table as possible and decaying rules which are not checked or slightly checked by the güvenlik duvarı would be as bottom of the rule set as possible. Finally, we have recommended different types of firewall hardening mechanisms to enhance the performance of the firewall.

BÖLÜM 1. GİRİŞ

Bilgi işlem ve ağ teknolojilerinin ortaya çıkışıyla, iş servislerini daha etkin ve verimli bir şekilde kullanmamızı sağlamaktadır. Teknoloji ile birlikte çalışmaya başlandığı zaman, daha üretken ve başarılı olunmaktadır. İnternet, birbirine bağlı ağlardan oluşan çeşitli bilgi ve iletişim olanakları sağlayan, küresel bir bilgisayar ağıdır. İnternet, bilgi otobanı ve bilgi bankası katlanarak arttığı için gündelik hayata ve İnternet bağımlılığının hayati bir parçası haline geldi.

Bilgisayarlar ağ üzerinde iletilen ve bilgisayarlarda depolanan önemli sayısal verilerimizin artmasıyla birlikte, İnternet, saldırganlar için önemli bir alan haline gelmektedir. Bilgisayar güvenliği ve ağ performansı gittikçe artmakta ve eskisinden daha önemli ve kritik hale gelmektedir. Bilgi işlem alanındaki tüm gelişmeler, verilerin güvenliği sağlanmazsa etkisiz ve geçersiz hale gelmektedir. Bu nedenle, İnternet üzerinden dolaşan paketlerin güvenliğini sağlamak için profesyonel topluluğun ağ trafiğini kontrol etmek için büyük çabalar göstermektedir.

Ağ güvenliği, güvenlik duvarının verimliliğine büyük ölçüde bağlıdır. Güvenlik duvarları, çoğu işletme ve kurumda özel ağların güvenliğini sağlamak amacıyla ağ trafiğinin akışını kontrol etmek için en yaygın olarak kullanılan güvenlik mekanizmasıdır. Güvenlik duvarı, bir ağa gelen veya çıkan her paketin incelenmesi ve istenmeyen saldırgan şirketin güvenli ağına bağlanmasını önleyerek bir kuruluşun güvenlik kurallarını uygulamaya yardımcı olmaktadır. Güvenlik duvarı yerel bir özel ağ ile internet arasında izolasyon sağlar ve bir ağ ile dış dünyayı birbirinden ayıran bir çit olarak düşünülebilir.

Güvenlik duvarı, üzerinde yapılandırılan kurallara dayanarak güvenli bir ağın sınırları boyunca paketlerin geçişini kontrol eder ve ihlalcilerinin çoğunluğu güvenlik duvarı

kurallarının yanlış konfigürasyonundan kaynaklandığının açıkça görülmektedir. Bu ihlallerinin çoğu insan hatasından kaynaklanan problemdir. Gartner'ın yaptığı bir araştırmada, 2020 yılına kadar, güvenlik duvarı ihlallerinin% 99'unda, kusurların değil basit güvenlik duvarı yanlış konfigürasyonlarından kaynaklı olacağı öne sürülmektedir [1].

Güvenlik duvarlarının yanlış yapılandırılması, özel ağın saldırganlara karşı savunmasız kalmasına neden olmaktadır. IBM Security Services'in 2014 Siber Güvenlik İstihbarat İndeksi, yanlış yapılandırmaların en çok insan hatasından kaynaklandığını bildirmektedir. Hatalı yapılandırmalar, bilgisayar korsanlığı tarafından hiçbir zaman kullanılmasa bile ciddi ticari sorunlara neden olabilmektedir. Temmuz 2015'te United Airlines'taki yönlendiricinin yanlış yapılandırması, ABD havaalanlarında iki saatten fazla, 90'a yakın uçağın havalanmamasına attı - uçuşlara ve olumsuz tanıtımların yaygınlaşmasına neden olmuştur [2].

1.1. Tez Motivasyonu

Bir güvenlik duvarı yapılandırma işlemi, kuralların karmaşıklığı ve bağımlılığı nedeniyle zorlu, sıkıcı ve hataya eğilimli bir süreçtir. Güvenlik duvarı ilk savunma mekanizması olarak kullanmanın yanı sıra güvenlik duvarıun yanlış konfigürasyonu, özel ağın saldırganlara karşı savunmaz kalmasına neden olabilir. Güvenlik duvarı tarafından sağlanan güvenlik korumasının etkinliği esas olarak güvenlik duvarın konfigürasyon kurallarının kalitesine bağlıdır. Bir güvenlik duvarı politikası, genellikle birbirleriyle mantıksal olarak gizemli binlerce kuraldan oluşabilir ve başka birçok kurallarla çak ilişkilendirilebilir.

Güvenlik duvarı kurallarının net ve çatışmasız tutmak her zaman zor, sıkıcı ve zahmetli bir iştir. Çeşitli nedenlerden dolayı güvenlik duvarın, tek bir kurala veya uzun süre kontrol edilmeyen kurallara veya ilişkisiz olan ve ağda veya güvenlik duvarı kurallarında herhangi bir etkisi olmayan kurallara sahip olmak için birbiriyle birleştirilebilen yinelenen kurallar veya kurallar içerebilir dağınık olarak

düzenlenebilir. Bu nedenle, güvenlik duvarlarının güvenli olması için etkili politika yönetimi mekanizmaları ve araçları önemlidir.

1.2. Tezin Amacı

Güvenlik duvarı düzgün yapılandırılması ile ağın, saldırıların ve güvenlik risklerinin çoğunu karşılayabilmesine karşın, güvenlik duvarının yanlış konfigürasyonu ve güvenlik duvarı saldırılarını korumak için çok fazla zaman, para ve diğer kaynaklar boşa gitmektedir.

Ağ güvenliği politika yönetiminin pazar lideri AlgoSec tarafından yapılan ankete göre, en yaygın güvenlik ağ geçitleri güvenlik duvarı ve diğer ağ cihazları, güvenlik duvarı için en büyük yatırım gerektiren ve çoğu ağ kesintisine neden olmaktan sorumlu tutuluyor [3]. Temmuz 2015'te United Airlines'ta yapılan yanlış yapılandırma, iki saatten fazla bir süredir ABD havaalanlarında 90'tan fazla uçağın temelini attı - uçuşlara ve olumsuz tanıtımların yaygın şekilde bozulmasına neden oldu [4]. Bu ve çeşitli nedenlerden ötürü, güvenlik duvarı kurallarının konfigürasyonu önceden ve sonrasından sürekli olarak düzenli bir şekilde izlenmesi gerekmekte ve daha iyi bir mekanizmanın geliştirilmesi gerekmektedir

Yukarıda verilen gerekçelere bağlı olarak tezin amacı güvenlik duvarı kurallarını optimize edip güçlendirerek güvenlik duvarını ve paket eşleme zamanını geliştirecek bir algoritma ve bütüncül bir yaklaşım tasarlamak ve uygulamaktır. Bu bütüncül yaklaşım, çakışan kuralları tespit edip çözerek, benzer işlevlere sahip kuralları kaldırarak, aynı hedef trafiğe sahip kuralları birleştirerek ve kural listesinde mümkün olan en üstte eşleşen kuralları içeren kuralları yeniden düzenleyerek gerçekleştirilecektir.

1.3. Tezin Katkısı

Güvenlik duvarı olmayan bir ağın güvenliği olduğunu düşünmek zordur. Güvenlik duvarın güvenliği esas olarak üzerinde yapılandırılan kurallara bağlı olduğundan,

kuralları doğru bir şekilde yapılandırmak ve uygun bir kural yönetiminin uygulanması her zaman çok önemlidir. Bu çalışma, otomatik eşzamanlı güvenlik duvarı kuralları optimizasyonu ve sıkılaştırma tekniğinin tasarlanmasını paket eşleme süresinin toplam gecikmesini en aza indirgeyerek ve bir ağın güvenliğini artırmasını önermektedir. Böylece, gereksiz kuralları otomatik olarak algılayan ve çözen Fazlalık Kural Anomalisi Tespiti ve Çözümü Algoritması, alakasız kuralları kaldıran, benzer işleve sahip kuralları bir araya getiren Gölge Kural Anomalisi Tespiti ve Çözümü Algoritması ve ayrıca paket eşleşmesinin yüksek frekanslı kuralların mümkün olduğunca güvenlik duvarı listesinde olacağı kuralları yeniden düzenleyen Paket Eşleştirme Zaman Optimizasyonu Algoritması algoritmaları geliştirilip kurumsal bir ağ sistemi üzerinde hem siber güvenliğin artırılmasına hem de güvenlik duvarının paket eşleştirme süresinin azaltılmasına katkı sağlanmıştır.

1.4. Tez Organizasyonu

Bu tez 6 bölüme ayrılmıştır. Bölüm 1 bu giriş ve ilgili çalışmalar kısımıdır. Bölüm 2'de çalışmanın teorik altyapısı açıklanmış ve değerlendirilmiştir. Bölüm 3'te güvenlik duvarı politikasının yapısal analizi ve önerilen sistemleri analiz etme ve yönetme yolları tartışılmıştır. Bölüm 4'te tezin ana kısmı oluyor. Bölüm 5'te, çalışmanın ve sonucunun özetli ve analizi yapılmıştır. Bölüm 6'da ise, sonuç ve gelecekteki çalışmalara öneride bulunarak bitirilmiştir.

BÖLÜM 2. TEORİK ARKA PLAN

2.1. Bilgisayar Ağları

Gelişmekte olan bilgi işlem ve ağ teknolojilerinin ortaya çıkması, iş hizmetlerini daha verimli ve etkin bir şekilde gerçekleştirmemizi sağlamıştır. Bir teknoloji ile çalışmaya başladığımızda, daha üretken olmaya başlayabiliriz. Hepimizin parçası olduğumuz insan ağları gibi, bilgisayar ağları da bilgi ve kaynakları paylaşmamıza izin veriyor. Bir bilgisayar ağı, ağ kaynaklarının paylaşılması için birbirine bağlanan iki veya daha fazla bilgi işlem cihazından oluşur. Sadece iki bağlı bilgisayardan oluşan en temel bilgisayar ağı, ek bilgisayarlar katıldığında ve kaynaklarını paylaştıklarında kaynaklarını eklediklerinde genişletilebilir ve kullanılabilir hale gelebilir. İşletmede, ağlara bağımlılık, evlerde veya okullarda olduğundan daha yaygındır. Ağlar bireylerin ve işletmelerin paradan tasarruf etmelerine yardımcı olur, ancak aynı zamanda gelir yaratmaya da yardımcı olur. Günümüzde, orta derecede gelişmiş ülkelerde bile hemen hemen tüm bireyler, evlerinin tamamında ağ bileşenlerine sahip olacaklar

Ağlar coğrafi sınırlara (sinyalin kapsadığı mesafete) göre sınıflandırılır ve literatürde beş temel coğrafi sınıflandırma bulunmaktadır: Bunlar:

1. Vücut Alan Ağı (Body Area Network, BAN)
2. Kişisel Alan Ağı (Personel Area Network, PAN)
3. Yerel Alan Ağı (Local Area Network, LAN)
4. Şehirsel Alan Ağı (Metropolitan Area Network, MAN)
5. Geniş Alan Ağı (Wide Area Network, WAN)

Konfigürasyonlarına göre, ağlar iki tür, eşler arası ve istemci / sunucu ağları olarak sınıflandırılır. Eşler arası ağlar daha az sayıda bilgisayarın dâhil olduğu ve sıkı

güvenliğe ihtiyaç duyulmadığı durumlarda daha yaygın olarak uygulanır. P2P'de tüm bilgisayarlar aynı statüye sahiptir ve birbirleriyle eşit düzeyde iletişim kurarlar. İstemci / sunucu ağları daha büyük ağlar için daha uygundur. Merkezi bir bilgisayar veya sunucu, ağda paylaşılan dosya ve uygulamalar için depolama yeri görevi görür ve ayrıca, istemci bilgisayarlar olarak adlandırılan diğer bilgisayarların ağ erişimini de denetler.

2.2. TCP / IP Modeli

Ağ modeli, bir ağdaki iki bilgisayar arasındaki iletişimi temsil eder. Ağ mimarisini katmanlara ayırmaya dayanır. Her katmanın kendi işlevleri vardır ve doğrudan yukarıdaki ve altındaki katmanlarla etkileşim kurar.

TCP / IP, verilerin paketlere nasıl bölüneceğini, hedefe nasıl yönlendirileceğini, iletileceğini ve yönlendirilmesini sağlayan uçtan uca iletişim sağlayarak, verilerin internet üzerinden nasıl değiştirileceğini belirtir. TCP / IP modeli dört temel katmandan oluşur. Bunlar Uygulama Katmanı (Application layer), Transport layer (iletim katmanı), Internet layer (İnternet katmanı) ve Network Access layer (ağ erişim katmanıdır). Aşağıda detayları verilen her katman, üstündeki ve altındaki katmanda belirli bir hizmet sağlamaktan sorumludur [5].

Uygulama Katmanı - Application Layer: Bu katman, TCP / IP modelinin en üst katmanıdır. Belirli uygulamalar için veri gönderir ve alır. Protokolleri, DNS, HTTP, SMTP, FTP, POP3 ve çok daha fazlasını içerir.

İletim Katmanı - Transport layer: Bu katman, uçtan uca iletişim aygıtları arasında uygulama katmanı hizmetlerini taşımak için bağlantı yönelimli veya bağlantısız hizmetler sağlar ve isteğe bağlı olarak iletişim güvenilirliğini sağlayabilir. TCP ve UDP bu katmanın temel protokolleridir.

İnternet Katmanı - Internet layer: Bu katman, paketlerle ilgilenir ve paketleri ağ sınırlarının ötesine taşımak için bağımsız ağları bağlamaktadır. Internet Protokolü IP, TCP / IP için temel ağ katmanı protokolüdür. Ağ katmanındaki diğer yaygın olarak kullanılan protokoller, ICMP, IGMP ve ARP'dir.

Ağ Erişim Katmanı - Network Access layer: Bu katman fiziksel ağ bileşenleri üzerindeki iletişimi yönetir ve yerel alan ağı genelinde bilgi iletmekten sorumludur. Ethernet ve Token Ring ortak bu katmanında en yaygın olarak kullanılan protokollerdir.

Tablo 2.1. TCP / IP ağ katmanları ve katmaları ile ilgili protocol örnekleri

Layer #	TCP/IP Network Layer Name	Example
Layer 4	Application	HTTP, HTTPS, SMTP, DHCP
Layer 3	Transport	TCP, UDP
Layer 2	Internet	IP(v4, v6), ARP, ICMP
Layer 1	Network Access	Ethernet, Token Ring, FDDI

2.3. Ağ Güvenliği

Küresel internet bağlantısındaki artış ve kablosuz ve mobil ağların yaygınlaşması ile ağ saldırıları farklı bir boyut kazanmaya başlamıştır. Kullanıcılar, iş hizmetlerinde izinsiz eylemler nedeniyle istenmeyen güvenlik sızıntılarından hala muzdariptir. Güvenlik, istihdamın güvene dayalı olması nedeniyle kullanıcıların etik davranışlarına bağlıdır. Ancak, World Wide Web'in çok fazla kullanımı, uzak ağ operasyonları ve tüm büyük ölçekli bilgi sistemleri ile güvenlik kavramları geliştirilmeli ve birleştirilmelidir. Dolayısıyla, ağ güvenliği hem araştırmada hem de sanayi toplumlarında dikkat odağı olmuştur [16].

Ağ oluşturma aşamalarında ve daha sonra internetin geliştirmesinde, ağlar üzerinde yapılan araştırmaların daha çok bağlantı hızı veya daha iyi kullanılabilirlik ile ilgili konuları önemsedikleri görülmektedir. Bu gelişme döneminde, internet sadece birkaç bilgisayar kullanıcısının erişime sahip olduğu bir ayrıcalıktı. Ağlar ve internetin yaygın hale gelmesiyle birlikte güvenlik kritik bir konu haline geldi.
Bilgi güvenliğini tanımlamak için kullanılan üç temel terim vardır:

a. Gizlilik: Sadece yetkili tarafların bilgiye erişimini sağlamakır. Şifreleme, gizliliği sağlamak için yaygın olarak kullanılan bir araçtır. Kimlik doğrulama ve yetkilendirme, veri gizliliğini doğrulamak için kullanılır.

b. Bütünlük: Bilginin yetkisiz taraflarca değiştirilmemesini (veya yetkili kişilerce yanlış bir şekilde değiştirilmesini) ve güvenilebilmesini sağlamaktır. Veri bütünlüğünü doğrulamak için kontrol toplamı (checksum) ve imza (hash) yöntemleri kullanılır.
c. Erişebilirlik: gerekli olduğunda bilginin erişilebilir olmasını sağlamatır. Verilerin basit yedeklemelerine ek olarak, DoS saldırısı durumunda sistemlerin erişilebilir kalmasını sağlamayı da içerir. Kullanılabilirlik ayrıca kritik verilerin silinmeden korunması gerektiği anlamına da gelmektedir.

Verilerin her bir kısmı açık bir ortam üzerinden iletilir ve böylece, saldırganların verilere kolaylıkla erişimi vardır. Böyle durumlarda güvenlik daha da zorlaşıyor. Mesajların işlenmesi ve kodlanması için mobil cihazda mevcut olan kaynakların eksikliği, bu zorlukların geleneksel ağlara göre üstesinden gelmesini daha da zorlaştırıyor.

Bu nedenle, ağın tüm giriş noktalarının korunması gereklidir. Ağ güvenliğindeki en önemli faktörler; şifreleme, güvenilir şifreler, virüsten koruma yazılımları kullanımı ve modern gelişmiş ağ güvenlik cihazlarıdır.

En yaygın ağ güvenliği cihazları şunlardır:

- Aktif cihazlar: fazla trafiği engelleyen güvenlik duvarları, antivirüs tarama cihazları ve içerik filtreleme cihazları gibi.
- Pasif cihazlar: istenmeyen trafiği tanımlayan ve raporlayan izinsiz giriş algılama cihazları.
- Önleyici cihazlar: ağları tarayan ve olası güvenlik sorunlarını belirleyen sızma testi cihazları ve güvenlik açığı değerlendirme cihazları.

Yukarıda bahsedilen cihazlardan, güvenlik duvarları, çoğu şirket için en yaygın ve ilk savunma aygıtı olarak kullanılmaktadır.

2.4. Güvenlik Duvarları

Güvenlik duvarları, çoğu işletmede ve kurumda özel ağların güvenliğini sağlamak için en yaygın şekilde kullanılan güvenlik mekanizmalarıdır. Bunlar, yönetsel olarak tanımlanan politikalara dayalı olarak trafik kurallarına izin vererek veya bunları etkisiz hale getirerek ağlar arası ağ trafiğini kontrol etmektedir [15].

Güvenlik duvarları, özel bir ağ ile genel internet arasındaki girişte ilk savunma hattı veya güvenlik görevlisi olarak hareket eden ve tüm gelen ve giden paketleri güvenlik kurallarına göre inceler.

Saldırganları dışarıda tutacak bir duvar fikri binlerce yıl öncesine dayanıyordu. İki bin yıl önce, Çinler Çin Seddini, kuzeydeki komşu kabilelerden koruma amacıyla inşa ettiler. Avrupalı krallar ve Osmanlı sultanları, kendilerini yağma ve yağma amaçlı kasıtlı gruplardan korumak için yüksek duvarlı kaleler inşa ettiler [8].

Güvenlik duvarı sözcüğü, kelimenin tam anlamıyla, bir yangının yayılmasını durdurmak için yapılmış tuğla, çelik veya diğer malzemelerden yapılmış bir duvara benzetilmektedir. Bilgisayar dünyasında da bir güvenlik duvarı benzer bir amaca hizmet eder. Ancak, bir bilgisayarın güvenlik duvarı, güvenilir verinin aktarılmasını sağlayan ve güzenilir olmayan verileri ise engelleyen bir duvardan daha fazla bir filtredir.

Özel bir ağın güvenliğini sağlamak için, trafiğin kontrol edilmesi gerekmektedir. Ağ güvenlik duvarı ağa ve ağa erişimini sınırlayan bir sistemdir. Genellikle güvenilir, bir özel ağ ve güvenilmeyen bir ortak ağ arasında konumlandırılır. Güvenlik duvarı, yalnızca önerilen bir plana göre onaylanmış trafiğe izin verir. Güvenlik duvarı, düşük seviyeden yüksek seviyeye kadar olan ve iyi organize edilmiş saldırılardan oluşan güvenlik tehditlerini en aza indirir.

