
GAZİ ÜNİVERSİTESİ
Gazi
1926

EV, OFİS VE IoT AĞLARININ AĞ GEÇİDİNDE BÜTÜNLEŞİK TEHDİT YÖNETİMİ İLE GÜVENLİĞİN SAĞLANMASI

Tamer SAY

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ŞUBAT 2019

Tamer SAY tarafından hazırlanan "EV, OFİS VE IoT AĞLARININ AĞ GEÇİDİNDE BÜTÜNLEŞİK TEHDİT YÖNETİMİ İLE GÜVENLİĞİN SAĞLANMASI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Mustafa ALKAN

Elektrik Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. .....

İkinci Danışman: Dr. Öğr. Üyesi Murat DÖRTERLER

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. .....

Başkan: Prof. Dr. Turhan MENTEŞ

İstatistik Ana Bilim Dalı, Hacettepe Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. .....

Üye: Dr. Öğr. Üyesi İbrahim Alper DOĞRU

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. .....

Üye: Doç. Dr. Ercan Nurcan YILMAZ

Elektrik Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. .....

Tez Savunma Tarihi: 06/02/2019

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Tamer SAY

06/02/2019

EV, OFİS VE IoT AĞLARININ AĞ GEÇİDİNDE BÜTÜNLEŞİK TEHDİT YÖNETİMİ İLE GÜVENLİĞİN SAĞLANMASI

(Yüksek Lisans Tezi)

Tamer SAY

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Şubat 2019

ÖZET

Günümüz bilgi ve iletişim teknolojilerinde güvenliğin sağlanması ve sürdürülebilirliği kritik öneme sahiptir. En büyük ağ olan internet birçok tehdit unsurunu bünyesinde barındırmaktadır. Bu tehditlerin çeşidi, karmaşıklığı ve sayısı her geçen gün artmaktadır. Evlerimize interneti sağlayan modemler ağ geçidi gibi kritik bir rol üstlenmelerine rağmen artan güvenlik tehditlerine karşı etkisiz ve yetersiz kalmaktadır. Akıllı ev cihazları, giyilebilir cihazlar, algılayıcılar gibi çok çeşitli IoT cihazlarının ev ve ofis ağlarına katılması sonucunda cihaz sayısındaki artışla birlikte güvenlik gereksinimi de artmıştır. Karmaşıklaşan ağ yapılarında güvenliğin sağlanması oldukça zorlaşmıştır. IoT cihazlarının evlerde kritik konumlarda kullanılması nedeniyle ev, ofis ve IoT ağlarında güvenliğin artırılması kaçınılmaz olmuştur. Ağ geçidi olan modemlerin yerine veya modemlerle birlikte çalışabilen güvenlik çözümlerinin kullanımı uzmanlık gerektirmedir. Bu nedenle modemlerin üzerindeki güvenliği artırıcı önlemler almak kritik öneme sahiptir. Ağ geçidi olan modemler üzerinde genellikle bir güvenlik duvarı bulunmaktadır. Basit seviyeli bu güvenlik duvarı çözümleri, gelişen tehditlere karşı yetersiz kalmakta zamanla güncelliğini yitirmektedir. Bu tez çalışmasında ev, ofis ve IoT ağlarına yeni katılan cihazlar ve teknolojiler için tehdit unsurlarının tespit edilerek önlenmesiyle zararlıları büyük ölçüde önleyebilecek bir ağ geçidi özelliğinde bütünleşik tehdit yönetimi çözümü geliştirilmiştir. Sızma testi yöntemleri uygulanarak geliştirilen ve test edilen çözümün gelişmiş saldırı tespit sistemi kabiliyeti ile tehdit algılama beceresi ölçülmüş; bu ölçümlerin sonucunda uygulanan güvenlik sıkılaştırmaları sayesinde çözümün tehdit önleme mekanizması güçlendirilmiştir. Bütünleşik tehdit yönetimi uygulaması sayesinde ev, ofis ve IoT ağlarında bulunan cihazların güvenliğinin artırılması büyük oranda gerçekleştirilmiştir. Kolay yönetilebilir ve düşük maliyetli olan bu çözümün açık kaynak kodlu olması sayesinde gelecekte yapılacak çalışmalara ışık tutması sağlanmıştır.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Ağ güvenliği, bütünleşik tehdit yönetimi, ağ geçidi güvenliği
Sayfa Adedi	:	77
Danışman	:	Prof. Dr. Mustafa ALKAN
İkinci Danışman	:	Dr. Murat DÖRTERLER

SECURING HOME, OFFICE AND IoT NETWORKS ON GATEWAYS WITH UNIFIED THREAT MANAGEMENT

(M. Sc. Thesis)

Tamer SAY

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

February 2019

ABSTRACT

Ensuring the security of daily-use technologies is as important as it is difficult. The largest network, the internet, contains many threats. The variety, complexity and number of these threats are increasing exponentially day by day. Although modems have a critical role as a gateway, they become ineffective and inadequate against increased security threats. The need for security has increased due to the inclusion of a wide range of IoT devices to home networks. Ensuring security of complex networks has become very challenging. Due to the use of IoT devices in critical locations, it is inevitable to enhance security of home, office and IoT networks. Usage of security devices that can work with modems or other solutions that are used instead of modems requires expertise. Thus, it is critical to take measures to increase security on modems. Most modems have the firewall mechanisms to defend the network. These simple firewall solutions has become ineffective against evolving threats. In this thesis, we aimed to develop a gateway security solution that can prevent threats effectively by analyzing network traffic of devices on home, office and IoT networks. Thanks to this developed gateway solution, it is aimed to increase security pro-actively for current devices and the devices joining in the future. This easy-to-manage and low-cost solution is open-source, enabling this thesis to shed light on future works.

Science Code	:	92403
Key Words	:	Network security, unified threat management, gateway security
Page Number	:	77
Supervisor	:	Prof. Dr. Mustafa ALKAN
Co-Supervisor	:	Dr. Murat DÖRTERLER

TEŞEKKÜR

Çalışmalarım boyunca desteğini esirgemeyen, tecrübeleri ile her zaman doğru yolu gösteren danışmanlarım saygıdeğer Hocam Prof. Dr. Mustafa ALKAN'a ve Dr. Murat DÖRTERLER'e teşekkürlerimi sunarım. Çalışmalarımın tüm aşamalarında yardımlarını esirgemeyen Dr. Öğr. Üys. İbrahim Alper DOĞRU'ya desteklerinden dolayı teşekkür ederim. Maddi ve manevi desteğini hayatım boyunca hissettiğim aileme ve bu tezi hazırlamam konusunda beni sürekli olarak teşvik eden, desteğini esirgemeyen Yurdum Yayıncılık ve Yazılım San. Tic. ve Ltd. Şti. ailesine teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ACL	Access Control List
ARM	Acorn RISC Machine
BTY	Bütünleşik Tehdit Yönetimi
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GPON	Gigabit Passive Optical Network
GPS	Global Positioning System
HTTP	Hyper-Text Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
KRACK	Key Reinstallation Attack
LAN	Local Area Network
NAT	Network Address Translation
RAM	Random Access Memory
RFC	Request for Comments
RFID	Radio Frequency Identification
RISC	Reduced Instruction Set Computing
SDN	Software Defined Network
SIP	Session Initiation Protocol
SOHO	Small Office Home Office
SSH	Secure Shell
SSL	Secure Sockets Layer
STS	Saldırı Tespit Sistemi

Kısaltmalar	Açıklamalar
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
XSS	Cross Site Scripting

1. GİRİŞ

Günlük hayatımızın değişmez bir parçası haline gelen internet ile dünya üzerindeki insanlar ve nesneler birbirleriyle kolay bir şekilde iletişim kurabilmektedir. İnternet, sağladığı birçok faydanın yanı sıra birçok tehdit unsurunu da bünyesinde barındırmaktadır. Artan cihaz sayısının yanı sıra kötücül yazılımların ve kötü niyetli kişilerin sayısı da hızla artış göstermektedir. Gelişen internet teknolojileri ile birlikte ağa katılan bileşenlerin sayısındaki artış katlanarak yükselmektedir. Ağa bağlanan cihazlardaki sayı artışı ağ kavramını bütünüyle farklılaştırmış ve yeni kavramların ortaya çıkmasına neden olmuştur. IoT (Internet of Things) kavramı yaşamımızın neredeyse tüm alanındaki cihazlarda değişime yol açarak nesnelerde akıllılaşmayı sağlamıştır. 2020 yılında internete bağlanan cihaz sayısının 13,6 milyar ile 50 milyar arasında olacağı tahmin edilmektedir [1-2]. Bu hızlı gelişim bazı kısıtlamaları aşma ihtiyacını da beraberinde getirmektedir. IP (Internet Protocol) adreslerinin dördüncü sürümden altıncı sürüme geçiş süreci hazırlığı da bunlardan bir tanesidir.

Günümüzde çeşitli güvenlik problemleri IoT ile yapılan saldırılarda ve ev kullanıcıları odaklı saldırılarda görülmektedir. Buzdolabını, klimayı, garaj kapısını, akıllı eşyaları internete bağlama çabası kontrol edebilme, izleyebilme ve takip edebilme gibi çeşitli özellikler kazandırma hedefiyle her şeyi uzaktan, bir merkez noktadan kontrol etme arzusu içermektedir. IoT cihazlarının düşük güç tüketimi, düşük kaynak kullanımı, sınırlı batarya ömrü gibi özelliklere sahip olmaları üzerlerinde geliştirme yapılmasını oldukça zorlaştırmaktadır. Bu cihazların istismar edilmesiyle yapılan saldırıları önlemek için cihazların üzerinde güvenlik çözümü geliştirmek maliyetli, zahmetli ve çok çeşitli olmaları nedeniyle zaman alıcıdır. Hayatı kolaylaştırma içgüdüsü ile üretilen ürünlerle birlikte geliştirilen çözümlerin üretim ve kurulum aşamalarında oluşacak tasarım eksiklikleri, algoritmik hatalar, güvenlik testlerindeki eksiklik gibi çeşitli nedenler kötü amaçlı kişiler için önemli fırsatlar ortaya çıkarmaktadır. Son yıllarda yapılan hizmet dışı bırakma saldırılarının birçoğu ve en etkili olanlarının IoT cihazları kullanılarak gerçekleştirildiği tespit edilmiştir. Siber saldırılar yapılarak ele geçirilmiş cihazların bir merkezden komuta edilerek yönetilmesi ile gerçekleştirilen saldırılar hizmet dışı bırakma saldırılarında önemli bir yere sahiptir [3].

Günümüzde kullanılan güvenlik çözümleri gelişmiş yöntemlerle saldırıları tespit ederek kullanıcılara ve cihazlara koruma sağlamaktadır. Bu çözümlerin birçoğu kurumsal yapıları korumak için geliştirilen genellikle yüksek maliyetli ve yüksek sistem gereksinimi ihtiyacı olan ticari çözümlerdir. Kullanımı uzmanlık gerektiren bu çözümler derin paket analizi, anti-virüs ile virüs aktivitesi önleme, içerik filtreleme gibi yöntemler kullanan bu uygulamalar bütünleşik/birleşik tehdit yönetimi (BTY) olarak adlandırılmaktadır [4]. Bu tür güvenlik uygulamaları yüksek kabiliyetli olup saldırı tespitinde önemli bir yere sahip olmasına karşın yüksek maliyetli olmaları nedeniyle küçük ölçekli ağlarda kullanıcılar tarafından tercih edilmemektedir.

Ağa katılan cihaz sayısının ve çeşitliliğinin arttığı günümüzde cihazların internet bağlantısı kurdukları veya internete çıkış yaptıkları noktalarda güvenliği sağlamak daha verimli bir çözüm olarak düşünülmüştür. Aynı çözüm yöntemi mevcut olarak kullanılan cihazlar olan bilgisayarlar, cep telefonları, tablet bilgisayarlar gibi cihazlar için de geçerli olması nedeniyle daha kapsayıcı nitelikte bir çözüm geliştirilmiştir.

Bu çalışmamızda ev, ofis ve IoT ağları gibi küçük ölçekli ağlardaki bileşenlerinin güvenlik sorunlarının önüne geçilmesi üzerine saldırı tespit ve önleme kabiliyetli bir bütünleşik tehdit yönetimi çözümü geliştirilmiştir. Geliştirilen çözümle ağa katılan tüm cihazlarının güvenliğinin artırılması amaçlanmıştır. Çalışmamızın tüm katmanlarında açık kaynak teknolojiler kullanılarak geliştirme maliyetini en aza indirmek ve geliştirme sürecini en hızlı şekilde tamamlamak hedeflenmiştir. Açık kaynak kodlu yazılımların temelinde yatan farklı bakış açıları ile geliştirilmiş olması ile kaliteyi sağlama ve kolay uygulanabilir olma gibi özellikler göz önünde bulundurularak en uygun çözümün ortaya çıkarılması hedeflenmiştir [5]. Çalışmamızın bir diğer amacı ise açık kaynak kodlu yazılımların sistemlerdeki güvenliği sağlamadaki başarılarını test etmektir. Literatürdeki açık kaynak kodlu güvenlik duvarı ve türevi yazılımlar üzerine yapılan karşılaştırma çalışmaları incelenmiştir. Geliştirilen çözüm literatürdeki mevcut çalışmalarla karşılaştırılarak performans ve saldırı tespit başarımı ölçülmüştür.

Sonuç olarak geliştirilen çözümün ev, ofis ve IoT ağlarındaki başarımı ölçülmüş ve BTY uygulamasının küçük ölçekli olarak nitelendirilebilecek ağlarda güvenliği sağlamada yüksek başarım sunduğu görülmüştür. Yapılan karşılaştırmalar sonucu BTY uygulamasının ev, ofis

ve IoT ağlarında çeşitli saldırı tiplerinde %100 saldırı tespit kabiliyeti olduğu tespit edilmiştir.

Çalışmamızın literatür taraması bölümünde literatürdeki çalışmalar sunulmuştur; üçüncü bölümünde küçük ölçekli ağlarda yaşanan güvenlik sorunlarından bahsedilmiş; dördüncü bölümünde kullanılan uygulamalar ve yöntemler belirtilmiş; beşinci bölümde deneysel çalışmalar sonucu elde edilen bulgular tartışılmış; altıncı bölümde sonuçlara yer verilmiştir.

2. LİTERATÜR TARAMASI

Ev kullanıcıları, küçük işletmeler ve IoT ağları için internet bağlantı noktası veya ağ geçidi üzerinde güvenlik duvarı kullanılması veya geliştirmesi literatürde çok sık görülmeyen bir yaklaşımdır. İnternet bağlantısını sağlayan cihazlar olan modemler veya erişim noktaları (access points), anahtarlar (switch), yönlendiriciler ve benzeri cihazlar internet erişimini sağlamasının yanı sıra genellikle bünyesinde bir güvenlik çözümü barındırmaktadırlar. Fakat gelişen teknoloji ve özellikle son yıllarda ağlara katılan yeni cihazlar ile birlikte bu cihazların sağladığı güvenlik çözümleri yetersiz kalmakta ve gelişen saldırı tiplerine karşı cevap verememektedir. Güvenlik açısından eksiklerin yanı sıra modemlerin kaynak, bant genişliği ve istemci sayısındaki kısıtları bu cihazlarda zamanla performans kaybı ile hizmet kalitesinden ödün verilmesine neden olmaktadır [6].

Çalışmamız kapsamında literatürde yer alan çözümlerin ve kavramların incelemesi yapılmıştır. Kişisel güvenlik duvarı (personal firewall) olarak ele alınan çalışmalarda genellikle bilgisayarlar üzerinde kullanılan anti-virüslere ek güvenlik duvarı uygulamaları olarak geliştirilen çözümler yer almaktadır [7-12]. Ev otomasyon sistemleri (home automation systems) olarak ele alınan çalışmalarda genellikle dizüstü bilgisayarlar, cep telefonları gibi gündelik hayatta kullanılan cihazlar ile yangın algılayıcıları, gaz algılayıcıları gibi cihazların fiziksel güvenliğinin sağlanması ve cihazların otomatize edilmesi üzerine çalışmalar yapıldığı görülmüştür [13-17]. Akıllı ev sistemleri (smart home systems) ve akıllı ev ortamları (smart home environments) üzerine yapılan çalışmalarda ev ortamının fiziksel olarak denetimi (monitoring) üzerinden güvenliği sağlama çalışmaları yapıldığı tespit edilmiştir [16-19]. Akıllı ev kontrol sistemleri (smart home control systems) üzerine yapılan çalışmalar incelendiğinde ev içerisinde kullanılan cihazların uzaktan yönetilebilirliği (management) üzerine çalışmalar yapıldığı saptanmıştır [20-22]. Literatürdeki çalışmamız kapsamına uygun kavramların; küçük ofis / ev ofis (SOHO, small office / home office), ev ağ geçitleri (home gateways), yerleşim ağ geçitleri (residental gateways), ev ağ güvenliği (home network security) ve IoT ağ güvenliği (IoT network security) çalışmaları olduğu görülmüştür [23-27]. Bu çalışmalar detaylı olarak incelenerek ev, ofis ve IoT ağları gibi küçük ölçekli ağlardaki ağ güvenliğini sağlamada mevcut problemler ve zorluklar araştırılmış; geliştirilen çözüm yöntemleri hakkında incelemeler yapılmıştır. İncelenen

çalışmalarda genellikle Ev ve ofis ağlarına yönelik yapılan çalışmalarda genellikle basit güvenlik önlemlerinin önerildiği çözümlerin yer aldığı görülmektedir.

IoT cihazlarının günümüzde çok çeşitli hale getirmesi ile sadece belirli cihazlara hitap eden güvenlik çözümleri geliştirmesi yöntem olarak genellikle tercih edilmemektedir. Ağ geçidi gibi kritik noktalarda güvenliği artırıcı çözümler geliştirmek güvenliği sağlamada ekstra bir katman oluşturması nedeniyle daha etkili çözümler olarak ortaya çıkmaktadır [23, 28-31]. Bazı tehdit unsurları son kullanıcı ürünlerine kadar ulaştığında teknik açıklıkları istismar etmenin yanı sıra insan faktörünü göz önünde bulundurarak sosyal mühendislik saldırıları gerçekleştiği görülmektedir. Sahte içerikli mesajlar ile kişilere oluşturulan sahte içeriğin gerçek adresinden geliyormuş gibi iletilerek kişilerin bilgilerini elde etme saldırılarına oltalama saldırıları denmektedir. Oltalama saldırıları sosyal mühendislik saldırılarının en iyi örnekleri arasındadır. Bu tür saldırıların başarılı olma oranını en aza indirebilecek çözüm yöntemleri genellikle saldırıların kullanıcılara ulaşmadan tespit edilerek önlenmesi üzerinedir. Genellikle epostalar aracılığıyla yapılan oltalama saldırıları çok çeşitli problemlere yol açarak kullanıcılara zarar vermekle sonuçlanmaktadır [32-35].

Son yıllarda yapılan saldırıların kurumsal ağlardan çok son kullanıcıları, bireyleri hedef aldığı bilinmektedir [36]. Bir güvenlik çözümünü kullanmak tek başına yeterli olmamakla birlikte güvenlik çözümünün doğru bir şekilde yapılandırılmış olması ve güncelliğini sürekli olarak koruyor olması kritik öneme sahiptir. Kişisel güvenlik duvarlarının güvensizliği üzerine yapılan bir çalışmada belirtilen “güvenlik duvarları çeşitli saldırılardan bilgisayarları koruması beklenirken, bunun sadece teoride gerçek olduğu, gerçek dünya örneklerinde çoğu testin başarısız olduğu” [11] ifade edilmektedir. Bu çalışmada güvenlik duvarlarının saldırı tespiti birçok saldırıya karşı yetersiz kaldığı sonucu elde edilmiştir. Sosyal mühendislik saldırıları gerçek dünya örneklerinden tespiti zor saldırılardan bir tanesidir. Çoğu bilgisayar kullanıcısının güvenlik uygulamaları uyarılarını sinir bozucu bulduğu için çözümü bu güvenlik uygulamalarını kapatmakta veya uyarıları göz ardı etmekte bulmaktadır [10]. Güncelleme uyarılarını göz ardı eden kullanıcıların anti-virüs programları ve bu programların güvenlik duvarları virüsler tarafından kolaylıkla atlatılabilir ve manipüle edilebilir hale geldiği görülmektedir [12]. Bu nedenle sosyal mühendislik saldırılarını tespit edebilmek ve önleyebilmek adına özellikle eposta içeriğinde olmak üzere gelişmiş saldırı tespit yöntemlerinin uygulanması kritik öneme sahiptir.

Makine öğrenmesi ve yapay zekâ alanında yapılan çalışmalarıyla elde edilen sonuçlar sayesinde özellikle sosyal mühendislik içeren saldırı tipleri büyük oranda tespit edilebildiği belirtilmektedir. Oltalama saldırılarının makine öğrenme yaklaşımıyla tespiti ve spam epostaların tespiti üzerine yapılan çalışmalarda geleneksel yöntemlere göre daha yüksek başarı elde ettiği görülmüştür [34, 37-39]. Çetin Kaya ve Oktay Yıldız tarafından yapılan makine öğrenmesi yöntemleri kullanarak saldırı tespit etme çalışmalarında makine öğrenmesi yöntemlerinin başarım oranları karşılaştırılmıştır [37]. Çalışmada saldırı tespitinde makine öğrenmesi yöntemlerinin kullanımında yüksek başarı oranları elde edilebildiği görülmüştür. İlgili karşılaştırma çalışmasında destek vektör makineleri ve yapay sinir ağları kullanılarak geliştirilen saldırı tespit sistemlerinin hizmet dışı bırakma ve bilgi tarama saldırılarında %100 oranında başarı gösterdiği sonucuna ulaşıldığı belirtilmektedir. Oltalama saldırılarının yapay sinir ağları yöntemiyle tespit edilmesi üzerine yapılan çalışmada %97,99 oranında başarılı sonuç elde edildiği belirtmektedir. Bayes algoritması ile geliştirilen saldırı tespit uygulamasında ise hizmet dışı bırakma saldırılarının %99,62'si ve bilgi tarama saldırılarının tamamı tespit edilebildiği sonucu elde edilmiştir.

Son yıllarda sık görülen saldırılardan ağır tahrip niteliğine sahip hizmet dışı bırakma ve türevi saldırılarda yüksek etkiye sahiptir. Bu saldırıları tespit etmede kullanılan algoritmalar genellikle belirli IP adreslerinden yapılan anormal aktivitelerin analizi üzerinden çalışma göstermektedir. Son yıllarda hizmet dışı bırakma saldırılarının yeni türleri ortaya çıkmaktadır. Çok fazla sayıda cihazın saldırılarda kullanılması sebebiyle saldırıları tespit etmede ve önlemede eksikliklerin olduğu görülmektedir [3]. Sıkça görülen hizmet dışı bırakma saldırıları, ev, ofis ve IoT ağ elemanları kullanılarak gerçekleştirilebilecek saldırı türleri olduğu belirtilmektedir [40]. Son yıllarda daha sık rastlanılan hizmet dışı bırakma saldırından biri ise DNS (Domain Name System) sunucularına yönelik yapılan saldırılar ve DNS sunucuları kullanılarak gerçekleştirilen DNS amplifikasyonu saldırılarıdır [41-42]. Bu tür saldırının bir örneğine son zamanlarda rastlanılmış ve yaklaşık 1 Tbps büyüklükte olduğu duyurulmuştur [43]. 150.000 IoT cihazının katıldığı düşünülen bu saldırıda güvenlik kameraları, buzdolapları, klimalar gibi çok çeşitli cihazların kullanıldığı tespit edilmiştir. 21 Ekim olayı olarak isimlendirilen bir diğer hizmet dışı bırakma saldırısı ise DNS hizmetini aksatmaya yönelik gerçekleştirilen hizmet dışı bırakma saldırısıdır [44]. İlgili saldırıda, bir açıklıkla ele geçirilmiş, uzaktan yönetilebilen 100.000 botnet üyesi cihazın kullanıldığı düşünülmektedir. 21 Ekimde gerçekleşen bu saldırıda verilen maddi zararının yaklaşık yedi milyar dolar olduğu belirtilmiştir [45]. Çoğu, varsayılan parolası değiştirilmeden kullanılan

IoT cihazlarının zombi ağ elemanlarına dönüştürülmesine karşı gerekli önlemlerin alınmasının önemi ciddi zararlar vermesi sonrasında anlaşılmıştır.

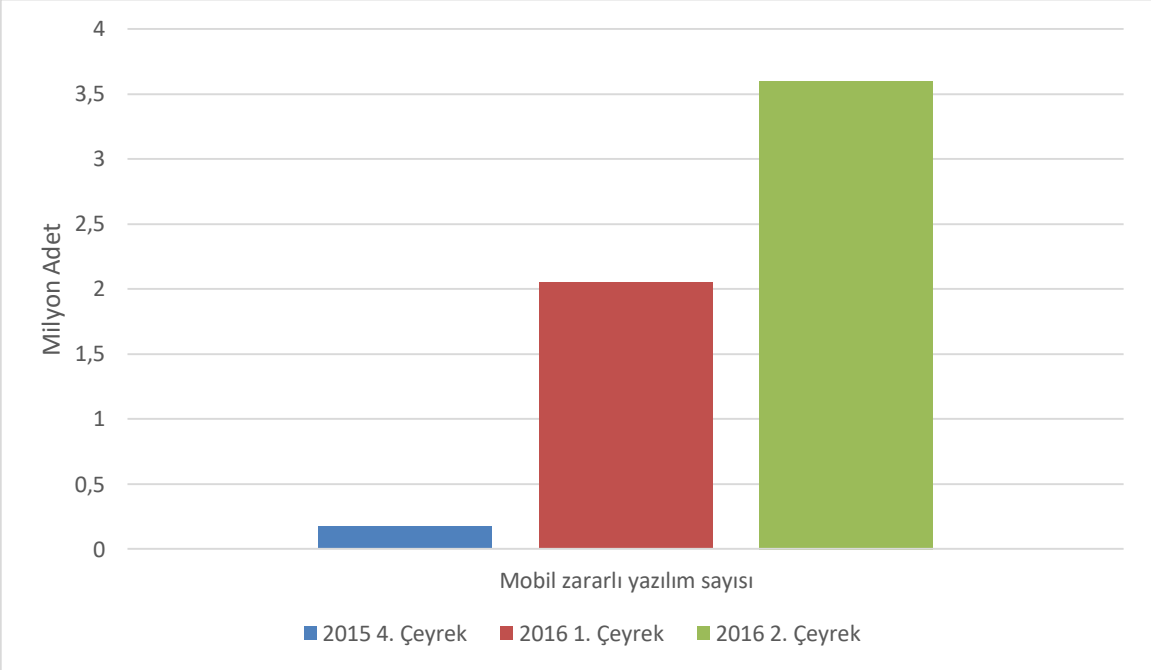
İlk olarak 2016 yılında tespit edilen Mirai, son yılların en tehlikeli saldırılarını gerçekleştiren zararlı yazılımlardan birisi olarak aktiflik göstermektedir. IoT kullanılarak oluşturulan botnet ordusu ile bilinen en büyük botnet ordularından biri olduğu belirtilmektedir [3]. 1.2 milyon aktif IoT cihazına bulaştığı tespit edilmiştir [46]. Yapılan bir DDoS (Distributed Denial of Service) saldırıları sırasında Mirai zararlısı bulaşmış 164 ülkeden 170.000 aktif IoT cihazının saldırıda aktif olarak kullanıldığı belirtilmektedir [47]. Mirai kullanılarak OVH ve Dyn firmalarına karşı gerçekleştirilen DDoS saldırısında 620 Gbps bant genişliği büyüklüğünde saldırı kapasitesi tespit edilmiş olup bilinen en büyük saldırılardan birisi olarak nitelendirilmektedir. OVH firmasına yapılan saldırı analizi sonucunda IoT cihazlarının yetersiz güvenliğinin saldırı kaynağının büyük bir bölümünü oluşturduğu net bir şekilde ifade edilmektedir [48].

Bir siber güvenlik firmasının yayımladığı zararlı yazılım analizleri raporuna göre fidyeci yazılımların yüksek artış gösterdiği, geliştiği ve son kullanıcıları hedef alma oranın arttığı açıkça belirtilmektedir [36]. En çok bilinen fidye yazılım örnekleri, CryptoLocker, CryptoWall, Locky ve TeslaCrypt fidyeci yazılımlarıdır [49]. Bu saldırı yöntemi ile genellikle sahte bir eposta ile kandırılan kullanıcıların cihazlarındaki veriler şifrelenmekte ve şifrelenmiş verilerin çözülmesi karşılığında fidye talep edilmektedir [50]. Kullanılan şifreleme yöntemleri çok güçlü bilgisayar kullanılarak bile kırılamayacak veya kırılması yıllar sürecek güçlü algoritmalar olarak ifade edilmektedir. Saldırının gerçekleşmesi ve verilerin şifrelenmesi işlemi aşamalarında uzak sunuculardan bağlantılar kurulduğu örnekleri tespit edilmiştir.

Kaspersky tarafından yayınlanan zararlı yazılım analiz raporuna göre son yıllardaki popüler saldırıların yine PDF uzantılı dosyaları ve SWF uzantılı flash teknolojisini kullandığına dikkat çekilmiştir [36]. Mobil güvenlik konusunda ise güvenlik kaygılarının arttığı, tehdit unsurlarının daha geniş kitleleri hedeflediği, daha odaklı ve çok çeşitli saldırıların gerçekleştiği bilgisi verilmektedir. Başlıca örnekleri, Rio olimpik oyunların gerçekleşme tarihine yakın, bu olimpik oyunları anımsatan zararlı yazılım içeren epostaların çoğunlukla gözlemlenmesi, elektrik şebekeleri üzerinden Android cihazlara sızabilen zararlı yazılımların tespit edilmesi ve Trojan-Banker.AndroidOS.Asacub isimli bankacılık

uygulamalarını hedef alan zararlı yazılımın yaygınlaştığına dikkat çekilmesidir. İlgili analiz raporuna göre üç aylık bir süreçte toplamda 170 milyon saldırı tespit edildiği, 54 milyon yeni zararlı site adresinin tanımaya başlandığı ve 300 bin fidye yazılımı aktivitesinin durdurulduğu belirtilmektedir [36]. Kullanıcıların anti-virüs ve benzeri uygulamaları kullanmadığı, rahatsız edici bulduğu için kapattığı günümüzde [10] sadece bir anti-virüs firması için oldukça yüksek sayıda saldırı tespiti yapıldığı görülmektedir. Fidye yazılımlarındaki yüksek artış sayısı ev kullanıcılarının halen yoğun bir şekilde hedef olarak tercih edildiğini göstermektedir. Mobil zararlı yazılımlarındaki sayı artışı Çizelge 2.1'de gösterilmektedir.

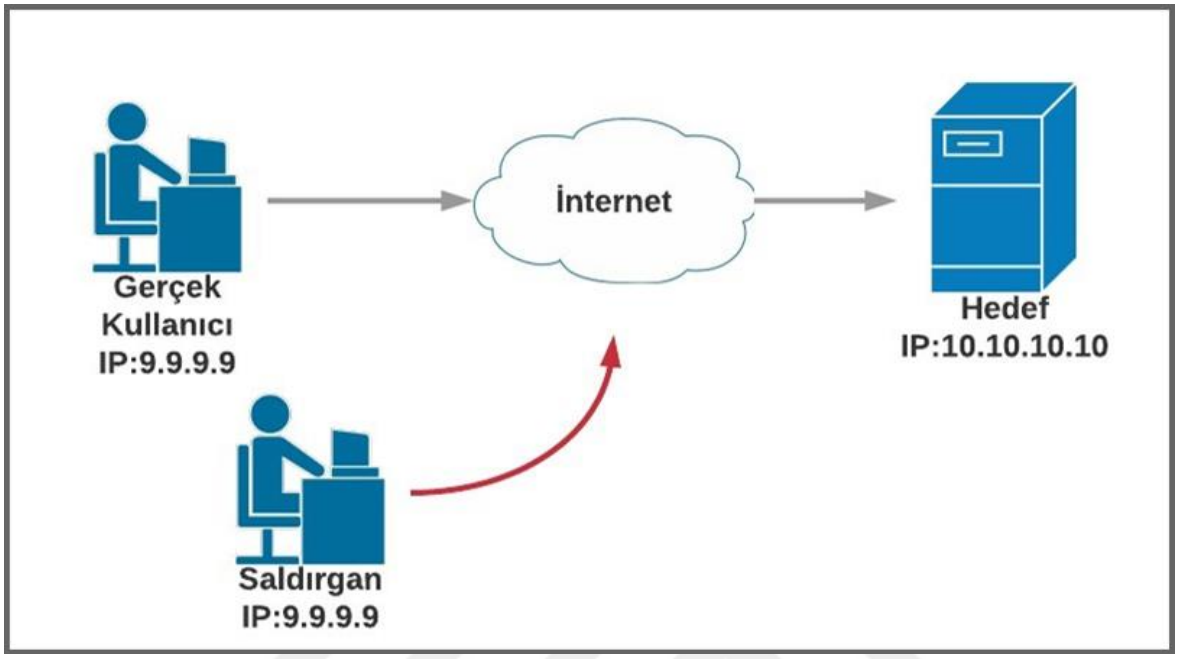
Çizelge 2.1. 2015 ve 2016 yıllarında çıkan mobil zararlı yazılımların sayısı



Mobil zararlı yazılımlarındaki sayıca artışın her geçen gün katlandığı görülmektedir. 2015 yılı dördüncü çeyreğinde 190 000 olan mobil zararlısının yaklaşık altı ay içerisinde 3,7 milyon sayısına ulaştığı belirtilmektedir [36].

IP adresi sahteciliği (IP Spoofing) hizmet dışı bırakma saldırılarında saldırı etkisini artırmada sık kullanılan yöntemlerden birisidir. Yapılan saldırılarda her cihaz için birden fazla IP adresi kaynakmış gibi gösterilerek hedef sistemlere istek gönderilmesi ile gerçekleştirilmektedir. Bu sayede hedef sistemler gerçekte olana göre kat ve kat daha fazla

adresten bağlantı talebi aldığı algısı oluşturularak meşgul edilmektedir. IP adresi sahteciliği gerçekleşme aşaması ve yöntemi Şekil 2.1'de gösterilmektedir.



Şekil 2.1. IP sahteciliği yöntemi gösterimi

Saldırı alan hedef sistemlerdeki ağın bant genişliğine veya hedef sistemin kapasitesine göre eşik değer aşıldığında ise hedef yanıt veremez hale gelir ve saldırı başarılı olmaktadır. Bu saldırılara bir örnek üçlü el sıkışmanın (three-way handshake) sadece ilk adımının başarılı olmasının yeterli olduğu, SYN Flood olarak isimlendirilen saldırıdır. Saldırgan hedeften bir cevap beklemez, hedefe mümkün olduğunca fazla isteği farklı kaynaklardan gösterme çabasındadır [51-52]. Bu saldırı tipi çok fazla sayıdaki cihazın aynı anda belirli hedefler üzerine istek yapması ile gerçekleşmektedir.

Internet Society tarafından yapılan IP sahteciliği ile gerçekleştirilen hizmet dışı bırakma saldırılarında yansıma (reflection) ve amplifikasyon etkilerinin önemine dikkat çekilmiştir [52]. Yetkilendirme gerektirmeden çalışan internet protokollerinin kullanılmasıyla saldırıların etkisinin artıldığı ve hedeflerde tahrip gücü yüksek etkilere sebep olduğu belirtilmiştir. En çok kullanıcı cihazlarında olduğu tespit edilen amplifikasyon sağlayan bileşenlerin çeşitli saldırı tiplerinde 50 kata kadar saldırı gücünü artırabildiği belirtilmiştir. Yapılan çalışmanın sonucunda açık kaynak teknolojiler ile anti-sahtecilik uygulamalarının uygulanması gerekliliği vurgulanmıştır.

Marc Kührer ve arkadaşları tarafından yapılan hizmet dışı bırakma saldırılarında amplifikasyon etkisi oluşturacak istismar edilebilir cihazların tespiti üzerine yapılan çalışmada en çok yönlendiriciler istismar edilebilir olduğu tespit edilmiştir [53]. 20 milyon IP adresi üzerinde 13 farklı TCP (Transmission Control Protocol) taraması yapılan çalışmada saldırı güçlendirici etkenlerin yoğunluğu önemli bir tehlike olarak göze çarpmaktadır. 20 milyon IP adresinden 5 milyondan fazla saldırı etkisi artırabilecek adres bulunduğu tahmin belirtilmektedir. Amplifikatör olarak adlandırılan saldırıların etkisini artırma kabiliyetli bileşenlerin en çok yönlendirici cihazlarda olduğu tespit edilmiştir. Açıklık tespit edilen cihazlardaki zafiyetlerin protokollere göre oranı Çizelge 2.2'te gösterilmektedir.

Çizelge 2.2. İstismar edilebilir protokollerin taranan cihazlarda bulunma yüzde oranları

Protokol	Cihaz (%)			
	Yönlendirici	Gömülü sistemler	Yazıcılar	Diğer
FTP	83,5	15,5	0,0	0,9
HTTP	48,8	44,5	0,9	5,3
NetBIOS	25,3	35,1	12,8	26,8
SIP	14,4	47,2	0,2	38,2
SSH	10,1	77,3	0,0	12,6
Telnet	93,3	3,8	0,2	2,7

İstismar edilmesi ile amplifikatör olarak kullanılabilecek en çok cihazın yönlendiriciler olduğu tespit edilmiştir. Saldırı etkisi artırıcı amplifikatör olarak kullanılabilecek yönlendiricilerin en çok FTP ve Telnet protokollerinde istismar edilebilir olduğu sonucuna ulaşılmıştır. Yönlendiriciler dışında istismar edilebilir olduğu tespit edilen bileşenlerin yönlendiriciler aracılığıyla internet bağlantısı kurması nedeniyle yönlendiriciler üzerine geliştirilecek güvenlik önlemleri diğer bileşenler içinde kritik öneme sahiptir.

Mathy Vanhoef ve Frank Piessens tarafından keşfedilen ve KRACK, (Key Reinstallation Attack) olarak isimlendirilen saldırı vektörü 15 yıldır kullanılan WPA2 (Wi-Fi Protected Access) protokolündeki dörtlü el sıkışmanın istismar edilmesi sonucu gerçekleştirilmektedir [54]. KRACK saldırısı ile WPA2 protokolü kullanan bir kablosuz ağda parola kullanmadan

tüm ağ trafiği dinlenebilmektedir [55]. 802.11r standardını destekleyen modemler, yönlendiriciler, erişim noktası cihazları ve sinyal güçlendirici (repeater) cihazların birçoğunun KRACK saldırısından etkilendiği belirtilmektedir. Saldırıya karşı tek çözüm modemler ve yönlendiricilerde bulunan yazılımların güncellemesi olarak belirtilmektedir. Bir güncelleme mekanizması bulunmayan veya üreticisi tarafından artık güncelleme sunulmayan tüm cihazlar bu saldırıya karşı sürekli bir açık hedef halinde bulunmaktadır.

2018 Mayıs ayında tespit edilen ve GPON (Gigabit Passive Optical Network) özellikli yönlendirici ve modemleri etkileyen açıklık bu cihazların istismarına ve saldırganlar tarafından uzaktan yönetebilmesine olanak sağlamaktadır [56]. Uzaktan kod çalıştırması ile cihazların ele geçirilmesine olanak sağlayan açıklık ile kullanıcı cihazları botnet ağlarına dâhil edilerek uzaktan kontrol edilebilmektedir. Tespit edilen 5 farklı botnet ağının bu açıklığı kullandığı tespit edilmiştir. Bu botnet ordularının bu açıklığı kullanmak için adeta bir yarış içerisinde olduğu görülmektedir. Muhstik isimli botnet ağının bu açıklığı kullanması ile ilgili aşamaları tarama, bulaşma ve yönetim olduğu görülmüştür [57]. Açıklık barındıran cihazların taranması işlemi gerçekleştirerek raporlama sunucularına açıklığı barındıran GPON cihazları belirtilmektedir. İlgili cihazlar için zararlı yazılım bulaşma aşamasında dağıtım sunucusundan zararlı yazılımı indirilerek kurulum işlemi tamamlanmaktadır. Yönetim aşamasında ise zararlı yazılım bir merkezden iletilen komutları kullanarak çeşitli saldırılarda silah olarak kullanılabilmektedir.

2013 yılında tespit edilen SOHO Pharming, bir diğer yönlendirici cihazları hedefleyen saldırıdır. Yaklaşık 300 000 cihaza bulaştığı tespit edilen bu zararlı DNS protokolünü istismar etmektedir. SOHO Pharming zararlısının yönlendiriciler üzerindeki DNS ayarlarında değişiklik yaparak kullanıcıları saldırganlar tarafından oluşturulmuş sahte sitelere yönlendirdiği tespit edilmiştir [58]. Yönetim-komuta merkezine ait IP adresleri tespit edilen bu zararlının ilgili IP adreslerindeki sunucuların devre dışı bırakılmasıyla faaliyetleri durdurulmuştur.

2018 yılında keşfedilen VPNFilter isimli diğer bir IoT zararlısının ise 54 ülkede 500 000 cihaza bulaştığı tespit edilmiştir. Çoğunlukla küçük ölçekli ağ yönlendirici cihazına veya modemine bulaşan bu zararlının sahte sitelere yönlendirmeler yaptığı ve internet trafiğinde dinleme yapabilmesi gibi çeşitli kabiliyetleri olduğu tespit edilmiştir [59]. Toplam 16 cihazı etkilediği düşünülen VPNFilter zararlısı halen aktif olarak çalışmaktadır.

Craig Heffner ve Derek Yap tarafından yapılan küçük ölçekli ağ modemlerindeki güvenlik tehditleri üzerine yapılan analiz çalışmasında dört farklı modemin çeşitli saldırılara karşı tepkileri test edilmiştir [60]. Yapılan bu analiz çalışmasında üzerlerine saldırı testleri gerçekleştirilen modemlerin ele geçirilebildiği, XSS (Cross Site Scripting) gibi basit saldırılara karşı bile herhangi bir güvenlik mekanizması bulunmadığı görülmüştür. Modemlere bağlı olan diğer kullanıcıları da etkileyebilecek DNS sorgularının sahteciliğinin ağ üzerinde kolayca yapılabildiği gösterilmiştir. Çalışmanın sonucunda yönlendirici üreticilerinin güvenlik üzerine birçok geliştirme yapmakta olduğu fakat ev ağ cihazlarının bu geliştirmelerden halen çok geride kaldığı vurgulanmıştır.

Navinkumar Maheshwari ve Haresh Dagale tarafından yapılan IoT uygulamalarında güvenli iletişim ve güvenlik duvarı mimarisi üzerine yapılan çalışmada IoT elemanları kullanılarak gerçekleştirilen saldırılar ile IoT elemanları üzerindeki geliştirme zorukları incelenmiştir [61]. IoT elemanlarının kapasiteleri gereği ağ geçidi cihazlarıyla kısıtlı güvenlik kontrolü gerçekleştirdiği belirtilirken sadece paket analizi ile IP adresi kontrolü üzerinden hizmet dışı bırakma saldırılarının önüne geçilebileceği vurgulanmıştır. Paket filtreleme mekanizması yöntemlerinin IoT cihazlarının üzerinde uygulanmasının güç ve hafıza tüketimi nedeniyle etkin bir yöntem olmadığı belirtilmiştir.

Naman Gupta ve arkadaşları tarafından yapılan çalışmada IoT cihazlarının yer aldığı yerel ağ, LAN (Local Area Network) üzerinde konumlandırılan fiziksel bir güvenlik geçidi kullanılmıştır [31]. Modem ile IoT cihazları arasında Raspberry Pi konumlandırılan bu çalışmada ticari çözümlerin yüksek maliyetli olması ve açık kaynak olmamaları nedeniyle geliştirmeye kapalı olmalarına vurgu yapılmaktadır. Oluşturulan orta katman ile TCP/IP'nin ağ katmanındaki kontrol mekanizmaları ile IoT cihazlarının güvenliğinin sağlanması amaçlanmıştır. Kullanılan işletim sistemi belirtilmeyen çalışmada Linux sistemlerde yer alan IPTables güvenlik yazılımı kullanıldığı belirtilmektedir. Beyaz liste uygulaması ile sadece belirli cihazların erişim kurmasına izin verilen sistemde önbellekleme mekanizması yer aldığı belirtilmiştir. Zararlı yazılım bulaşan cihazların yüksek bant genişliği kullanması sonucunda tespit edilebileceği belirtilmesine karşın güvenlik geçidinin istismar tespiti sonrası uygulayacağı yöntemler belirtilmemektedir. Sonuç olarak önerilen çözüm için IoT cihaz sayısındaki artış ile Raspberry Pi'ın zamanla yetersiz kalacağı öngörüsünde

bulunulmuştur. Bu problemin çözümüne ilişikin daha fazla sayıda Raspberry Pi konumlandırıması veya daha güçlü bir cihaz kullanılabileceği önerilmiştir.

Sajad Shirali-Shahreza ve Yashar Ganjali tarafından SDN (Software Defined Network) tabanlı güvenlik duvarı ile ev kullanıcıları cihazlarının korunması üzerine yapılan çalışmada IoT cihazlarının saldırılar ile ele geçirilmesi ve farkedilmemesi üzerine vurgu yapılmaktadır [30]. Kısıtlı veri işleme, düşük güç tüketimi gibi özelliklere sahip olan IoT cihazlarının özel üretim donanım ve yazılımlar ile çalışması nedeniyle geleneksel anti-virüs çözümleri ile korunamayacağı belirtilmektedir. Çalışmada ev ağlarında konumlandırılan güvenlik duvarı çözümlerinin fonksiyonel yapısının IoT ağları için uygun olmadığı belirtilmektedir. Mevcut yerleşke güvenlik duvarı çözümlerinin belirli portlarda engelleme yapması, belirli protokolleri engellemesi gibi basit problemleri çözmesinin IoT ağları için yeterli olmadığı belirtilmektedir. Genellikle TCP/IP'nin ikinci ve üçüncü katmanında filtreleme yapabilen mevcut güvenlik çözümlerinin aktif botnet ordularına karşı güncellenebilir aktif bir veri tabanı bulunmaması nedeniyle mümkün olmadığı belirtilmiştir. Karmaşık saldırıları tespit etmek için imza tabanlı kontrol, derin paket analizi ve farklı ağlardan öğrenme yöntemi gibi yöntemlere ihtiyaç duyulan IoT ağlarında gelişmiş yöntemlerin uygulanması gerekliliği vurgulanmaktadır. Kurumsal yapılarda kullanılan ticari güvenlik duvarı çözümlerinin incelendiği bu çalışmada gelişmiş güvenlik duvarı çözümlerinin toplam sahip olma maliyetinin yüksek olması nedeniyle kullanılamayacağı tespiti yapılmıştır. Ev, Ofis ve IoT ağlarında SDN tabanlı bir güvenlik duvarı kullanımı sunan bu çalışmada sonuç olarak maliyet, kurulum ve kullanım yönünden kolaylık sağlayacağı düşünülen bir çözüm önerilmiştir.

Vahid Asghari ve arkadaşları tarafından BTY'nin ağlarda uygulanması üzerine yapılan çalışmada PfSense güvenlik duvarı yazılımı kullanılmıştır [62]. Açık kaynak kodlu BTY uygulamalarından Untangle, PfSense ve Endian üzerine yapılan araştırmalar sonucunda toplam uygulanma maliyeti ve daha kararlı yapıda olması nedeniyle PfSense tercih edildiği belirtilmektedir. Çalışmanın sonucunda BTY olarak kurulan PfSense'in toplam altı aylık kullanımı sürecinde iyi bir performans sağladığı belirtilmiştir. PfSense'in en önemli avantajlarının uygun maliyet ve kullanım kolaylığı olduğu belirtilmektedir.

Mingphum Arunwan tarafından güvenlik duvarı yazılımlarının savunmaya dayalı performans karşılaştırması üzerine yapılan çalışmada PfSense ve Endian çözümleri çeşitli

saldırı tipleri uygulanarak kıyaslanmıştır [63]. Hedef sisteme port tarama, ölüm pingi, flooding ve parola deneme saldırıları gerçekleştirilen güvenlik duvarlarının tepkileri log analiz yöntemleri ile incelenerek saldırı tespit kabiliyetleri ölçülmüştür. Sonuç olarak PfSense'in birçok saldırı tipinde Endian'a göre daha üstün olduğu tespit edilmiştir.

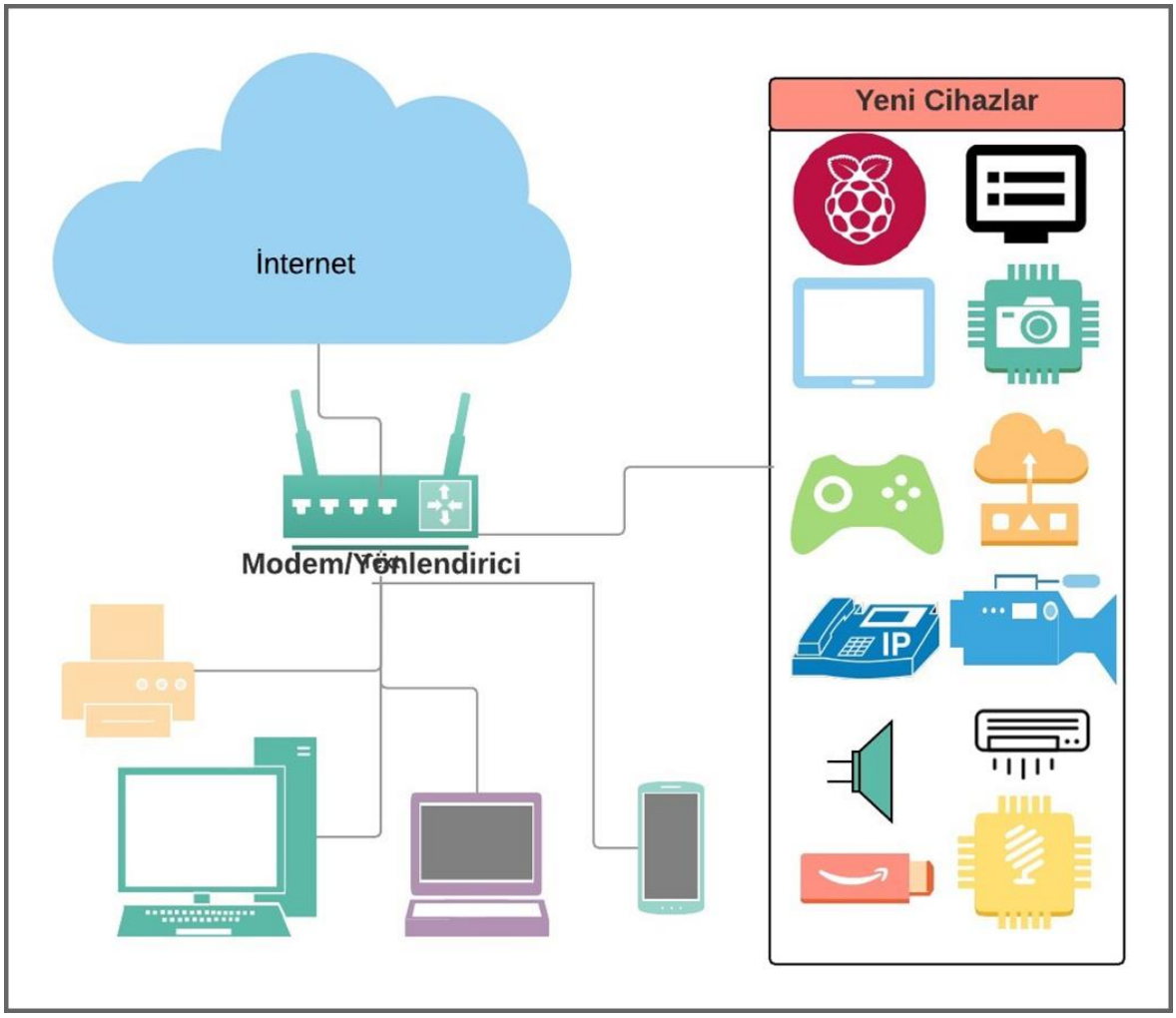
3. EV, OFİS VE IoT AĞLARI

Bu bölümde ev, ofis ve IoT ağları ile günümüzde kullanılan siber güvenlik kavramları hakkında bilgiler bulunmaktadır.