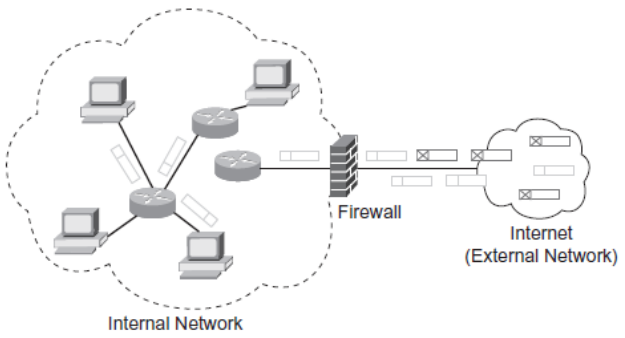
Ağ trafiğinin etkin bir şekilde izlenmesini sağlamak için, güvenlik duvarı ağdaki bir anahtar noktaya yeleştirilmektedir. Genellikle, korumalı ağı daha az güvenilir bir ağa bağlayan ağ geçidine yerleştirilir. Güvenlik duvarının ağ kenarında konumlandırılması genellikle gereklidir. Çünkü ağa giren veya çıkan tüm trafiğin

izlenmesi ve filtrelenmesinin sağlanması için en iyi yer burasıdır. Bir ağ topolojisinde güvenlik duvarının konumlandırılmasından dolayı, bir ağın trafik hacminin artması nedeniyle güvenlik duvarına yüklenen yükün de artacağı açıktır. Güvenlik duvarları, ağ protokolü yığındaki bir veya daha fazla katmandaki trafiği filtreleyerek, çoğunlukla OSI ağ modelinin uygulama, iletim, ağ ve veri bağlantı katmanlarında çalışır.

Genel olarak, güvenlik duvarları ilk savunma hattı olarak görülür. Ancak onları bir örgütün son savunma hattı olarak görmek daha iyi olabilir. Kurumlar kendi iç sistemlerinin güvenliğini yüksek bir öncelik haline getirmelidir. Dâhili sunucular, kişisel bilgisayarlar ve diğer sistemler, güvenlik yamaları ve virüsten koruma yazılımları ile güncel tutulmalıdır.

Bir güvenlik duvarı aynı zamanda, aşağıdaki ölçütleri karşılayan iki ağ arasındaki makine olarak da tanımlanabilir [8]:

a. Güvenlik duvarı iki ağ (dâhili ve harici) arasındaki sınırdır.
b. İki ağ arasındaki tüm trafik güvenlik duvarından geçmelidir;
c. Güvenlik duvarında, bazı trafiği engellerken diğer trafiğin ise geçmesine izin veren bir mekanizma vardır. (bu genellikle filtreleme olarak adlandırılır).



Şekil 2.1. Bir kuruluş ağının güvenlik duvarı

2.4.1. Güvenlik duvarı türleri

Güvenlik duvarları farklı kriterlere dayanarak sınıflandırmaktadır.

a. Katmanlı mimariye göre:

Güvenlik Duvarı katmanlı mimari modeli ile ilgili iki ana kategoride sınıflandırılabilir: ağ katmanı ve uygulama katmanı güvenlik duvarları [18].

1. Ağ katmanı güvenlik duvarları:

Bu tür güvenlik duvarın temel özellikleri, tüm trafiğin doğrudan ağ katmanından yönlendirilmesidir. Ayrıntılı olarak, güvenlik mekanizması kaynak ve hedef bilgileri de dâhil olmak üzere tüm paket bilgilerini denetleyebilir ve ardından paket trafiğine izin verilip verilmeyeceğine karar vermek için yerel politikayı karşılaştırabilmektedir.

Bir paket filtreleme güvenlik duvarı, en basit ağ katmanı güvenlik duvarı türüdür. Paket filtreleme güvenlik duvarı, IP paket özelliklerinde bulunan basit bir işlem felsefesine sahiptir. Paket yerel ağın güvenlik politikası tarafından tanımlanan kurallara uyuyorsa, paketin girilmesine izin verilmektedir [9] [18]. İzin verilmediği durumlarda paket atılıp yerel ağdaki girişi engellenmektedir. Bir paket filtresi sadece IP adreslerini, port numaralarını ve iletim protokolü türünü dikkate alır. Ayrıca, tüm bu bilgiler paket başlığında bulunduğundan, paket verilerinin (payload) denetlenmesine gerek yoktur.

2. Uygulama katmanı güvenlik duvarları:

Uygulama katmanı güvenlik duvarları, ağdaki trafiği, iletim ve uygulama katmanını filtreleyebilmektedir. Uygulama katmanında filtreleme ayrıca, vekil sunucu (proxy) gibi yeni hizmetler de sunmaktadır. Vekil sunucular ağlar arasında doğrudan trafiğe izin vermez ve bunlar üzerinden geçen trafiğin ayrıntılı bir şekilde günlüğe kaydedilmesini ve denetimini gerçekleştirmektedir [9][18]. Vekil sunucu görevi gören bir güvenlik duvarı, paketlerin içeriğini potansiyel olarak

denetleyebilmektedir. Uygulama katmanı güvenlik duvarları, Saldırı Tespit Sistemi (Intrusion Detection Systems) olarak da kullanılabilmektedir. IDS, bir ağ veya sistemi kötü amaçlı etkinlik veya politika ihlalleri için izleyen bir aygıt veya yazılım uygulamasıdır.

b. Özeliklerine göre

Güvenlik duvarın özeliklerine göre iki çeşit güvenlik duvarı mevcuttur; yazılım ve donanım.

Donanım güvenlik duvarları, piyasada bağımsız makineler olarak bulunabilen cihazlardır. Bu tür bir güvenlik duvarı, güvenilmeyen ağ ile bağlantıdan hemen önce, yerel bir ağın makinelerine veya yerel ağın kendisine doğrudan bağlanabilir. Donanım güvenlik duvarları, yerel güvenlik politikasını uygulamak için paket süzgeçlerini inceleyen bir koruma yöntemi olarak paket filtrelemeyi kullanmaktadır [9]. Büyük ölçekli ağlarda, donanım güvenlik duvarları daha karmaşık yapılandırmalar gerektirmektedir.

Öte yandan, yazılım güvenlik duvarları kişisel bir bilgisayara veya bir iş LAN sunucusuna kurulan bir uygulama ile özelleştirilebilmektedir. Yazılım güvenlik duvarları, ağ yöneticisine birçok yararı olan çok ağ katmanlı güvenlik sağlayabilmektedir. Yazılım güvenlik duvarları, güvenli olmayan uygulama koruması, truva atları ve e-posta solucanı algılama sistemleri ve izinsiz giriş koruması ile gelmektedir [8]. Bir yazılım güvenlik duvarının temel özelliği, sadece bir makineye kurulabilmesidir. Bu, tüm ağ trafiğini izlemek için ağın güvenlik duvarının kontrol noktasına yüklenmesi gerektiği anlamına gelmektedir.

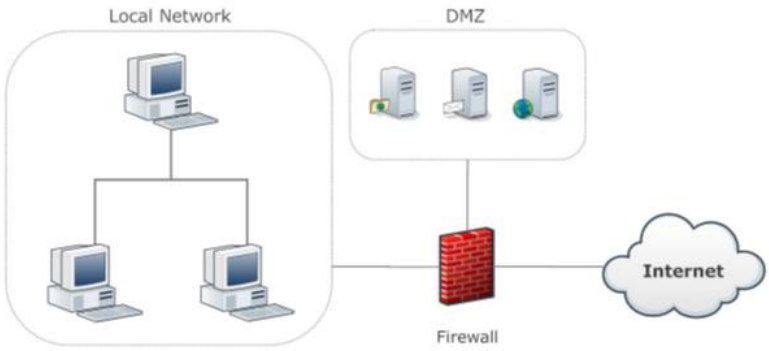
2.4.2. Güvenlik duvarı topolojileri

Daha önce de belirtildiği gibi, güvenlik duvarları bir dahili ağ ile güvenilmeyen ağ (internet) arasındaki engeller olarak çalışmaktadır. Altyapı söz konusu olduğunda, bir güvenlik duvarı kurmak için kullanılabilecek farklı topolojiler vardır. Bunlardan en önemlileri aşağıda sunulmuştur.

a. Demilitarized Zone – DMZ

DMZ, güvenli ve kesintisiz erişim sağlamak için dâhili ve harici ağ arasında ayrı bir ağın eklendiği bir güvenlik duvarı topolojisidir. Bu mimari sayesinde DMZ, harici bir ziyaretçiyi bir web sunucusu ve SMTP gibi herhangi bir hizmetle değil, ziyaretçinin iç ağın geri kalan kısmına erişim fırsatı vermeden izole bir bağlantıyla sağlamayı başarmaktadır. Ayrıca bir ağ içinde bulunan bir makineyi diğer makinelerden izole edebilir. Bu, farklı internet bağlantılarıyla çalışan ancak aynı iş ağını kullanan kuruluşlara yardımcı olabilmektedir.

Esas fikir, DMZ'nin saldırganların dâhili ağın sistemlerine doğrudan erişmesini önlemek için tasarlanmıştır. Sonunda erişimine izin verilen ilk makine bir web sunucusu, bir SMTP veya bir FTP sunucusu olabilir.



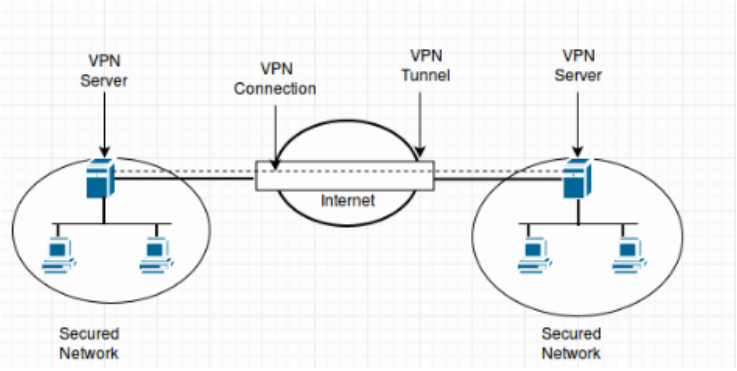
Şekil 2.2. DMZ ağ topolojisi

b. Virtual private networks – VPN’ler

IPsec sayesinde VPN, uygulama kolaylığı ve güvenlik seviyesi nedeniyle son yıllarda yaygın bir şekilde kullanılmaktadır. VPN'ler, bir ortak ağda çalışan sanal olarak paylaşılan ağlardır. VPN'lerde, makineler yalnızca paketler hedeflerine ulaştığında şifrelenmiş paketleri ortak ağ üzerinden almayı başarırken, şifrelenmiş paketleri değiştirmeyi başarmaktadır [10]. IPsec teknolojisi boyunca VPN verileri

şifreleyebilirken, şifre çözme anahtarı sadece paketin alıcısı, VPN içinde bulunabilir.

Kuruluşlar, tüm kuruluşların bulunduğu yere güvenli bir bağlantı kurmak için VPN'yi kullanmaktadır. Örneğin: dünyanın 4 farklı kıtasında 4 ofisin bulunduğu çok uluslu bir şirket İnternet üzerinden VPN, kurumun ofisleri arasında iletişimi sağlamak için en uygun altyapı olacaktır [11].



Şekil 2.3. VPN ağ topolojisi [11]

c. Ağ adresi çeviricisi - Network address translator - NAT

NAT tek başına bir güvenlik duvarı değildir, ancak güvenlik duvarının dağıtımı ile birlikte güvenliği zorlamaya kesinlikle yardımcı olmaktadır. NAT, Internet genel adreslerini dahili özel adreslerle güvenli bir şekilde bağlamayı başarmaktadır. NAT, adresleri genelden özele çevirir ve bunun tersini de yapmaktadırç Böylece, yalnızca yönlendiriciyi trafiğin nereye yönlendirildiğini bilirlerken adresleri gizler.

2.4.3. Güvenlik duvarı kuralları

Daha önce tartışıldığı gibi, bir güvenlik duvarı, paketlerin belirli kurallara göre güvenli bir ağın sınırları boyunca geçişini kontrol eden bir ağ elemanıdır. Güvenlik duvarı kural kümesi, belirli özel koşulları sağlayan paketlerde gerçekleştirilen eylemleri tanımlayan sıralı filtreleme kurallarının bir listesini içermektedir. Kurallar condition (durum) ve action (eylem) biçiminde belirtilmiştir. Kural alanındaki bir koşul, genellikle farklı filtre parametrelerine sahip farklı kural mantığı ile sağlanmaktadır. Kural filtreleme bölümünde IP, UDP veya TCP

başlıklarında herhangi bir alanı kullanmak mümkündür. Ancak, pratik deneyim en yaygın kullanılan alanların: protokol türü, kaynak IP adresi, kaynak portu, hedef IP adresi ve hedef portu olduğunu göstermektedir. Belirli filtreleme için bazen TTL ve TCP flags (bayrakları) gibi bazı alanlar kullanılmaktadır [12]. Bir kuraldaki eylem, belirli bir ağ trafiğine izin veren veya reddedilen bir eylemin tanımlanmasına izin vermektedir.

Aşağıda, bir güvenlik duvarı politikasında yaygın olarak kullanılan paket filtreleme kuralları biçimidir [12]:

<order> <protokol> <src_ip> <src_port> <dst_ip> <dst_port> <action>

Her filtre alanı, tek bir değer veya değerler aralığı olabilir. IP adresi alanlarındaki "*" sembolü, 0 ile 255 arasında bir IP adresi aralığını temsil eder. "-" sembolü, verilen IP adresleri arasında bir dizi IP adresi anlamına gelir. Örneğin, bu adres 192.168.1. * analamı 192.168.1.0 - 192.168.1.255 arası IP adreslerini ve 192.168.1.10 – 30 IP adresi ise 192.168.1.10 - 192.168.10.30 arasında bulunan IP aralığını temsil etmektedir. Aynısı port numaraları için de geçerlidir.

Güvenlik duvarı kuralları ağın bir tarafından (LAN veya WAN) diğerine geçişi engeller veya trafiğe izin verir. Gelen kurallar, dış ağdan iç ağa gönderilen paketleri ve giden kuralları, yerel kullanıcıların hangi dış kaynaklara erişebileceğini belirlemektedir.

2.4.4. Güvenlik duvarı kurallarını yapılandırma

Güvenlik duvarında bir güvenlik ilkesi uygulamak için, kuruluş ağ güvenliği gereksinimlerinden türetilmiş bir dizi filtre kuralları tanımlanır. Güvenlik duvarı tarafından sağlanan güvenlik korumasının etkinliği temel olarak güvenlik duvarında yapılandırılan kuralların kalitesine bağlıdır. Ne yazık ki, güvenlik duvarı politikalarını yapılandırma ve yönetme süreci zorlu ve can sıkıcıdır. Kuralların karmaşıklığı ve karşılıklı bağımlılığı nedeniyle hatalara açık bir görevdir [20]. Bu nedenle, güvenlik duvarlarının güvenli olması için etkili yönetim mekanizmaları ve politika yönetimi araçları çok önemlidir.

Yazma kuralları, “Ağımızdaki ana bilgisayarlardan gelen taleplere cevap vermedikçe, dışarıdan gelen trafiğe izin vermeyin” veya “İçeriden tüm trafiği engellenmediği sürece içeriye izin vermeyin” diyen kadar basit olabilir.

Örnek güvenlik duvarı kuralları:

Tablo 2.2. Paket filtreleme güvenlik duvarı kurallarına bir örnek

Order (R)	Port	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	*.*.*.*	any	191.120.33.41	25	permit
2	TCP	140.192.37.30	any	*.*.*.*	21	deny
3	TCP	*.*.*.*	any	161.120.33.*	21	deny
4	TCP	140.192.37.*	any	*.*.*.*	21	permit
5	TCP	*.*.*.*	any	161.120.33.*	22	permit
6	TCP	140.192.37.*	any	*.*.*.*	80	deny
7	TCP	150.162.10.3	any	161.120.30.40	80	permit
8	TCP	*.*.*.*	any	161.120.33.43	53	permit
9	UDP	*.*.*.*	any	161.120.33.43	53	permit
10	UDP	35.12.20.16	80	200.10.21.35	80	permit
11	*	*.*.*.*	*	*.*.*.*	*	deny

Paketler bir güvenlik duvarından geçtikçe, başlık bilgileri sırayla bir kuralın alanları ile karşılaştırılır. Bir paket başlık bilgisi bir kuralın bir alt kümesi ise, bir eşleşme olduğu söylenir ve kabul veya reddedilecek ilgili eylem gerçekleştirilir. Aksi halde, paket bir sonraki sıralı kural ile karşılaştırılır ve eşleşme bulunmazsa reddedilen varsayılan kural uygulanır ve paket bırakılır [9].

Örneğin, ilk kuralı göz önünde bulundurularak:

Protocol = TCP, *Source IP = *.*.*.*,* *Source port = any,*
Destination IP = 191.120.33.41*,* *Destination port = 25,* *Action = permit*

Bu kural, her hangi bir iç kullancıdan 192.120.33.41 IP adresi ve port numarası 25 olan belirli bir bilgisayar için giden bir dizi TCP paketini tanımlar. Bu nedenle, iç

ağdan bir paket kümesi kuralı temel alır. 192.120.33.41'e gitmek ve SMTP hizmetine erişmek için kabul edilecektir.

Yukarıdaki güvenlik duvarı politikasının dördüncü kuralına baktığımızda [tablo 2.3] kaynak IP adresi alanında görünen tek "*", 140.192.37.0'dan 140.192.37.255'e kadar bir IP adresi aralığını ve "*. *. * Sembolüdür. Hedef IP adresindeki * ", yerel ağın dışındaki tüm ana bilgisayarları temsil eder.

2.4.5. Anomali kavramına genel bakış

Bir paket birden fazla kuralla eşleştiğinde, bu ilk kural uygulanır. Bu nedenle, iki kural ile eşleşen paketler kümesi ayrılmazsa, anormallik oluşturacaktır. Anomali, aynı paketle eşleşen iki veya daha fazla filtreleme kuralının varlığıdır [13]. Örneğin, bir kural ile eşleşen paketler kümesi, sonraki kural tarafından eşleştirilenlerin bir üst kümesi olabilir. Bu durumda, ikinci kuralın eşleştirebileceği tüm paketler, birinciyle eşleştirilecek ve ikinci kural hiçbir zaman idam edilmeyecektir. [14]'te güvenlik duvarı politikasına dayanarak anomaliler dört farklı kategoride sınıflandırılmıştır.

a. Gölge anomalisi - Shadowing anomaly :

Bir kural, farklı bir eylem gerçekleştirirken gölgeli kurallarla da eşleşen tüm paketlerle eşleşen bir veya daha önceki kurallar kümesi tarafından gölgelenebilir. Böylece, gölgeli kural asla geçerli olmayacaktır.

b. Genelleştirme anomalisi - Generalization anomaly:

Bir kural, bu kuralla eşleşen paketlerin bir alt kümesi aynı zamanda önceki kural (lar) ile eşleştirilirse ancak farklı bir eylemde bulunursa, bir veya daha fazla kuralların genelleştirilmesidir.

c. Korelasyon anomalisi - Correlation anomaly:

Farklı filtreleme eylemleri olduğunda iki kural ilişkilendirilir ve ilk kural, ikinci kuralla eşleşen bazı paketlerle eşleşir ve ikinci kural, birinci kuralla eşleşen bazı paketlerle eşleşir. Bu durumda, bu kuralların kesişimiyle eşleşen paketlere bir kural izin verilebilir, ancak başkaları tarafından reddedilebilir.

d. Fazlalık anomalisi - Redundancy anomaly:

Yineleme kuralı kaldırılırsa, güvenlik ilkesi bundan etkilenmeyecek şekilde aynı eşleşmeyi ve eylemi üreten başka bir kural varsa, kural gereksizdir.

2.4.6. Güvenlik duvarı kurallarını optimize etme

Güvenlik duvarı kuralları çoğunlukla farklı ağ yöneticileri tarafından farklı zamanlarda yazılır ve yerel ağın yeni güvenlik gereksinimlerine uyacak şekilde sürekli olarak güncellenir. Bu, kuralların sayı ve karmaşıklıkta politika büyümesi ile sonuçlanır.