Çeşitli amaçlarla iki ya da daha fazla cihazın birbirleri ile iletişim kurabildikleri yapıya ağ denilmektedir. Ağa katılan cihazların sayısı nedeniyle ev, ofis ve IoT ağları için küçük ölçekli ağ kavramı kullanılmaktadır. Ağa yeni katılan cihazlar için IoT cihazları kavramı kullanılmıştır.

Ev ve küçük ölçekli ofis ağları literatürdeki çeşitli çalışmalarda SOHO kısaltmasıyla ifade edilmektedir. Evlerde veya ofislerde kurulan, bilgisayarlar, cep telefonları ve tabletler gibi kullanıcı cihazlarının birbirleri ile iletişim kurmasını sağlayan ağa yerel ağ denilmektedir. Kurulan ağ ile kullanıcı cihazları birbirleriyle iletişim kurabilmekte ve veri alışverişi yapabilmektedir. IoT cihazlarının ağa katılımı ile evlerde ve ofislerde kurulan ağlarda çok çeşitli cihazlar kullanılır hale gelmiştir. Heterojen ağlar olarak da nitelendirilen bu ağlar genellikle bir modem aracılığıyla kurularak ağ veri alışverişi yapılması sağlanır. Modemler, TCP/IP protokolü ile çalışan işletim sistemi ve yazılımdan oluşan cihazlardır.

Algılayıcılar, buzdolabı, klima, televizyon, video oynatıcı gibi akıllı cihazlar, akıllı ampuller, yazıcılar, kameralar, oyun konsolları, akıllı saatler, akıllı yatak teknolojileri, akıllı tartılar gibi cihazlar ve gündelik hayatta kullandığımız bilgisayarlar, akıllı telefonlar, tabletler, giyilebilir teknolojiler gibi cihazlar için IoT cihazları kavramı olarak isimlendirilmektedir. Günümüzde mevcut olarak kullanılan cihazlara ek olarak ağa dâhil olan yeni cihazların gösterimi Şekil 3.1'deki gibidir.



Şekil 3.1. Ev ağında bulunan ve ağa yeni katılan IoT ağ elemanları

Ağda mevcut olarak kullanılan ve son yıllarda katılan yeni cihazlar kablolu veya kablosuz protokollerle bağlandıkları modemler üzerinden internet bağlantısı kurmaktadırlar.

3.1. Siber Güvenlik

Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden, ağlardan ve birbirine bağlı iletişim kurabilen sistemlerden oluşan bilgi sistemi ortamlarına siber uzay denilmektedir [64]. Siber güvenlik ise siber uzaydaki sistemlerin ve tüm bireylerin korunmasını, bu ortamda ortaya çıkan her türlü bilginin ve verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, olası güvenlik problemlerin tespitini, bu problemlere yanıt verilmesini, bir zarar söz konusu ise olayın giderilmesi gibi tüm durumları ve süreçleri ifade eden kavramdır.

Siber güvenlik üç temel unsur üzerinden ele alınmaktadır. Bunlar, gizlilik, bütünlük ve erişilebilirliktir [65]. Gizlilik, bilginin erişimine açık olan kişiler haricindeki kimselerin eline geçmesi kavramıdır. Bütünlük, bilginin herhangi bir dış müdahaleye maruz kalmamasını ifade eder, bu müdahale bilgiyi değiştirme, silme veya zarar verme olabilir. Erişilebilirlik veya kullanılabilirlik ise bilgiye ulaşması gereken kişilerin istedikleri zaman ulaşabilmeleri ve yetkileri dâhilinde bilgiyi işleyebilmeleri demektir. Bu üç etkenden birisi bile sağlanmadığında gerçek anlamda güvenlikten bahsetmek mümkün değildir.

Güvenliği tehdit eden açıklıklara zafiyet denilmektedir. Zafiyetlerin saldırganlar tarafından tespit edilerek kullanması ile siber saldırılar gerçekleşmektedir. Bu yüzden zafiyetlerin saldırganlar tarafından keşfedilmeden tespit edilerek giderilmesi önemlidir. Zafiyetlerin neden olduğu tehditler ise, sisteme girme, yetkisiz erişim sağlama, sistemin çalışmasını engelleme, bozma, verileri değiştirme veya silme, kimlik sahteciliği, kişisel bilgileri kötüye kullanma, bireylerin mahremiyetine girme olarak ifade edilmektedir [66].

3.2. Nesnelerin İnterneti (IoT)

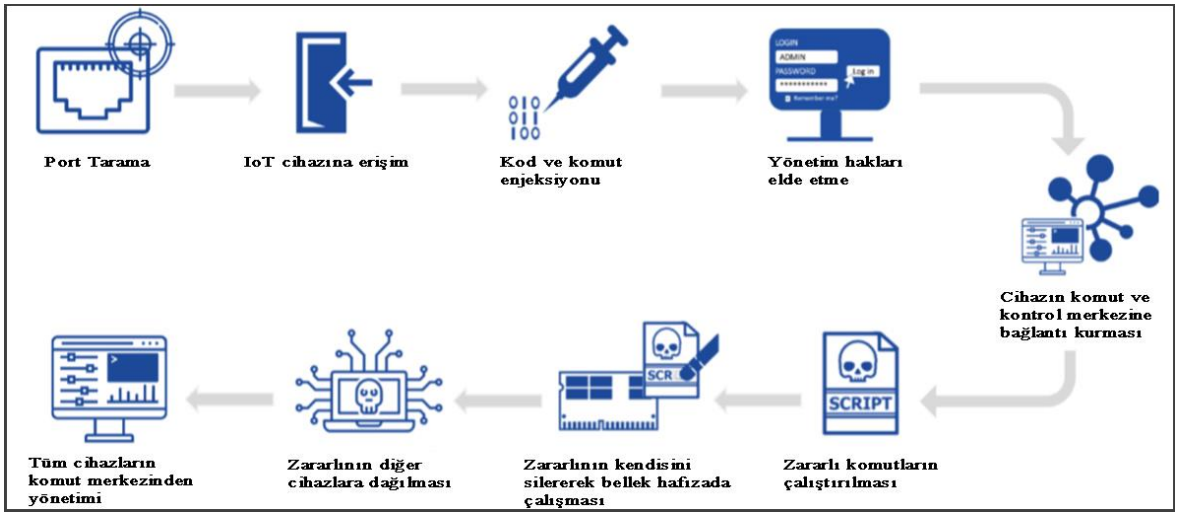
IoT, dünya çapında eşsiz bir adrese sahip birbirine bağlı nesnelerin oluşturduğu ağ olarak tanımlanmaktadır. Farklı tiplerdeki çeşitli verileri, RFID (Radio Frequency Identification), GPS (Global Positioning System), kızılötesi algılayıcılar, lazerler gibi cihazlar ve teknolojilerle işleme IoT olarak ifade edilmektedir [67]. Ortak bir altyapı ve bütünlük içerisinde IoT gerçek zamanlı olarak toplanılan veri veya süreçlere denilmektedir. Nesnelerden, ses, ışık, sıcaklık, konum, mekanik, elektriksel yük, kimyasal, biyolojik değerler gibi çeşitli veriler toplanmaktadır. Bu da IoT'nin kapsam olarak çok geniş bir çevreye hitap ettiğini göstermektedir. IoT altyapısının hedefi, akıllı nesneler arasında bağlantı kurarak bu nesnelerin hep birlikte çalışmasını sağlamak ve hayatımıza kolaylık sunarken yönetilebilirlik, gözlemlene bilirlik ve ölçeklenebilirlik özellikleriyle çeşitli açılardan tasarruf edilebilmesine olanak sağlamaktadır [67-68].

IoT'nin oluşturduğu ağın amacı makineler arası, makine ve insan arası ve insanların birbirleri arasındaki iletişiminde bağlayıcı rol oynamaktadır. Konumu, güç tüketimi, batarya ömrü gibi çeşitli faktörler nedeniyle IoT kapsamında geliştirilen ve kullanılan cihazlar için güvenliği sağlamak kritik olduğu kadar güçtür. IoT ekosistemindeki ürünler, kapsam gereği

donanım, yazılım ve ağ elemanları gibi orta katman elemanlarının bütününü içermesi nedeniyle yönetilebilirliği ve güvenliğinin sağlanması açısından zor bir konumdadır [68-69].

IoT ağlarında yer alan özellikle algılayıcı cihazlar çok basit seviyede veri üreterek internet trafiği oluşturmaktadır. Basit seviyeli donanıma sahip olan bu tür cihazlar düşük güç tüketimleri sayesinde üzerlerinde bulunan bataryalar ile uzun süre kullanılabilirler. Uzun ömürlü kullanım hedefiyle üretilen bu algılayıcılar üzerinde basit seviyeli güvenlik önemleri alınabilmektedir. Yüksek güç ihtiyacı olan gelişmiş güvenlik yöntemleri bu cihazlar üzerinde genellikle uygulanmamaktadır. İncelenen çalışmalarda da hem cihaz çeşitliliğinin yüksek olması hem de düşük sistem kapasitesi nedeniyle IoT ağlarında ağ üzerinde konumlandırılabilecek harici, ek cihazların önerisi sıklıkla vurgulanmaktadır [23, 28, 31].

Bir IoT cihazının herhangi bir güvenlik mekanizmasına sahip olmaması veya basit seviyeli güvenlik yöntemleri kullanıyor olması bu cihazların istismarını çok kolay hale getirebilmektedir. Saldırganlar internet üzerinde çeşitli yöntemlerle sürekli olarak aktif sistemleri tarama yaparak ağ haritaları çıkartmaya ve istismar edilebilir cihazları tespit ederek ele geçirmeye çalışmaktadır. Ele geçirilen cihazların verileri okunabilir, bu cihazlar üzerinden hassas bilgilere erişim sağlanabilir veya ele geçirilmiş çok sayıdaki cihaz bir merkezden yönetilerek hizmet dışı bırakma ve benzeri saldırılar gerçekleştirilebilmektedir. İnternet üzerindeki IoT cihazlarının tespit edilmesi, ele geçirilmesi ve bir merkezden yönetilerek saldırılarda kullanılması üzerine Avrupa Ağ ve Bilgi Güvenliği Ajansı, ENISA (The European Union Agency for Network and Information Security) tarafından yapılan çalışmada IoT saldırılarının gerçekleşmesi aşamaları Şekil 3.2'de gösterilmektedir [70].



Şekil 3.2. ENISA'ya göre IoT saldırılarının gerçekleşme aşamaları

Doğrudan erişilerek kod enjekte edilmesi yöntemiyle uzaktan kontrol edilebilir bir silah haline gelen IoT cihazları tek başına zarara yol açabileceği gibi toplu halde gerçekleştirilen saldırılarda da kullanılabilmektedir. Çok sayıda IoT cihazının ele geçirilmesiyle yapılan hizmet dışı bırakma saldırıları günümüzde sıklıkla görülmektedir [3, 44, 47].

3.3. Ev, Ofis ve IoT Ağlarının Güvenliği

Bir açıklığı, hatayı veya kontrol zayıflığını kullanarak bilgi güvenliğinin üç temel özelliği olan gizlilik, bütünlük ve erişilebilirlikten birini veya birkaçını ihlal eden etkenler tehdit unsuru olarak nitelendirilmektedir. Zafiyetleri kullanarak siber saldırılar gerçekleştiren saldırganlar, hedefledikleri sistemlerde hizmet dışı bırakma, hizmetleri aksatma, bilgi çalma, bilgi değiştirme veya bütünlüğünü bozma, mahrem bilgileri dağıtma, itibarı zedeleyici müdahalelerde bulunma gibi çeşitli saldırılar düzenlemektedirler. Siber dünyadaki tehditler her geçen gün gelişerek daha karmaşık hale gelmekte ve birçok alanda kullanıcılara etki etmektedir. Tehditler geliştikçe tehditlere karşı koruma yöntemlerinin, yazılımların, ağın ve güvenlik ürünlerinin değişmesi kaçınılmazdır. Ülkelerde siber güvenlik komutanlıkları kurulmakta ve ülkelerin diğer ülkelere karşı gerçek dünyada olduğu gibi siber dünyada da üstünlük sağlamada büyük adımlar attığı bilinmektedir [71]. Uluslararası boyutta gözlemlenen bu gelişmeler özel firmalar arasında da bulunmaktadır. Rekabette üstünlük kazanma, bilgi kaçakçılığı, siber casusluk gibi çeşitli sebeplerle gerçekleştirilen siber saldırılar genellikle büyük firmalar arasında görülmekte ve büyük zararlara yol açtığı bilinmektedir.

Günümüzde en çok görülen siber güvenlik olayları bilgi çalınması, bilgilerin değiştirilmesi, bilgilerin bozulması veya şifrelenmesi gibi bilgi güvenliğinin temel unsurlarından gizlilik ve bütünlüğe karşı yapılmış olaylar olarak göze çarpmaktadır. Erişilebilirliği önlemeye yönelik saldırılarda ise son yıllarda en çok küçük ölçekli ağ elemanları kullanılarak büyük hedeflere karşı gerçekleştirilen yüksek bant genişliğinde hizmet dışı bırakma saldırıları sıklıkla görülmektedir. Kullanıcılara yönelik son yıllarda popüler hale gelen saldırılardan birisi de fidyeci yazılımlardır. İlk olarak 2005 yılında görülen bu yazılımlar günümüzde son kullanıcıları hedefleyen en tehlikeli saldırılardan olarak değerlendirilmektedir [49, 72]. Güçlü şifreleme algoritmaları kullanılarak gerçekleştirilen bu saldırı türünde kişilerin cihazlarındaki veriler şifrelenmekte ve bu şifrelenmiş verilerin çözülmesi karşılığından fidye talep edilmektedir. Günümüzde görülen çoğu fidye yazılımı mevcut teknolojiler ile kırılamayacak veya kırılması yıllar sürecek algoritmalar kullanmaktadır. Fidye yazılımlarının ilk örnekleri zayıf yazılım tasarımı ve zayıf algoritmalar sebebiyle kırılmıştır. Fidye yazılımlarının bir kısmı taşıdıkları imzalar ile anti-virüsler tarafından tanınır hale gelmiştir, bu sayede şifreleme işlemi öncesinde tespit edilerek önlenebilmektedir. Son yıllarda sıklıkla görülen bir diğer saldırı tipi ise hizmet dışı bırakma saldırılarıdır. Genellikle bilgisayarların birer zombi haline dönüştürülmesi ile gerçekleştirilen bu tip saldırılar son yıllarda daha çok IoT cihazları kullanılarak gerçekleştirilmeye başlanmıştır. Üzerlerinde bir güvenlik mekanizması bulunmayan veya basit güvenlik önlemine sahip bu cihazların kolay istismar edilebilmesi ve sayıca çok olmaları nedeniyle daha yoğun bir şekilde saldırılara maruz kaldıkları görülmektedir.

Ev, ofis ve IoT ağları karakteristik olarak kurumsal yapılarda oluşturulan ağlardan daha güvensiz ağlardır. IoT cihazlarının yaygınlaşmasıyla birlikte kurulan ağlar cihaz çeşitliliği açısından heterojen bir yapıya dönüşmüştür. Ev, ofis ve IoT gibi küçük ölçekli olarak nitelendirilebilecek bu ağlarda güvenliği sağlamak zordur. Ağ üzerinde çeşitli protokoller kullanarak çalışan birçok cihazın olması ağ iletişimini sağlamada kullanılacak cihaz tercihini zorlaştırmaktadır. Raspberry Pi ve benzeri tek kart cihazlar kullanılarak geliştirilen çalışmalar bulunmaktadır. Bu çalışmalarda Raspberry Pi ve benzeri cihaz kullanımının mevcut zorlukları kısmen çözdüğü, gelişmiş ağ işlemleri için daha güçlü cihaz kullanımının kaçınılmaz olduğu sonucu elde edilmektedir.

3.3.1. Açık kaynak kodlu güvenlik çözümleri

Açık kaynak kodlu yazılım, yazılım dünyasında uzun bir süredir var olan fakat son yıllarda daha çok popüler hale gelen bir yazılım geliştirme metodolojisidir. Açık kaynak yazılımlar, kaynak kodları herkes tarafından erişilebilir yazılımlar için kullanılmaktadır. Kaynağının açık olması yapılan değişiklikleri paylaşmayı zorunda kılmamaktadır. Bu geliştirme metodolojisinde yazılımı daha iyi kodlayabilme – geliştirebilme kaygısı bulunmaktadır [73]. Bir ücreti olmaması, farklı bakış açıları ile kaliteli kodlamaya sahip olması ve adaptasyon konusunda kolaylıklar sağlaması nedeniyle açık kaynak kodlu yazılımlar sıkça tercih edilmektedir. Kişiler herhangi bir lisans bedeli ödemeden bu yazılımları cihazlarına indirip kullanabilmektedirler. Toplam edinim maliyeti açısından cazip olan açık kaynak kodlu yazılımlar daha kolay yaygınlaşabilmektedir. Yazılımın yaygınlaşması zamanla daha kaliteli kod yapısına sahip olmasına ve daha kullanışlı bir yazılım olmasına olanak sağlamaktadır.

Kamuda açık kaynak kodlu yazılımların Türkiye'deki kullanımı ile ilgili yapılan bir çalışmada açık kaynak kodlu yazılımların kamu için önemi belirtilmiştir [74]. İlgili çalışmada açık kaynak kodlu yazılımların güvenilir olması, kaliteli olması, esnek olması ve toplam edinim maliyeti gibi çeşitli etkenler ile diğer yazılımlara göre bir adım önde olduğu belirtilmektedir. Güvenlik ve toplam edinim maliyeti dünya genelinde açık kaynak kodlu yazılımların tercih edilmesindeki en büyük etkenler arasında yer almaktadır. Açık kaynak kodlu yazılımların güvenlik açısından olumlu bir değere sahip olup olmaması konusu tartışmaya açık olarak görülse de bir yazılımın dünyanın dört bir yanından uzman kişiler tarafından birlikte geliştiriliyor olması kod kalitesi açısından önemli bir ölçüt olarak değerlendirilmektedir. Diğer bir yaklaşım ise kodlarına kolay ulaşılabilmesi sayesinde kullanım şeklinin isteğe ve ihtiyaca göre adapte edilebilmesi esnekliğinin sağlanabilmesi açık kaynak kodlu yazılımlar için önemli bir özellik olarak belirtilmektedir.

Açık kaynak kodlu güvenlik çözümlerinin en çok bilinen uygulaması olan PfSense güvenlik duvarı çözümü günümüzde birçok alanda kullanılmaktadır. Uzun yıllardır geliştirilen bu yazılım günümüzde halen geliştirilmekte ve küçük/büyük birçok ağın korunmasında görev almaktadır. Birçok özelliği bünyesinde barındıran bu çözüm tamamen açık kaynak kodlu olup kodlarına ulaşılarak indirilebilir, kurulabilir ve geliştirilip yeni özellikler katılarak kullanılabilmektedir. PfSense, güvenlik duvarı olmanın ötesinde bir bütünleşik tehdit yönetimi uygulaması olarak geliştirilmektedir [62].

Günümüzde aktif olarak geliştirilen ve sık kullanılan diğer açık kaynak kodlu güvenlik duvarı ve saldırı tespit uygulamaları; iptables, IPCop, Endian, Untangle, OPNSense, Snort ve Suricata uygulamalarıdır. Bu uygulamalardan PfSense, Endian ve OPNSense BTY uygulamaları olarak kullanılmaktadır. Snort ve Suricata saldırı tespit sistemi (STS), saldırı önleme sistemi ve ağ güvenlik gözetleme araçları olarak kullanılmaktadır [75]. STS uygulamalarının en çok bilinen örneği ise Snort uygulamasıdır. Snort gerçek zamanlı analiz, log kaydı oluşturma ve uyarı sistemi olarak kullanılmaktadır. Öne çıkan önemli özelliklerinden birisi ise neredeyse tüm işletim sistemlerinde çalışabilmektedir. Snort kodları kullanılarak türetilmiş Gnort ise grafik işlemci kullanarak yüksek performans sunmaktadır [76-77]. Saldırı tespiti, anlık paket analizi, virüs taraması gibi işlemler yüksek güç gerektiren işlemlerdir. Bu tür uygulamalar yüksek maliyetli olması ve kullanım uzmanlığı gerektirmesi nedeniyle genellikle kurumsal ağlarda kullanılmaktadır.

Ev, ofis ve IoT ağlarında ağ geçidi üzerinde güvenliği sağlamak adına Raspberry Pi ve benzeri uygulamalar ile geliştirilen çözümler önerilmektedir [23, 31, 78]. İlgili uygulamaların zamanla yetersiz kalacağı öngörüsü ve mevcut donanımsal kısıtları nedeniyle yapılan birçok çalışmada daha gelişmiş çözümlerin geliştirilmesi vurgusu yapılmaktadır. Raspberry Pi ve benzeri donanımların işlemci ve çevre elemanları kurumsal ağlarda kullanılan güvenlik uygulamalarını çalıştırmada yetersiz kalmaktadır. Amerikan savunma bakanlığı tarafından sunulan küçük ölçekli ağların güvenliğinin sağlanması için en iyi yöntemler önerisinde ev, ofis ve IoT ağları için güvenlik duvarı kabiliyeti olan cihazları kullanılması vurgulanmıştır [79]. Açık kaynak kodlu çözümler sayesinde toplam edinim maliyetini sadece donanım maliyetine indirgenebilmektedir. Mevcut modem ve benzeri cihazlara göre daha yüksek sistem gereksinimine ihtiyaç duyan bütünleşik tehdit yönetimi uygulamaları açık kaynak kodlu olmaları sayesinde sadece donanım maliyeti ile uygun maliyetle geliştirilebilmektedir.

3.3.2. Bütünleşik tehdit yönetimi

Güvenlik duvarı özelliğinin yanı sıra içerik filtreleme, derin paket analizi, anti-spam gibi çeşitli güvenlik bileşenlerinin bir araya getirilmesiyle ile ortayan çıkan uygulamara bütünleşik/birleşik tehdit yönetimi denilmektedir [4].
Yüksek sistem kaynağı gereksinim olan BTY uygulamaları genellikle ticari ve yüksek maliyetli ürünler olarak günümüzde görülmektedir.

Açık kaynak kodlu BTY çözümlerinden en çok bilinen PfSense, FreeBSD tabanlı işletim sistemi üzerinde çalışabilen bir güvenlik yazılımıdır. HTTP, DNS ve eposta protokollerine göre filtreleme yapabilen yeni nesil güvenlik duvarı çözümlerinin ilk örneklerindendir. FreeBSD üzerinde çalışmasına rağmen FreeBSD bilgisi gerektirmeden basit bir arayüz aracılığıyla yönetilebilmektedir. Bünyesinde kendine has komut yazım biçimi olan PfSense yapılandırılması halinde yönlendirici görevi de üstelenebilmektedir [62]. Pfsense, kendi yazılımı ile birlikte özelleştirilmiş bir FreeBSD dağıtımı ile birlikte dağıtılmaktadır. Ağ iletişimi ve kontrol mekanizmalarına güçlü paket inceleme çözüm yöntemleri getirerek BTY, yönlendirici, yük dengeleyici ve durum denetimli güvenlik duvarı olarak kullanılabilmektedir.

Açık kaynak kodlu olması sayesinde PfSense temel alınarak geliştirilen çözümlere günümüzde rastlamak mümkündür. OPNSense bu uygulamalardan bir tanesi olarak PfSense uygulamasından daha iyi özelliklere sahip olduğu yapılan karşılaştırma çalışmalarında belirtilmektedir [80]. Yapılan bir çalışmaya göre OPNSense uygulamasının daha gelişmiş kod mimarisinde geliştirilmiş olması, ağ yönetimi için daha kabiliyetli olması ve modern ara yüzü nedeniyle PfSense uygulamasından daha üstün olduğu vurgulanmaktadır. Yazılım dünyasındaki yeniliklere adapte olmuş, Rest-API, iki seviyeli yetkilendirme gibi gelişmiş özellikleri bünyesinde barındıran OPNSense eklenti desteği de sunmaktadır. Aktif olarak geliştirilen ve haftalık güncellenen bir BTY uygulaması olan OPNSense, esnek yapısıyla küçük-büyük birçok yapıda kullanılabilmektedir. OPNSense güvenlik duvarı çözümü durum denetleyici yapı sunmakta ve durum tablosu üzerinde kontrollere izin vermektedir. Vekil sunucu, VPN (Virtual Private Network), VLAN (Virtual LAN), anti-virüs motoru, saldırı tespit sistemi, trafik filtreleme ve şekillendirme, yük dengeleme gibi birçok ağ güvenlik yönetimi işleminin yapılabilmesine olanak sağlamaktadır.

Suricata saldırı tespit ve önleme sistemi

Saldırı tespit sistemleri incelendiğinde genellikle Snort ve Snort tabanlı geliştirilmiş çözümlerin kullanıldığı görülmektedir. Oldukça esnek ve kullanışlı olan Snort en çok kullanılan saldırı tespit uygulamasıdır. Çalışmamız kapsamında STS'ler incelendiğinde Snort ve Suricata yazılımları arasında yapılan karşılaştırmalar genellikle Suricata'yı son yıllardaki yeni özellik geliştirmeleri nedeniyle bir adım öne çıkartmaktadır. Snort tekli iş parçacığı modelinde çalışabilirken Suricata çoklu iş parçacığı yönteminde çalışabilmektedir.

Bu sayede Suricata, paket analizi ve saldırı tespitinde daha yüksek performans sağlamaktadır [81]. Çoklu iş parçacığı yönteminde çalışması nedeniyle daha yüksek bellek gereksinimi bulunmaktadır. Suricata gelişmiş HTTP kütüphanesi sayesinde saldırı tespit oranı olarak Snort'a göre daha yüksek başarım göstermektedir [82]. Suricata'nın son zamanlarda sık görülen saldırılarından hizmet dışı bırakma saldırılarına karşı başarı oranı olarak daha iyi olduğu tespit edilmiştir [81-84].

3.4. Ev, Ofis ve IoT Ağlarında Kullanıcılar

Günümüzde internete bağlanan IoT cihazları sayısının 6,4 ile 9 milyar arasında; masaüstü, dizüstü ve akıllı telefon gibi kullanıcı cihazlarının ise 9 milyar civarında bir sayıya ulaştığı belirtilmektedir [1]. Toplamda internete bağlanan bileşen sayısının 2016 yılı itibariyle 18 milyar seviyelerine ulaştığı belirtilmiştir [1]. Masaüstü ve dizüstü bilgisayarlar, tabletler, televizyonlar, IoT cihazları gibi çeşitli cihazlar genellikle bir internet sağlayıcısının fiziksel olarak evlere sağladığı hat üzerinden internet bağlantısı kurmaktadır. Fiziksel olarak kurulan bağlantıyı sağlayan modemler üzerindeki kablolu veya kablosuz dağıtım aracılığıyla internet iletişimi ağdaki diğer cihazlara dağıtımı gerçekleşmektedir. Kullanıcılar modem veya erişim noktası cihazı tarafından tahsis edilen IP adresi ile yetkilendirilerek internete erişim sağlar. Kullanıcılar bu cihazlara çeşitli kimlik doğrulama yöntemleri ile bağlanarak internet trafiğine erişebilirler. Bu cihazların kurduğu internet trafiği bilgi alışverişi sürecinde birçok protokol ve yöntem sürekli olarak kullanılmaktadır. Bu süreçlerden haberdar olmayan kullanıcılar internet bağlantısı kurulması ile birer ağ elemanı olarak internette yer almaktadır.

Siber güvenliğin sağlanması açısından birçok faktörün temelinde farkındalık bulunmaktadır. Siber güvenlikte en zayıf halka olan kullanıcılar siber güvenliği, yorucu, sıkıcı, dikkat dağıtıcı, sinir bozucu bulmakta, uygulanan güvenlik çözümlerini ve süreçlerini genellikle göz ardı etmektedir [10]. İşletim sistemi, anti-virüs gibi yazılımların güncelleştirme uyarılarını göz ardı eden kullanıcılar için siber tehditler kritik öneme sahiptir. Fidye yazılımları örneğinde olduğu gibi, zararlı bir e-posta ekini saldırganlar tarafından sosyal mühendislik yöntemleri ile kandırılması sonucunda açan kullanıcılar için güvenlik çözümlerinin devreye girerek müdahale etmesi önemlidir. Rahatsız edici olduğu için pasif duruma getirilmiş veya güncelliğini kaybetmiş güvenlik çözümleri siber güvenliğin sağlanması noktasında eksik kalan noktalardan olarak nitelendirilmektedir.

Ev, Ofis ve IoT ağlarında kullanılabilecek ev kullanıcıları için kolay kullanım sunan çözümler basit seviyede güvenlik sağlaması nedeniyle etkin bir çözüm olarak nitelendirilmemektedir. Gelişmiş saldırıları önleyen çözümlerin hem yüksek maliyetli olması hem de kurulum ve kullanım açısından uzmanlık gerektirmesi ev kullanıcılarının bu tür çözümleri tercih etmesini zorlaştırmaktadır.

3.5. Sızma Testleri İle Ağ Güvenliğinin Sağlanması

Siber güvenliğin sağlanmasında özellikle kurumsal yapılarda açıklıkların ve istismar edilebilecek zayıf noktaların önceden tespiti için sızma testleri gerçekleştirilmektedir. Çeşitli siber saldırı araçları ve yöntemleri kullanılarak bilişim sistemlerine karşı siber saldırgan öngörüsü ile gerçekleştirilen saldırı testleriyle zayıf noktalar istismar edilerek ulaşılabilecek en uç noktaya ulaşılmaya ve bilgi toplanmaya çalışılmaktadır. Tespit edilen tüm açıklıkların raporlanmasıyla güvenlik sıkılaştırma yöntemleri uygulanarak açıklıklar giderilmekte ve zayıf noktalar güçlendirilmektedir. Periyodik olarak gerçekleştirilmesi önem arz eden sızma testleri sayesinde güvenliğin artırılmasında ve sürekliliğinin sağlanmasında önemli bir adım atılmaktadır.

Sızma testi gerçekleştirilecek bilişim sistemleri hakkında sahip olunan bilgi miktarına göre çeşitlenen sızma testi yöntemleri ile zafiyetler tespit edilmeye çalışılır. Sızma testleri sırasında çeşitli araçlar ve uygulamalar yardımcı olarak kullanılmaktadır. Bilgi toplama, ağ haritasını çıkartma, zafiyet tarama, zafiyet istismarı ve hak yükseltme gibi aşamalar uygulanarak gerçekleştirilen sızma testlerinde her aşamada kullanılmak için geliştirilmiş araçlar mevcuttur. Bu araçlardan alınan çıktılar sayesinde test aşamalarında ilerlenerek sızma testleri uygulanır ve sonuç olarak raporlamada tüm bulgular kanıt olarak sunulur. Günümüzde sızma testi araç ve uygulamaları genellikle bir işletim sistemi paketinde bütün şekilde veya bir yazılım deposunda (repository) toplu şekilde tutulmaktadır [85]. Sızma testlerinde en sık kullanılan işletim sistemleri; Kali, Parrot Security ve BlackArch'tır.

Çalışmamız kapsamında BTY geliştirilme, test, kontrol, performans ve başarım ölçümü aşamalarında sızma testi yöntemleri ve araçları kullanılmıştır. Kullanılan saldırı araçlarının oluşturduğu ağ trafiği analiz edilerek geliştirilen BTY üzerinde bu saldırıların tespit edilmesi ve önlenmesine yönelik kurallar bütünü uygulanmıştır.

Sızma testlerinde sıklıkla kullanılan Kali Linux işletim sistemi üzerindeki araçlar sayesinde sızma testi yöntemleri kolaylıkla uygulanabilmektedir. Saldırı benzetimi araçlarından Pytbull ve Fragrouter STS başarım testlerinde kullanılmaktadır. Bu uygulamalar Kali Linux işletim sistemindeki farklı amaçlar için kullanılan çeşitli yazılımları arka planda çalıştırarak saldırı gerçekleştirebilmektedir.

Pytbull bünyesinde 8 farklı saldırı türünde toplam 300 adet, Fragrouter ise 22 farklı saldırı türünde benzetim yapabilmektedir. Pytbull, saldırı testlerini Nmap, Nikto, tcprelay, apache2-utils gibi hazır kütüphaneleri arka planda kullanarak saldırı benzetimi gerçekleştirmektedir. Pytbull uygulaması hatalı paketler, kötü trafik, hizmet dışı bırakma saldırıları, güvenlik sistemleri atlatma teknikleri, kaba kuvvet saldırıları gibi kategorilerde saldırı benzetimi yapabilmektedir. Kali Linux işletim sistemi üzerinde istemci olarak çalıştırılan Pytbull uygulaması, STS'nin bulunduğu sunucu tarafındaki Pytbull uygulaması ile iletişime geçerek saldırı benzetimlerini sırasıyla gerçekleştirmektedir.

Fragrouter, TCP/IP kullanan ağlarda IP paketlerini parçalara ayırarak hedef sisteme gönderimini sağlayan bir uygulamadır. Fragrouter istemci tarafında tek başına çalışan bir uygulama olarak güvenlik yazılımları üzerinden veri gönderimini parçalara ayırarak gönderme yöntemi ile saldırı benzetimi yapabilmektedir. Parçalara ayrılan verinin analizi basit güvenlik uygulamaları tarafından yapılamayacağından bu yöntemle güvenlik uygulamaları atlatılabilmektedir. Fragrouter, ağdaki BTY uygulamasının üzerindeki STS'nin parçalanmış veri geçişi ile yapılabilecek saldırılar için bir tespit yöntemi uygulayıp uygulamadığını test etmek için kullanılmaktadır.

4. MATERYAL VE METOT

Bu bölümde geliştirilen bütünleşik tehdit yönetimi çözümü için tercih edilen donanım, yazılım, ek uygulamalar ve geliştirme metodolojisi hakkında bilgiler bulunmakladır.

Literatürdeki ev ve ofis ağlarında gerçekleşen saldırıların önlenmesi üzerine yapılan araştırmalar sonucunda güvenlik problemlerinin önüne geçilebilmesi için fiziksel bir güvenlik duvarı geliştirilmesi için gerekli araştırmalar yapılmıştır. Yapılan incelemeler sonucunda ev ve ofis ağlarında kullanılan modemlerde güvenlik duvarının olmaması veya basit kalması nedeniyle birçok saldırının tespit edilemediği, özellikle IoT cihazlarının ağ üzerinden kolaylıkla istismar edilebildiği görülmüştür. Ev ve ofis ağlarındaki güvenlik problemlerini çözmek üzere geliştirilen uygulamalardaki donanımların zamanla yetersiz kalabileceği öngörüsü bu alanda yapılan çalışmalarda sıklıkla belirtilmektedir. Bu öngörü ile birlikte ağ trafiğinin ve cihaz sayısının katlanarak artacağı tahminleri göz önünde bulundurularak geliştirilen BTY çözümünde yüksek sistem kaynaklarına sahip donanım kullanılması uygun görülmüştür. Ev, ofis ve IoT ağlarının kurumsal ağlara göre daha küçük ölçekli olması ve kullanıcı profiline hitaben maliyet analizi yapılarak uygun olacağı düşünülen donanım tercih edilmiştir.

Ev ve ofis ağları üzerinde gerçekleştirilen saldırıların benzetimi sanallaştırma ortamı üzerinde gerçekleştirilerek bu saldırıları tespit ve önleme yöntemleri uygulanmıştır. Saldırı tespit sistemi ile saldırıların önlenmesi ve oluşabilecek yeni saldırıları tiplerinin STS uygulamasının veri tabanına otomatik eklenmesi ile saldırı tespit kabiliyetinin devamlı olması sağlanmıştır. Otomatik saldırı veri tabanı güncellemesi sayesinde geliştirilmesi ardından bir yazılım güncellemesi almayan modemlerin güvenliğinin artırılması ve sürekli güncel kalması sağlanmıştır.

4.1. Materyal

Bu bölümde geliştirilen çözümde kullanılan bütünleşik tehdit yönetimi yazılımı ve tercih edilen donanım çözümü hakkında bilgiler bulunmaktadır. Yapılan incelemelere istinaden geliştirilen yapıda cihaz olarak ev ve ofis ağlarının genellikle sahip olduğu bant genişliği değerlerin çok üzerinde yüksek performans değerlerine ulaşabildiği tespit edilen PcEngines

tercih edilmiştir. Günümüzde ev ağları için sağlanabilecek en yüksek bant genişliğinin 100 Mbit/s olarak sağlandığı internet sağlayıcıları sitelerinde belirtilmektedir. İncelenen çalışmalarda PcEngines cihazının ev ağları için sağlanan bant genişliğinin çok daha üzerinde değerlerde trafik işleyebildiği görülmüştür [86-87]. Ev, ofis ve IoT ağlarında güvenliği sağlama üzerine yapılan çalışmalarda genellikle PfSense ve IPTables yazılımları tercih edilmektedir. Bir görsel ara yüzü bulunmaması ve BTY uygulamalarına göre daha az kabiliyetli olması nedeniyle tercih IPTables kullanımı uygun bulunmamıştır. PfSense uygulaması ile yapılan çalışmalar araştırılarak elde edilen performans ve başarım değerleri incelenmiştir. İncelemeler sonucunda PfSense'e göre daha yüksek performans sağladığı ve bünyesindeki STS ile daha başarılı saldırı tespit değerlerine ulaşabildiği görülen bir PfSense yansısı OPNSense tercih edilmiştir. Geliştirilen BTY uygulamasının saldırı tespit kabiliyeti ve kullanılabileceği konuma uygunluğu konusunda sanallaştırma ortamı üzerinde performans ve saldırı benzetimi gerçekleştirilmiştir. Sızma testi yöntemleri uygulanarak gerçekleştirilen saldırı benzetiminde Kali Linux işletim sistemi ve araçları kullanılmıştır.

4.1.1. Yazılım seçimi

Güvenliği en iyi şekilde sağlamanın başlıca ölçütleri, yazılımların ve işletim sistemlerinin güvenilirliği, kesintisiz hizmet kalitesi sunması, güncelleme konusunda kolaylık sağlaması ve saldırı tespit kabiliyetleri olarak görülmektedir. Zayıf tasarımlara sahip, basit algoritmalar ile geliştirilmiş yazılımlar, sistemlerin çalışmasında aksaklıklara yol açabilmekte veya görevlerini yerine getiremeye bilmektedir. Bir hizmet dışı bırakma saldırısına maruz kalan güvenlik duvarının yanıt veremez hale gelmesi veya çalışmasına olanak sağladığı diğer cihazların iş süreçlerini aksatması saldırının başarılı olduğunu göstermektedir.

Bu bölümde açık kaynak kodlu güvenlik duvarı, saldırı tespit sistemi ve güvenlik merkezli işletim sistemi yazılımları incelenmiş, geliştirilen sistemde tercih edilen işletim sistemi ve yazılımların genel özellikleri ve kabiliyetleri hakkında incelemeler yapılmıştır. Geliştirilen BTY uygulamasında kullanılan bileşenlerin sürüm bilgisi Çizelge 4.1'de gösterildiği gibi kaydedilmiştir.

Çizelge 4.1. Geliştirilen çözümde kullanılan uygulamaların sürümleri

Uygulama	Sürüm
FreeBSD işletim sistemi	11.1-RELEASE-p9
OPNSense güvenlik duvarı	18.1.7_1-amd64
Suricata STS	4.0.4
Squid vekil sunucu	3.5.27_3
C-ICAP anti-virüs motoru	1.5_1
OpenSSL şifreleme aracı	1.0.2o 27 Mar 2018

Geliştirme ve test aşamasında işletim sistemi ile BTY elemanlarının son kararlı sürümlerinin kullanımına dikkat edilmiştir.

Geliştirilen sistemde yazılım katmanından çeşitli ağ görevlerini yerine getirmesi beklenmektedir. Bunlar;

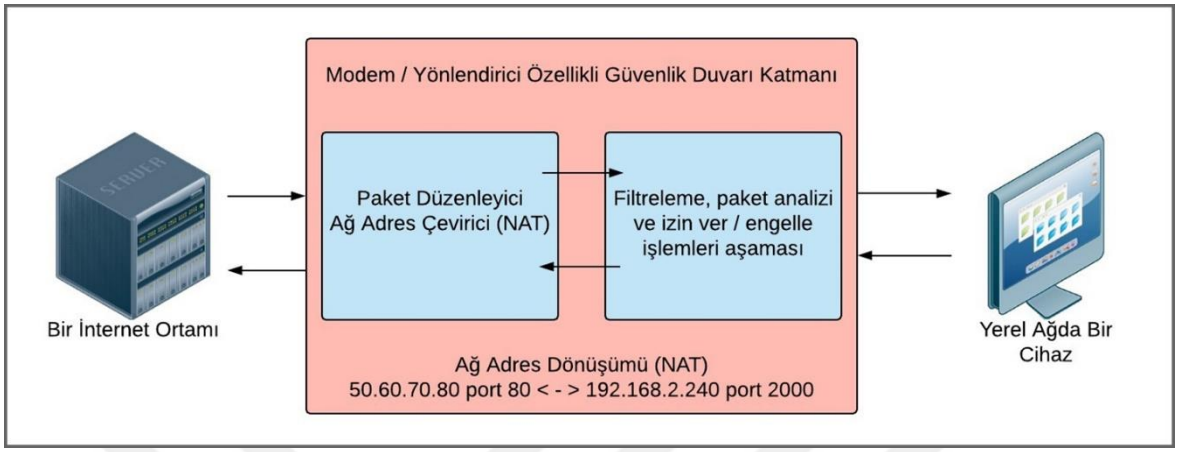
- Yerel ağdaki cihazlara IP dağıtımı
- Yerel ağdaki cihazların adres sorguları yapabilmesini sağlamak
- Ağ adres dönüştürme işlemi
- Yönlendirme işlemini gerçekleştirmek
- Yerel ağ içerisinde iletişimi kurmak
- Yerel ağ ile internet arasındaki iletişimi sağlamak

Ağ görevlerine ek olarak uygulanan güvenlik geliştirmeleri sayesinde ağ geçidi üzerinde trafik akışı sağlanırken zararlı aktiviteler önlenebilmektedir. Geliştirilen BTY uygulamasında ağ işlemleri FreeBSD işletim sistemi tarafından gerçekleştirilmektedir.

Bütünleşik tehdit yönetimi OPNSense

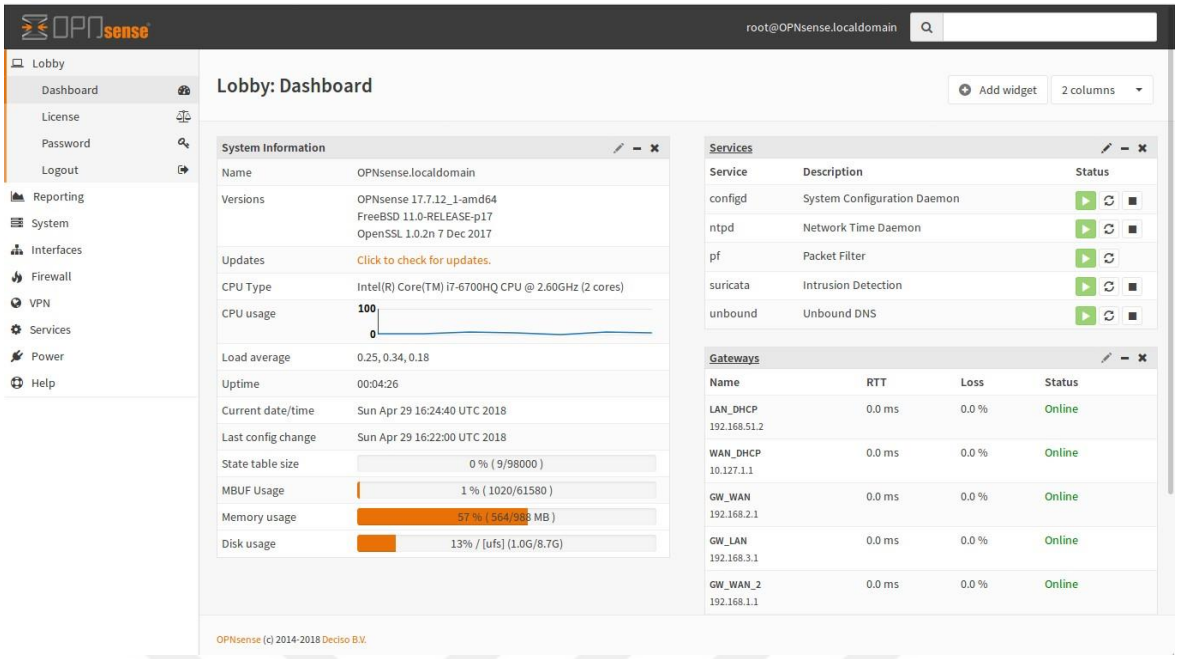
Genellikle kurumsal ağlarda kullanılan ve güvenliği sağlayan bir bekçi konumunda olan güvenlik duvarı, ağın gözetleyici bir elemanı olarak kullanılmaktadır. Bütünleşik tehdit yönetimi sayesinde ev, ofis ve IoT ağlarında ağ görevlerini yerine getirirken gelişmiş yöntemler ile saldırılar önlenebilmektedir.

BTY'nin ağ trafiğinin yerel ağdaki cihazlardan internet üzerine yönlendirmesi ve trafik üzerinde saldırı tespiti uygulama aşamaları Şekil 4.1'de gösterilmektedir.



Şekil 4.1. OPNSense BTY trafik akışı ve güvenlik uygulamaları konumlandırılması

OPNSense bünyesinde alias, hosts, ağ tanımı, portlar, URL (Uniform Resource Locator) tablosu, Geo IP, spam listesi, ACL (Access Control List) ve anti-virüs motoru gibi çeşitli özellikler barındırmaktadır. Bu sayede geleneksel yöntemlerin ötesinde saldırı tespitinde daha başarılı sonuçlar elde edebilmektedir. Erişim kontrol listeleri, vekil sunucu ile trafiğin güvenlik duvarı üzerinde açılması ve derin paket analizi yöntemleri gelişmiş tehditlerin önlenmesinde önemli rol oynamaktadır. Paket analiz yöntemleri ile gelişmiş zararlı yazılım aktiviteleri önlenebilmektedir. Çalışmamızda kullanılan bütünleşik tehdit yönetimi OPNSense kullanım ara yüzü Resim 4.1'de gösterilmektedir.

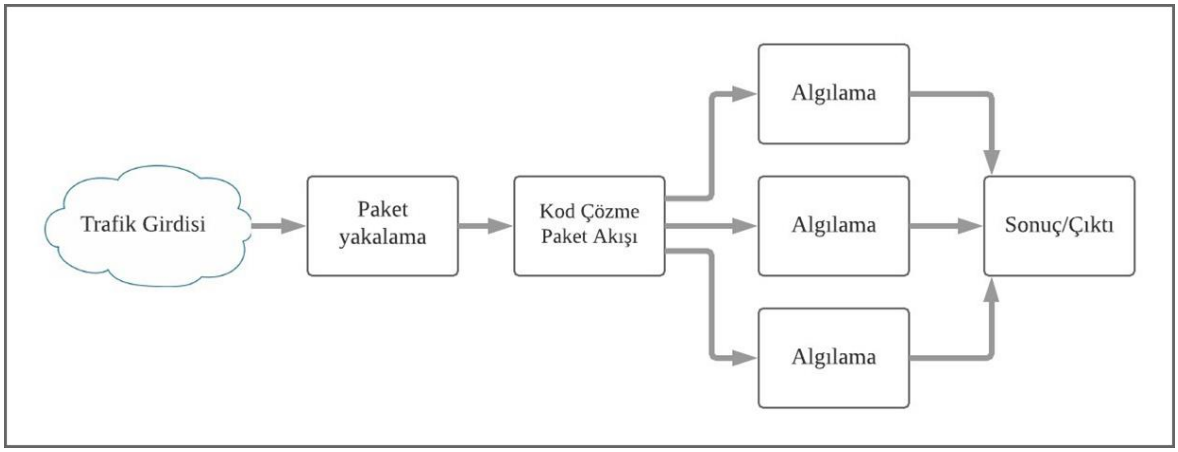


Resim 4.1. OPNSense BTY kullanım ara yüzü

OPNSense BTY'nin tüm ağ trafiği araçları ve güvenlik bileşenleri ara yüzü üzerinden yönetilebilmektedir.

Suricata ile saldırı tespit ve önleme

Sistemlerin ağ iletişimi kurduğu noktalarda ağ paketlerini inceleyerek çeşitli yöntemlerle anomali analizi yapabilen saldırı tespit sistemleri sayesinde zararlı aktiviteler önlenebilmektedir. İyi TCP/IP bilgisi gerektiren Suricata STS uygulaması doğru yapılandırılması halinde yüksek trafikli ağlarda bile başarılı bir şekilde saldırı tespiti yapabilmektedirler. Suricata'nın en önemli çalışma şekli olan "inline IPS" (Intrusion Prevention System) yöntemi sayesinde gelişmiş saldırılar yüksek ağ performans adına ödün vermeden önlenebilmektedir. Bu yöntem sayesinde ağ geçidi üzerinden geçen trafik üzerinde herhangi bir yansılama yapmadan saldırılar algılanabilmekte ve bağlantı önlenmektedir. Suricata STS saldırı algılama süreci Şekil 4.2'de gösterilmektedir.