Güvenlik duvarı performansını optimize etmek için farklı teknikler ve yöntemler kullanılır. Onlardan bazıları:

a. Çatışma tespiti ve çözümü: Aynı paketle eşleşebilecek iki veya daha fazla filtreleme kuralı olduğunda, güvenlik duvarı kuralları çakışması ortaya çıkar.
b. Yedekleme kurallarının kaldırılması: Aynı paketle eşleşen başka bir kural varsa ve bu kural kaldırıldığında güvenlik politikasını etkilenmeyecek bir kuraldır.
c. Kuralların birleştirilmesi: kuralların birleştirilmesi, anormallikleri ortadan kaldırdıktan sonra güvenlik duvarı kurallarını optimize etmenin bir yoludur ve kurallar çatışmasız hale gelmiştir. Kurallar birbirine uymuyorsa ve kuralların tüm parametreleri tek bir parametre dışında eşitse, iki veya daha fazla kural tek bir kuralda birleştirilebilir.

d. Güvenlik duvarı kurallarının yeniden sıralanması: Güvenlik duvarı kurallarını yeniden sıralama, güvenlik duvarı kural kümesinin sırasını optimize etmek için paket eşleştirme istatistiklerini kullanan bir mekanizmadır.
e. Alakasız kuralların kaldırılması: Güvenlik duvarı performansının iyileştirilmesi için kullanılabılecek başka bir yöntem gereksiz kuralları ortadan kaldırmaktadır. Alakasız kurallar, güvenlik duvarını geçen ağ yollarındaki hiçbir paketi eşleştiremeyen kurallardır.
f. Kural bütünlüğü: Politika bütünlüğü, güvenlik duvarı kuralları arasındaki sırayı çok doğru ve düzenli bir şekilde sürdürme sürecidir.

BÖLÜM 3. GÜVENLİK DUVARI KURALLARININ YAPISAL ANALİZİ

Güvenlik duvarı kuralları kurumun ihtiyaç ve hedeflerine göre tanımlanır. Güvenlik duvarı kuralları tanımlandıktan sonra, ağda ciddi güvenlik ihlallerine yol açabilecek çakışmalar için test edilmeleri gerekir. Bu bölümde, öncelikle güvenlik duvarı kural kümelerinde meydana gelebilecek farklı ilişki ve çatışma türleri tartışılmaktadır. Sonrasında ise çeşitli güvenlik duvarı kural yapıları, temsilleri ile analiz yöntemleri belirlenmektedir.

Tablo 3.1. Örnek güvenlik duvarı kuralları I

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.192.37.10	Any	161.120.33.41	25	Deny
2	TCP	10.0.1.*	Any	*.*.*.*	80	permit
3	TCP	10.0.1.54	Any	*.*.*.*	80	Deny
4	TCP	140.192.37.30	Any	*.*.*.*	25	Permit
5	TCP	140.192.37.*	Any	*.*.*.*	25	Deny
6	TCP	10.0.0.*	Any	150.0.0.70	21	Deny
7	TCP	10.0.0.14	Any	150.0.0.*	21	Permit
8	TCP	140.192.37.*	Any	*.*.*.*	25	Deny
9	TCP	140.192.37.5	Any	*.*.*.*	80	Permit

3.1. Güvenlik Duvarı Kuralları Arasındaki İlişkiler

Güvenlik duvarı kurallarının çatışmalarını ve optimizasyon tekniklerini tartışmadan ve analiz etmeden önce, bir güvenlik duvarı kuralı içinde olabilecek tüm ilişkileri modellemek önemlidir. Al-Shaer, kuralların ağ alanlarını aşağıdaki gibi karşılaştırarak güvenlik duvarı kuralları arasındaki ilişkileri açıklamaktadır [13].

a. Tamamen ayrık - Completely disjoint:

Rx ve Ry iki kural olduğunu varsayalım; Rx'deki her alan bir alt küme veya bir üst küme değilse veya Ry'deki karşılık gelen alana eşit değilse, Rx ve Ry kuralları tamamen ayrılır. Örneğin, Tablo 3.1.'de, R1 ve R2 tamamen ayrılır. Çünkü R1'deki

her bir parametre R2'de karşılık gelen alana bir alt-küme ya da üst küme ya da eşit değildi. R3 ve R4 de tamamen ayrıktır.

b. Tam eşleme - Exactly matching:

Rx ve Ry iki kural olduğunu varsayalım; Rx'deki her alan, Ry'deki ilgili alana eşitse Rx ve Ry Kurallar tam olarak eşleşmektedir. Örneğin, Tablo 3.1.'de, R5 ve R8 tam olarak eşleşmektedir, çünkü R5'deki her bir parametre, R8'deki karşılık gelen parametre ile aynıdır.

c. Kapsayıcı eşleme - Inclusive matching:

Rx ve Ry iki kural olduğunu varsayalım; eğer Rx ve Ry tam olarak eşleşmezlerse ve Rx'deki her alan bir alt kümedeyse veya Ry'deki karşılık gelen alana eşitse, iki kural arasında kapsayıcı eşleme bulunmaktadır. Örneğin, Tablo 3.1.'de R4, R5 ile büyük ölçüde eşleşir. R4 ilişkinin alt kümesi, R5 ise ilişkinin üst kümesidir. Böylece, R4 ve R5 arasında inclusive matching mevcuttur.

d. Kısmen eşleme / Kısmen ayrılma - Partially matching/ partially disjoint:

Rx ve Ry iki kural olduğunu varsayalım; Rx'den en az bir alt küme veya üst küme veya eşit olan parametre Ry'deki karşılık gelen alana varsa ve Rx'den en az bir altküme veya üst küme veya eşit olan parametre Ry'deki karşılık gelen alana eşit değilse, partially matching mevcuttur. Örneğin, Tablo 3.1.'de, R8 ve R9 kısmen ayrılır (kısmen eşleşir).

e. Korelasyon eşleme - Correlated matching:

Rx ve Ry iki kural olduğunu varsayalım; Rx'deki bazı alanların alt kümeleri veya Ry'deki karşılık gelen alanlara eşit olması durumunda Rx ve Ry ile ilişkilendirilir ve Rx'deki alanların geri kalanı Ry'daki karşılık gelen alanların üst kümesidir. Örneğin, R6 ve R7, Tablo 3.1.'de ilişkilendirilmiştir.

3.2. Anomaliler

Güvenlik duvarı, özel ağların güvenliğini sağlamak için en çok kullanılan güvenlik mekanizması olduğundan, güvenlik duvarı politikalarını dikkatle tasarlamak ve yönetmek çok önemlidir. Firewal yapılandırmaları karmaşık yapısı nedeniyle güvenlik duvarı kuralları genellikle hata eğilimlidir. Mevcut analiz yöntemlerinin çoğu, herhangi iki kural arasındaki anormallikleri dikkate alır ve çok azı, anomalileri keşfetmek için aynı anda ikiden fazla kuralı birlikte kullanabilmektedir.

Ehab S. Al-Shear ve diğ. [14], Anomalileri, aynı paketi eşleştirebilecek iki veya daha fazla filtreleme kuralının varlığı olarak tanımlar. Anomaliler gölge anomalisi, genelleşme anomalisi, korelasyon anomalisi ve artıklık anomalisi olmak üzere 4 tipte anomalileri sınıflandırmışlardır.

Tablo 3.2. Örnek güvenlik duvarı kuralları II

Order ®	Protocol	Source IP	Port	Destination IP	Port	Action
1	TCP	165.0.0.70	Any	180.0.0.*	22	Permit
2	TCP	140.185.40.*	Any	160.0.0.40	80	Permit
3	TCP	140.185.40.25	Any	160.0.0.40	80	Deny
4	TCP	170.0.0.*	Any	175.0.0.70	21	Deny
5	TCP	170.0.0.14	Any	175.0.0.*	21	Permit
6	TCP	170.0.0.*	Any	175.0.0.*	21	Deny
7	TCP	Any	Any	Any	Any	Deny

1. Gölge anomalisi - Shadowing anomaly:

Bir kural, geçerli kuralla eşleşen tüm paketlerle eşleştiğinde kural gölgelenir. Bir kural, farklı bir eylem gerçekleştirirken gölgeli kurallarla da eşleşen tüm paketlerle eşleşen bir veya daha önceki kurallar kümesi tarafından gölgelenebilir. Böylece, gölgeli kural asla geçerli olmayacaktır. Genel olarak, Ry Rx'i sırayla takip ederse ve Ry Rx'in bir alt kümesi eşleşmesi durumunda, Rx kuralına göre Ry gölgelenir. Her iki kural da farklı action sahibi olmalıdır. Gölgeleme, güvenlik duvarı kuralarında çok önemli bir hatadır ve kabul edilen bir trafiğin engellenmesine veya izin verilmeyen bir trafiğin izin vermesine neden olabilir.

Örneğin, Tablo 3.2.'de, Kural 2 farklı bir eylemle Kural 3'ün bir alt küme eşleşmesidir. Bu nedenle Kural 3'ün Kural 2'ye tabi olduğunu ve Kural 3'ün hiçbir zaman aktive olmayacağını söyleyebiliriz. Bu sırayla ilgili iki kural, 140.185.40.25'ten gelen ve 160.0.0.40'a giden tüm HTTP trafiğinin gölgeleneceğini ve hiçbir zaman etkinleştirilmeyeceğini ima etmektedir.

2. Korelasyon anomalisi - Correlation anomaly:

Farklı filtreleme eylemleri olduğunda iki kural ilişkilendirilir ve ilk kural, ikinci kuralla eşleşen bazı paketlerle eşleşir ve ikinci kural, birinci kuralla eşleşen bazı paketlerle eşleşir. İki kuralın sırası tersine çevrilirse, ortaya çıkan politikanın etkisi farklı olacaktır. Genellikle Rx ve Ry kuralı, Rx ve Ry korelasyon ilişkideyse ve Rx ve Ry'nin eylemleri farklıysa, bir korelasyon anomalisine sahiptir.

Örneğin, tablo 3.2.'de, kural 4, kural 5 ile korelasyon halindedir. Bu sıralamayı içeren iki kural, 170.0.0. * Gelen ve 175.0.0.70 olan tüm FTP trafiğinin reddedildiğini ima eder. Ancak, siparişleri tersine çevrildiyse, aynı trafik kabul edilir.

Bu çalışma korelasyon anomalisini bir hata olarak düşünmemektedir, ancak anormal uyarı olarak görmektedir, bu nedenle bu tip bir anomali için herhangi bir işlem yapılmayacaktır.

3. Genelleştirme anomalisi - Generalization anomaly:

Bir kural, farklı eylemleri varsa ve ilk kural ikinci kuralla eşleşen tüm paketlerle eşleşebilirse, önceki kuralın genelleştirilmesidir. Genelleştirme genellikle trafiğin belirli bir bölümünü genel bir filtreleme eyleminden çıkarmak için kullanılır. Rx ve Ry iki kural için, Eğer Rx sırayla Rx'i takip ederse ve Ry Rx'in bir superset maçıysa ve Ry ve Rx'in eylemleri farklıysa. Ry'nin kural Rx'in genelleştirilmesi olduğunu söylüyoruz.

Örneğin, Tablo 3.2.'de, Kural 6, Kural 5'in genelleştirilmesidir. Bu iki kural, 170.0.0.14 numaralı trafikten başka 170.0.0.* Adresinden gelen tüm FTP trafiğinin reddedileceğini belirtir. Eğer iki kuralın sırası tersine çevrilirse, sonuçta ortaya çıkan politikanın etkisi değiştirilecek ve kural 5, kural 6 tarafından gölgeleneceği için artık geçerli olmayacaktır.

Bu çalışma, generalization anomalisini anomali uyarı olarak ele alır ve bu tür anomaliler için herhangi bir işlem yapmaz.

4. Fazlalık anomalisi - Redundancy anomaly:

Fazlalık kuralı, bir gelen paket üzerinde başka bir kural ile aynı işlem gerçekleştirir, böylece gereksiz kural kaldırılırsa dahi güvenlik politikası bundan etkilenmez. Genellikle. Eğer Rx ve Ry iki kuralı varsa, Rx sırayla Ry'den önce gelirse ve Rx, Ry'in bir alt kümesi veya üst kümesi veya tam eşleşmesi olursa ve Rx ve Ry'in eylemleri aynıysa redundency anomali olduğunu söyleyebiliriz.

Yedekli bir kural, filtreleme kuralı listesinin boyutunu artırır ve bu nedenle, paket filtreleme işleminin arama süresini ve alan gereksinimlerini artırır. Bu çalışma, fazlalığı ciddi bir hata olarak görmektedir ve bu anomaliyi tespit etmek ve çözmek için yeni bir algoritma önermektedir. Örneğin, Tablo 3.2.'de Kural 7 Kural 6'ya göre artıktır. R6 kaldırılırsa dahi kural listesini etkilemez.

3.3. Güvenlik Duvarı Kuralları Analiz Yöntemleri

Güvenlik duvarında neler yazıldığını, beklendiğini ve ağda neyin gözlendiğini anlamak için güvenlik duvarı kuralları analiz edilmelidir. Bu bölümde, güvenlik duvarı kurallarının yapısını analiz etmek ve temsil etmek için kullanılan farklı analiz yöntemleri tartışılmaktadır. Bu yöntemleri kullanarak güvenlik duvarı kuralları içindeki ilişki ve anomalileri kolayca keşfedilebilir. En yaygın bilinen analiz metotları policy tree metodu, raining 2D box model, graph teorisi ve grid gösterimidir.

a. Politika ağacı - Policy tree:

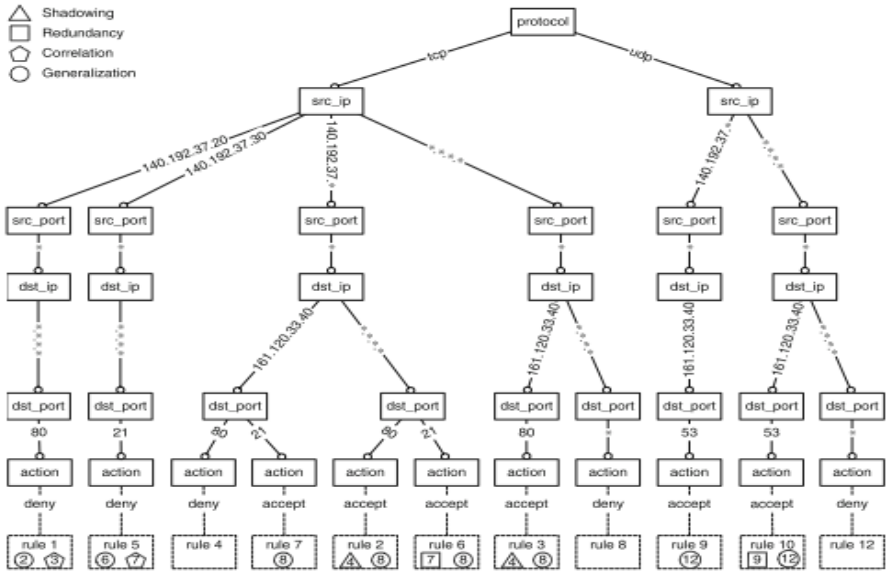
Alshaer et al [12], policy tree analiz yöntemini şu şekilde açıklamıştır. Politika ağacı, yöntemleri analiz eden yaygın güvenlik duvarı politikasından biridir. Ağaç modeli, güvenlik duvarı kurallarının basit bir temsilini sağlar ve aynı zamanda, kurallar arasındaki ilişki ve anormalliklerin keşfine de olanak tanımaktadır [13]. Bir politika ağacındaki her düğüm bir ağ alanını temsil eder ve bu düğümdeki her bir dal ise ilişkili alanın olası bir değerini temsil eder [13].

Örnek: [13] güvenlik duvarı politikalarını analizi için aşağıdaki örnek kural kümesini kullanmıştır.

Tablo 3.3. Politika ağacı için örnek güvenlik duvarı kuralı [13]

	protocol	source address : port	destination address : port	action
1	tcp,	*.*.*.*:any,	161.120.33.41:25,	permit
2	tcp,	140.192.37.30:any,	*.*.*.*:21,	deny
3	tcp,	*.*.*.*:any,	161.120.33.*:21,	deny
4	tcp,	140.192.37.*:any,	*.*.*.*:21,	permit
5	tcp,	*.*.*.*:any,	161.120.33.*:22,	permit
6	tcp,	140.192.37.*:any,	*.*.*.*:80,	deny
7	tcp,	*.*.*.*:any,	161.120.33.40:80,	permit
8	tcp,	*.*.*.*:any,	161.120.33.43:53,	permit
9	udp,	*.*.*.*:any,	161.120.33.43:53,	permit

Şekil 3.1. Tablo 3.3'teki güvenlik duvarı kuralları için ilke ağacı. [13]



b. Raining 2D kutu modeli - Raining 2D box model:

Bu bölümde örnek bir güvenlik duvarı kural kümesinin yapısı, anormallikleri ve birleştirme kurallarını tespit etmek için analiz etmektedir. Mevcut analiz yöntemlerinin çoğu, herhangi iki kural arasındaki anomalileri dikkate alırlar [37] ve çok azı yöntemler anomalileri keşfetmek için aynı anda ikiden fazla kuralı birlikte ele almaktadır.

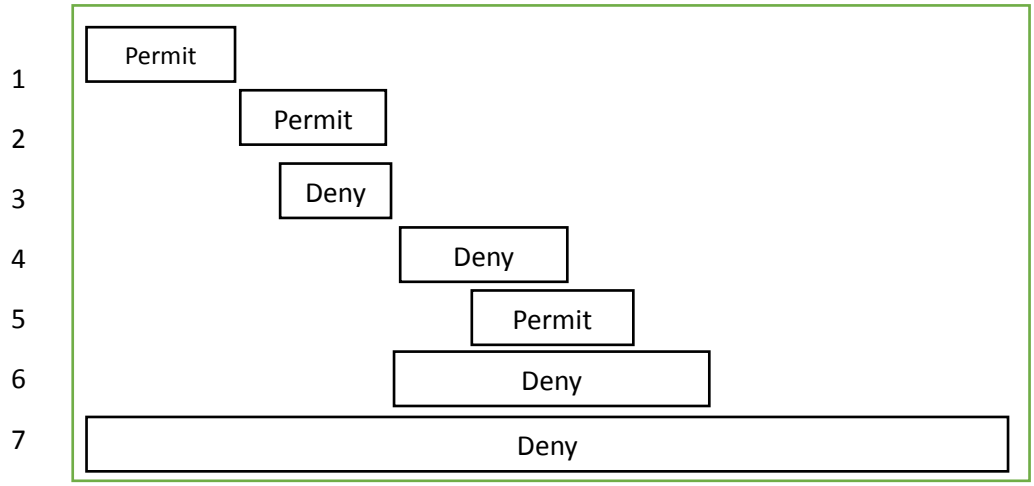
Raining 2D box modeli yapısal analiz metodu, aynı anda ikiden fazla kuralı dikkate aldığından ve aralarındaki tüm anormallikleri keşfetmektedir. Bu çalışmada güvenlik duvarı kurallarını analiz etmek için bu yöntem kullanılmıştır. Box model, filtreleme kurallarının basit bir temsilini sağlar ve aynı zamanda bu kurallar arasındaki ilişkilerin ve anomalilerin kolayca bulunmasını sağlamaktadır. İlke grafiğindeki her kutu bir kuralı temsil eder.