Şekil 4.2. Suricata STS saldırı tespiti çalışma mekanizması

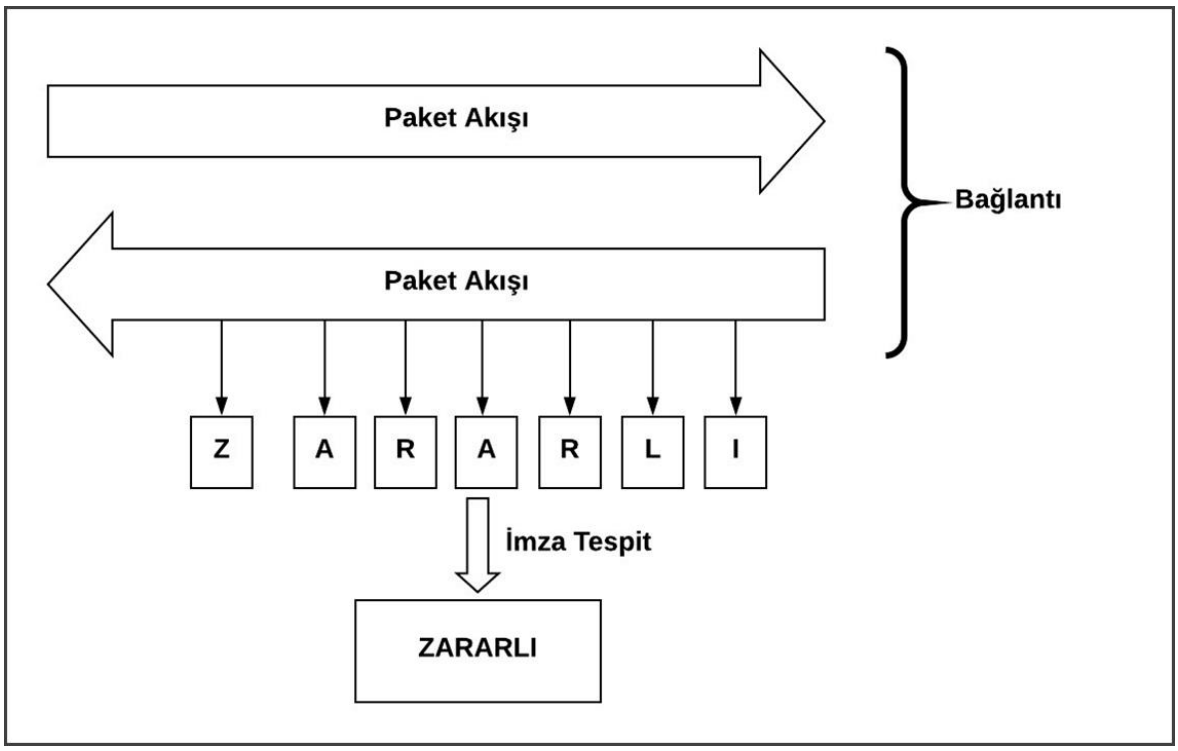
Suricata gelişmiş paket takip teknikleri ile zararlı tespiti yapabilmektedir. Şekil-x'te gösterildiği gibi Suricata'ya trafik girdisi ayarlanması durumunda LAN, WAN (Wide Area Network) veya iki ağ tarafından aynı olacak şekilde ayarlanabilmektedir. Bu sayede ağ geçidi gibi önemli bir noktada konumlandırılması durumunda ağın tüm trafiğini analiz edebilmektedir. Çoklu iş parçacığı modelinde çalışması sayesinde konumlandırıldığı noktada ağ trafiğini aksatmadan ve yavaşlatmadan yüksek başarım gösterebilmektedir.
İmza algılama tabanlı çalışan Suricata kullanıcılar tarafından özel kural yazımına olanak sağlamaktadır. Bu sayede konumlandırıldığı nokta için özel kurallar oluşturulabilmektedir. Suricata kural yazım biçimi Çizelge 4.2'de gösterilmektedir.

Çizelge 4.2. Saldırı tespit sistemi kural yazım biçimi

Kural Örneği	Kullanım Şekli
! 10.20.30.40	10.20.30.40 adresi hariç tüm adresler
$HOME_NET	Kurallarda belirtilen HOME_NET değişkeni
[60, 70, 80]	60, 70, 80 portları
!80	80 portu hariç tüm portlar
[$EXTERNAL_NET, !$HOME_NET]	EXTERNAL_NET olan, HOME_NET olmayan

STS Kural Yazım örneği:
İşlem protokol kaynak_ip kaynak_port yön hedef_ip hedef_port seçenekler
alert tcp 192.168.1.110 any → any any (msg:"192.168.1.110 adresinden gelen trafik";)

STS atlatma yöntemlerinden olan paketleri parçalara bölerek iletme yöntemine karşı geliştirilmiş paket takibi ile saldırı algılama Suricata'nın saldırı tespitinde yüksek başarım göstermesini sağlamaktadır. Suricata paket yeniden birleştirme yöntemi uygulayarak zararlı trafik analizi yapabilmektedir. Paket takibi ve paket birleştirme ile analiz için kayan pencere algoritması uygulanır. Bu sayede zararlı aktivitelerin parçalara bölünerek gönderilmesi ve hedefte birleştirilerek STS atlatılması yöntemi Suricata tarafından önlenmiş olmaktadır. Bağlantı sırasında alışverişi yapılan ağ paketlerinin akışı ve paket analiz yöntemi mekanizması Şekil 4.3'de gösterilmektedir.



Şekil 4.3. Paket birleştirme yöntemiyle saldırı tespiti

Zararlı içeriğin paketlere bölünerek gönderilmesi sırasında paketleri takip ederek birleştirme ve birleştirilen paketlerin incelenmesi aşaması Şekil 4.3'te gösterilmiştir. ZARARLI kelimesinin harfleri birer paket olarak gösterilen bu örneğe göre Suricata paket birleştirmesi sırasında ZARAR, ARAR, RAR gibi sıralı paketleri de inceleyerek zararlı paket imzası tespit etmeye çalışmaktadır. Eşleşen bir zararlı imzası algılanması durumunda paket trafiğinin işletilmesi önlenmektedir.

Geliştirilen BTY uygulamasında Suricata üzerinde çeşitli kural listeleri girilerek saldırı tespiti açısından birçok imza veri tabanı entegrasyonu sağlanmıştır. Otomatik güncellenme

özelliği açık olan imza veri tabanı entegrasyonu sayesinde saldırı tespit sistemi üzerindeki kurallar otomatik olarak güncellenebilmektedir. Bu sayede saldırı tespit mekanizmasının güncel kalması sağlanmaktadır.

4.1.2. Donanım seçimi

Ev ve ofis ağları gibi küçük ölçekli ağlar incelediğinde internet trafiği ortalamasının Türkiye standartlarında genellikle 8 Mbit/s – 16 Mbit/s civarında olduğu bilinmektedir. Türkiye'deki internet sağlayıcıları tarafından sağlanan internet bant genişliğinin en yüksek olduğu değerler genellikle 100 Mbit/s olduğu görülmektedir. Günümüzde bulunulan konuma göre değişmekle birlikte bu değerin çok daha altında değerler ev kullanıcılarına daha yüksek değerler ise orta ve büyük ölçekli işletmelerin kullanımına sunulmaktadır. Küçük ölçekli ağlar için belirtilen ortalama değerlerdeki bir bant genişliğini işleyebilecek donanımların son yıllarda popüler olan Raspberry Pi, Orange Pi, LattePanda, Asus Tinker Board, PcEngine gibi tek kart çözümler olduğu görülmektedir. Daha güçlü çözümler ile geliştirme yapılabilmesi mümkün olsa da maliyet analizi yapıldığında ev kullanıcıları için yüksek maliyetlerin ortaya çıkması uygun bulunmamaktadır.

Kullanılabilecek tek kart çözümler incelendiğinde genellikle ARM (Acorn RISC Machine) mimari işlemciler kullanılarak küçük boyut, düşük maliyet, düşük güç tüketimine karşı iyi performans hedeflendiği görülmektedir [23, 88]. LattePanda ve PcEngines kartlarının diğer kartların aksine x86 (64 bit) mimarisinde işlemciye sahip olduğu bilinmektedir. ARM işlemciler x86 mimari işlemcilere göre çok daha düşük güç tüketimi özelliği sunmaktadır. Bu nedenle kabiliyetleri daha kısıtlı, performansları x86 işlemcilere göre daha düşüktür. Düşük güç tüketimi ARM işlemcilerin mimarisi olan RISC (Reduced Instruction Set Computing) yapısından kaynaklanmaktadır. Paket analizi, yüksek sayıda bağlantı engelleme, durum tablosu tutma, saldırı tespiti gibi karmaşık işleri yapması beklenen güvenlik duvarı gibi bir yazılım veya donanım için ARM işlemci kullanmak performans kaybına neden olabilmektedir. ARM işlemcili Raspberry Pi kullanılarak geliştirilen ev güvenlik duvarı çözümlerinde cihazın sistem kaynaklarının zamanla yetersiz kalacağı öngörüsü yapılmaktadır. Bu nedenle x86 mimari işlemciye sahip PcEngines ve LattePanda kartları çalışma kapsamında kullanımı uygun bulunmuştur. Bu kartlar arasında yapılan maliyet analizi ile PcEngines kartının daha uygun maliyetli bir çözüm olacağı tespit edilmiştir.

PcEngines geliştirme kartı

İşlemci mimarisi x86 olan PcEngines günümüzde bu mimaride çalışan birçok işletim sistemini desteklemektedir. Çeşitli modelleri mevcut olan bu kart halen geliştirilmekte ve yeni modelleri ile günümüz teknolojilerine uygun hale gelmektedir. PcEngines geliştirme kartı gösterimi Resim 4.2'deki gibidir.

Resim 4.2. PcEngines geliştirme kartı

İnternet bağlantısı kurulmasını sağlayan ağ portlarına sahip olan PcEngines, x64 işlemci mimarisi sayesinde Unix ve Linux türevi işletim sistemlerini çalıştırabilmektedir. PcEngines ile yapılan bir çalışma ile farklı işletim sistemleri ve yönlendirici kullanılarak sistem kaynağı kullanımı karşılaştırması yapılmıştır [86]. Bant genişliği gerçek değerinin 940 Mbit/s olduğu bu ağ üzerinde yönlendirici konumuna yerleştirilen PcEngines'in yönlendirici yazılımı, PfSense yazılımı ve IPFire yazılımı ile yapılan testlerine yer verilmiştir. Yazılımların işleyebileceği en yüksek bant genişliği ve tepki süresi değerleri ölçülerek karşılaştırma yapılmıştır. Ağ üzerinde yapılacak bir istek, isteğin yanıtının dönüşü arasındaki süreye tepki süresi veya gecikme süresi denilmektedir. Anlık olarak oluşan trafiğin boyutuna bant genişliği denilmektedir. Yapılan karşılaştırmaya dair sonuçlar Çizelge 4.3'de gösterilmektedir [86].

Çizelge 4.3. PcEngines ile yapılan testlerde bant genişliği ve tepki süresi sonuçları

Donanım ve Yazılım	Bant Genişliği (Mbit/s)	Ortalama Tepki Süresi (sn)
Yönlendirici (PcEngines)	940	0,310
PcEngines + PfSense	620	0,45
PcEngines + IPFire	940	0,538

Bant genişliği değerinin daha yüksek ve ortalama tepki süresinin daha düşük olmasının en iyi kabul edildiği testlerde sonuçların kullanılan yazılıma göre değişkenlik gösterdiği tespit edilmiştir. PcEngines APU2C0 modeli kullanılan ve gerçek ağ bant genişliği 940 Mbit/s olan testlerde edinilen değerler donanım yeterliliği konusunda PcEngines'in uygun bir donanım olduğunu göstermektedir. Linux türevi işletim sistemi olan IPFire'ın daha iyi bant genişliğini yönetebilmesi üzerinde bulunan modüllerin PfSense'e göre daha az sayıda olmasından kaynaklanmakta olduğu görülmüştür. Daha gelişmiş özelliklere sahip olan PfSense, bant genişliğinde daha düşük değerler sunması paket analizleri, durum tutma, saldırı tespit ve analiz gibi çeşitli işlemlerden geçirerek yapması nedeniyle IPFire'a göre daha yavaş kalmaktadır. Diğer yandan yapılan testlerde belirtildiği üzere IPFire işletim sistemi dört çekirdekten tam güç alırken PfSense işlemcide tek çekirdek kullanarak trafik işlemektedir [86]. Bu noktada PfSense uygulamasından türetilen OPNSense'in çoklu çekirdek desteklemesi nedeniyle daha iyi performans sağlayabileceği tahmini yapılabilmektedir. Yapılan bu karşılaştırmanın sonucunda PcEngines donanımının geliştirilmesi hedeflenen çözüm için yeterli sistem gereksinimlerini sağlaması nedeniyle ev, ofis ve IoT ağları için uygun bir çözüm olduğu düşünülmüştür.

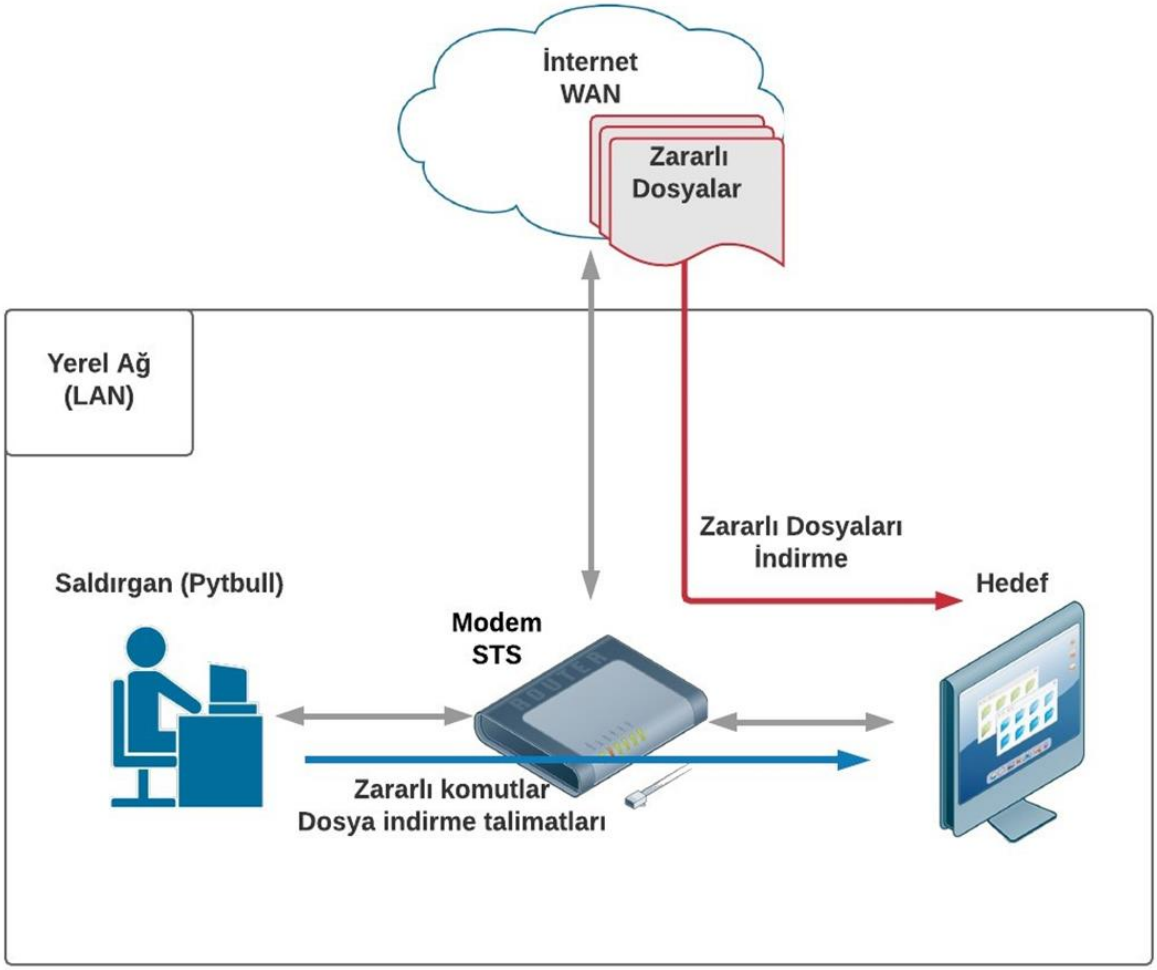
4.2. Geliştirme Metodu

Tüm geliştirme ve analiz süreçleri sanallaştırma yazılımları üzerinde cihazın donanımsal değerleriyle aynı ortam oluşturularak gerçekleştirilmiştir. Sızma testi araçları ve metodolojileri kullanılarak çözümün başarımı test edilmiştir. Geliştirilen uygulamanın kalite ve başarım değerlendirmesi benzer çalışmalardaki metriklere göre elde edilen değerlerle karşılaştırılarak değerlendirilmiştir.

4.2.1. Saldırı ve savunma tabanlı geliştirme metodolojisi

Çalışmamız kapsamında BTY çözümünü geliştirirken zararlı yazılım aktiviteleri analiz edilerek bu aktivitelere karşı saldırı tespit mekanizmaları geliştirilmiş ve saldırı tespit/önleme yazılımları ile bu zararlı aktiviteler durdurulmaya çalışılmıştır. Zararlı aktivitelerin gerçekleştiği sırada OPNSense güvenlik duvarı, Suricata'nın log kayıtları ve gözlem araçları olan Netflow, collectd uygulamaları üzerinden ağ trafiği analiz edilmiştir. Sızma testlerinde sıklıkla kullanılan Kali Linux birçok bilgi edinme, tarama yapma, saldırı gerçekleştirebilme ve benzeri yazılımı bünyesinde barındırmaktadır. Pytbull ve Fragrouter uygulamaları saldırı tespit/önleme sistemlerini test etmek amacıyla oluşturulmuş saldırı benzetim uygulamalarıdır.

Pytbull uygulamasının STS üzerinde testler gerçekleştirebilmesi ve STS algılama mekanizmasını test edebilmesi için istemci olarak farklı bir Linux makine üzerine; sunucu uygulaması olarakta STS'nin üzerinde ağ iletişimi kuran bir makineye kurulması gereklidir. STS'nin bulunduğu sunucudaki yazılımlar STS log kayıtlarını inceleyerek saldırı tespitinin başarımını ölçmektedir. Yapılan saldırı tiplerine karşılık sunucu tarafındaki Pytbull, Suricata STS loglarını okuyarak ilgili saldırıya karşılık log analizi yapmaktadır. İlgili log kayıtlarında yapılan saldırıya karşılık gelen bir log mevcut ise STS saldırıyı algılamış olarak işaretlenmektedir. Bir saldırı türüne karşılık log mevcut fakat saldırı türü tespit edilememişse kısmen tespit edilmiş olarak işaretlenmekte; bir log kaydı mevcut değilse ilgili saldırı başarılı olarak işaretlenmekte ve çıktı vermektedir. Bazı saldırı türleri için sunucu taraflı Pytbull'un internette bulunan farklı kaynaklardan zararlı kod içeren dosyalar indirmesi sağlanarak STS'nin başarım ölçümü yapılmaktadır. Pytbull uygulamasının saldırı gerçekleştirme ve log analizi ile saldırı tespitini algılama mekanizması Şekil 4.4'te gösterilmektedir.

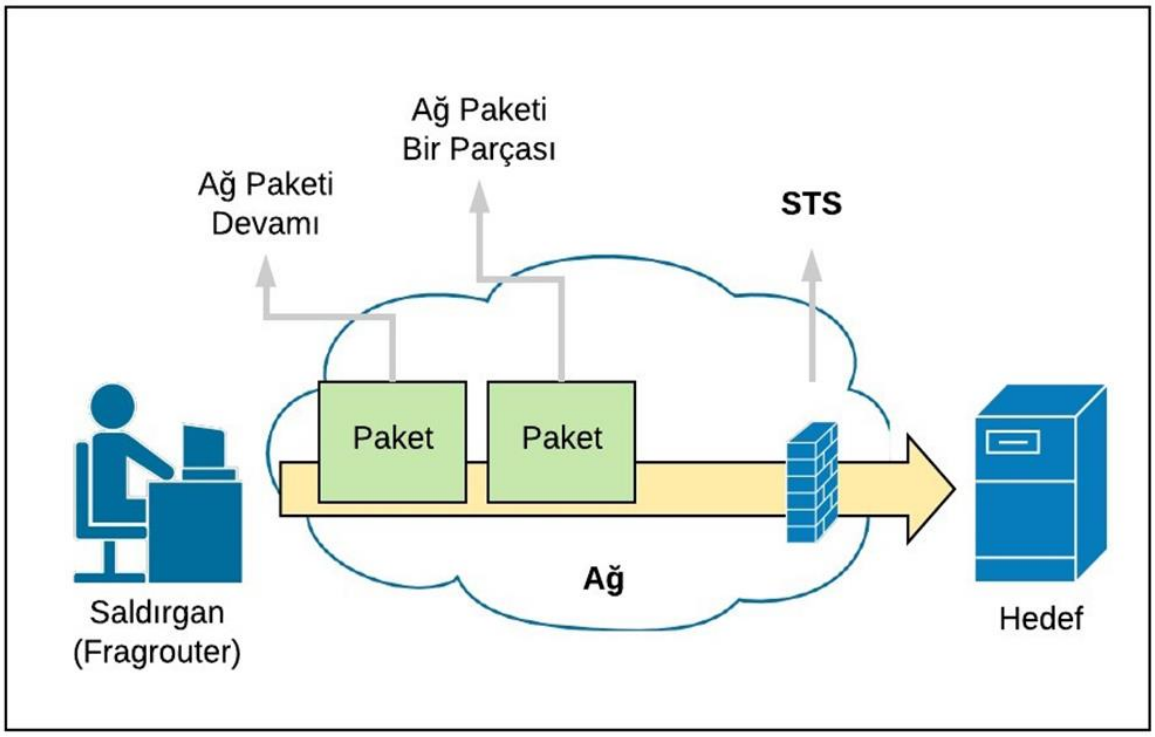


Şekil 4.4. Pytbull uygulamasının saldırı benzetiminde oluşturduğu trafik akışı şeması

Yapılan saldırı tiplerine karşılık sunucu tarafındaki Pytbull, Suricata STS loglarını okuyarak ilgili saldırıya karşılık log analizi yapmaktadır. İlgili log kayıtlarında yapılan saldırıya karşılık gelen bir log mevcut ise STS saldırıyı algılamış olarak işaretlenmektedir. Bir saldırı türüne karşılık log mevcut fakat saldırı türü tespit edilememişse kısmen tespit edilmiş olarak işaretlenmekte; bir log kaydı mevcut değilse ilgili saldırı başarılı olarak işaretlenmekte ve çıktı vermektedir. Bazı saldırı türleri için sunucu taraflı Pytbull'un internette bulunan farklı kaynaklardan zararlı kod içeren dosyalar indirmesi sağlanarak STS'nin başarım ölçümü yapılmaktadır.

Saldırı tespit sistemi üzerinde parçalara ayrılarak gönderilen paketlerin incelenmesi testleri için Fragrouter yazılımı kullanılmaktadır. STS üzerinde parçalanmış veri birleştirmesi gibi bir işlemin olmaması veya parça veriye dair bir imzanın olmaması bu tür saldırı yöntemini tespit edilemez hale getirmektedir. Saldırıları gizleme yöntemi genellikle STS arkasında bulunan, sürümü ve açıklığı tespit edilen yazılımların istismar edilmesi aşamasında

kullanılmaktadır. Zafiyeti tespit edilen sistemlere saldırıların tespit edilmemesi için saldırı kodları parçalar halinde iletilerek STS atlatılmış olunur. İstemci tarafından saldırı yapılmasına olanak sağlayan Fragrouter uygulamasının çalışma mekanizması Şekil 4.5'de gösterilmektedir.



Şekil 4.5. Fragrouter uygulamasıyla veriyi parçalar halinde paketlere bölme işlemi

Tez çalışması kapsamında geliştirilen BTY, Fragrouter uygulaması ile veriyi parçalara bölerek gönderme yöntemiyle [89] test edilerek sonuçları değerlendirilmiştir.

4.2.2. Paket analizi ile saldırı tespiti

TCP/IP, ağ cihazları arasındaki iletişimi sağlamak için geliştirilmiş bir protokoller takımıdır. TCP/IP kuralları sayesinde ağ iletişimi kurmak isteyen iki cihaz arasındaki iletişim en uygun ağ geçitleri üzerinden güvenilir bir şekilde sağlanır. TCP/IP gönderilecek verinin ağ paketleri adı verilen küçük parçalara bölünmesi ve doğru sırada birleştirilmesinden sorumludur. İletişim kuran cihazlar arasında ağ paketi kaybı yaşanması sonucunda kaybolan paket tespit edilerek TCP/IP tarafından kurtarılır ve veri kaybı olmaksızın iletişim sağlanır.

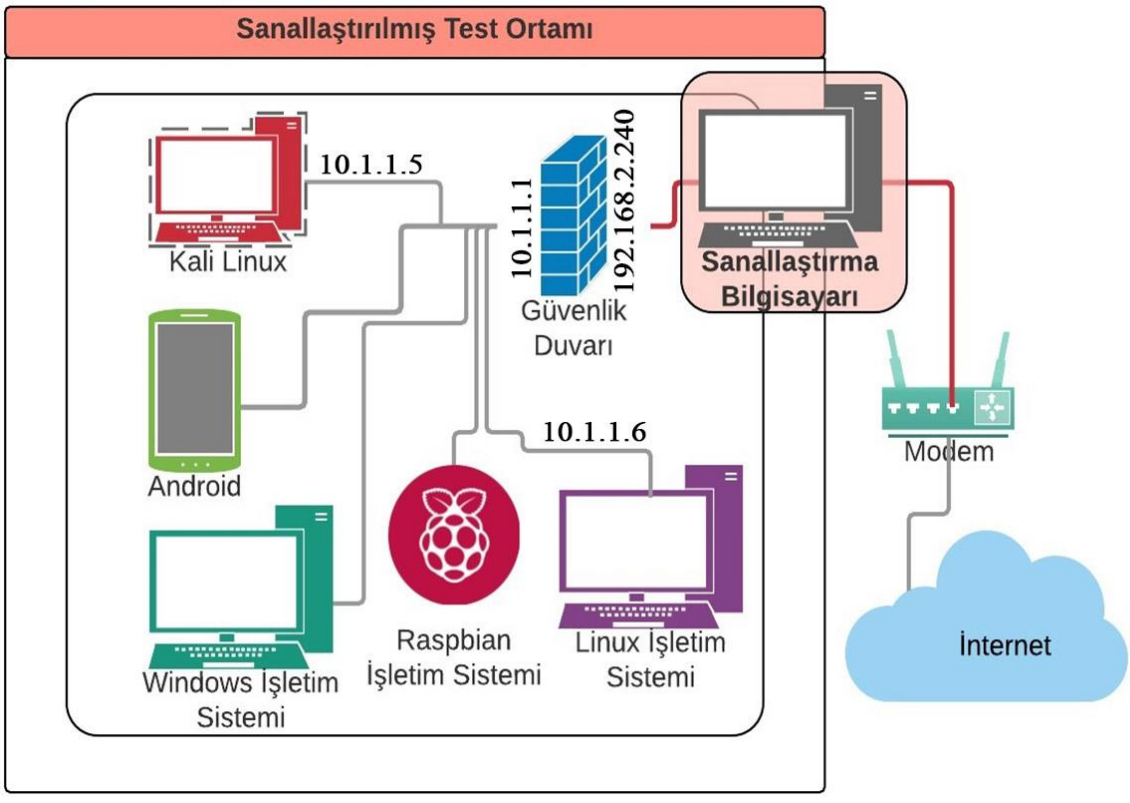
OPNSense, bünyesindeki Suricata ve paket filtreleme yapısı ile üzerinden geçen trafiği analiz edebilmektedir. Ağ cihazları tarafından kurulan bağlantıların durumunu bir durum tablosunda tutabilen OPNSense bağlantılar için kaynak ve hedefe göre filtreleme yapabilmektedir. Kaynak ve hedef IP adresi, kaynak ve hedef port numarası, protokol türü, paket boyutu, TCP paket bayrağı, paketteki veri boyutu gibi çeşitli ölçütlere göre filtreleme yapılabilmektedir. OPNSense ile birlikte çalışan Suricata sayesinde ağ paketleri üzerinde derin paket analizi yöntemleri uygulanabilmektedir. İletişim sırasında OPNSense üzerinden geçmekte olan her paket güvenlik duvarından geçmeden hemen önce paket analizi ile incelenmektedir. Suricata STS bünyesindeki "inline IPS" modu sayesinde anlık olarak trafik analizi yapabilmektedir [90]. Ağ paketleri içerisindeki verilerin incelenmesini sağlayan bu mod sayesinde ağ geçidi üzerinde saldırı önleme yöntemleri uygulanabilmektedir. Suricata'nın bu modu sayesinde ağ paketlerinin bir kopyasının alınarak trafik haritası oluşturulması yerine anlık analiz sonucu paketlerin geçmesi, yok sayılması veya engellenmesi işlemi uygulanabilmektedir.

5. DENEYSEL ÇALIŞMALAR

Bu bölümde yönlendirici özellikli güvenlik duvarı ve saldırı tespit sisteminin geliştirilmesi aşamaları açıklanmış ve yapılan testler ile çözümün başarısı ölçülmüştür.

5.1. Sanallaştırılmış Test ve Geliştirme Ortamı

Çalışma kapsamında tüm geliştirme ve test süreçleri sanallaştırma ortamı üzerinde gerçekleştirilmiştir. OPNSense BTY yazılımı ve Surricata STS kurulumları sanallaştırma ile bir orta katman oluşturacak şekilde kurulmuştur. Sanallaştırılan ortamda işletim sistemleri işlemci, hafıza, disk, internet erişim adresleri ve ağ bağlantısı gerçek ortamla aynı olacak şekilde ayarlanmıştır. Test benzetim anında en doğru performans sonuçlarını almak için tercih edilen donanım olan PcEngines'in ilgili modeli ile aynı değerlerde hafıza, işlemci ve disk değerleri BTY uygulamasının kullanımına atanmıştır. Sanallaştırılmış test ortamı Şekil 5.1'de gösterilmektedir.



Şekil 5.1. Sanallaştırılmış test ortamı

Geliştirme ve test aşamalarında Windows 10, Linux Debian 9, Android Emulator ve Raspbian işletim sistemleri kullanılmıştır. Kali Linux işletim sistemi saldırı testleri için kullanılmış olup; ağdaki diğer cihazlara, internetteki farklı adreslere ve OPNSense BTY üzerine doğru çeşitli saldırılar yapması sağlanarak saldırı tespit ve performans testleri ölçümü gerçekleştirilmiştir.

İnternet ve ağ trafiği kurulabilmesi için oluşturulan sanal ortam üzerindeki LAN ve WAN portları için sanal ağ ara yüzleri kullanılmıştır. Sanallaştırma ortamının internet erişimi, ev ağında bulunan fiziksel bir modem üzerinden köprü bağlantı kurularak gerçekleştirilmiştir. Sanallaştırma ortamında bulunan diğer işletim sistemleri tüm ağ trafiği erişimini OPNSense BTY üzerinden gerçekleştirmektedir. Bu sayede ağ trafiği üzerinde gerekli incelemeler ve analizler yapılabilmektedir.

LAN ve WAN sanal portları kullanılarak geliştirilen sistemde LAN iç ağı temsil etmekte WAN ise iç ağın internet ile iletişimi sağlayan port olarak kullanılmaktadır. İlgili portlar için sanal ağ ara yüzü ve IP adresi ataması yapılarak internet bağlantısı kurulması sağlanmaktadır.

5.1.1. Saldırı benzetimi senaryosu

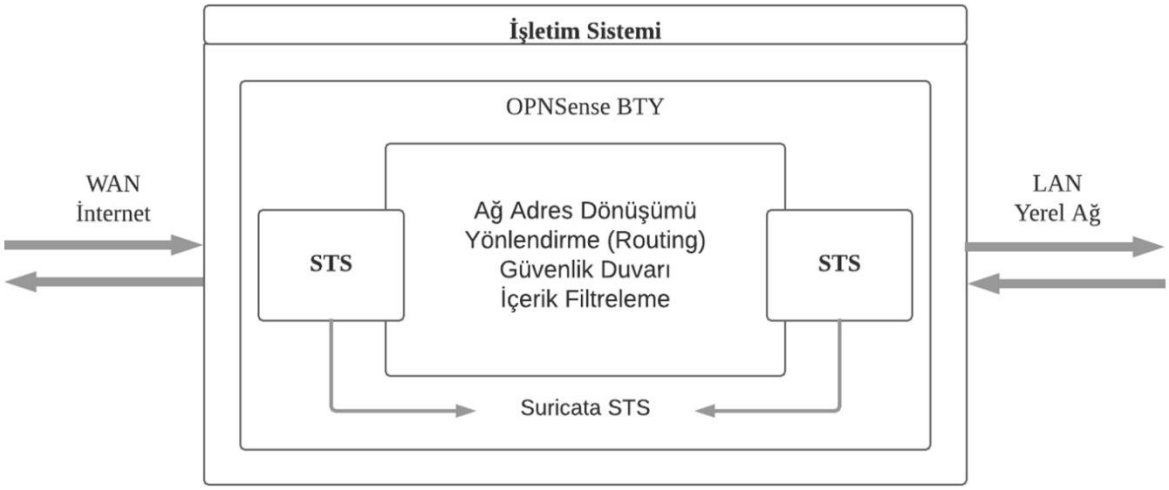
Sanallaştırılmış test ortamı üzerinde BTY tarafından DHCP (Dynamic Host Configuration Protocol) kullanılarak kurulan ağ bağlantısı sayesinde ortam üzerindeki tüm işletim sistemleri kendi aralarında ve internet ortamıyla bağlantı kurabilmektedir. Saldırgan olarak görev üstlenen Kali Linux işletim sistemi ağ üzerindeki BTY uygulamasına ve diğer işletim sistemlerine çeşitli saldırılar düzenleyerek bu cihazların saldırı tipine göre tepkisini ölçmektedir. Kali Linux üzerindeki Nmap, Nikto, ab, Pytbull, Fragrouter gibi araçlar ile çeşitli saldırı benzetimleri yapılarak ağ üzerindeki saldırı analizi gerçekleştirilerek ağın, güvenlik duvarının ve saldırı yapılan işletim sistemlerinin tepkileri ölçülmektedir.

Yerel ağ üzerinde konumlandırılan Kali Linux, ağ üzerindeki diğer cihazlara ve ağ geçidinde konumlandırılan BTY'ne karşı saldırılar düzenlemektedir. Çeşitli saldırı türleri uygulanan benzetimler sırasında trafiğin boyutu, paket sayısı ve saldırı algılama başarımı OPNSense BTY üzerindeki ağ işlemleri kısmından ölçülen değerler ile elde edilmiştir.

Birincil senaryo olarak yerel ağda konumlandırılan Kali Linux, Pytbull saldırı uygulaması ile aynı ağdaki farklı bir işletim sistemine saldırı benzetimi gerçekleştirmektedir. İkinci bir saldırı senaryosu olarak Pytbull uygulaması geçit modunda (gateway mode) OPNSense BTY doğrudan hedef gösterilerek saldırı benzetimi gerçekleştirilmiştir. Son senaryo olarak Kali Linux üzerindeki Fragrouter uygulaması STS atlatma tekniklerini aktif olarak uyguladığı sırada aynı işletim sistemi üzerindeki Pytbull uygulaması saldırıları yerel ağ üzerindeki farklı bir işletim sistemine hedef olarak gerçekleştirmektedir. Tüm saldırı benzetimleri sırasında ağ trafiği BTY üzerinden geçmesi nedeniyle OPNSense tarafından analiz edilmekte ve STS üzerinden geçirilmektedir. Bu sayede saldırılar tespit edilebilmekte ve trafiğe dair ölçümler sağlanabilmektedir.

5.2. Trafik Akışı ve Paket Analizi

OPNSense güvenlik yazılımı, bünyesinde barındırdığı ağ adres dönüştürücü ve güvenlik bileşenleri ile bir yönlendirici ve bütünleşik tehdit yönetimi yazılımı olarak kullanılabilmektedir. OPNSense yazılımının trafik akış ve işleme çalışma süreci Şekil 5.2'de gösterilmektedir.



Şekil 5.2. OPNSense ağ trafiği akış süreci ve güvenlik duvarı konumu

Yerel ağdaki bir cihaz internet üzerindeki herhangi bir ortam ile iletişim kurmak istediğinde ilk olarak yerel ağdaki ağ geçidine bağlantı talebini iletmektedir. Ağ geçidi üzerinde adres dönüşüm işlemi gerçekleştirilerek internet bağlantısı kurulması sağlanmaktadır.

NAT (Network Address Translation) adı verilen bu işlem ev, ofis ve IoT ağlarında modemler tarafından gerçekleştirilirken sanallaştırılmış test ortamında OPNSense tarafından gerçekleştirilmektedir. Bu sayede tüm LAN trafiğine ait ağ paketleri incelebilmektedir.

- em1 sanal ağ arayüz kartı: LAN (10.1.1.1/24),
- em0 sanal ağ arayüz kartı: WAN (192.168.2.240/24),
- Kali Linux IP adresi: 10.1.1.5,
- Saldırı hedefi: 10.1.1.6,
- LAN ağ geçidi 10.1.1.1 olacak şekilde ayarlanmıştır.

5.3. Ağ Geçidi Ayarları ve Güvenlik Duvarı Kuralları

LAN arayüzü için 10.1.1.1 ağ geçidi ve 10.1.1.1/24 IP adresi havuzu DHCP sunucusunda ayarlanmıştır. WAN ara yüzü için ağ geçidi 192.168.2.240 olarak atanmıştır. WAN ara yüzü için RFC (Request for Comments) 1918'de (10.0.0.0/8, 172.16.0.0/12) belirlenen ağlardan ulaşım engellenmiştir. Uygulamanın kendi üzerinden (loopback, 127.0.0.0/8) üzerinden erişimlerde engellenmiştir. VLAN, VPN ve HA modülü servisleri kullanımda olmayacağından pasifleştirilmiştir. Ağ trafik analizleri için OPNSense'in ağ trafiğini izleyebilen ve istatistikler çıkartabilen NetFlow modülü aktifleştirilmiştir. Collectd uygulaması aktifleştirilerek detaylı analizler çıkartılması sağlanmıştır.

İsim çözümleme işlemini ve önbelleklemesini yerine getiren Dnsmasq ve Unbound modülleri aktifleştirilerek DNS sorgularının yetkili sunucular üzerinde gerçekleştirilmesi sağlanmıştır. DNS sorgularını yetkili olmayan sunuculara gönderimini önlemek için LAN üzerinde 53 ve 853 portu üzerinde UDP (User Datagram Protocol) protokol sıkılaştırmaları yapılmıştır. Transparan vekil sunucu (transparent proxy) Squid ayarları gerçekleştirilerek site adresi temelli izleme, içerik filtreleme ve paket analizi yapılabilmesine olanak sağlanmıştır. Saldırı önleme özelliği aktifleştirilmiştir. Kullanıcıya herhangi bir uyarı verilmeyeceğinden zararlı bağlantılara dair kayıtlarının log dosyasına yazması ayarlanmıştır. İlgili log dosyalarının zamanla cihaz diskini doldurması öngörüsü ile otomatik eski logları temizleme mekanizması aktifleştirilmiştir. Web adresleri filtreleme özelliği aktifleştirilerek web site adres listeleri girişi yapılabilmesi sağlanmıştır.

SSL (Secure Sockets Layer) kara listeleme özelliği aktifleştirilerek SSL sertifikasının Sertifika Otoritesi (Certificate Authority) ve tespit edilen zararlı yayın yapan adreslerin SSL Sertifika parmak izine (fingerprinting) göre engelleme işlemi uygulanmıştır. Anti-virüs motoru aktifleştirilerek paket analizi yapılması ve virüs tespitine olanak sağlanmıştır. Anti-virüs motoru olarak ICAP ve Clamav kullanılmakta olup Symantec veri tabanı bağlantısı gerçekleştirilmiştir. Bir kısmı "ET Open/scan" kuralları arasında da olan Shodan, Nessus, ZoomEye, Censys gibi ağ tarama ve kaydetme veri tabanı servislerinin IP adresleri engellenmesi işlemi ve User-Agent bilgileri kara liste olarak sisteme girilmiştir. Açık kaynak olarak entegrasyonu sunulan çeşitli zararlı içeriklerin yayınını yapan [91] web site adreslerinin IP kaydı güvenlik duvarına eklenmiştir. İlgili kayıtlar arasından, kötücül yazılım dağıtımı yapan adresler ve sahte haber yayını yapan adresler listesi tercih edilmiştir. Spamhaus DROP ve EDROP sisteme eklenerek saldırıya uğramış veya zararlı yazılımların yayılımını yapan adreslerin bulunduğu liste güvenlik duvarına eklenmiştir. Donanımın çalışmasını aksatacak veya tamamen bozulmasını sağlayacak ayarlar BTY dokümantasyonunda sağlanan verilere göre ayarlanmıştır. Tunables (performans ayarları) tablosundaki sistem değerleri geliştirme yapılan cihazın özelliklerine göre ayarlanarak en iyi saldırı tespit ve engelleme başarımı sağlanması için ayarlanmıştır. Sanallaştırılmış test ortamında tüm donanım kontrol mekanizmaları kapalı durumdayken saldırı benzetimleri gerçekleştirilmiştir.

Gerçekleştirilen ayarlar ile OPNSense BTY uygulamasının ağ görevlerini yerine getirebilir ve saldırı tespit işlemlerini gerçekleştirebilir hale gelmesi sağlanmıştır.

5.4. Suricata Saldırı Tespit Sistemi Kuralları

Saldırı tespit ve önleme sistemi olan Suricata modülü için girilen kurallar ile güvenlik duvarının saldırılara karşı hızlı tespit yapabilme ve kurallara göre saldırıları önleme özelliği aktifleştirilmiştir. Snort kuralları ile uyumlu çalışan Suricata için kural listeleri çeşitli internet adreslerinden, Snort ve Suricata geliştiricilerinden temin edilmiştir. Bu listelere ek olarak güncel kural listeleri paylaşımı yapan adreslerin eklenti desteği aktifleştirilmiştir.

Gelişmiş bir kurallar listesi olan Emerging Threats firmasının kural listesinin periyodik güncellenebilir olarak sisteme entegrasyonu sağlanmıştır.

STS kuralları paylaşımı yapan abuse.ch entegrasyonu ile kredi kartı zararlı yazılımları yayan, toplayan adresler, truva atı ve türevi yazılım yayını yapan adresler, fidye yazılımı dağıtan adresler, SSL sertifikası istismar adresleri kara listesi, zararlı içerik paylaşımı yapan linklerin listesi STS kurallarına dahil edilmiştir. Doğrulama, dizine kaydetme, web sitesi tarama, eposta adresleri toplama gibi özellikleri bulunan çeşitli servislerin User-Agent bilgileri toplanarak sisteme eklenmiştir [92]. Bu uygulama ile yaklaşık 1,5 milyon zararlı adres ve 7 bin kadar User-Agent için kural girilerek bağlantı önleme işlemi gerçekleştirilmiştir.

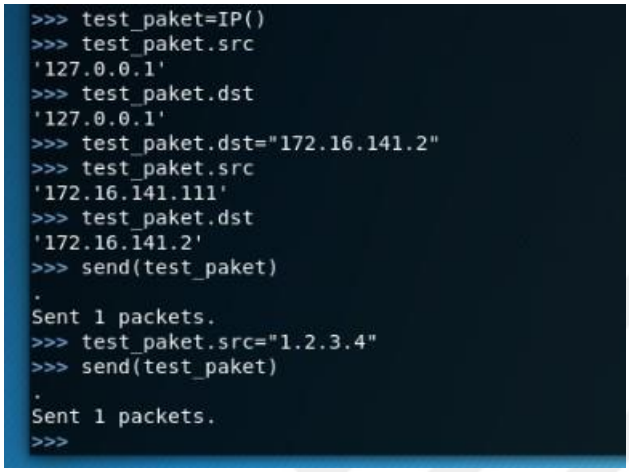
Suricata STS bünyesinde toplam 10725 kural aktif olarak kullanılmaktadır. Suricata tarafından aktif olarak kullanılmayan kural listeleri dosyaları disk üzerinden silinerek kaldırılmıştır. Pasif olmasına karşın Suricata listesinde yer alan kural listeleri Suricata tarafından okunmaktadır. Bu dosya okuma süreci dosyaların boyutuna göre Suricata uygulamasının başlangıç bellek hafıza değeri gereksinimini artırmaktadır. Bu nedenle kullanılmayan tüm kurallara ait dosyalar kaldırılmıştır. Bu sayede Suricata daha düşük bellek hafıza değerlerinde başlayabilmekte ve çalışabilmektedir.

5.5. Güvenlik Duvarı Kural Testleri

Yapılan testler ile LAN ve WAN ara yüzü IPv4 ve IPv6 internet bağlantıları başarı ile sağlanmıştır. WAN ara yüzüne seçilen bir LAN adresi üzerinden iletilen bağlantı isteği güvenlik duvarı tarafından kabul edilmemiş, bağlantı talebi başarılı bir şekilde iptal edilmiştir. Geliştirme aşamasında kullanılan SSH portu (22. port) test aşamasında kapatılarak test edilmiş, kuralların doğru bir şekilde işletildiği doğrulanmıştır. WAN ara yüzüne gelen bağlantı taleplerinin düşürülmesi başarılı bir şekilde gerçekleştirildiği gözlemlenmiştir.

DNS sorguları yapılarak testler gerçekleştirilmiştir. Hatalı DNS kayıtlarına dair sonuç dönmediği, farklı DNS sunucuları yetkiliymiş gibi gönderilen isteklerin uygulama üzerindeki Unbound çözümü tarafından cevap verildiği yetkili olmayan adreslere bir isteğin yapılmadığı gözlemlenmiştir. Vekil sunucu ayarlarının test edilebilmesi için internet trafiği gözlemlenmiş ağ geçidine bağlı diğer işletim sistemleri üzerinde HTTP ve HTTPS trafiği testleri ile web bağlantısı erişim testleri gerçekleştirilmiştir.

Kali Linux üzerinde bulunan Scapy ve UTscapy uygulamaları ile gerçekleştirilen ağ saldırıları ile güvenlik duvarı test edilmiştir. ARP sahteciliği ve IP sahteciliği saldırılarında güvenlik duvarının başarıyla saldırıları önlediği görülmüştür. Geçerli bir IP paketi ve sahte kaynak adrese (1.2.3.4) sahip bir IP paketinin oluşturulma ve gönderilme aşamaları Resim 5.1'de gösterilmektedir.



Resim 5.1. Scapy uygulaması ile paket oluşturma ve gönderme işlemleri

Scapy uygulaması ile istenilen özelliklerde oluşturulan paketler ile hedef sistemlerde testler gerçekleştirilmiştir. Oluşturulan test_paket isimli IP paketine ilk olarak ağ geçidi IP adresi hedef olarak ve Scapy uygulamasının kurulu olduğu işletim sisteminin IP adresi kaynak olarak eklenerek paket gönderimi sağlanmıştır. İkinci senaryo olarak kaynak adres farklı bir sisteme ait sahte bir IP adresi olan 1.2.3.4 ile değiştirilerek ağ geçidine gönderilmiştir. Güvenlik duvarının paketin geldiği kaynak ve paket başlığındaki bilgilerin uyuşmaması nedeniyle paketi yok saydığı görülmüştür.

Nmap uygulaması ile ağ taraması gerçekleştirilmeye çalışılmıştır. Güvenlik duvarı üzerinde Nmap ağ tarama trafik analizine göre oluşturulmuş kurallar Nmap'in tarama yapabilmesini önlemiştir. Kullanılan Nmap komutları:

- nmap -sS -p- 10.1.1.1
- nmap -sU -p- 10.1.1.1

İlk komut ile SYN tarama (-sS) işlemi ve varsayılan değerin aksine taranabilecek tüm portların taranması (-p-) komutu hedef ağ geçidi (10.1.1.1) için uygulanmıştır.

İkinci komut ile UDP taraması ve tüm portların taranması işlemi gerçekleştirilmiştir.

5.6. Saldırı Testleri

Geliştirilen bütünleşik tehdit yönetimi uygulamasının güncel saldırılara karşı tepkisi ve başarısı ölçülmüştür. Nmap ve Scapy uygulaması ile güvenlik duvarı kuralları, Pytbull ve Fragrouter ile Suricata STS kuralları kapsamlı bir şekilde test edilmiştir.

Sunucu tarafında 34567 portunda çalıştırılan Pytbull'a istemci tarafından Pytbull uygulaması kurulu sunucunun IP adresi belirterek bağlantı kurulmaktadır. Sunucu tarafından yer alan Pytbull dinleme modunda bağlantı beklemektedir. İstemcinin sunucu tarafıyla iletişime geçmesi ile Pytbull bünyesindeki saldırılar sırasıyla işletilmektedir.

Sunucu (hedef) komutu: ./pytbull-server.py -p 34567
İstemci (saldırgan) komutu: ./pytbull -c config/config.cfg -t 10.1.1.6

Pytbull uygulaması ile yapılan STS saldırıları ve açıklamaları Çizelge 5.1'de gösterilmektedir.

Çizelge 5.1. Pytbull uygulamasındaki saldırı türleri ve açıklamaları

Saldırı Türü	Açıklaması
Bad Traffic	İnternet protokollerinin standartlarına uymayan, farklı boyutlarda paket gönderilmesi ile tepkinin ölçülmesi
Brute Force	Başta dosya transfer protokolü olmak üzere çeşitli protokoller üzerinde kaba kuvvet saldırıları gerçekleştirerek parola tespit edilmeye çalışılması
Client Side Attacks	Sunucu tarafında çalıştırılan bir uygulamaya gönderilen komutlar neticesinde zararlı dosya trafiği oluşturarak STS mekanizmasının ölçülmesi
Evasion Techniques	STS atlatma yöntemlerinin uygulanarak algılama mekanizmasını yanıltarak veri aktarımı gerçekleştirilmesi
Fragmented Packets	Parçalı veri gönderimi yöntemiyle hedefte paket birleştirmesi yaparak algılama mekanizması üzerinde verilerin algılanmasının önlenmesi
DDoS	Yoğun paket gönderimi yaparak hedef veya aracı uygulamaların yanıt verebilmesinin önlenmesi, hizmet dışı bırakma saldırıları

Pytbull uygulaması STS sistemlerinin çeşitli konumlarda kullanılan çeşitlerine düşünülerek geliştirmesi sayesinde birçok protokolde çeşitli türlerde saldırı benzetimi yapabilmektedir. Pytbull bu saldırıları gerçekleştirirken Nmap, Nikto, ab, Scapy ve Hping3 gibi uygulamalardan faydalanmaktadır.

Fragrouter uygulaması kullanılarak STS atlatma tekniklerinden olan verileri parçalı olarak gönderme yöntemi uygulanarak saldırı benzetimi yapılmıştır. Bu sayede STS uygulamasının gelişmiş saldırılara karşı tepkisi ölçülmüştür. Fragrouter'un bünyesinde bulunan 22 farklı yöntem çeşitli saldırılar ile birlikte sıralı olarak uygulanmıştır.

Elde Edilen İstatistikler

Pytbull uygulaması ile yapılan testler sonucu ağ taramaya ve harita çıkartmaya yönelik tüm testlerin başarıyla tespit edildiği görülmüştür. Benzer bir şekilde Pytbull bileşenlerinden olan hping3 tarafından üretilen saldırılar STS tarafından tespit edilmiş ve önlenmiştir. Hizmet dışı bırakma saldırılarının istemci tarafında yoğun sistem kaynakları kullanımı gerçekleştirdiği fakat yüksek bant genişliğine ulaşmadan tespit edilerek önlendiği görülmüştür. Nmap uygulaması ile gerçekleştirilen ağ tarama testlerinde OPNSense BTY uygulamasının %100 oranında tarama aktivitesini yakaladığı ve önlediği görülmüştür.