İşte analiz etmek için örnek güvenlik duvarı kuralı ayarlandı:

Tablo 3.4. 2D kutu modelinin yağmurlanması için örnek güvenlik duvarı kuralı ayarlandı

Order ®	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	165.0.0.70	Any	180.0.0.*	22	Permit
2	TCP	140.185.40.*	Any	160.0.0.40	80	Permit
3	TCP	140.185.40.25	Any	160.0.0.40	80	Deny
4	TCP	170.0.0.*	Any	175.0.0.70	21	Deny
5	TCP	170.0.0.14	Any	175.0.0.*	21	Permit
6	TCP	170.0.0.*	Any	175.0.0.*	21	Deny
7	TCP	Any	Any	Any	Any	Deny

Şekil 3.2. Tablo 3.4'ün güvenlik duvarı kuralları için raining 2D box modeli

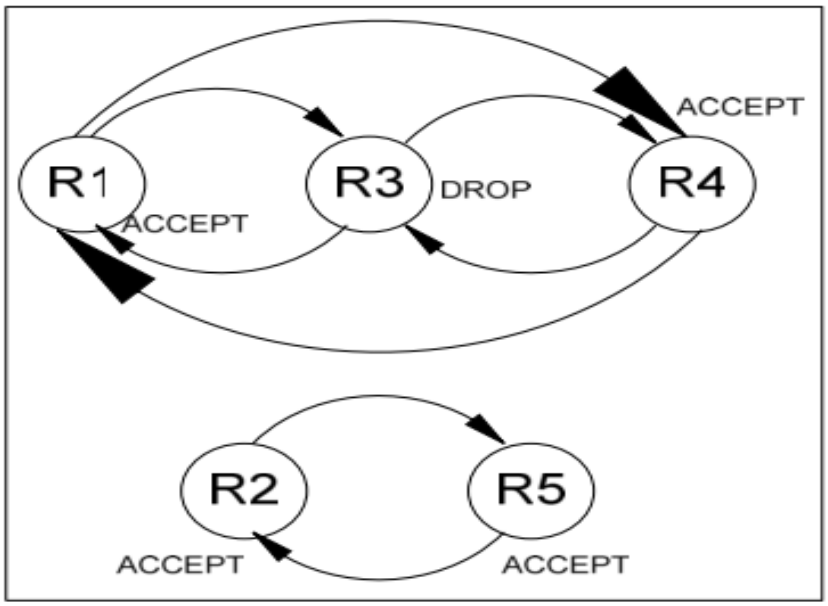


Tihomir Katić et al [22], directed cyclical graph kullanarak bir güvenlik duvarı politikasındaki kurallar arasındaki ilişkileri ve çatışmaları açıkladı ve modelledi. Ayrıca, gölgeli veya gereksiz kurallar arasındaki ilişkileri de göstermektedir. Yönlendirilmiş bir döngüsel grafikte, kurallar döngü olarak sunulmaktadır ve ilişkiler döngüleri birleştiren oklar olarak gösterilmektedir.

Tablo 3.5. Grafik teorisi için örnek güvenlik duvarı kuralı [22]

```
R1: iptables -A FORWARD -p ALL
      -i eth0  -s 10.0.0.0/24  -o eth1
      -d 10.1.0.5  -j ACCEPT
R2: iptables -A FORWARD -p ALL
      -s 172.20.0.0/24  -j ACCEPT
R3: iptables -A FORWARD -p ALL
      -s 10.0.0.0/24 -j DROP
R4: iptables -A FORWARD -p ALL
      -d 10.1.0.5 -j ACCEPT
R5: iptables -A FORWARD -p ALL
      -s 172.20.0.0/28 -d 10.1.0.10
      -j DROP
```

Şekil 3.3. Tablo 3.5 Güvenlik duvarı politikası için grafik gösterimi [22]



d. Grid gösterimi - Grid representation:

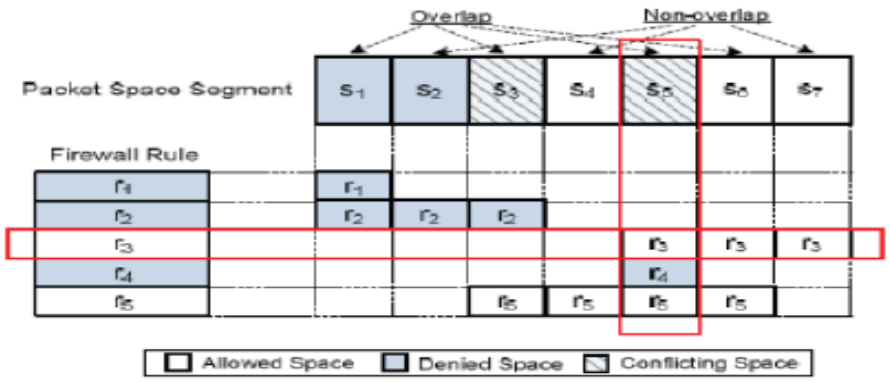
Hemkumar D et al [27], güvenlik duvarı kurallarını analiz etmek için bir grid gösterimi olarak sunmuştur. Grid gösterimi, matris temelli bir görselleştirmesidir. Matrisin yatay ekseni boyunca boşluk bölümleri görüntülenir, kurallar dikey eksen boyunca gösterilir ve bir kesimin kesişimiyle bir kuralın bir kuralı gösteren bir griddir. [27].

Hemkumar D et al [27], güvenlik duvarı politikalarının analizi için grid gösterim yöntemini göstermek üzere aşağıdaki örnek kuralı kullanmıştır.

Tablo 3.6. Grid temsili için örnek güvenlik duvarı kuralı [27]

Rule	Protocol	Source IP	Source Port	Dest IP	Dest Port	Action
R1	UDP	110.12.3.*	*	170.40.1.*	93	Deny
R2	UDP	110.12.*.*	*	170.40.1.*	93	Deny
R3	TCP	110.12.*.*	*	170.48.*.*	42	Allow
R4	TCP	110.12.2.*	*	170.48.1.*	42	Deny
R5	TCP	110.12.2.*	*	*	*	allow

Şekil 3.4. Tablo 3.6.'nın grid temsili



Raining 2D box model metodolojisi, kurallar arasındaki çatışmaları keşfetmek için aynı anda ikiden fazla güvenlik duvarı kuralını birlikte ele almaktadır. Bu model kolayca anlaşılabildiğinden, güvenlik duvarı kurallarındaki anomaliler arasındaki ilişkiyi araştırmak için bu metodoloji kullanılmıştır.

3.4. Raining 2D Box Modeli Kullanarak Kural Anomali Analizi

Bu bölümde, örnek bir güvenlik duvarı kural kümesinin yapısı, kurallar arasındaki ilişkiyi incelemek ve anomalileri tespit etmek için analiz edilmektedir. Yukarıda belirtildiği gibi, mevcut analiz yöntemlerinin çoğu, herhangi iki kural arasındaki anomalileri dikkate almaktadır. Çok az yöntemler ise anomalileri keşfetmek için aynı anda ikiden fazla kuralı birlikte ele almaktadır.

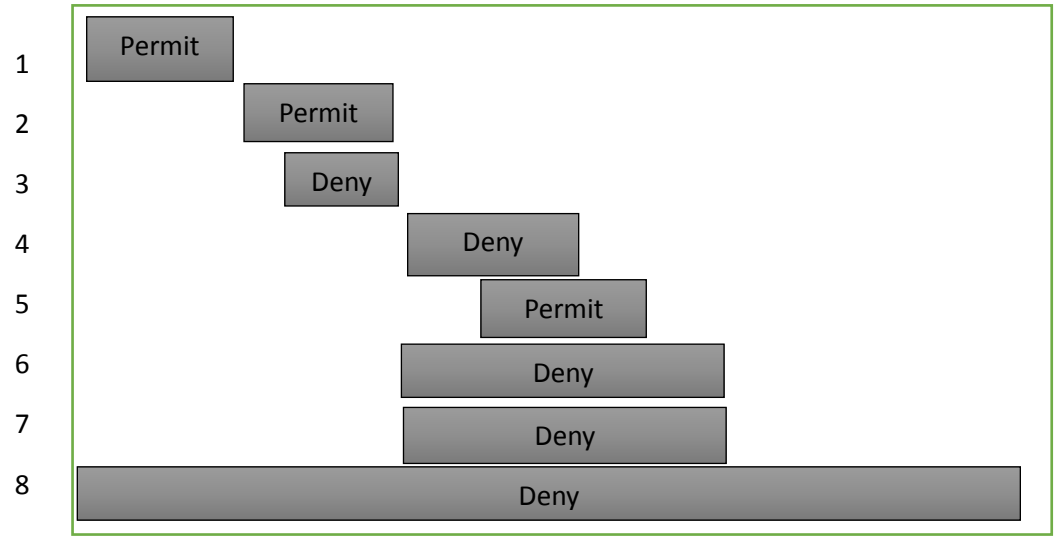
Raining 2D kutu modeli yapısal analiz yöntemi, filtreleme kurallarının basit bir temsilini sağladığından ve aynı zamanda bu kurallar arasındaki ilişkilerin ve anormalliklerin kolayca bulunmasına olanak tanıdığından, bu çalışma güvenlik duvarı kurallarını analiz etmek için bu yöntemi kullanmıştır. İlke grafiğindeki her kutu bir kuralı temsil eder.

İşte analiz etmek için örnek bir güvenlik duvarı kuralları:

Tablo 3.7. Örnek güvenlik duvarı kural seti III

Order ®	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	165.0.0.70	Any	180.0.0.*	22	Permit
2	TCP	140.185.40.*	Any	160.0.0.40	80	Permit
3	TCP	140.185.40.25	Any	160.0.0.40	80	Deny
4	TCP	170.0.0.*	Any	175.0.0.70	21	Deny
5	TCP	170.0.0.14	Any	175.0.0.*	21	Permit
6	TCP	170.0.0.*	Any	175.0.0.*	21	Deny
7	TCP	170.0.0.*	Any	175.0.0.*	21	Deny
8	TCP	Any	Any	Any	Any	Deny

Şekil 3.5. Tablo 3.7.'nin raining 2D kutu modeli



Yukarıdaki örnek güvenlik duvarı kural kümeleri arasındaki ilişkiler

a. Tamamen ayrık - Completely disjoint:

Bölüm 4.1.1'de açıklanan tamamen ayrık bir ilişki tanımına dayanarak, Tablo 3.7 ve Şekil 3.5'ten aşağıdaki ilişkiler elde edilebilir.

- R1 - R2, R3, R4, R5, R6 ve R7 ile tamamen ayrılır.
- R2 - R4, R5, R6 ve R7 ile tamamen ayrılır
- R3 - ayrıca R4, R5, R6 ve R7 ile tamamen ayrılır

b. Kapsayıcı eşleme - Inclusive matching:

Bölüm 3.1.3.'te açıklanan kapsayıcı eylem ilişkisinin tanımına göre, aşağıdaki ilişkiler Tablo 3.7. ve Şekil 3.5.'ten elde edilebilir:

Tüm kurallar R7 varsayılan kuralı ile kapsayıcı bir şekilde eşleşmiştir.

- R3 ve R2 ile kapsamlı olarak eşleşmiştir.
- R4, R6 ve R7 ile kapsamlı olarak eşleştirilmiştir.
- R5, R6 ve R7 ile kapsamlı olarak eşleşmiştir.

c. Korelasyon eşleme- Correlated matching:

Tablo 3.7.'de verilen örnek kuraldan, Şekil 3.5. ve bölüm 3.1.5.'de açıklanan korelasyonlu eşleşmenin tanımına göre şunu söyleyebiliriz ki;

- R4 ve R5 birbiriyle korelasyon olarak eşleşmiştir.

d. Tam eşleme - Exactly matching:

Bölüm 3.1.2.'de açıklanan kapsayıcı uyum ilişkisinin tanımına göre, aşağıdaki ilişkiler Tablo 3.7. ve Şekil 3.5'ten elde edilebilir:

- R6 ve R7 tam olarak eşleştirilmiştir.

Yukarıdaki örnek güvenlik duvarı kural kümesi arasındaki anomaliler

a. Gölge anomalisi - Shadow anomaly:

Farklı kurallara sahip oldukları ve iki kuralın tam olarak eşleştikleri veya ikinci kuralın birinci kuralın kapsayıcı bir eşleşmesi olduğu durumlarda iki kural anormalliği gölgelemektedir. Her iki kural da farklı eylemlere sahip olmaktadır.

Tablo 3.7. deki örnekten kural2 ve kural 3'ü göz önüne alarak:

Rule 2:	140.185.40.*	Any	160.0.0.40	80	Permit
Rule 3:	140.185.40.25	Any	160.0.0.40	80	Deny

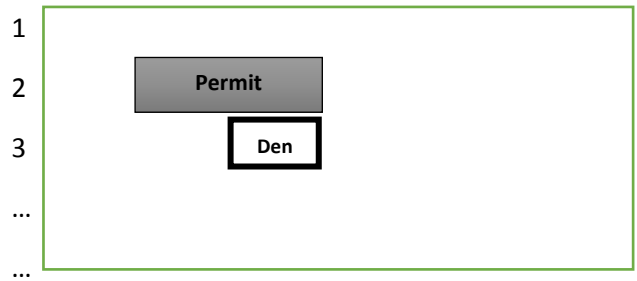
……..... *Shadow anomali tespit edilmiştir.*

Açıklama:

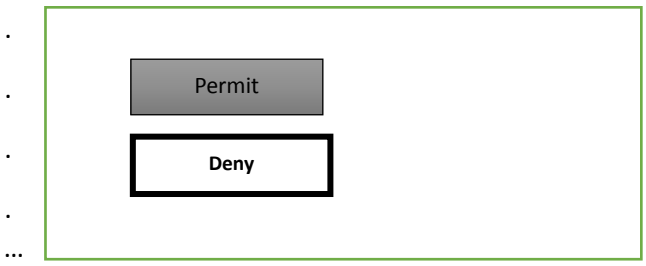
Kural 2, 160.0.0.40 IP adresine sahip tek bir hedef ana bilgisayara gitmek için kaynak IP adresinden 140.185.40. * Gelen tüm paketlere izin verir. Kural 3, 160.0.0.40 hedef IP adresine gitmek için 140.185.40.25 IP adresi olan (140.185.40. * Alt kümesi olan) tek bir ana bilgisayardan paketleri reddeder. R3'e giden tüm paketler R2 tarafından kontrol edildiğinden ve her iki kuralın da farklı eylemleri olduğundan, R2'nin eylemi uygulanır ve Kural3'ün eylemi hiçbir zaman geçerli olmaz. Ve böylece Rule3'ün Rule2 tarafından gölgelenmiş olduğu sonucuna varabiliriz.

Aşağıda Şekil 3.6.'da gösterildiği gibi R2 ve R3'ü, 2D box modelini kullanarak modellenebilmektedir.

Şekil 3.7. ayrıca meydana gelebilecek diğer gölge anomalisi biçimlerini de göstermektedir.



Şekil 3.6. Shadow anomalisi



Şekil 3.7. Shadow anomalinin başka biçimi

Şekil 3.6. ve Şekil 3.7.'de gösterildiği gibi, 2D box modeli temsilini kullanarak shadow anomalisini temsil etmek ve doğrulamak kolaydır.

b. Korelasyon anomalisi - Correlation anomaly:

Iki kuralın eylemi farklıysa ve iki kural korelasyonlu eşleştirmede bulunursa, correlation anomaly olduğunu söyleyebiliriz.

Tablo 4.7.'deki örnek kural kümesinden Kural 4 ve Kural 5'i dikkate alarak:

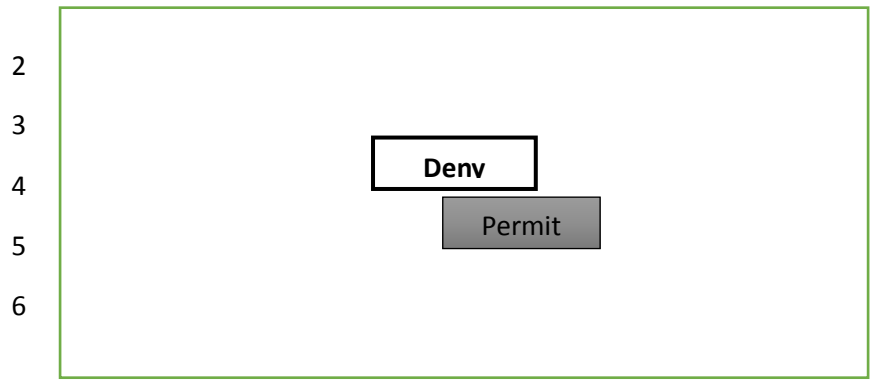
Rule 4:	170.0.0.*	Any	175.0.0.70	21	Deny
Rule 5:	170.0.0.14	Any	175.0.0.*	21	Permit

……..…….. *Correlation anomaly tespit edilmiştir.*

Açıklama:

Kural 4'ten geçen paketlerin bazıları ayrıca Kural 5'ten geçer ve her ikisi de gerçekleştirilecek farklı eylemlere sahiptir. Kural 4'te 170.0.0.* 'dan alınan tüm paketlerin, 175.0.0.70 IP adresiyle tek bir hedefe gitmesi engellenir, ancak 170.0.0. * üyesi olan tek bir kaynağın 170.0.0.14'e tekrar girilmesine izin verilir. adresi 170.0.0. * Kural 5. Bu açıkça, Kural 4 ve Kural 5 arasında korelasyonlu bir ilişki olduğunu ve dolayısıyla korelasyon anomalisinin tespit edildiğini göstermektedir.

R4 ve R5, aşağıdaki gibi 2D box modeli kullanılarak temsil edilebilir.



Şekil 3.8. Correlation anomalisi

c. Genelleştirme anomalisi - Generalization anomaly:

İki kural, farklı eylemlere sahip olduğunda ve ilk kural, ikinci kuralın kapsayıcı bir eşleşmesindeyse genelleştirme anomalisi bulunmaktadır.

Tablo 3.7.'deki örnek kural kümesinden Kural 5 ve Kural 6 göz önüne alındığında:

Rule 5: TCP 170.0.0.14 Any 175.0.0.* 21 Permit

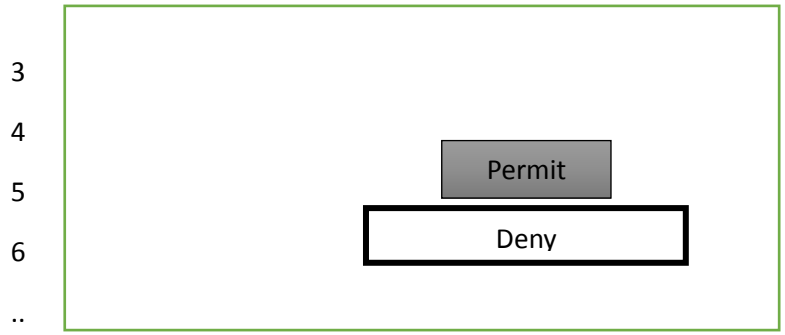
Rule 6: TCP 170.0.0.* Any 175.0.0.* 21 Deny

…… *Generalization anomaly tespit edilmektedir.*

Açıklama:

Kural 6, kaynak IP adresinden çıkacak tüm paketleri reddeder 170.0.0. * Ve bir hedef IP adresine gidiyor 175.0.0.*. Ancak Rule5, 175.0.0.*. Hedef IP adresine giden 170.0.0.14 kaynak IP adresine sahip tek bir ana bilgisayardan paketleri (170.0.0 alt kümesidir. *) Sağlar. R5, R6'nın bir alt kümesi olsa bile, R6'dan önce kontrol edilir ve eylemin gerçekleştirilmesine izin verilir. Bu nedenle, Kural5 ile Kural 6 arasında kapsayıcı bir ilişki ve genelleme anomalisi olduğu sonucuna varabiliriz.

Kural5 ve Kural 6, Şekil 3.9.'da gösterildiği gibi raining 2D kutu modeli kullanılarak modellenebilir.



Şekil 3.9. Generalization anomalisi

d. Fazlalık anomalisi – Redundancy anomaly

İki kural da tam olarak eşleşen veya kapsayıcı eşleştirmede bulunursa ve aynı eylemde bulunduklarında, fazlalık anomalisi bulunur.

Tablo 3.7'den R6 ve R7'i, örnek kural ölarak göz önüne alındığında:

Rule 6: TCP 170.0.0.* Any 175.0.0.* 21 Deny

Rule 7: TCP 170.0.0.* Any 175.0.0.* 21 Deny

……. *Redundancy anomaly tespit edilmiştir.*

Açıklama:

Kural 6 ve Kural 7'de aynı eylem ve aynı parametreler vardır. Kural 6, Kural 7'nin tüm filtreleme işlemlerini yapabilir.

Tablo 4.6.'dan R7 ve R8'i, örnek kural ölarak göz önüne alındığında:

Rule 7: TCP 170.0.0.* Any 175.0.0.* 21 Deny

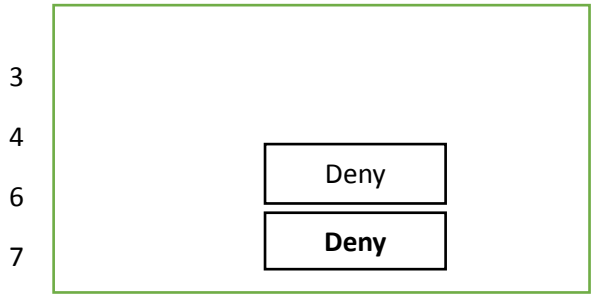
Rule 8: TCP Any Any Any Any Deny

…….*Redundancy anomaly tespit edilmektedir.*

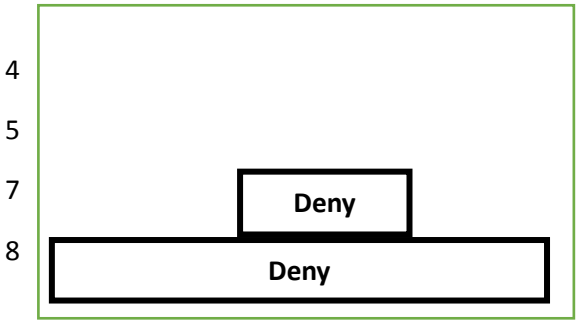
Açıklama:

Fazlalık kuralı, aynı kuralı aynı paket üzerinde başka bir kural ile gerçekleştirir, Böylece gereksiz kural kaldırıldığında, güvenlik politikası bundan etkilenmez. Burada Kural 6 ve Kural 7'de aynı eylem vardır ve Kural 7, Kural 6'ya uyan tüm paketlerle eşleşen varsayılan kuraldır. Bu nedenle, Kural 7, Kural 6'nın tüm filtreleme işlemlerini yapabilmektedir. Bu nedenle, Kural 6'nın kaldırılması güvenlik duvarı politikasındaki hiçbir şeyi değiştirmeyecektir. Bu, gereksiz anomali oluşumunu göstermektedir.

R6 ve R7, R7 ve R8, 2D box modeli modeli kullanılarak Şekil 4.10. ve Şekil 4.11.'de gösterildiği gibi modellenebilir.



Şekil 3.10. Redundancy anomalisi I



Şekil 3.11. Redundancy anomalisi II

BÖLÜM 4. GÜVENLİK DUVARI KURALLARININ OPTİMİZASYONU

4.1. Güvenlik Duvarı Kuralları Optimizasyonu

Güvenlik duvarı ilkeleri, sırayla işlenen kuralların bir listesinden oluşur. Güvenlik duvarına bir veri paketi geldiğinde, güvenlik duvarı onu politikadaki bir kuralla eşleştirmeye çalışır. Bir kural eşleştiğinde, paket, paketin bırakılması veya iletilmesi gibi tanımlanan eyleme göre işlenmektedir [38].

Bir paket birden fazla kuralla eşleştiğinde, yalnızca ilk kural yürütülmektedir. Böylece, bir paket iki veya daha fazla ayrık olmayan kurallarla eşleşirse, anomali olur. Anomali, ağdaki aynı paketle eşleşebilecek iki veya daha fazla filtreleme kuralının olmasıdır.

4.1.1. Anomali tespiti ve çözümü

Güvenlik duvarı ilkeleri, yukarıdan aşağıya doğru işlenen kuralların bir listesinden oluşturmaktadır. Güvenlik duvarına bir veri paketi geldiğinde, güvenlik duvarı onu politikadaki bir kuralla eşleştirmeye çalışmaktadır. Paket eşleştirmesi işlenirken, farklı türdeki anomaliler olabilmektedir. Bu anomalilerden gölge ve fazlalık, güvenlik duvarı kural kümesinde ki ciddi hatalardır. Bu çalışma tekniklerini önermekte ve bu iki anomali türünü tespit etmek ve çözmek için bir uygulama geliştirmektedir.

a. Gölge anomalisi - Shadowing anomaly:

Önceki bölümlerde ele alındığı gibi, bir kural önceki kurallardan biri geçerli kurala uyan tüm paketlerle eşleştiğinde gölgelenir ve her ikisi de farklı eylemler gerçekleştirmektedir, böylece gölgeli kural asla değerlendirilmez. Gölgeli kural

kaldırılırsa dahi, güvenlik ilkesi bundan etkilenmez. Gölgelendirme anomali bir hatadır ve gölgeli kuralları bulmak ve gölgeli kuralı yeniden sıralayarak veya kaldırarak uygun bir eylemi gerçekleştirmesi için yöneticiyi uyarmak önemlidir.

Bu çalışma, verilen kural kümesinden gölge anomalisini tespit etmek ve çözmek için iki yaklaşımı ele almaktadır.

1. İki kural tam olarak eşleşiyorsa ancak farklı eylemler varsa, iki kuraldan birini optimizasyon prosedüründe kaldırmak önemlidir. Bu nedenle yönetici hangi kuralın kaldırılacağına karar verir.
2. İki kural kapsayıcı eşleme ilişkisinde ise ve ikinci kural birinci kuralın alt kümesidir, ancak farklı eylemlere sahipse, kuralları yeniden sıralamak veya ikinci kuralı en iyileştirme yordamında kaldırmak önemlidir. Bu nedenle yönetici, ya iki kuralları yeniden sıralamaya ya da zaten gölgelenmiş olan ikinci kuralı kaldırmaya karar verir. Yeniden sıralama yapılırken, güvenlik duvarı kural kümesinde sorun olarak kabul edilmeyen genelleştirme anomalisinin gerçekleşmesi beklenmektedir.

Örnek:

Tablo 4.1. Shadowıng anomalisi örnek

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.*	All	160.0.0.40	80	Permit
2	TCP	140.185.40.*	80	160.0.0.40	80	Deny

Açıklama:

Kural1 ve Kural2 aynı ağ trafiği ile eşleşir ve Kural2, Kural 1'in alt kümesidir. R1, 140.185.40. * Ağından gelen kaynak IP adresiyle trafiği eşleştirir ve R2, 140.185.40.25 kaynağından (140.185.40. * ‘dan bir üye adresi) olan trafik IP adresiyle trafiği eşleştirir. Her iki kuralın eylemleri de farklıdır. Rule2, Kural 1

tarafından gölgelenmiştir ve asla değerlendirilmeyecektir. Son olarak gölgeli kurallara uygun eylem yapılmaktadır.

Kural 2, Kural 1 tarafından gölgelenmiş olduğundan, iki çözümden biri yapılmalıdır.

Çözüm 1: Gölgeli kuralı kaldırma (R2)

Kural 2'yi kaldırırken güvenlik duvarı kural kümesinde değişiklik olmaz.

Tablo 4.2. Gölgeli kural kaldırıldıktan sonra - gölgelenme anomalisinden arındırılmıştır

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.*	All	160.0.0.40	80	Permit

Çözüm 2: Kuralları yeniden sıralamak

İki kuralı yeniden düzenlerken genelleştirme anomalisi olur.

Tablo 4.3. Kurallar yeniden düzenlendikten sonra - gölge anomalisinden arındırılmışdır

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.*	All	160.0.0.40	80	Deny
2	TCP	140.185.40.*	80	160.0.0.40	80	Permit

Gölge Kural Anomalisi Tespiti ve Çözümü Algoritması (Shadowing Anomaly Detection and Resolution Algorithm)

Giriş: optimize olmayan rasgele bir kural kümesi

Çıktı: Shadow anomalisinden arındırılmış bir kural kümesi

Başla:

Aşama 1: iki gölge anomalisi formatını tanımla

S1, S2 = false

Aşama 2: Toplam kural sayısını ve kural sırasına ait değişkeni belirle

n=total number of rules – toplam kurallar

R[i]=güvenlik duvarı rule of order i - kural i

Aşama 3: Her bir kural ile alakalı parametreleri oku - 6 parametre

Protocol (P), source IP address (SIP), source port number (SP), destination IP address (DIP), destination port number (DP), Action (A)

Aşama 4: Her bir kuralda 5 parametersi aynı olan, fakat aksiyonu farklı olanları bul/ara

```
for i=1 to n-1
    for j=i+1 to n
If parameters of Rule[i] are equal to parameters of Rule[j]
         AND action[i] is not equal to action[j]
            S1 = true
            Display "Shadow Anomaly Detected [S1]"
            goto Step6 //Aşam 6
            end if
      end for
 end for
```

Aşama 5: Altküme ya da üstküme ilişksi olan fakat aksiyonu farklı olanları bul/ara karşılaştır

```
      for k=2 to n
      if parameters of Rule[k] are subsets of corresponding
                    parameters of Rule[k-1] AND action[k] is
not equal to              action[k-1]
                  S2 = true
            Display "Shadow Anomaly Detected [S2]"
            goto Step6 //Aşam 6
             end if
      end for
```

Aşama 6: Anomalileri kaldır

```
A. if S1==true
      remove R[i] OR R[j]
    end if

B.  if S2==true
      remove R[k] or swap Rule[k,k-1]
   end if
```

Aşama 7: Kural R[i]'yi kaldır

Delete rule R[i] from the güvenlik duvarı ruleset

Aşama 8: R[i] ve R[j] yeri değiştir

```
temp =Ri
Ri=Rj
Rj=temp
```

Aşama 9: Gölge anomalisinden arındırılmış kural kümesini elde et

Bitti

b. Fazlalık Anomalisi - Redundancy Anomaly:

Önceki bölümlerde ele alındığı gibi, gereksiz kurallar keşfedildiğinde artıklık anomalisi ortaya çıkmaktadır. Yedekli kural aynı işlemi başka bir kuralla aynı paketlerde gerçekleştirir. Ve aynı pakette eşleşecek olan politikada daha düşük tanımlanan herhangi bir kural gereksizdir ve asla kontrol edilmez. Yedekli kuralların kaldırılması, güvenlik duvarı politikasının davranışı üzerinde hiçbir etkinin olmayacağı kesindir ve kaldırılmalıdır [39].

Yedekli kuralların kaldırılması, arama süresini ve alan gereksinimlerini azaltarak güvenlik duvarının performansını artıracaktır [38].

Bu çalışma, gereksiz anomaliyi ciddi bir hata olarak ele almakta ve bunları belirlenen kural setinden tespit etmek ve çözmek için iki yaklaşım önermektedir:

1. İki kural tam olarak eşleşiyorsa ve aynı eylemde bulunuyorsa, iki kuraldan birini optimizasyon prosedüründe kaldırmak önemlidir. Bu nedenle sistem ikinci kuralı otomatik olarak kaldırır.
2. İki kural tamamen birbiriyle eşleşen bir ilişki içerisindeyse ve aynı eylemi gerçekleştiriyorsa, optimizasyon prosedüründe alt küme kuralını kaldırmak önemlidir. Bu nedenle sistem, alt küme kuralını otomatik olarak kaldırır. Bu iki biçimde yapılabilir:
   a. İlk kural, ikinci kuralın bir alt kümesi eşleşmesiyse, ilk kuralı otomatik olarak kaldırır.
   b. İkinci kural, birinci kuralın bir alt kümesi eşleşmesiyse, ikinci kuralı otomatik olarak kaldırır.

Örnek

Tablo 4.4. Redundancy anomalisi örnek

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.10	All	160.0.0.40	80	Deny
2	TCP	140.185.40.*	All	160.0.0.40	80	Deny
3	TCP	140.185.40.*	All	160.0.0.40	80	Deny
4	TCP	140.185.40.25	All	160.0.0.40	80	Deny

Açıklama

Güvenlik duvarı kuralları yukarıdan aşağıya doğru kontrol edildiğinden, aşağıdaki gibi uygun eylemler gerçekleştirilir. Kural1, aynı eylemi olan Kural2'nin bir altkümesi eşleşmesidir ve aynı eyleme de sahiptir. Bu nedenle Kural1 otomatik olarak kaldırılmalıdır. Rule2 ve Rule3 aynı ağ trafik ile eşleşir ve aynı eyleme sahiptir, bu nedenle Kural 3 otomatik olarak kural kümesinden kaldırılmalıdır. Kural 4'ün 140.185.40.25 kaynağının IP adresi 140.185.40. * Alt kümesidir. Bu nedenle Kural 4 asla kontrol edilmez ve otomatik olarak kaldırılmalıdır.

Fazlalık kurallar kaldırıldıktan sonra sadece belirgin bir kural kalmaktadır.

Çözüm: fazlalık kuralların aşama aşama kaldırılması.

Aşama 1:

Kural1 ve Kural2 (Tablo 4.4.) artıklık için kontrol edilir. Kural1, Kural 2'nin bir alt kümesi olduğundan ve Kural1, Kural2 ile aynı paketle eşleştiğinden dolayı kaldırılır.

Tablo 4.5. Tablo 4.4.'daki gereksiz kuralları kaldırma – adım

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.*	All	160.0.0.40	80	Deny
2	TCP	140.185.40.*	All	160.0.0.40	80	Deny
3	TCP	140.185.40.25	All	160.0.0.40	80	Deny

Aşama 2:

Kural1 ve Kural2 (Tablo 4.5.) anomali için kontrol edilir. Kural 1 ve Kural 2 aynı eylemle aynı filtreleme ölçütlerine sahiptir. Böylece ikisinden biri (Kural 2) kaldırılmalıdır.

Tablo 4.6. Tablo 4.5 dan. - adım II'nin gereksiz kurallarının kaldırılması

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.*	All	160.0.0.40	80	Deny
2	TCP	140.185.40.25	All	160.0.0.40	80	Deny

Aşama 3:

Kural1 ve Kural2 (Tablo 5.6.) yedeklilik için kontrol edilir. Kural 2, Kural 1'in bir alt kümesi olduğundan ve Kural2, Kural 1 ile aynı paketle eşleştiğinden, kontrol edilmez. Yani Rule2 kaldırılmalıdır.

Tablo 4.7. Çizelgeden arta kalan serbest format

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.185.40.*	All	160.0.0.40	80	Deny

Fazlalık Kural Anomalisi Tespiti ve Çözümü Algoritması (Redundancy Anomaly Detection and Resolution)

Giriş: optimize olmayan rasgele bir kural kümesi

Çıktı: Fazlalık anomalisinden arındırılmış bir kural kümesi

Başla:

Aşama 1: Üç tane farklı fazlalık anomalisi formatını tanımla

```
R1, R2, R3 = false
```

Aşama 2: Değişkenleri belirle

`n`= toplam kural sayısı total number of rules –

`R[i]`=Kural i

Aşama 3: Her bir kuralın altı tane paramretreyi oku

Protocol (P), source IP address (SIP), source port number (SP), destination IP address (DIP), destination port number (DP), Action (A)

Aşama 4: Her bir kural için bütün parameterlerin eşitliği için karşılaştır

```
for i=1 to n-1
      for j=i+1 to n-1
            If parameters of Rule[i] are equal to
      parameters of            Rule[j] AND action[i]
      is equal to action[j]
                  R1 = true
                  Display "Redundancy Anomaly Detected -
            1"
                  goto Step6 //Aşam 6
```

```
            end if
          end for
        end for
```

Aşama 5: Aksiyonu aynı olan bütün alt ve üst küme kuralları karşılaştır

```
for k=2 to n
   if parameters of Rule[k] are supersets of
   corresponding      parameters of Rule[k-1] AND
   action[k] is equal to         action[k-1]
          R2 = true
           Display "Redundancy Anomaly Detected
- 2"
           goto Step6 //Aşam 6
       end if
      if parameters of Rule[k] are subsets of
   corresponding         parameters of Rule[k-1]
   AND action[k] is equal to        action[k-1]
          R3 = true
         Display "Redundancy Anomaly Detected -
3"
          goto Step6 //Aşam 6
       end if
end for
```

Aşama 6: Anomalileri bul

```
A.
   if R1 == true then
      remove R[j]
   end if
B.
   if R2 == true  then
      remove R[k-1]
   end if
C.
   if R3 == true then
      remove R[k]
```

```
        end if
```

Aşama 7: Kural [i]'yi kaldır

Delete rule R[i] from the güvenlik duvarı ruleset – kural kaldır

Aşama 8: Fazlalık anomalisinden arındırılmış kural kümesini elde et

Bitti

4.1.2. Güvenlik duvarı kurallarını birleştirme

Güvenlik duvarı kural kümesi herhangi bir anomaliden arındırıldıktan sonra, iki veya daha fazla kuralı tek bir kuralda birleştirerek daha da optimize edilebilmektedir. Daha küçük bir politika oluşturmak için kuralların birleştirilmesi, yönetim ve performans açısından daha iyidir.

Aşağıdaki durumlarda iki veya daha fazla kural tek bir kuralda birleştirilebilir:
- Tüm parametreleri tek bir parametre haricinde diğer tüm parametreler eşittir ve
- Eylemler benzer olmalıdır.

Bu çalışma, iki birleşme durumu analiz etmektedir.

Durum 1:

İlk durum, birleştirilebilecek tüm kuralların sıralı olarak bir araya gelmesidir. Bu süre zarfında, tüm kurallar tek bir kural olarak birleştirilir.

Örenk 1:

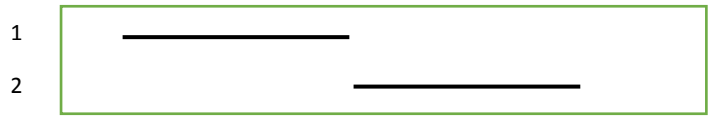
Kaynak protokolü dışında aynı parametrelerle ayarlanmış örnek bir kural:

Yalnızca iki protokolün (TCP / UDP) ağ üzerinden geçtiğini varsayarsak, aşağıdaki iki çatışmasızr kural tek bir kuralda birleştirilebilir.

Tablo 4.8. Örnek güvenlik duvarı kuralları I - kuralları birleştirmek

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	190.150.140.38	80	190.180.39.*	*	ACCEPT
2	UDP	190.150.140.38	80	190.180.39.*	*	ACCEPT

Şekil 4.1. Tablo 4.8.'in grafiksel gösterimi şekil

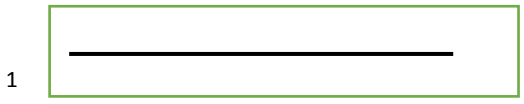


Bu iki kural aşağıdaki kuralla birleştirilebilir. Protocol * hem TCP hem de UDP protokollerini temsil eder.

Tablo 4.9. Birleştirilmiş Tablo 5.8.

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	*	190.150.140.38	80	190.180.39.*	*	ACCEPT

Şekil 4.2. Tablo 4.9.'ün grafiksel gösterimi şekil



Örnek 2:

IP adresi dışında aynı parametrelere sahip başka bir örnek.

Tablo 4.10. Örnek güvenlik duvarı kuralları II - kuralları birleştirmek

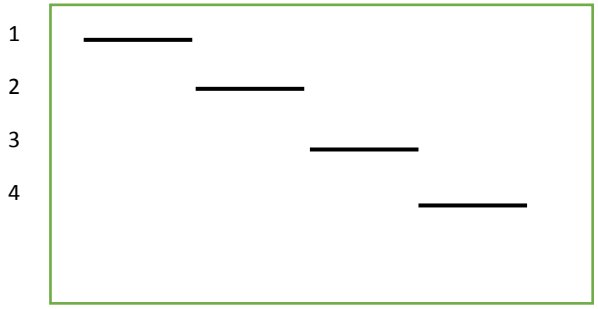
Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	100.0.0.0/26	Any	50.0.0.0/24	443	Permit
2	TCP	100.0.0.64/26	Any	50.0.0.0/24	443	Permit
3	TCP	100.0.0.128/26	Any	50.0.0.0/24	443	Permit
4	TCP	100.0.0.192/26	Any	50.0.0.0/24	443	Permit

Kuralları birleştirdikten sonra

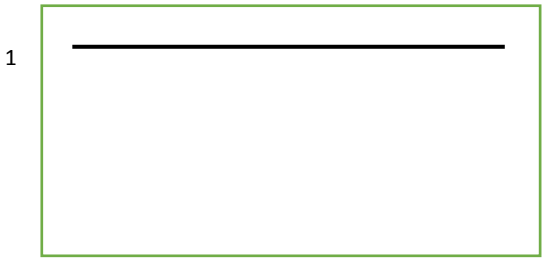
Tablo 4.11. Kombine Tablo 4.10.

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	100.0.0.0/24	Any	50.0.0.0/24	443	Permit

Şekil 4.3. Tablo 4.10.'un grafiksel gösterimi



Şekil 4.4.1 Tablo 4.10.'un grafiksel gösterimi



Şekil 4.5. Tablo 4.11.'in grafiksel gösterimi

Durum II.

İkinci durum, birleştirilecek kuralların sıralı olmamasıdır.

İşte örnek kural.

Tablo 4.12. Örnek güvenlik duvarı kuralları III - kuralları birleştirmek

Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	100.0.0.0/26	Any	50.0.0.0/24	125	Permit
2	TCP	100.0.0.64/26	Any	50.0.0.0/24	120-130	Permit
3	TCP	100.0.0.96/26	Any	50.0.0.0/24	140	Deny
4	TCP	100.0.0.128/26	Any	50.0.0.0/24	120	Permit
5	TCP	100.0.0.192/26	Any	50.0.0.0/24	110-135	Permit

Tablo 4.12.'de görüldüğü gibi, Kural 1, 2, 4 ve 5, kaynak IP adresi dışında aynı parametrelere sahiptir ve Kural3, birden fazla parametresi olan diğer kurallardan farklıdır. Kural kuralı, Kural 1, 2, 4 ve 5 için yapılabilir.