Saldırı benzetimi sırasında iletilen trafiğin %97,85'i Pytbull uygulamasının kurulu olduğu istemci tarafından üretilmiş ve ağa gönderilmiştir. Pytbull'un uyguladığı 300 farklı saldırı benzetimi sırasında Suricata STS tarafından 2418 paket şüpheli olarak işaretlenmiş ve saldırı tespit uyarısı olarak log kaydında görülmüştür. Bu log kayıtları ağ paketlerinden zararlı olanların imzalarının tespiti sonucu oluşturulmuştur. Yapılan her bir saldırı için çeşitli sayılarda paketler oluşturulmaktadır. Sadece zararlı kod içeren veya zararlı olduğu Suricata STS tarafından algılanan paketler için log kaydı oluşturulmuştur. Çeşitli saldırı tipleri için saldırının türü ve eğer veri tabanında mevcutsa saldırının bilinen ismi STS log kayıtlarında görülmektedir. Birtakım saldırılar için ise sadece zararlı olduğu tespit edilen paketler log kaydına düşmektedir.

Pytbull tarafından oluşturulan ağ trafiğine yönelik LAN ve WAN ağ ara yüzlerindeki istatistikler Çizelge 5.2'de gösterilmektedir.

Çizelge 5.2. Pytbull saldırıları sırasında ağ trafiğindeki paket sayısı ve toplam boyut

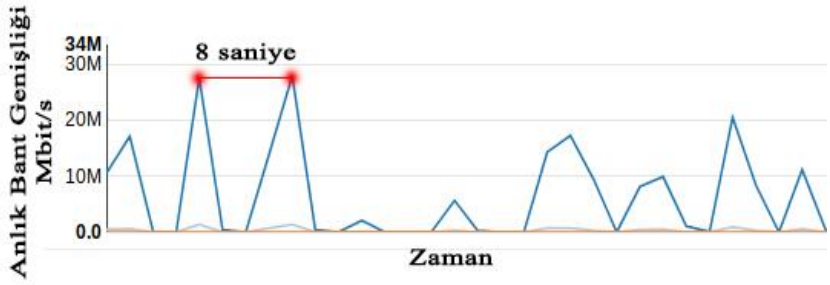
	Paket Sayısı		Toplam Boyut	
	Gelen	Giden	Gelen	Giden
Paket değerleri	1 383 338	3 860 819	84,56 MB	4,20 GB
Başarılı aktarım	1 373 598	3 860 819	84,14 MB	4,20 GB

Yapılan saldırılar LAN üzerinde beş milyon üzerinde paket oluşumuna ve 4,5 GB boyutunda trafik oluşumuna sebep olmuştur. Paket sayısının yüksek sayıda olması özellikle hizmet dışı bırakma saldırılarında ağı meşgul etmek ve ağdaki güvenlik mekanizmasının sınırlarını zorlamak için üretilmektedir. İlgili zararlı trafiğin üretildiği ve BTY tarafından işlendiği zaman aralığına ait sistem kaynakları kullanma değerleri bir sonraki bölümde yer almaktadır. Hizmet dışı bırakma saldırıları anında BTY tarafından sorunsuz hizmet sağlanırken zararlı paketlerin algılanarak ağ trafiğinin dengelenmeye çalışıldığı görülmüştür. Normal ağ trafiğinin dışında TCP/IP iletişimi için gerekli paketlerin sırasız, başlık bilgileri hatalı veya eksik, kaynağı veya hedefi geçersiz adreslerden oluşan paketlerin BTY üzerine gönderilerek algılama mekanizması test edilmiştir. Hatalı ve zararlı paketlerin tespit edilebilen aktivitesi BTY tarafından Çizelge 5.3'deki gibi ölçülmüştür.

Çizelge 5.3. BTY tarafından önlenen ağ paketleri sayısı

	Paket Sayısı	
Paket Trafik Yönü	LAN	WAN
Gelen	438 640	380 261
Giden	0	38

WAN giden paket sayısı testler sırasında gerçekleştirilen DNS sorguları ve BTY'nin kendisi tarafından kurulan sistem güncellemesi, işletim sisteminin sorguları gibi çeşitli süreçler tarafından oluşturulmaktadır. Bu paketlerden zararlı olduğu tespit edilenler engellenmiştir. Pytbull uygulamasının oluşturduğu trafik kapasitesi en yüksek değeri gelen trafik için toplamda (LAN ve WAN) 55 Mbit/s ve giden trafik için 56 Mbit/s olarak kaydedilmiştir. Pytbull uygulaması tarafından oluşturulan çeşitli saldırıların OPNSense BTY tarafında her sekiz saniyede bir log kaydı oluşturabildiği kaydedilmiş ve Şekil 5.3'de gösterilmiştir.

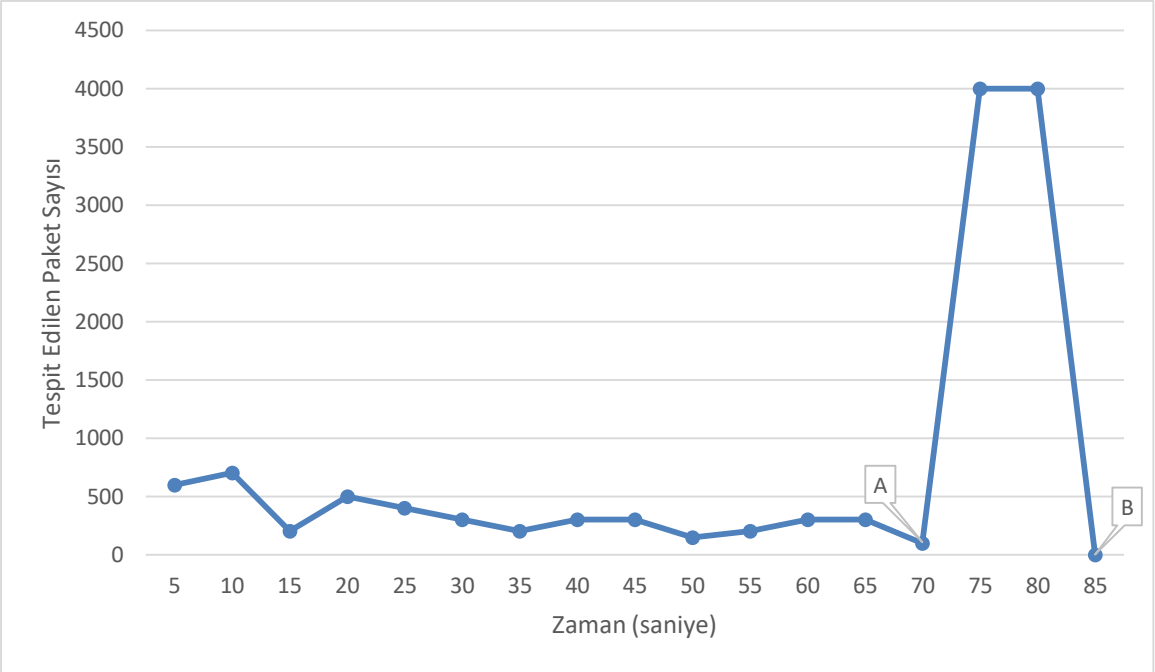


Şekil 5.3. BTY log kaydı oluşturma grafiği

OPNSense BTY log kayıtlarında Pytbull uygulamasının çeşitli saldırılarda yeterince hızlı saldırı üretemediği görülmüştür. Şekil 5.3'te iki farklı log kaydı oluşturulması arasında geçen süre gösterilmiştir. Ortalama olarak 8 saniyede bir log kaydı üretildiği görülmüştür. Suricata'nın hızlı algılama mekanizması sayesinde tespit ettiği zararlı için log kaydını hızlıca kaydedebildiği ve sonraki paket analizleri için hızlıca hazır konuma geldiği görülmüştür.

Yapılan testlerin STS atlatma teknikleri uygulandığı analiz çalışmasında 15 farklı saldırı türünden 12 tanesi tespit edilerek %80 başarı elde edilmiştir. Toplam 352 247 paket gönderimi gerçekleşen testler sırasında en yoğun trafiğin hizmet dışı bırakma saldırısı testleri sırasında üretildiği tespit edilmiştir.

Pytbull üzerinde bulunan STS atlatma ve ağ tarama uygulamalarından Ncrack, Nmap ve Nikto uygulamalarının testler gerçekleştiği sırada ağda ölçülen paket sayısı Şekil 5.4'deki gibi olduğu görülmüştür. Tespit edilen paket sayısı, BTY uygulaması tarafından LAN üzerinden gelen toplam paket sayısı değerinden alınmıştır. %97,85'i saldırı üreten istemci tarafından oluşturulan paketlerin ağ üzerindeki ölçümü için BTY bileşenlerinden Netflow ve collectd uygulamalarında faydalanılmıştır. Şekil 5.4'deki A anına kadar; ab ve hping3 ile gerçekleştirilen testler tarafından oluşturulan trafik A ve B noktaları aralığındaki kısım olarak kaydedilmiştir. A ve B noktaları arasında hizmet dışı bırakma saldırıları gerçekleştirilmiştir. Bu nedenle ağdaki en yoğun paket trafiğin bu aralıkta oluşturulduğu gözlemlenmiştir.



Şekil 5.4. Pytbull saldırıları sırasında OPNSense BTY üzerindeki paket sayısı

Her beş saniyede bir toplam paket sayısına göre ölçüm yapılan testler sırasında 75. ve 85. ölçüm aralıklarında ab ve Hping3 tarafından hizmet dışı bırakma saldırıları uygulanarak testler gerçekleştirilmiştir. Bu uygulamaların testler gerçekleştirdiği an ağdaki en yoğun paket trafiği olduğu zaman aralığı olarak kaydedilmiştir. Bu aralıktaki paket trafiği STS atlama teknikleri uygulanarak gerçekleştiren diğer saldırılara göre altı/yedi kat daha fazla paket oluşturduğu tespit edilmiştir.

Fragrouter uygulaması ile STS atlatma teknikleri uygulanarak Suricata'nın saldırı tespit algoritması için saldırı benzetimi gerçekleştirilmiştir. Pytbull uygulaması yardımıyla uygulanan yöntemlerde Fragrouter saldırılarının büyük bir çoğunluğu Suricata tarafından tespit edilmiştir.

Pytbull uygulaması ile yapılan saldırılar sonucunda toplamda 2987 satır güvenlik duvarı log kaydı oluşturulmuştur. 2878 pakete bloklama yapılırken 109 paketin güvenlik duvarından geçmesine izin verildiği görülmüştür. Oluşturulan zararlı paketlerin %96 oranında engellenebildiği ölçülmüştür.

Fragrouter uygulaması yardımıyla gerçekleştirilen saldırılar toplamda 3025 satır güvenlik duvarı log kaydı oluşturmuştur.

Fragrouter uygulamasıyla iletilen ağ paketlerinin bloklanan, izin verilen ve toplam değerleri Çizelge 5.4'te gösterilmektedir.

Çizelge 5.4. Fragrouter uygulaması ile saldırı benzetimi log kayıt istatistikleri

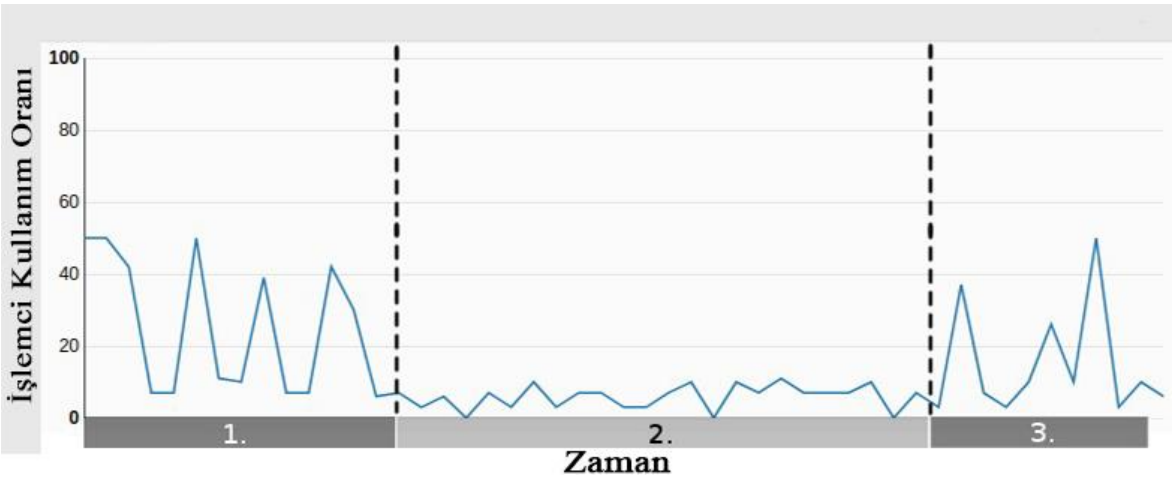
	Bloklanan	İzin Verilen	Toplam	Başarılı (%)
Log Kaydı	2941	84	3025	97

Fragrouter ile yapılan saldırıların sonucunda saldırıların %97'sinin tespit edilerek önlenebildiği görülmüştür.

5.7. Kapasite ve Performans Testleri

Geliştirilen güvenlik çözümünün sanallaştırılmış test ortamında çalıştırılması sonucunda elde edilen kaynak tüketim değerleri ölçülerek değerlendirilmiştir [93]. Çözümün aktif olarak çalıştığı sırada ve yük testleri gerçekleştirilerek yapılan testler ile performans değerleri ölçülmüştür. Güvenlik duvarı çözümünün başlangıç anında, atıl durumda ve bir takım testler gerçekleştirildiği sırada elde edilen işlemci kullanım oranları Çizelge 5.5'de gösterilmektedir.

Çizelge 5.5. Güvenlik duvarı işlemci kullanımı grafiği



Çizelge 5.5'te 1. kısımda görülen değerler güvenlik duvarının çalışmaya başladığı anda; 2. kısımda elde edilen görülen değerler güvenlik duvarının atıl olarak bekleme durumunda ve

3. kısımda elde edilen değerler ise çeşitli yük testi uygulamasıyla yüksek sayıda paketin oluşturulduğu anda BTY tarafından kaydedilmiştir.

Yapılan farklı bir diğer yük testi ile güvenlik duvarının atıl olarak bulunduğu andaki değerler ile aktif olarak çalıştığı ve ağır yük testi sırasında elde edilen bellek hafızası, işlemci ve OPNSense durum tablosu değerleri karşılaştırılarak değerlendirilmiştir. Güvenlik çözümünün atıl durumdayken tükettiği kaynak değerleri Çizelge 5.6'da gösterilmektedir.

Çizelge 5.6. BTY çözümünün atıl durumundayken kaynak kullanım değerleri

Bileşen	Değerler
İşlemci (1, 5, 15 dakika ortalaması)	0,32, 0,25, 0,19
Bellek Hafızası (RAM)	573/988 MB
Durum Tablosu	%0 (8/98 000)

Çizelge 5.6'da yer alan değerlerin elde edildiği anda oluşturulan ağda bir trafik yer almamaktadır. Ağdaki diğer işletim sistemlerinin atıl bulunduğu konumda ağda sadece işletim sistemlerinin güncelleme kontrolü ve ağ iletişimi kurulması için gerekli protokollerin paketleri ağ üzerinde bulunmaktadır. Güvenlik çözümünün test ortamındaki işletim sistemlerinin normal internet trafiği gerçekleştirdiği sırada tükettiği kaynak değerleri Çizelge 5.7'de gösterilmektedir.

Çizelge 5.7. Güvenlik çözümünün ağ trafiğini izlediği anda kaydedilen değerler

Bileşen	Değerler
İşlemci (1, 5, 15 dakika ortalaması)	0,46, 0,43, 0,42
Bellek Hafızası	608/988 MB
Durum Tablosu	%0 (15/98 000)

Çizelge 5.7'de gösterilen değerlerin elde edildiği sırada ağda yer alan diğer işletim sistemleri tarayıcı trafiği ve ping paketleri göndererek çeşitli ağ paketleri üretmektedir. BTY'nin diğer işletim sistemleri üzerinden internet üzerindeki farklı bir ortama karşı yük testi gerçekleştirdikleri sırada ölçümlediği kaynak tüketimi değerleri Çizelge 5.8'de

gösterilmektedir. İnternet ortamına yük testi sırasında ab ve Hping3 uygulamaları kullanılmıştır.

Çizelge 5.8. Ağ güvenlik çözümü üzerinde yük testi yapıldığı andaki değerler

Bileşen	Değerler
İşlemci (1, 5, 15 dakika ortalaması)	0,63, 0,61, 0,60
Bellek Hafızası	843/988 MB
Durum Tablosu	%6 (6516/98 000)

Sistem üzerindeki yük testlerinde en yüksek hafıza kullanımının anti-virüs motoru ICAP'ın yeniden başlatılması aşamasında toplam 800 MB ve Squid vekil sunucusunun aktif olarak çalıştığı sırada toplamda 840 MB kullanım ile gerçekleştiği gözlemlenmiştir. En yüksek işlemci kullanımının ise işlemcinin %63 oranında kullanıldığı tespit edilen saldırı tespit ve önleme yazılımı Suricata'nın kural listelerini güncelleme aşamasında gerçekleştiği görülmüştür. Durum tablosu değerleri güvenlik duvarı tarafından kullanılan bir tablo olarak kurulan bağlantıların durumunu takip etmekte için tutulmaktadır. OPNSense tarafından varsayılan olarak atanan bu tablo boyutu tez çalışması kapsamında yer almadığından değerlendirilmemiş; gelecek çalışmalara ışık tutması için Çizelge 5.6, 5.7 ve 5.8'de paylaşılmıştır.

Yapılan çeşitli testler sırasında kaydedilen işlemci kullanım oranları Çizelge 5.9'da gösterilmektedir.

Çizelge 5.9. Güvenlik duvarı işlemci kullanım oranları karşılaştırması

	İşlemci Kullanım Oranları (%)		
	Son 1 dakika	Son 5 dakika	Son 15 dakika
Trafiksiz	32	25	19
Normal Trafik	46	43	42
Yoğun Trafik	63	61	60

Toplamda tahsis edilen 1 GB (1024 MB) hafızanın 988 MB'lık kısmı uygulama tarafından kullanılabilmektedir. Bellek hafıza kullanım değerleri ölçülen uygulamanın %85 ile yük testi anında en yüksek değere ulaştığı kaydedilmiştir. Uygulamanın tek başına çalıştığı an trafiksiz, diğer işletim sistemlerinin normal internet erişimi kurduğu an normal trafik ve ağır yük testleri yapıldığı yoğun trafik anında ölçülen değerler Çizelge 5.10'da gösterilmektedir.

Çizelge 5.10. Güvenlik duvarı RAM hafıza kullanım değerleri

Test Anı	Bellek Hafıza Kullanımı (MB)
Trafiksiz	573
Normal Trafik	608
Yoğun Trafik	843

Yapılan testler ile güvenlik duvarı çözümünün bellek hafıza kullanım değerlerinin tercih edilen sistem özelliklerini aşmadığı tespit edilmiştir. Gerçekleştirilen saldırı testleri sonucunda elde edilen paket ve boyut istatistikleri Çizelge 5.11'daki gibidir.

Çizelge 5.11. Saldırı benzetimi sonucu toplam gönderilen ve alınan ağ trafik değerleri

	Gelen	Giden	Toplam
Paket Sayısı	2 180 000	242 000	2 422 000
Boyut	2,18 GB	230,12 MB	2,40 GB

Gerçekleştirilen saldırı testlerinde daha önceki çalışmalara göre daha yüksek ağ trafiği oluşturulan saldırılar gerçekleştirilmiştir [84]. Yük testi harici tüm saldırı benzetim senaryolarında daha yüksek sayıda ağ paketi ve daha yüksek bant genişliğinde trafik ağda üretilerek testler gerçekleştirilmiştir.

Geliştirilen BTY çözümünde kullanılan Suricata STS uygulamasını test etmek için Pytbull kullanılan bir çalışmada [84] yüksek sistem kaynakları ve yüksek sayıda STS kuralı kullanıldığı görülmüştür. 2013 yılında gerçekleştirilen çalışmada Pytbull dışında farklı test araçları da kullanılmıştır. Özellikle yüksek bant genişliğindeki ağlarda hizmet dışı bırakma saldırıların benzetimi için gerçekleştirilen bu hizmet dışı bırakma saldırıları bu tez

çalışmasında kullanılmamıştır. Bu nedenle sistem kaynakları 2013 yılındaki çalışmaya göre çok daha düşüktür. İlgili çalışmada Suricata 1.2 sürümü kullanılmakta olup testlerin gerçekleştirildiği ortam fiziksel bir sunucudur. Bu tez çalışmasında ve 2013 yılında Pytbull aracı kullanarak gerçekleştirilen STS testlerinde kullanılan sistem bilgileri Çizelge 5.12'deki gibidir.

Çizelge 5.12. BTY'de ve daha önceki çalışmada kullanılan sistem kaynakları

Sistem Kaynakları	2013 Çalışması [84]	Tez Çalışması
İşlemci	2 x 12 core, 2.4 GHz	2 core, 2.6 GHz
Bellek Hafıza	8 x 8 GB RAM	2 GB RAM
Disk	6 x 2 TB disk	20 GB disk
Ortam	Fiziksel ortam	Sanal ortam

2013 yılında gerçekleştirilen çalışmada işlemci olarak yaklaşık 11 kat daha güçlü işlemci ve 32 kat daha büyük kapasitede bellek hafızası kullanıldığı kaydedilmiştir. Disk kapasitesi ilgili çalışmadaki Pytbull uygulaması dışında kullanılan testler nedeniyle yüksek tutulmuştur. Bu tez çalışmasında disk kapasitesi yönünden bu yönde bir ihtiyaç bulunmamaktadır. İlgili çalışmada fiziksel bir sunucu olarak tüm sistem kaynaklarının STS tarafından kullanılacak şekilde ayarlandığı bir ortam mevcuttur. Bu tez çalışmasında geliştirme ve test ortamı sanallaştırma üzerinde çalışmaktadır. Fiziksel ortamın sanallaştırma ortamına göre daha iyi kaynak kullanması nedeniyle daha performanslı çalışması ve daha iyi ölçüm oranları sunmasına karşın sanallaştırmadan kaynaklanan performans kaybı değerlendirmelerde göz ardı edilmiştir.

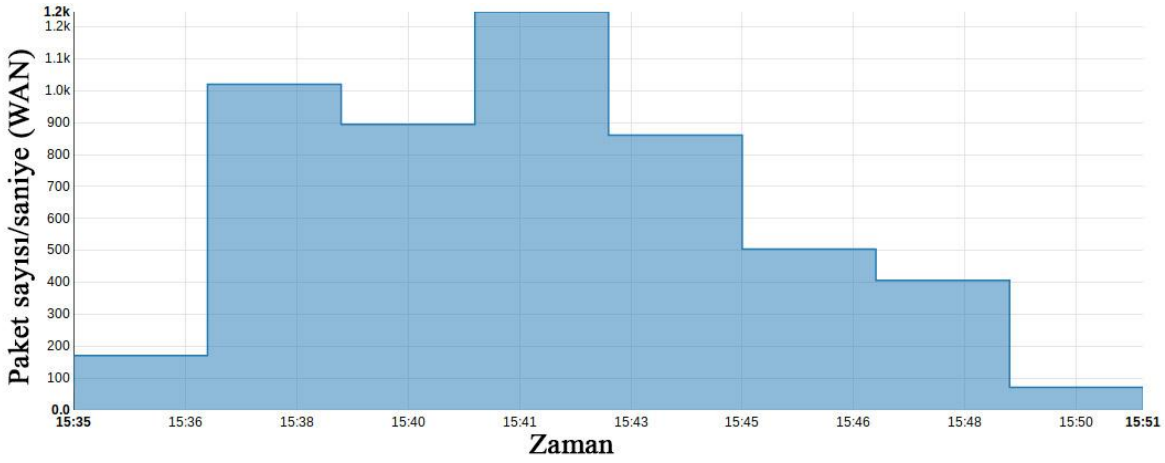
2013 yılında gerçekleştirilen çalışmada STS'de açık kaynak ve ücretli STS kural setleri kullanılmıştır. Tez çalışması kapsamında yer alan tüm kural setleri açık kaynak olup internet üzerinden ulaşılabilmektedir. ET/Open kural listesi OPNSense ile birlikte dağıtılmaktadır. Positive Research kural seti özellikle istemci taraflı saldırılarda zararlı dosya tespitinde kullanılan güncel bir kural seti olarak internette indirilerek kolaylıkla kurulabilmektedir. Bu tez çalışmasında ve ilgili çalışmada kullanılan kural setleri ve toplam sayılarında dair bilgiler Çizelge 5.13'de gösterilmektedir.

Çizelge 5.13. Suricata STS ve daha önceki çalışmada kullanılan kural sayıları

Kural Seti	2013 Çalışması [84]	Tez Çalışması
ET/Open	16 179	10 401
ET/Pro	13 154	-
Snort VRT	18 038	-
Positive Research (PT)	-	324
Toplam	47 371	10 725

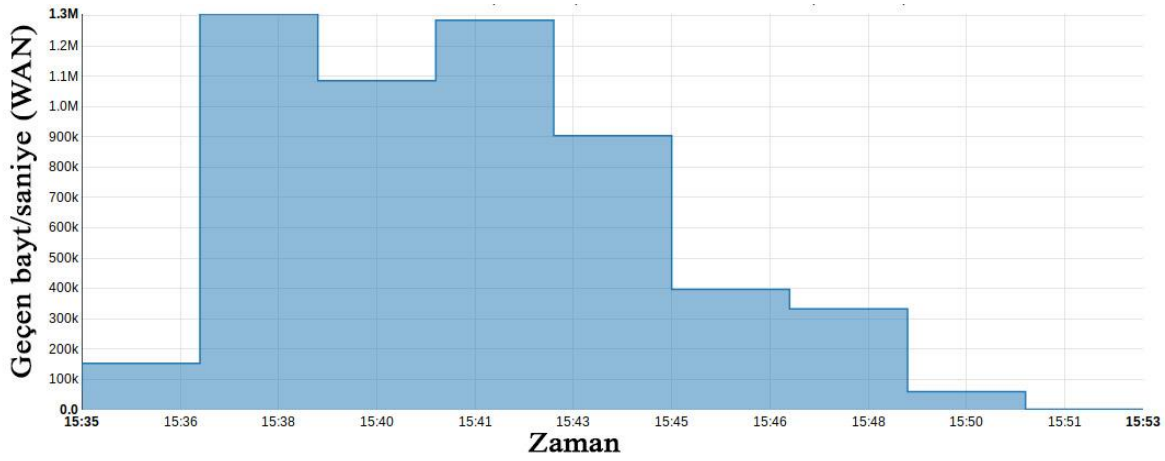
İlgili çalışmada kullanılan Suricata STS toplam kural sayısı bu tez çalışmasındaki toplam kural sayısından yaklaşık 4,4 kat fazladır.