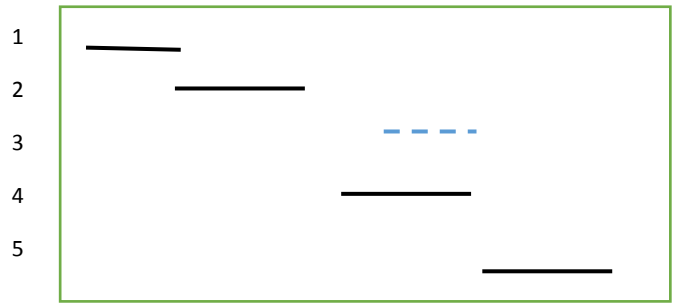
Bu beş kural aşağıdaki kurallara birleştirilebilir:

Tablo 4.13. Tablo 4.12'yi birleştirmesi

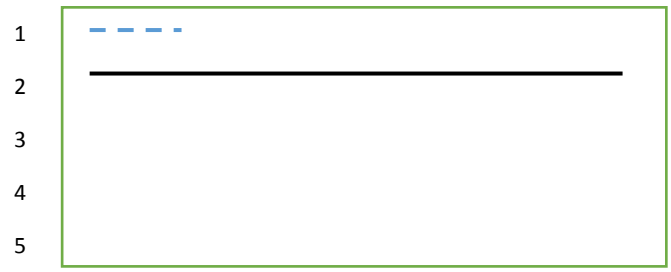
Order (R)	Protocol	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	100.0.0.96/26	Any	50.0.0.0/24	140	Deny
2	TCP	100.0.0.0/24	Any	50.0.0.0/24	110-135	Permit

Aşağıdaki şekilde grafik olarak gösterilebilir:

Şekil 4.6. Tablo 4.12.'nın grafiksel gösterimi



Şekil 4. 7. Tablo 4.13.'ün grafiksel gösterimi



4.2. Paket Eşleştirme Zaman Optimizasyonu

Bölüm 4.1.'de anomali tespiti, çözünürlük ve birleştirme teknikleri tartışılmakta ve mevcut güvenlik duvarı kurallarının anomalisiz ve optimize edilmiş formunun oluşturulması için yeni bir yöntem önerilmektedir. Güvenlik duvarı kuralı herhangi bir anomali durumdan arındırldıkten sonra, trafiğin paket eşleştirme zamanını iyileştirerek daha iyi duruma getirilebilmektedir. Bu bölüm, güvenlik duvarının paket eşleştirme süresini geliştirmek için yeni bir teknik önermektedir.

Bir güvenlik duvarının paket eşleştirme maliyeti, kuralları sıralayarak ve aşağıdaki üç kuralı uygulanarak azaltılabilir ve iyileştirilir. Birincisi, güvenlik duvarı tarafından sürekli kontrol edilen kuralları tespit edip onları mümkün olduğu kadar kural tablosunda en üst sıraya almaktadır. İkincisi, güvenlik duvarı tarafından kontrol edilmeyen (veya biraz kontrol edilen) ve çürüyen (eskimeye başlayan) ya da tablonun alt kısmında yer alan az sayıdaki (alakasız) kuralların tespit edilmesidir. Son olarak, kuralların entegrasyonunu sağlayarak kurallar arasındaki sırayı çok doğru ve düzenli bir şekilde korumaktadır.

Bu çalışma, paket eşleştirme zamanının optimizasyonu için uygun önlemleri almak ve kuralların sırasını düzenli olarak güncellemek için iki yaklaşım kullanmaktadır. Zaman ve performansa dayalı periyodik yaklaşımlar.

- Zamana dayalı periyodik yaklaşım: Güvenlik duvarı kural kümesini belirli bir süreye bağlı olarak güncellemektir.
- Performansa dayalı periyodik yaklaşım: kontrol edilen trafik sayısına göre belirlenen güvenlik duvarı kuralının güncellenmesi işlemidir.

Her iki yaklaşımı kullanırken, performans yaklaşımına öncelik verilmektedir. Bu nedenle, tanımlanan paket sayısı kontrol edildiğinde, güvenlik duvarı kuralı otomatik olarak güncellenir ve uygun önlemleri alınmasını önermektedir. Belirli bir süre içinde kontrol edilen trafik sayısı, tanımlanan trafik sayısı kadar değilse, periyodik güncelleme tetiklenecek ve paket eşleştirme süresi optimize edilmektedir.

Paket eşleştirme zaman optimizasyonu aşağıdaki üç aşamada yapılır.

a. Güvenlik duvarı kuralları yeniden sıralama
b. Alakasız kuralları önerme (kaldırma)
c. Kuralların bütünlüğünü korumak

4.2.1. Güvenlik duvarı kuralları yeniden sıralama

Güvenlik duvarı kuralları yeniden sıralama, güvenlik duvarı kural kümesinin sırasını optimize etmek için paket eşleştirme istatistiklerini kullanan bir mekanizmadır. Kuralların yeniden düzenlenmesi, güvenlik duvarının paket eşleştirme süresini iyileştirir ve ağ trafiğinin davranışını kolayca anlamaya olanak tanır.

Bir kuralın eşleşme oranı (olasılık), tüm kural kümesi için eşleşen toplam paket sayısıyla eşleşen bir kuralın kaç kez bölünmesiyle hesaplanabilir. Algoritma da her bir filtreleme kuralı için eşleşme oranını hesaplar ve artan bir düzen kural kümesi oluşturur. Daha sonra, en yüksek olasılığa sahip kural, tablonun en üstünde olmalıdır.

$$P_R = \frac{R_k}{\sum_{k=1}^{n} R_k} \quad \text{---------- (1)}$$

Burada, PR bir R kuralına uyan bir paketin olasılığıdır.

RK, Kural K tarafından eşleştirilen paketlerin sayısıdır.

n, güvenlik duvarı kural listesindeki toplam kural sayısıdır

Yeniden sıralama veya sıralama, bir diziyi girdi olarak alan, dizide belirtilen işlemleri gerçekleştiren ve sıralanmış bir diziyi çıkaran komut dizilerinden oluşan bir yöntemdir.

Güvenlik duvarı kurallarını yeniden sıralamak için farklı sıralama algoritmaları vardır. İnsertion sıralaması dizileri neredeyse sıralandığında ya da yalnızca çok sayıda elemanın büyük bir dizide yanlış yerleştirildiği durumlarda ekleme sıralama

pek çok açıdan daha iyidir [41]. Eleman sayısı az olduğunda da yararlı olabilir. İlk yeniden sıralamadan sonra, güvenlik duvarı k0uralları neredeyse sıralanabilir veya sadece birkaç öğe yanlış yerleştirilmiş olabilir. Bu nedenlerden dolayı, ekleme sıralama, paket eşleştirme zamanının optimizasyonu için kural listesini yeniden sıralamak için uygun bir sıralama algoritması olabilir [40]. Algoritmanın ne kadar hızlı çalıştığını ve ne kadar alanda çalıştığını da göz önünde bulundurmak önemlidir. Kurallar zaten sıralandığında, ekleme sıralama en az zaman alır (N sayısı).

4.2.2. Alakasız kurallar

Güvenlik duvarının paket eşleştirme süresini en iyi hale getirmenin ikinci yolu, alakasız kuralları kaldırmaktadır. Bir güvenlik duvarı kural kümesinde, belirli bir süre boyunca etkin olmayan kurallar olabileceği yaygındır. Bir kuralın hem kaynak hem de hedef adresleri, güvenlik duvarı aracılığıyla erişilebilen herhangi bir alanla eşleşmiyorsa, bir kural alakasız olabilir. Alakasız kurallar, filtreleme işlemine gereksiz ek yük getirir. Filtreleme kuralının olabildiğince küçük tutulması genel güvenlik duvarı performansının iyileştirilmesine yardımcı olur.

Bu çalışma, eşleşen trafik sıklığını kullanarak alakasız kuralları tespit etmek ve çözmek için bir algoritma önermiştir. Yöntem, önceki yeniden sıralama algoritması ile birlikte tanımlanır. Bu özel kural için bir paketin eşleşme olasılığı sıfırsa veya sıfıra çok yakınsa, algoritma bu kuralın kaldırılmasını önerir.

4.2.3. Kuralların bütünlüğü

Politika bütünlüğü, güvenlik duvarı kuralları arasındaki sırayı çok doğru ve düzenli bir şekilde sürdürme sürecidir. Güvenlik duvarı kural kümesinin yeniden düzenlenmesine rağmen, güvenlik duvarı kural kümesinin varsayılan kuralının kural listesinin sonunda olması gerektiği açıktır.

Paket Eşleştirme Zaman Optimizasyonu (PEZO) Algoritması (Optimize Packet Matching Time Algorithm – OPMT)

Giriş: Anomalisiz güvenlik duvarı kural seti

Output: Eşdeğer ancak daha etkili bir güvenlik duvarı kural seti

Başla

Aşama 1: Açıklama

T= toplam paket sayısı

n= toplam kurallar sayısı

t[]= her bir kural için kontrol edilen paket sayısı

r[]=kurallar dizisi

w[]= her kurallın yüzde oranı

Aşama 2: Toplam paket sayısı hesapla - Calculate total number of packets checked by the güvenlik duvarı –

```
for (i=1; i<=n; i++)
    T=sum t[i]
end for
```

Aşama 3: Her kurallın yüzdesini hesapla - Calculate weight of each rule

```
for (i=1;i<=n ; i++)
       w[i]=t[i]/T
end for
```

Aşama 4: Varsayılan (son) kuralı hariç, insertion sıralama kullanarak azalan sırayla sırala - Sort weight in descending order using insertion sort (DSC), excluding the default (last) rule. -

```
for (p= 2; p<=n-1; p++)
   for (q=p; q>=1; q--)
      if (R[q]>R[p])
      swap (R[p,q])
      end if
end for
end for
```

Aşama 5: kuralların yerini değiştir - Rule[p,q]

```
temp =R[p]
R[p]=R[q]
R[q]=temp
```

Aşama 6: Sıralayan kralı elde et - Obtain sorted rule set

Aşama 7: Gereksız kurallarını tespit et - check for irrelevant rules

```
for (j=1;j<=n-1;j++)
      if w[j] == 0
        remove R[j]
      end if
end for
```

Aşama 8: Kuralı -Rule [i] kaldırmaya tavsiye et - Recommend to remove– Rule [i]

Aşama 9: Optimize olan kural seti elde et

Bitti

4.3. Güvenlik Duvarı Sıkılaştırması

Güvenlik duvarını güvenli hale getirmek karmaşık bir konudur ve durumdan duruma değişebilir. Güvenlik duvarı sertleştirme, güvenlik duvarını güvenlik açığı azaltarak güvenlik altına alma işlemidir [55]. Güvenlik duvarı ilkesi yazarken, gelecekteki güvenlik sorunlarını önlemek için olası güvenlik risklerini dikkate almak önemlidir. Farklı güvenlik politikaları ve kuralların yapılandırılması konusunda sıkı koruma kullanmak, güvenlik duvarı kuralları sertleştirilebilir.

Bu çalışma, güvenlik duvarı kurallarını sertleştirmek için aşağıdaki mekanizmaları önermektedir.

a. Varsayılan olarak engelleme:

Tüm trafiği varsayılan olarak engelle ve yalnızca belirli trafik işlemlerine açıkça izin ver. Böylece servis yanlış yapılandırması nedeniyle veri ihlali olasılığı azaltılabilir. Bu, bir güvenlik duvarı politikasında son kuralın tüm insan ticaretini reddetmesiyle sağlanabilir [55].

b. Belirli trafiğe izin ver

Ağ erişimine izin vermek için kullanılan kurallar daha spesifik olmalıdır. Bu, kural parametrelerini mümkün olduğunca çok parametre belirterek yapılabilir. Böylece, paket eşleştirmesi mümkün olduğunca hızlı yapılır [55].

c. Kaynak ve hedef IP adresleri belirtin

Hizmetin internet'teki herkes tarafından erişilebilir olması dışında, herhangi bir kaynak IP adresi doğru seçenektir. Diğer tüm durumlarda, kaynak adresi belirtmelisiniz.

d. Güvenli protokolleri kullanma

Güvenlik duvarlarını yapılandırırken, güvenli protokolleri göz önünde bulundurmak şiddetle tavsiye edilir. Güvenlik duvarlarını yapılandırırken aşağıdaki güvenli protokollerin kullanılması önerilir. Böylece, geçişteki verilerin doğruluğunu ve gizliliğini sağlamak [55].

- Uzaktan erişim için Telnet üzerinden SSH protokolünün tercih edilmesi gerekir, böylece veriler gerçek olur ve bilgiler de şifrelenir.
- Güvenli dosya transferi için FTP veya TFTP'den ziyade SCP kullanılmalıdır. SCP, veri aktarımı için Güvenli Kabuk (SSH) kullanır ve kimlik doğrulama için aynı mekanizmaları kullanır.

e. Backup – Yedekleme

Güvenlik duvarı kural tabanı ve yapılandırma dosyalarını düzenli olarak yedekleyin, böylece sistem arızası durumunda yedeklemeler kullanılabilir ve arıza süresinin azaltılmasına yardımcı olur.

Tablo 4.14. Genel anomali tesbiti ver çözüm çerçevesi

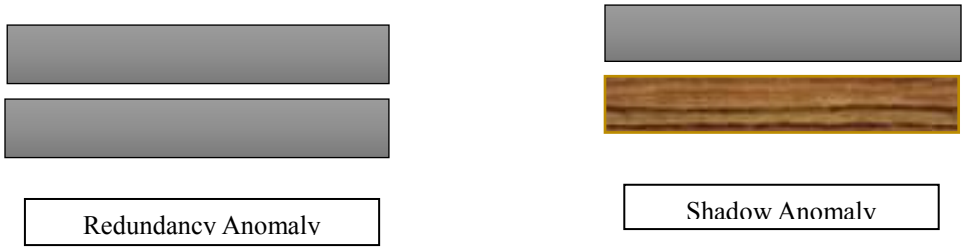
Name	Relation type	What to do	Action	Anomaly type	Resolution technique	By
1	Completely disjoint	—	—	—	—	—
2	Exactly matching	To be detected	same action	**Redundant**	**Remove the duplicate**	Automatic
			different action	**Shadow**	**Select and remove one of the two**	Admin
3	Inclusive matching	To be detected	—	**Shadow**	**Reorder or Remove the second**	Admin
			Rx is subset of Ry	**Redundancy**	**remove Rx**	Automatic
			Rx is superset of Ry	**Redundancy**	**remove Rxy**	Automatic
		—	—	Generalization	—	—
4	Correlated matching	—	—	Correlation	—	—

Combine	Same packet with only one parameter difference	After anomaly resolution	By: Admin

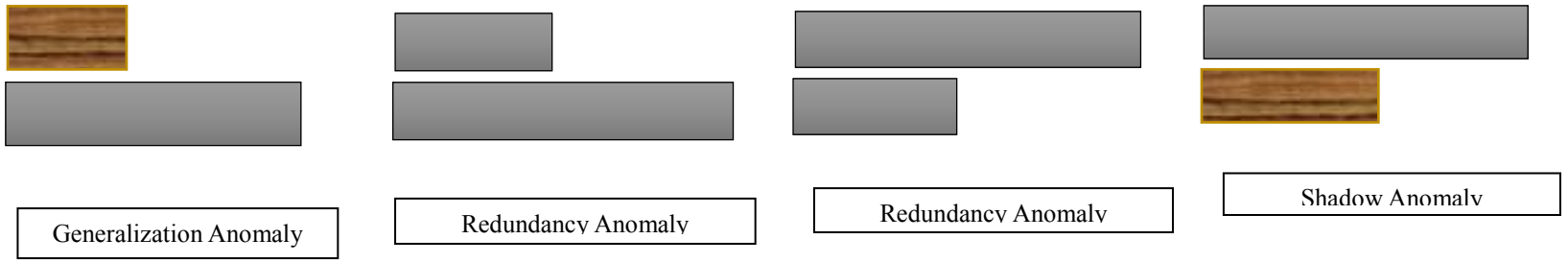
Reorder	Recommend to admin to reorder	Alarm periodically	By: Admin
Irrelevant rules	Recommend to admin to remove	Alarm periodically	By: Admin

General framework – Rules relations

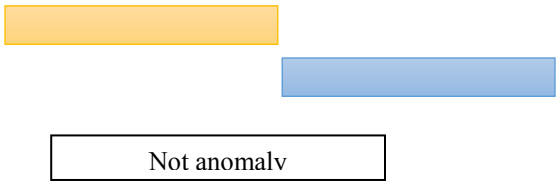
I. Exactly matching



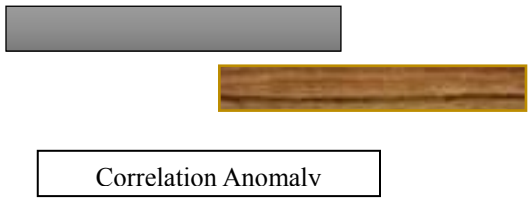
II. Inclusive matching



III. Completely disjoint matching



IV. Correlation matchi



Şekil 4.7. Genel çerçeve – kural ilişkileri

4.4. Araştırma Sonuçları

Güvenlik duvarları, bir ağın güvenliğini sağlamak için en çok kullanılan güvenlik mekanizmasıdır. Güvenlik duvarı, bir ağa gelen veya giden paketleri inceleyerek ağ erişimini sınırlar. Muayene, paket üstbilgisini ilk eşleşme veya varsayılan kural bulunana kadar bir kural listesiyle karşılaştırarak gerçekleştirilir. Diğer tüm teknolojiler gibi, güvenlik duvarı daha iyi bir performans sağlamak için uygun bir yapılandırma ve yönetim gerektirir. Güvenlik duvarını yönetmenin karmaşıklığı nedeniyle, kural çakışmaları ve kural uyuşmazlıkları olma olasılığı yüksektir. Dolayısıyla, bir güvenlik duvarına sahip olmak, mutlaka bir ağı güvenli bir hale getirmeyebilir.

Algoritmalar ve web tabanlı bir uygulama geliştirerek güvenlik duvarının kurallarını ve paket eşleştirme süresini optimize etmek için farklı teknikler sunduk. Bu tezde, bir güvenlik duvarının kuralların ve paket eşleştirme süresinin optimizasyonuna yardımcı olan üç algoritma sunulmuştur. İki, güvenlik duvarı anormalliklerini tespit etmek ve çözmek için üçüncüsü, paket eşleştirme zamanının optimizasyonu için bir algoritmadır.

Farklı güvenlik duvarı kuralları sıkılaştırma teknikleri de tartışılmaktadır. Kurallar ve çatışmalar arasındaki ilişkiyi kolayca tanımlamak ve analiz etmek için güvenlik duvarı kurallarının yapısal analizi de sunulmaktadır.

Bu tez çalışmasında gölge ve gereksiz anomaliler ciddi hatalar olarak kabul edilmektedir. Uygulama, güvenlik duvarının performansını arttırmak için uygun eylemi algılar ve alır. Tek bir parametre farklılığıyla benzer kurallar, kuralların sayısını en aza indirmek için uygulama tarafından birleştirilir. Bu nedenle, paket eşleştirme zamanının maliyeti en aza indirilecektir. Güvenlik duvarı kurallarını yeniden sıralayan ve ilgisiz kuralları kaldıran bir algoritma da geliştirilmiştir. Çok sayıda paket eşleştirme yüzdesine sahip kurallar mümkün olduğunca erken kontrol edildi ve kural listesinden kaldırılması için belirli bir süre kontrol edilmeyen kuralların kullanılması önerilir.

Standart (sıralanmamış) bir güvenlik duvarı algoritması ile paketleri işlemek için optimize edilmiş kural sipariş algoritmamız arasında bir işlem süresi karşılaştırması gerçekleştirdik. Rastgele 14 örnek filtreleme kuralını kullandık, bunların her biri paket eşleştirme yüzdesiyle ilişkilendirildi. 10.000 test paketinin test verilerini temsil ettiği varsayılmıştır. Test verileri, her bir kural için eşleşme yüzdelerine göre bölünür ve paket eşleştirme süresi hesaplanır. Grafik, azaltılmış ve daha iyi paket eşleştirme süresini gösterir.

A. Veri Seti

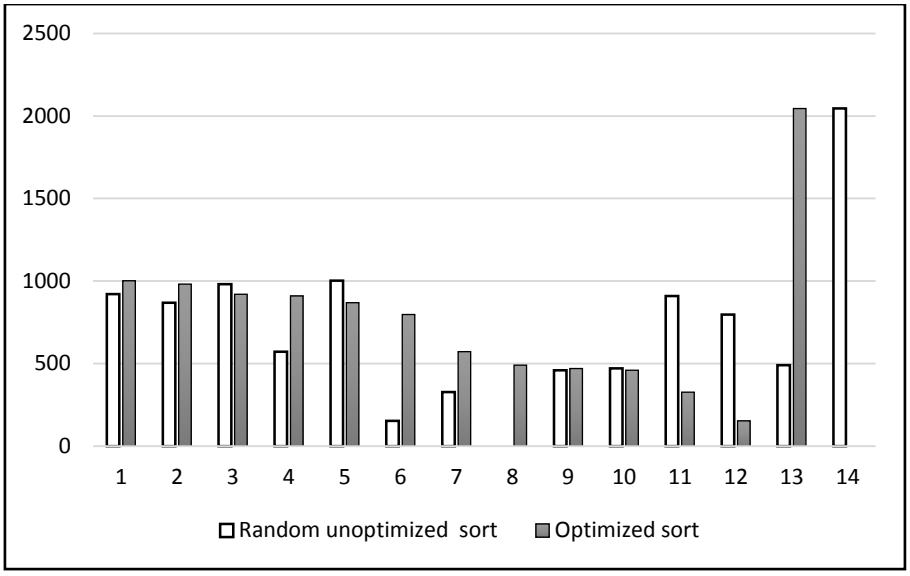
Algoritmamizi standart bir güvenlik duvarı algoritmasi ile karsilastirmak için, rasgele 14 örnek filtreleme kurali kullanmistir [Tablo 5.14], herbiri paket eşleme yüzdesiyle iliskilidir. 10.000 test paketinin test verilerini temsil ettiği varsayılmıştır. Test verileri, her bir kural için eşleşme yüzdelerine göre bölünür ve paket eşleştirme süresi hesaplanır.

B. Sonuçların analizi

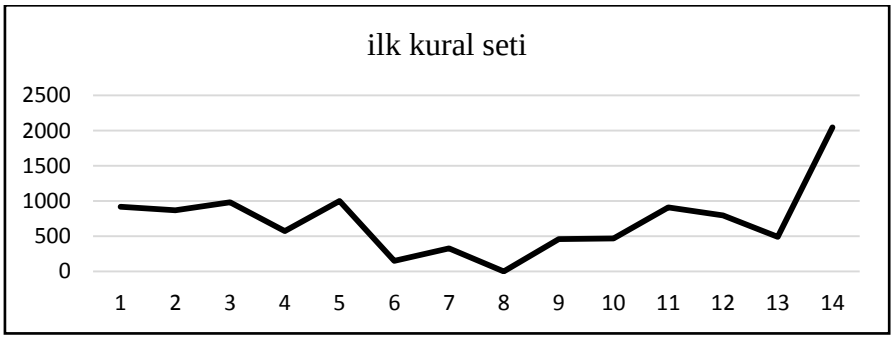
Çatışma tespiti ve çözümü için her algoritmaya dayalı web tabanlı bir RESTful web uygulaması yazılımı geliştirilmiştir. Aynı kuralları tek bir kuralda birleştirir. Uygulama NodeJS ve Express MongoDB veritabanı olarak kullanılarak geliştirilmiştir.

Bu çalışma, gölge ve gereksiz anomalileri ciddi hatalar olarak ele almaktadır. Uygulama, güvenlik duvarının performansını arttırmak için bu iki anormallik üzerinde uygun eylemi algılar ve kullanır. Tek bir parametre farklılığıyla benzer kurallar, kuralların sayısını en aza indirmek için uygulama tarafından birleştirilir. Bu nedenle, paket eşleştirme zamanının maliyeti en aza indirilecektir.

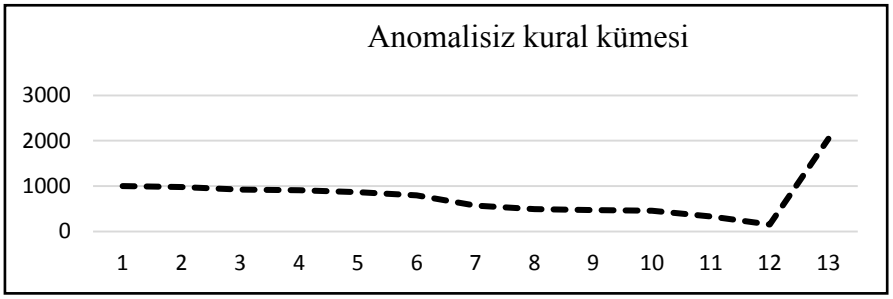
Çürüme ve baskın kuralları kolayca tespit etmek için güvenlik duvarı kurallarını yeniden düzenleyen bir algoritma da geliştirilmiştir. Önerilen algoritmaya dayanarak baskın kurallar mümkün olduğu kadar erken tabloda kontrol edilir ve paket eşleştirme süresi azalır.



Şekil 4.8. İki kural kümesinin karşılaştırması

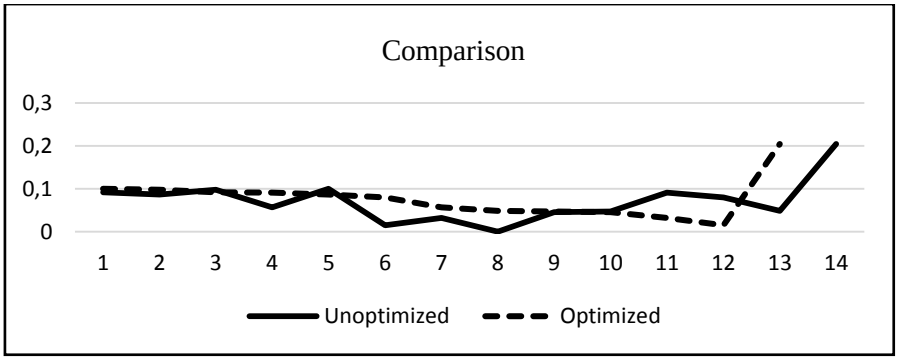


Şekil 4.9. Optimazsyon olmayan kural kümesi



Şekil 4.10. Optimize edilmiş kural kümesi

Grafikler, Tablo4.14.'te tartışılan 14 güvenlik duvarı ilke kurallarının her bir kuralının frekans dağılımını göstermektedir. X ekseninin her bir noktası bir kural sayısını temsil eder ve y ekseni frekans ölçeğini temsil eder. Bozulma kuralı (Kural8) kaldırıldıktan sonra, optimize edilmiş kural kümesinin 13 kuralı olur.



Şekil 4.11. Karşılaştırma 1

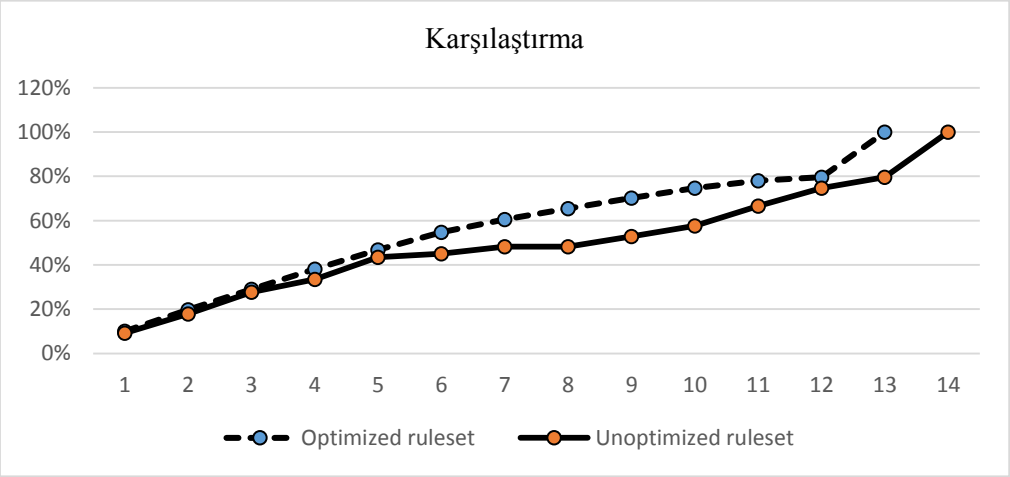
Tablo 4. 15. Frekans yüzdesine sahip, eşitsiz kural kümesi

Rule#	Frequency	%
Rule1	920	9%
Rule 2	869	18%
Rule3	982	28%
Rule4	573	33%
Rule5	1002	43%
Rule6	153	45%
Rule7	327	48%
Rule8	0	48%
Rule9	460	53%
Rule10	470	58%
Rule11	910	67%
Rule12	798	75%
Rule13	491	80%
Rule14	2045	100%

Tablo 4.16. Frekans yüzdesi ile optimize edilmiş kural kümesi

Rule#	Frequency	%
Rule1	1002	10%
Rule 2	982	20%
Rule3	920	29%
Rule4	910	38%
Rule5	869	47%
Rule6	798	55%
Rule7	573	61%
Rule8	491	65%
Rule9	470	70%
Rule10	460	75%
Rule11	327	78%
Rule12	153	80%
Rule13	2045	100%

Grafik, 14 güvenlik duvarı ilkesi kurallarının her kuralının olasılık dağılımını göstermektedir. X ekseninin her bir noktası bir kural sayısını temsil eder ve y ekseni olasılık ölçeğini temsil eder. Bozulma kuralı (Kural8) kaldırıldıktan sonra, optimize edilmiş kural kümesinin 13 kuralı olur. Şekil 6.4.'te gösterildiği gibi, optimize edilmiş kural kümesinin aldığı zaman nispeten kısadır.



Şekil 4.12. Karşılaştırma II

Şekil 4.12.'den, şu sonuca varabiliriz: Uyumsuz kural kurallarında, optimize edilmiş kural kümesinin ilgili kuralından daha az miktarda trafik işleyebilir. Örneğin, trafiğin% 50'si optimize edilmiş kural kümesindeki eylemine karar vermek için 5 kural tarafından kontrol edilirken, kuralsız sette 9 kural göz önünde bulundurulur. Yine Rule8 tarafından paketlerin% 48'i kuralsız kural tarafından kural eşleşmesi için kontrol edilir, ancak% 65'i optimize edilmiş kural kümesinde kontrol edilir.

BÖLÜM 5. SONUÇLAR VE ÖNERİLER

Güvenlik duvarları, bir ağın güvenliğini sağlamak için en çok kullanılan güvenlik mekanizmasıdır. Güvenlik duvarı yönetmenin karmaşıklığı nedeniyle, kural çatışmaları ve uyumsuzluklar kolaylıkla ortaya çıkabilmektedir.

Güvenlik duvarı kurallarını optimize etmek ve sıkılaştırmak için farklı yöntemler sunulmuştur. Optimizasyon süreci, çakışan kuralları tespit ederek ve çözerek, birleştirilebilen ve paket eşleştirme süresini en aza indiren kuralların birleştirilmesiyle gerçekleştirilmektir. Farklı güvenlik duvarı kuralları sıkılaştırma teknikleri de tartışılmaktadır. Kurallar ve çakışmalar arasındaki ilişkiyi kolayca belirlemek ve analiz etmek için güvenlik duvarı kurallarının yapısal analizi de sunulmaktadır.

Bu tez, güvenlik duvarı anomalilerini tespit etmek ve çözmek için farklı algoritmalar sunmuştur. Özellikle gölgelemer (shadow) ve fazlalık (redundancy) anomalileri değerlendirilmektedir. Kuralları eşleştirerek ve alakasız kuralları kaldırarak paket eşleştirme süresini optimize etmek için de bir algoritma önerilmiştir. Bu tezde tartışılan algoritmaları uygulamak için de web tabanlı bir uygulama yazılımı geliştirilmiştir.

Güvenlik duvarı alanında daha yapılacak çok şey olduğuna inanıyoruz ki gelecekteki araştırmalar için, bu model, 1) çevrimiçi dağıtılmış güvenlik duvarı paket eşleştirme zaman optimizasyon tekniklerini, 2) genelleme ve korelasyon anomalileri için diğer uygun eylemleri dikkate alarak ve 3) birleştirme algoritmasının çeşitli durumlarını dikkate alacak şekilde genişletilebilir.

KAYNAKLAR

[1] https://www.infosecurity-magazine.com/opinions/to-err-is-human-to-automate- divine/, Erişim Tarihi: 20.12 2017.

[2] https://www-03.ibm.com/security/uk-en/ ,Erişim Tarihi: 20.12 2017.

[3] https://www.algosec.com/press_release/human-error-considered-primary-cause - network-security-outages/, Erişim Tarihi: 25.12 2017.

[4] https://www.infosecurity-magazine.com/opinions/to-err-is-human-to-automate-divine/, Erişim Tarihi: 23.12 2017.

[5] http://www.omnisecu.com/tcpip/tcpip-model.php, Erişim Tarihi 25.11 2017.

[6] https://osi-model.com/, Erişim Tarihi: 30.11 2017.

[7] www.omnisecu.com/tcpip/osi-model.php, Erişim Tarihi: 30.11 2017.

[8] V. Rao Vemurı, Enhancing Computer Security with Smart Technology: Auerbach Publications, Taylor & Francis Group, Boca Raton, New York, 2006.

[9] John R. Vacca, Managing Information Security, Syngress, Elsevier, Second Edition, 2014.

[10] Ruıxı Yuan N, W. Tımothy Strayer, Virtual Private Networks: Technologies and Solutions, Addison-Wesley, 2001.

[11] https://www.accuwebhosting.com/blog/install-vpn-rras-remote-routing-access/, Erişim Tarihi: 05.01 2018.

[12] Ehab S. Al-Shaer, Hazem H., Hamed, Design and Implementation of Güvenlik duvarı Policy Advisor Tools, DePaul University, Chicago, IL, USA.

[13] Ehab Al-Shaer, Automated Güvenlik duvarı Analytics Design; Configuration and Optimization, Springer Publishing 2014.

[14] Ehab Al-Shaer and Hazem Hamed, Güvenlik duvarı Policy Advisor for Anomaly Discovery and Rule Editing. Proceedings of the 8th IFIP/IEEE International Symposium on Integrated Network Management, 24-28 March 2003, Colorado Springs, CO, USA.

[15] https://techterms.com/definition/güvenlik duvarı, Erişim Tarihi: 02.02 2018.

[16] http://www.conceptdraw.com/How-To-Guide/network-security-devices/, Erişim Tarihi: 02.02 2018.

[17] https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017, Erişim Tarihi: 24.11 2017.

[18] http://www.vesaria.com/Güvenlik duvarı/FAQ/sec19.php, ErişimTarihi: 30.11 2017.

[19] https://www.quora.com/What-are-the-functions-of-7-layers-of-the-OSI-refence model, Erişim Tarihi: 13.12 2017.

[20] https://support.rackspace.com/how-to/best-practices-for-güvenlik duvarı-rules-configuration/, Erişim Tarihi: 05.01 2018.

[21] Pası Eronen and Jukka Zıttıng, An Expert System for Analyzing Güvenlik duvarı Rul es, Proceedings of the 6th Nordic Workshop on Secure IT Systems, Tec hnical report IMM-TR-2001-14, Technical Univ. of Denmark, Nov 2001, pp. 100–107.

[22] Tıhomır Katıć, Predrag Pale, Optimization of Güvenlik duvarı Rules, Proceedings of the ITI 2007 29th International Conference on Information Technology Interfaces, June 25- 28, 2007, Cavtat, Croatia.

[23] Ms Swatı S. Kachare, Dr. P.K. Deshmukh, Güvenlik duvarı Policy Anomaly Management with Optimizing Rule Order, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 4, Issue 2, February 2015.

[24] Dmıtry Rovınıagın, Avıshaı Wool, The Geometric Efficient Matching Algorithm for Güvenlik duvarıs, IEEE Transactions on Dependable and Secure Computing, Volume: 8, Issue: 1, Jan.-Feb. 2011.

[25] ZOUHEIR TRABELSI, LIREN ZHANG, SAFAA ZEIDAN, Dynamic Rule an d Rule-field Optimization for Improving Güvenlik duvarı Performance and Security, IE T Information Security Volume: 8, Issue: 4, July 2014.

[26] Mahesh Nath Maddumala, Vıjay Kumar, Efficient Design of Güvenlik duvarı Temporal Policies, Proceedings of the IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 10-14 June 2016, Atlanta, GA, USA.

[27] Hemkumar D, Mohıt Chugh, Methods for Güvenlik duvarı Policy Detection and Prevention, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 7, July 2014.

[28] Weıpıng Wang ; Rong JI ; Wenhuı Chen ; Bo Chen ; Zhepeng Li, Güvenlik duvarı Rules Sorting Based on Markov Model, First International Symposium on Data, Privacy and E-Commerce (ISDPE 2007), 1-3 Nov. 2007, Chengdu, Sichuan, China.

[29] Umnıya Mustafa, Tımothy Wood, Zaınab AL Harthı, Mohammad M. Masud, Zouheır Trabelsı, Güvenlik duvarı Performance Optimization Using Data Mining Techniques, Proceedings of the 9th international Wireless Communications and Mobile Computing Conference (IWCMC), July 1–5, 2013, Cagliari, Sardinia, Italy.

[30] K. Golnabı, R.K. Min, L. Khan, E. Al-Shaer, Analysis of Güvenlik duvarı Policy Rules Using Data Mining Techniques, Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium NOMS, April 3-7, 2006, Vancouver, Canada.

[31] Ehab Al-Shaer, Hazem Hamed, Raouf Boutaba, Masum Hasan, Conflict Classification and Analysis of Distributed Güvenlik duvarı Policies, IEEE Journal on Selected Areas in Communications, Volume: 23, Issue: 10 Oct. 2005

[32] Muhammad Abedın, Syeda Nessa, Latıfur Khan, Bhavanı Thuraısıngham, Det ection and Resolution of Anomalies in Güvenlik duvarı Policy Rules, Proceedings of the 20th Annual IFIP Conference on Data and Applications Security and Privacy, Sophia Antipolis, France, July 31-August 2, 2006.

[33] Lin Zhang ; Mengxıng Huang, A Güvenlik duvarı Rules Optimized Model Based on Service-Grouping, Proceedings of the 12th Web Information System and Application Conference (WISA), 11-13 Sept. 2015, Jinan, China.

[34] Thawatchaı Chomsırı, Chotıpat Pornavalaı, Güvenlik duvarı Rules Analysis, International Conference on Security and Management (SAM06), January 2006, Las Vegas, Nevada, USA.

[35] Ehab AL-Shaer, Hazem Hamed, Raouf Boutaba, Masum Hasan, Conflict Classi fication and Analysis of Distributed Güvenlik duvarı Policies,IEEE Journal on Selected Areas in Communications, Volume: 23, Issue: 10th Oct. 2005.

[36] Muhammad Abedın, Syeda Nessa, Latıfur Khan, Bhavanı Thuraısıngham, Det ection and Resolution of Anomalies in Firewall Policy Rules, Proceedings of the 20th Annual IFIP Conference on Data and Applications Security and Privacy, Sophia Antipolis, France, July 31-August 2, 2006.

[37] Bılal Khan, Muhammad K. Khan, Maqsood Mahmud, Khaled Alghathbar, Security Analysis of Güvenlik duvarı Rule Sets in Computer Networks, Proceedings of the 4th International Conference on Emerging Security Information, Systems and Technologies, 18-25 July 2010, Venice, Italy.

[38] https://www.firemon.com/identify-remove-redundant-hidden-güvenlik duvarı-rules/, Erişim Tarihi: 20.05. 2018.

[39] https://www.manageengine.com/products/güvenlikduvarı/help/firewall-compliance/fir ewall-policy-optimization.html, Erişim Tarihi: 03.03 2018.

[40] https://www.firemon.com/identify-remove-redundant-hidden-güvenlik duvarı-rules/, Erişim Tarihi: 20.05 2018.

[41] https://brilliant.org/wiki/sorting-algorithms/, Erişim Tarihi: 10.02. 2018.

[42] https://en.wikipedia.org/wiki/Hardening (computing), Erişim Tarihi: 14.06.2018.

[43] B.Srıkanth, smt.k.Venkata RamanA, Güvenlik duvarı Policy Anomaly Detection and Resolution using Rule Based Approach, International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013

[44] Mımı Cherıan, Madhumıta Chatterjee, Optimized Firewall with Traffic Awareness, International Journal of Computer Networks and Applications (IJCNA) Volume 3, Issue 2, March – April (2016).

[45] Ian Mothersole, Martın J. Reed, Optimizing Rule Order for a Packet Filtering Güvenlik duvarı, Proceedings of the 2011 Conference on Network and Information Systems Security May 2011, Ile de Ré, La Rochelle, France.

[46] Ahmed Farouk, Hamdy N.agıza, Elsayed Radwan, Detecting Inconsistent Güvenlik duvarı Configuration Rules Using Range Algorithm, International Conference on Machine Learning and Computing, IPCSIT vol.3(2011), IACSIT Press, Singapore.

[47] Hajar Esmaeıl AS-Suhbanı, DR. S.D. Khamıtkar, Using Data Mining for Discovering Anomalies from Güvenlik duvarı Logs: a comprehensive Review, International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue:11, November 2017.

[48] P.R.Kadam, V.K. BhusarI, Redundancy Removal of Rules with Reordering them to Increase the Güvenlik duvarı Optimization, International Journal of Research in Engineering and Technology - IJRET, Volume: 03 Issue: 10 | Oct- 2014.

[49] Lin Zhang; Mengxıng Huang, A Güvenlik duvarı Rules Optimized Model Based on Service-Grouping, Proceedings of the 12th Web Information System and Application Conference (WISA), 11-13 Sept. 2015, Jinan, China.

[50] Tushar Subhash Pınjan , prof. Makrand Samvatsar, Optimization Algorithm for Packet Filtering Firewall, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 6, June 2014

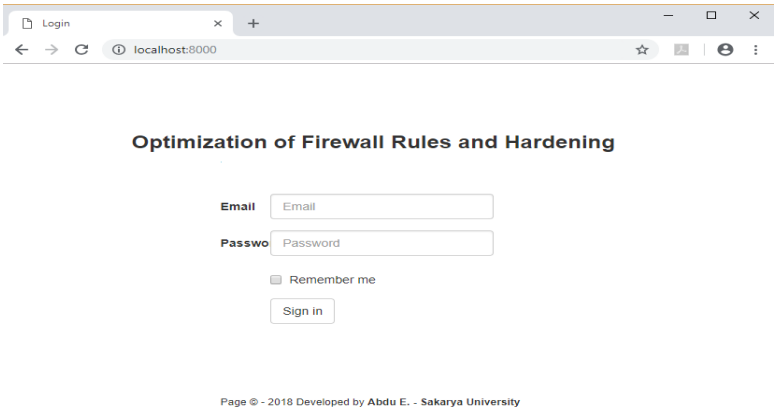
[51] Hongxın HU; GaıL-Joon Ahn ; Ketan Kulkarnı, Detecting and Resolving Güvenlik duvarı Policy Anomalies, IEEE Transactions on Dependable and Secure Computing, Volume: 9, Issue: 3 , May-June 2012.

[52] Frederıc Cuppens Nora Cuppens-boulahıa, Joaquın Garcıa-Alfaro, Detection and Removal of Güvenlik duvarı Misconfiguration, Proceedings of the 2005 IASTED International Conference on Communication, Network and Information Security, November 14 – 16, 2005, Phoenix, AZ, USA.

[53] Zhao, Liang, A. Shimae and Hiroshi Nagamochi. Linear-tree rule structure for firewall optimization, Proceedings of the 6th IASTED International Conference on Communications, Internet, and Information Technology, July 2 – 4, 2007, Banff, Alberta, Canada.

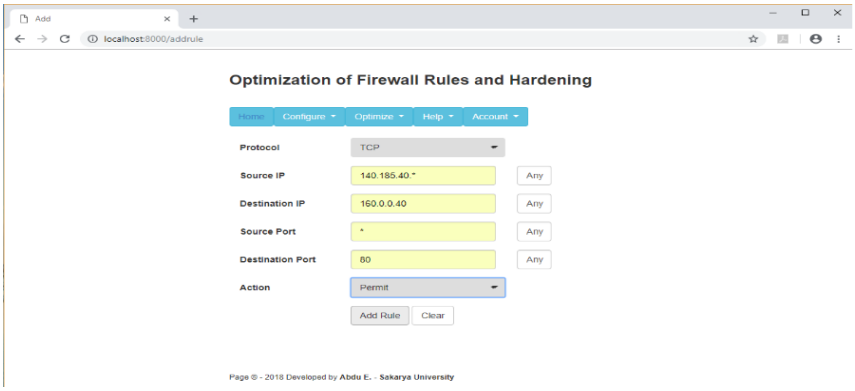
EKLLER

EK A: ana sayfa - Home page – Login ekranı



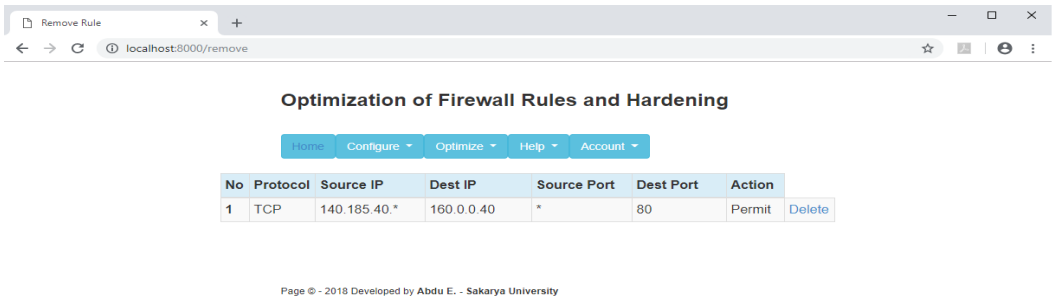
Şekil 1. Ana sayfa

EK B: Güvenlik Duvarı Kurallarının Eklenmesi



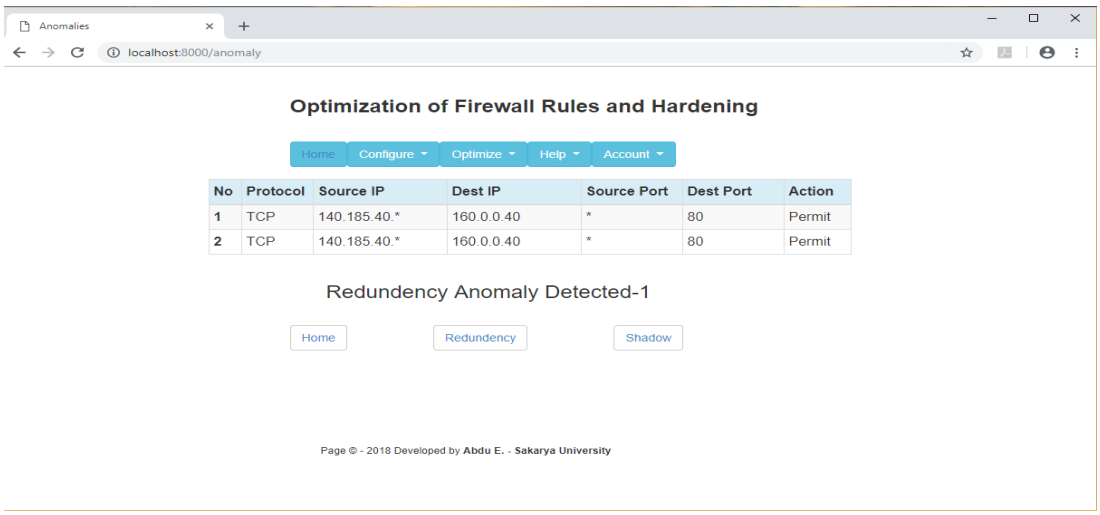
Şekil 2. Kurallari eklemek

EK C: Güvenlik duvarı kurallarının kaldırılması



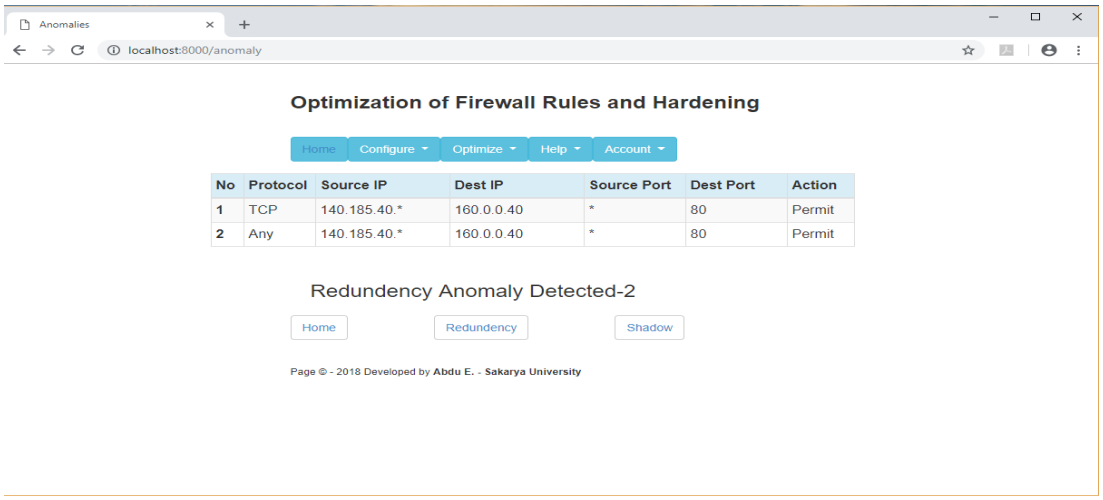
Şekil 3. Kural kaldırmak

EK D: Fazlalık Anomalısı – biçim 1



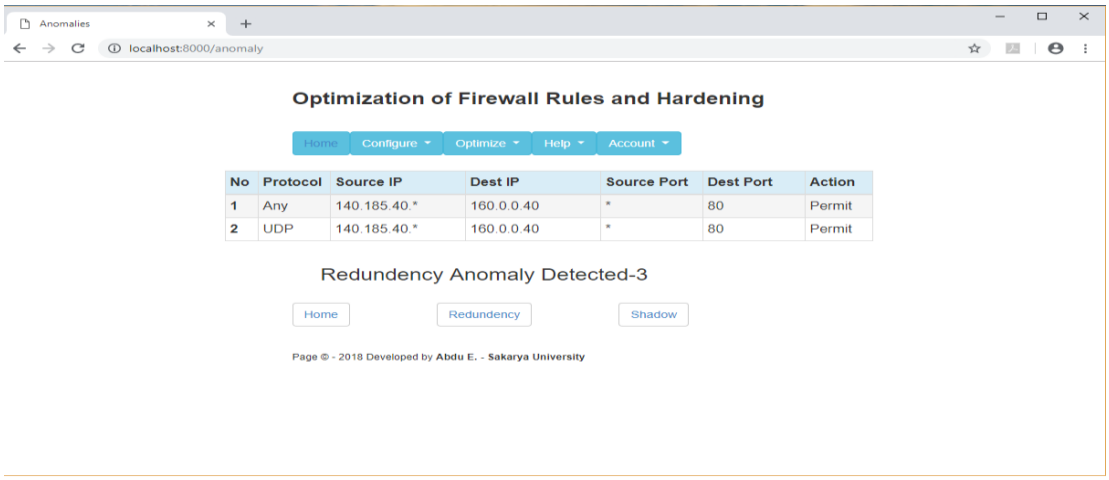
Şekil 4. Fazlalik anomalisi I

EK E: Fazlalık Anomalısı – biçim 2



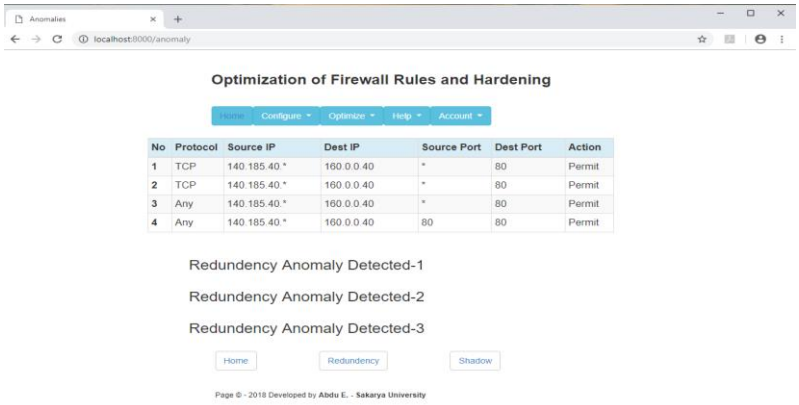
Şekil 5. Fazlalık anomalisi II

EK F: Fazlalık Anomalısı – biçim 3



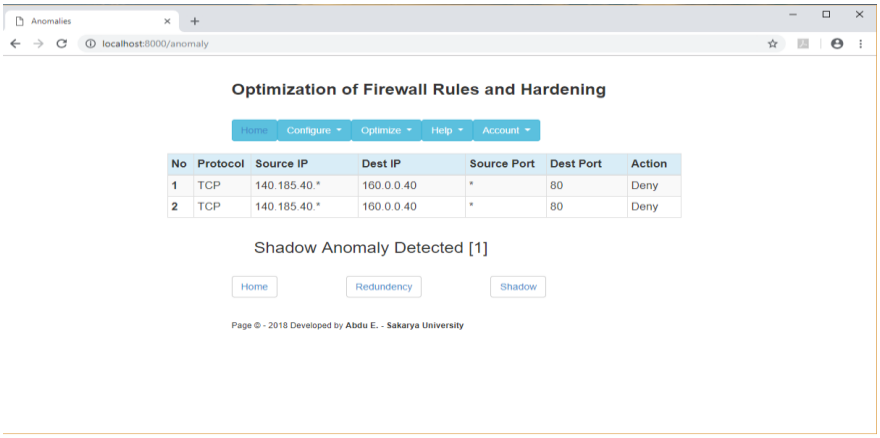
Şekil 5. Fazlalık anomalisi III

EK G: Fazlalık Anomalısı – biçim 1, 2 ve 3 – birlikte



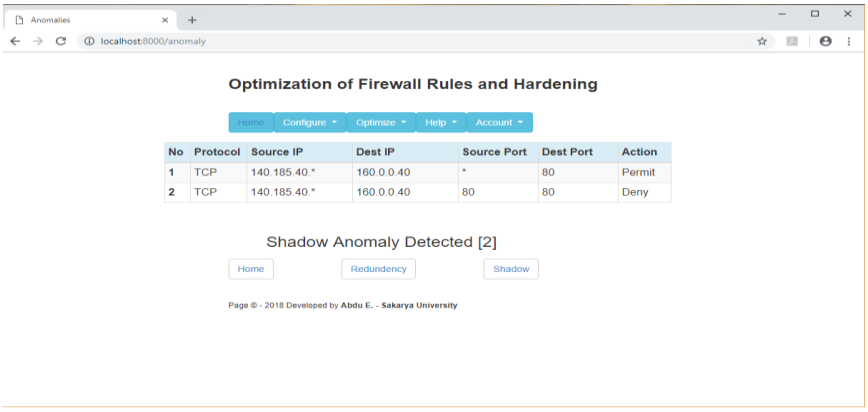
Şekil 6. Fazlalık anomalisi

EK H: Gölge anomalisi – biçim 1



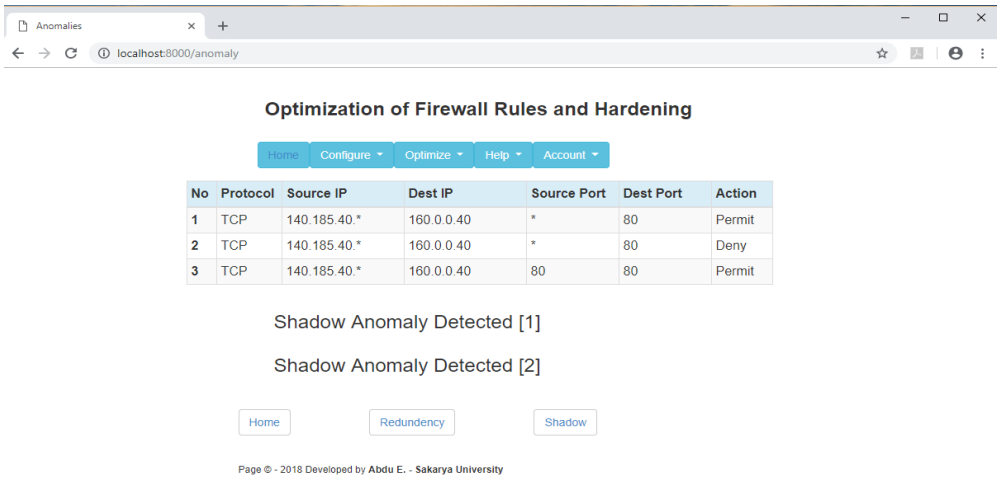
Şekil 7. Gölge anomalisi I

EK İ: Gölge anomalisi – biçim 2



Şekil 8. Gölge anomalisi II

EK J: Gölge anomalisi – biçim 1 ve 2 – birlikte



Şekil 8. Gölge anomalisi

EK K: Gölge anomalisinin çozumu - biçim 1

Birisini kaldırm - Remove one of the two rule

No	Protocol	Source IP	Dest IP	Source Port	Dest Port	Action
1	TCP	140.185.40.*	160.0.0.40	*	80	Permit
2	TCP	140.185.40.*	160.0.0.40	*	80	Deny

Home Back Remove

Şekil 10. Shadow resolution [1] - A

No	Protocol	Source IP	Dest IP	Source Port	Dest Port	Action	
1	TCP	140.185.40.*	160.0.0.40	*	80	Permit	Delete
2	TCP	140.185.40.*	160.0.0.40	*	80	Deny	Delete

Home Back

Şekil 11. Shadow resolution [1] – B

EK L: Gölge anomalisinin çozumu - biçim 2

Birisini kaldır ya da yeniden sırala - Remove one of the two rule or reorder the rules

No	Protocol	Source IP	Dest IP	Source Port	Dest Port	Action
1	TCP	140.185.40.*	160.0.0.40	*	80	Deny
2	TCP	140.185.40.*	160.0.0.40	80	80	Permit

Home Back Remove Reorder

Şekil 12. Shadow resolution [2] - A

EK M: Fazlalık anomalisinin çozumu - biçim 1

Otomatik olarak ikinci kuralı kaldır - Kural 2'yi kaldır

No	Protocol	Source IP	Dest IP	Source Port	Dest Port	Action
1	TCP	140.185.40.*	160.0.0.40	*	80	Deny
2	TCP	140.185.40.*	160.0.0.40	*	80	Deny

Home Back Remove Duplicates

Şekil 13. Redundance resolution [1]

EK N: Fazlalık anomalisinin çozumu - biçim 2

Otomatik olarak üsteki kuralı kaldı – R1'i kaldır

No	Protocol	Source IP	Dest IP	Source Port	Dest Port	Action
1	TCP	140.185.40.*	160.0.0.40	*	80	Permit
2	TCP	140.185.40.*	160.0.0.40	*	*	Permit

Home Back Remove Duplicates

Şekil 14. Redundance resolution [2]

EK O: Fazlalık anomalisinin çozumu - biçim 3

Otomatik olarak altaki kuralı kaldır – R2'i kaldır

No	Protocol	Source IP	Dest IP	Source Port	Dest Port	Action
1	Any	140.185.40.*	160.0.0.40	*	*	Deny
2	Any	140.185.40.*	160.0.0.40	*	80	Deny

Home Back Remove Duplicates

Şekil 15. Redundance resolution [3]

ÖZGEÇMİŞ

Abdu Endris MOHAMMED 29 Mayıs 1993'te Kemissie, Wollo, Etiyopya'da doğdu. İlkokul, ortaokul ve lise eğitimini Kemissie'de tamamladı. 2009 yılında başladığı Hawassa Üniversitesi Bilgisayar Bilimleri Bölümü'nü Temmuz 2013'te başarılı bir şekilde bitirdi. Ağustos 2013'ten Ağustos 2015'e kadar Dilla Üniversitesinde asistan olarak görev aldı. Eylül 2015'te Türkiye burslarını kazandı ve Sakarya Üniversitesinde eğitime başladı. Abdu Endris başaralı bir derecede bir yıllık Türkçe hazırlık sınıfını tamamladı ve Bilgisayar ve Bilişim Mühendisliği yüksek lisansından 2018 yılında mezuniyetini beklemektedir.