Tez çalışması kapsamında Pytbull üzerindeki çeşitli saldırıların benzetimi gerçekleştirilmiştir. Pytbull uygulaması ile gerçekleştirilen STS testleri sonucunda oluşturulan ağ paketleri ve boyutları ölçüm değerleri 2013 yılında yapılan çalışma [84] karşılaştırılmıştır. Pytbull tarafından gerçekleştirilen istemci taraflı saldırıların (Client Side Attacks) WAN ara yüzü üzerinde zararlı dosya indirerek oluşturduğu trafiğin değişimi Şekil 5.5'de gösterilmektedir.



Şekil 5.5. İstemci taraflı saldırıların oluşturduğu paket sayısı/zaman dağılımı

WAN ara yüzü üzerinden indirilen zararlı dosyaların oluşturduğu ağ trafiği paket boyutunun zamana göre değişimi Şekil 5.6'da gösterilmektedir.



Şekil 5.6. İstemci taraflı saldırıların oluşturduğu paket boyutu/zaman dağılımı

Pytbull'un sunucu tarafındaki uygulaması internette bir adreste yer alan zararlı dosyaları STS üzerinden sırasıyla indirmeye çalışarak geçen dosyaların STS tarafından zararlı olarak algılanıp algılanmadığını test etmiştir. İstemci taraflı saldırılar sonrasında WAN üzerinden toplamda 33,2 MB dosya geçişi ölçülmüştür.

Pytbull kullanılarak gerçekleştirilen saldırı testleri sonucu elde edilen değerler 2013 yılındaki benzer çalışma ile karşılaştırılmıştır. İlgili çalışmadaki ve tez kapsamında yapılan saldırılar sonucunda ağ üzerinde oluşan paket sayısı ve paket boyutu değerleri Çizelge 5.14'te gösterilmektedir.

Çizelge 5.14. Pytbull saldırı testleri ile oluşan ağ trafik değerleri ve karşılaştırması

	Paket Sayısı (Adet)		Geçen Paketleri Boyutu (MB)	
Saldırı Türü	2013 Çalışması	Tez Çalışması	2013 Çalışması	Tez Çalışması
Bad Traffic	2152	1872	3,7	3,5
Brute Force	1200	10 270	1,8	1,6
Client Side Attacks	3786	304 166	6,1	33,2
Evasion Techniques	52 323	1750	21,6	1,1
Fragmented Packets	2459	3556	4,4	3,0
DDoS	3312	542 160	2,3	280,5
Tüm Saldırılar	308 067	863 774	63,2	522,7

Pytbull uygulaması ile gerçekleştirilen saldırılar sonucunda STS'nin daha önceki bir çalışmaya göre daha yüksek trafiği daha düşük sistem kaynakları ile sorunsuz bir şekilde işletebildiği ve analiz yapabildiği görülmüştür. Pytbull bünyesindeki çeşitli saldırıların STS üzerine gerçekleştirilmesi sonucunda 2013 yılında yapılan çalışmaya göre çok farklı sonuçlar elde edildiği tespit edilmiştir. Özellikle hizmet dışı bırakma saldırılarında görülen bu farklılık, 163 kat daha fazla paket üretilmesi olarak sonuçlara yansımıştır. Elde edilen istatistikler sonucunda farklı sayılarda paket üretilmesinin sebebinin ilgili çalışmada Pytbull uygulamasının v2.0 Alpha (2011) sürümünün kullanımından kaynaklandığı tespit edilmiştir. Bu tez çalışmasında Pytbull 2.1 (2016) kararlı sürümü kullanılmıştır. Pytbull'un 2.1 kararlı sürümünde v2.0 Alpha sürümüne göre aynı sayıda saldırı testi olmasına karşılık çeşitli değerlerin daha yüksek oranlarda ayarlanmış olması nedeniyle daha yoğun paket üretimi gerçekleştiği görülmüştür. Saldırı testlerindeki daha fazla yoğun paket oluşmasının bir diğer nedeni ise bütünüyle tek bir saldırı olarak hesaplanan istemci taraflı saldırılara (Client Side Attacks) Pytbull'un yeni sürümlerinde daha fazla zararlı dosyanın eklenmesinden kaynaklanması nedeniyle olduğu tespit edilmiştir.

Çizelge 5.14'te gösterilen tüm saldırılar ile belirtilen değerler çalışmalarda gerçekleştirilen tüm saldırılara ait değerleri göstermektedir. 2013 yılında gerçekleştirilen çalışmada farklı saldırı benzetimlerinin çeşitli kombinasyonlarla yapıldığı belirtilmektedir. Bu tez çalışmasında Pytbull ve Fragrouter ile yapılan testlerin tek seferde çalıştırılması sonucunda toplamda 522,67 MB boyutunda paket trafiği yapıldığı görülmüştür. Bu değerin 2013 yılındaki çalışmaya göre 8 kat daha fazla olduğu tespit edilmiştir.

Geliştirilen BTY çözümü 2013 yılındaki çalışmadaki sistem kaynaklarına göre işlemci bakımından 11 kat ve bellek hafıza bakımından 32 kat daha düşük değere sahiptir. Buna karşılık dörtte bir oranından STS kuralı içermektedir. Saldırı benzetimleri sonucu elde edilen değerlere göre geliştirilen BTY çözümünün işlemci bakımından 11 kat; bellek hafıza bakımından 32 kat; STS kuralı bakımından dörtte bir oranında kural içermesine karşılık hizmet dışı bırakma saldırıları gibi yoğun kaynak tüketimi gerektiren bir saldırı tipinde 163 kat daha fazla anlık paket işleyebildiği görülmüştür. Bu sonuç BTY'nin ve bünyesindeki STS'nin paket analizi ve saldırı algılama mekanizmasının yıllara göre yüksek oranda geliştiğini, daha düşük kaynak kullanımında daha yüksek sayıda paket analizine olanak sağladığını göstermektedir. Gerçekleştirilen testlerde yüksek sayıda kural kullanmanın, Suricata'nın çalışmaya başlaması ile kuralları hafızasına alması anında ve hizmet dışı

bırakma saldırıları gibi yoğun trafik işlemek zorunda kaldığı anlarda yüksek oranda kaynak tükettiği görülmüştür. Özellikle Suricata'nın başlangıçta kuralları okuduğu anda pasif hale getirilmiş kuralların dahi performans kaybına sebep olduğu tespit edilmiştir. Bu nedenle yerleştirildiği konum göz önünde bulundurulduğunda kullanılması gerekli olmayan, pasifleştirilmiş kuralların Suricata'dan tamamen kaldırılarak daha iyi performans alınması sağlanmıştır.

6. SONUÇ VE ÖNERİLER

Tez çalışması kapsamında ev, ofis ve IoT gibi küçük ölçekli olarak nitelendirilebilecek ağlarda kullanılmak üzere saldırı tespit sistemi ve yönlendirici özelliği olan ağ geçidi güvenlik çözümü geliştirilmiştir. Geliştirilen bütünleşik tehdit yönetimi uygulaması ile ev, ofis ve IoT gibi küçük ölçekli ağlarda mevcut cihazlarla birlikte ağa yeni katılan IoT cihazlarının dışardan gelecek saldırılara karşı güvenliğinin artırılması ve kapasiteleri gereği bir savunma mekanizması içermeyen cihazların istismar edilmesi önlenmiştir. Kurumsal yapılarda kullanılan gelişmiş güvenlik duvarı ve saldırı tespit sistemi uygulamalarının küçük ölçekli ağlara uygulanması ile daha güvenli ağ iletişimi kurulması sağlanmıştır. Gerçekleştirilen gelişmiş siber saldırı testleri ve uygulanan güvenlik sıkılaştırmaları ile IoT cihazlarının saldırılar sonucu istismar olmasının yanı sıra son yıllarda görülen istismar edilmeleri ile saldırı aracı olarak da kullanılmasının önüne geçilmesi sağlanmıştır.

Mevcut ağ geçidi cihazlarındaki en büyük eksikliklerden olan güncelleme mekanizması eksikliği bütünleşik tehdit yönetimi uygulamasında yer alan periyodik güncelleme mekanizmasıyla giderilmiştir. Saldırı tespit sistemi kural listelerinin de periyodik olarak güncellenmesinin ayarlanmasıyla geliştirilen çözümün zararlı algılama veri tabanının tehditlere karşı sürekli bir koruma sunması sağlanmıştır. Gerçekleştirilen performans ve kapasite testleri ile çözümün kullanılmasının hedeflendiği ağın karakteristiğine göre yeterli kaynak tükettiği tespit edilmiştir. Tercih edilen donanım ve yazılım kaynaklarının maliyet analizi sonucunda hedef kullanıcı kitlesi için uygun maliyetli bir çözüm olduğu görülmüştür.

Kurumsal ağlarda saldırı tespit etmek için kullanılan profesyonel çözümlerin ev, ofis ve IoT ağlarında kullanılır hale getirilmesiyle küçük ölçekli olarak nitelendirilebilecek ağlarda güvenliğin artırılması sağlanmıştır. Yapılan çalışmalardaki sistem kaynaklarının zamanla yetersiz kalacağı öngörüsünün geliştirilen bütünleşik tehdit yönetimi ile giderildiği söylenebilmektedir. Buna ek olarak benzer çalışmalarda uygulanan temel güvenlik problemlerini çözmenin ötesinde zamanla ortaya çıkacak yeni güvenlik problemlerine karşı sürekli koruma sağlayan bir çözüm sunulmuştur. Zararlı aktivitelerin sahip olduğu imzaların bulunduğu veri tabanının güncellenmesinin otomatik olması sayesinde güvenliğin sürekliliği sağlanmıştır.

Saldırı tespit sistemine üzerine yapılan saldırı benzetimleri ile geliştirilen çözümün ağ kabiliyetleri ve kapasitesi ölçülmüştür. Hatalı ağ paketleri gönderimi, hizmet dışı bırakma saldırıları, kaba kuvvet saldırıları, parçalı paket gönderimi ile saldırı tespit sistemi atlatma yöntemleri gibi gelişmiş saldırı benzetim senaryolarının uygulandığı güvenlik çözümünün çeşitli saldırılardaki tepkisi gözlemlenmiştir. Ağ tarama ve haritalandırma yöntemlerinde %100'e varan; istemci taraflı saldırılarda %96 ve gelişmiş siber saldırılardan olan parçalı veri paketleri ile saldırı tespit sistemi atlatma saldırılarında %80 oranında saldırı tespit değerlerine ulaşılmıştır.

Geliştirme ve saldırı benzetimi aşamalarında açık kaynak kodlu uygulamalar kullanılan bu tez çalışmasında birçok uygulamanın testi gerçekleştirilmiştir. FreeBSD işletim sistemi üzerinde çalışan OPNSense bütünleşik tehdit yönetimi uygulamasının Suricata saldırı tespit sistemi ile birlikte gelişmiş, kapsamlı ve kararlılık açısından kullanıma uygun bir güvenlik çözümü olduğu sonucuna ulaşılmıştır. Bir bütünleşik tehdit yönetimi uygulaması olan OPNSense ilk olarak bir çalışmada kullanılmıştır. Suricata saldırı tespit sistemi uzun yıllardır geliştirilen imza tabanlı saldırı algılama olanağı sayesinde düşük sistem kaynaklarında dahi yüksek performans sunabilmektedir. Suricata 4.0 sürümünde yer alan algılama mekanizmasının çoklu iş parçacığı yöntemiyle çalışması sayesinde eski sürümlerine göre daha yüksek performans sağladığı ve anlık paket analiz kabiliyeti açısından daha yüksek bant genişliğinde trafik işleyebildiği görülmüştür.

Saldırı benzetimleri sırasında açık kaynak kodlu olan Pytbull ve Fragrouter uygulamaları kullanılarak testler gerçekleştirilmiştir. Pytbull'un son sürümü kullanılarak daha yeni saldırı veri tabanı ile güncel saldırıların testleri yapılabilmiştir. Pytbull ile yapılan testler sırasında hizmet dışı bırakma saldırılarının Suricata tarafından karşılanamadığı tespit edilmesi üzerine Suricata üzerindeki kural listelerinde ve OPNSense uygulamasında optimizasyon yapılmıştır. Gerçekleştirilen iyileştirmeler ve pasif kuralların yapıdan tamamen kaldırılması sayesinde Suricata'nın Pytbull saldırılarından hizmet dışı bırakma saldırılarını karşıladığı görülmüştür. Bu işlemler ile Suricata'daki kuralların pasif olmaları halinde dahi kaynak tüketimine sebep olduğu tespit edilmiştir. Fragrouter uygulaması kullanılarak parçalı veri gönderimi ile saldırı tespit sistemi atlatma teknikleri uygulanarak Suricata'nın tepkisi ölçülmüştür. Fragrouter ile birlikte saldırı benzetimi yapıldığı sırada Suricata üzerindeki kayıtlara göre %97 oranında paket engellemesi yapıldığı tespit edilmiştir.

Yapılan geliştirmeler ve testler sonucunda açık kaynak kodlu uygulamalar ile saldırılar gerçekleştirilirken açık kaynak kodlu diğer uygulamalar ile ağın güvenliğinin sağlanması amaçlanmıştır. Kullanılan uygulamaların açık kaynak kodlu olması sayesinde toplam edinim maliyeti düşmüş; geliştirme ve test süreçleri hızlanmıştır.

Gelecek çalışmalarda uygulamanın başarısını ve performansını artıracak çözümler yazılım tanımlı ağlar ve konteyner teknolojisi ile geliştirilmesi düşünülmüştür. Yazılım tanımlı ağ uygulamalarının mevcut saldırı tespit sistemleri ile birlikte çalışabilmesi sağlanması durumunda daha düşük sistem gereksinimde daha yüksek performans değerleri elde edilebileceği öngörülmektedir. Geliştirilen bütünleşik tehdit yönetimi uygulamasında kablosuz bağlantı protokollerinde sıkılaştırmalar yapılması ve kullanım ara yüzündeki kullanılmayan servislerin kaldırılması ile uygulamanın evlerde kullanılmaya hazır bir ürün haline geleceği düşünülmektedir. Saldırı benzetimi aşamasında kullanılan Pytbull uygulaması saldırı tespit sistemlerinde kullanılan açık kaynak kodlu yegâne uygulamalardan olmasına karşın geliştirmesi durdurulmuştur. Geliştirildiği programlama dilinin eski bir sürümünde çalışması ve arka planda kullandığı yazılımların eski sürümlerine ihtiyaç duyması kurulum aşamasını zorlaştırmaktadır. Bu uygulamanın daha güncel hale getirilmesi, daha güncel saldırı tiplerini yapabiliyor olması ve konteyner teknolojisi gibi bir yapıda çalışmasının sağlanmasıyla daha kullanışlı hale getirilebileceği düşünülmüştür.

KAYNAKLAR

1. İnternet: Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fspectrum.ieee.org%2Ftech-talk%2Ftelecom%2Finternet%2Fpopular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

2. İnternet: How the Next Evolution of the Is Changing Everything. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fdam%2Fen_us%2Fabout%2Fac79%2Fdocs%2Finnov%2FIoT_IBSG_0411FINAL.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

3. Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80-84.

4. Chao, Y., Bingyao, C., Jiaying, D. and Wei, G. (2009). The research and implementation of UTM. *International Communication Conference on Wireless Mobile & Computing*, 389-392.

5. İnternet: Open source forms the backbone of the most significant projects. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fopensource.com%2Fbusiness%2F14%2F8%2Fblack-duck-oss-survey-2014&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

6. İnternet: How Many Devices Can Connect to One Wireless Router? URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.lifewire.com%2Fhow-many-devices-can-share-a-wifi-network-818298&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

7. İnternet: Personal firewall with location detection. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fpatents.google.com%2Fpatent%2FUS20030097589&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

8. Zhang, Y., Li, J., Chen, L., Ji, Y. and Tang, F. (2017). A novel method against the firewall bypass threat in OpenFlow networks. *International Conference on Wireless Communications and Signal Processing*, 1-6.

9. Bauer, M. (2004). Paranoid penguin: seven top security tools. *Paranoid Penguin Linux Journal*, (12).

10. Raja, F., Hawkey, K., Jaferian, P., Beznosov, K. and Booth, K. S. (2010). It's too complicated, so i turned it off!: expectations, perceptions, and misconceptions of personal firewalls. *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*, 53-62.

11. Chiong, R. and Dhakal, S. (2008). On the insecurity of personal firewall. *International Symposium on Information Technology*, 1-10.

12. Alfayyadh, B., Ponting, J., Alzomai, M. and Josang, A. (2010). Vulnerabilities in personal firewalls caused by poor security usability. *IEEE International Conference on Information Theory and Information Security,* 682-688.

13. Waghmare, P., Chaure, P., Chandgude, M. and Chaudhari, A. (2017). Survey on: Home automation systems. *Trends in Electronics and Informatics,* 7-10.

14. Asadullah, M. and Raza, A. (2016). An overview of home automation systems. *2nd International Conference on Robotics and Artificial Intelligence,* 27-31.

15. Chowdhry, D., Paranjape, R. and Laforge, P. (2015). Smart home automation system for intrusion detection. *14th Canadian Workshop on Information Theory,* 75-78.

16. Dolezal, J. (2008). Design of Smart home Multi-layer Control system. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsupport.dce.felk.cvut.cz%2Fmediawiki%2Fimages%2Fd%2Fdb%2FDp_2008_dolezal_jan.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

17. Lobaccaro, G., Carlucci, S. and Löfström, E. (2016). A review of systems and technologies for smart homes and smart grids. *Energies,* 9(5), 348.

18. Brauchli, A. and Li, D. (2015). A solution based analysis of attack vectors on smart home systems. *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications,* 1-6.

19. Lalanda, P., Bourcier, J., Bardin, J. and Chollet, S. (2010). Smart home systems. *Smart Home Systems,* 1-18.

20. Li, M. and Lin, H.-J. (2015). Design and Implementation of Smart Home Control Systems Based on Wireless Sensor Networks and Power Line Communications. *IEEE Transactions on Industrial Electronics,* 62(7), 4430-4442.

21. Tsou, Y.-P., Hsieh, J.-W., Lin, C.-T. and Chen, C.-Y. (2006). Building a Remote Supervisory Control Network System for Smart Home Applications. *Systems, Man and Cybernetics IEEE International Conference,* 1826-1830.

22. Piyare, R. (2013). Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone. *International Journal of Internet of Things,* 2(1), 5-11.

23. Cosar, M. and Karasartova, S. (2017). A firewall application on SOHO networks with Raspberry Pi and snort. *International Conference on Computer Science and Engineering,* 1000-1003.

24. Poornachandran, P., Sreeram, R., Krishnan, M. R., Pal, S., Sankar, A. U. P. and Ashok, A. (2015). Internet of Vulnerable Things (IoVT): Detecting Vulnerable SOHO Routers. *International Conference on Information Technology,* 119-123.

25. Hsu, J., Hsu C. F., and Huang C. M. (2005). Design of an IPv6 SOHO Router Based on Embedded Linux System. *19th International Conference on Advanced Information Networking and Applications,* 2, 827-832.

26. Bento, A. (2003). SOHO Security: A Technical Briefing. *America's Conference on Information Systems*, 414.

27. Spinellis, D., Kokolakis, S. and Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7(3), 121-128.

28. Chamberlain, R. D., Chambers, M., Greenwalt, D., Steinbrueck, B. and Steinbrueck, T. (2016). Layered Security and Ease of Installation for Devices on the Internet of Things. *International Conference on Internet-of-Things Design and Implementation*, 297-300.

29. Erten, Y. M. and Tomur, E. (2004). A layered security architecture for corporate 802.11 wireless networks. *Symposium on Wireless Telecommunications,* 123-128.

30. Shirali-Shahreza, S. and Ganjali, Y. (2018). Protecting Home User Devices with an SDN-Based Firewall. *Transactions on Consumer Electronics*, 64(1), 92-100.

31. Gupta, N., Naik, V. and Sengupta, S. (2017). A firewall for Internet of Things. *9th International Conference on Communication Systems and Networks*, 411-412.

32. İnternet: More than 90% of successful cyber attacks worldwide begin with a phishing email. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.itgovernanceusa.com%2Fblog%2Fmore-than-90-of-successful-cyber-attacks-worldwide-begin-with-a-phishing-email&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

33. Baykara, M. and Gurel, Z. Z. (2018). Detection of phishing attacks. *6th International Symposium on Digital Forensic and Security*, 1-5.

34. Gupta, S., Singhal, A. and Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *International Conference on Computing, Communication and Automation,* 537-540.

35. Khonji, M., Iraqi, Y. and Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091-2121.

36. İnternet: Kaspersky IT Threat Evolution Q3 2016. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fmedia.kasperskycontenthub.com%2Fwp-content%2Fuploads%2Fsites%2F43%2F2018%2F03%2F07183248%2FKL_Q3_Malware_Report_ENG.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

37. Kaya, Ç. ve Yildiz, O. (2014). Makine Öğrenmesi Teknikleriyle Saldırı Tespiti: Karşılaştırmalı Analiz. *Marmara University Journal of Science*, 26(3), 108.

38. Basnet, R., Mukkamala, S. and Sung, A. H. (2008). Detection of Phishing Attacks: A Machine Learning Approach. *Soft Computing Applications in Industry*. Springer, Berlin, Heidelberg, 373-383.

39. Hijawi, W., Faris, H., Alqatawna, J., Al-Zoubi, A. M. and Aljarah, I. (2017). Improving email spam detection using content based feature engineering approach. *Conference on Applied Electrical Engineering and Computing Technologies*, 1-6.

40. Nakato H. (2016). *Network Security: Attacks and Defense Mechanism by Designing an Intelligent Firewall Agent*, Master Thesis, Sakarya Üniversitesi, Sakarya 126.

41. Kambourakis G., Moschos T., Geneiatakis, D. and Gritzalis, S. (2007). A Fair Solution to DNS Amplification Attacks. *Second International Workshop on Digital Forensics and Incident Analysis*, 38-47.

42. Kambourakis, G., Moschos, T., Geneiatakis, D. and Gritzalis, S. (2007). Detecting DNS Amplification Attacks. *International Workshop on Critical Information Infrastructures Security*, 185-196.

43. İnternet: 150,000 IoT Devices behind the 1Tbps DDoS attack on OVH. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsecurityaffairs.co%2Fwordpress%2F51726%2Fcyber-crime%2Fovh-hit-botnet-iot.html&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

44. İnternet: DDoS on Dyn Impacts Twitter, Spotify, Reddit. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fkrebsonsecurity.com%2F2016%2F10%2Fddos-on-dyn-impacts-twitter-spotify-reddit%2F&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

45. İnternet: Geçen haftaki siber saldırı ABD'ye 7 milyar dolara mal oldu. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cnnturk.com%2Fbilim-teknoloji%2Fteknoloji%2Fsiber-saldiri-sosyal-aglara-yasak-koydu&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

46. Hachinyan, O., Khorina, A. and Zapechnikov, S. (2018). A game-theoretic technique for securing IoT devices against Mirai botnet. *Conference of Russian Young Researchers in Electrical and Electronic Engineering*, 1500-1503.

47. Kambourakis, G., Kolias, C. and Stavrou, A. (2017). The Mirai botnet and the IoT Zombie Armies. *Military Communications Conference*, 267-272.

48. İnternet: The years go by, the threat remains: DDoS attacks observed by OVH. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.ovh.co.uk%2Fnews%2Farticles%2Fa2587.ddos-attacks-observed-by-ovh-in-2017&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

49. Moore, C. (2016). Detecting Ransomware with Honeypot Techniques. *IEEE Cybersecurity and Cyberforensics Conference*, 77-81.

50. Scaife, N., Carter, H., Traynor, P. and Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *36th International Conference on Distributed Computing Systems,* 303-312.

51. Nagaratna, M., Prasad, V. K. and Kumar, S. T. (2009). Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking Based Detection and Filtering. *International Conference on Advances in Recent Technologies in Communication and Computing*, 753-755.

52. İnternet: Addressing the challenge of IP spoofing. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.internetsociety.org%2Fwp-content%2Fuploads%2F2017%2F08%2FISOC-AntiSpoofing-20150909-en-2.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

53. Kührer, M., Hupperich, T., Rossow, C. and Holz, T. (2014). Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks. *8th USENIX Conference on Offensive Technologies,* 4.

54. Vanhoef, M., Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. *Special Interest Group on Security, Audit and Control, Conference on Computer and Communications Security,* 1313-1328.

55. Abo-Soliman, M. A. and Azer, M. A. (2017). A study in WPA2 enterprise recent attacks. *13th International Computer Engineering Conference*, 323-330.

56. İnternet: Botnets "competing" to attack vulnerable GPON fiber routers. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.zdnet.com%2Farticle%2Fbotnets-competing-to-attack-vulnerable-gpon-fiber-routers%2F&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

57. İnternet: GPON Exploit in the Wild - Muhstik Botnet Among Others. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fblog.netlab.360.com%2Fgpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en%2F&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

58. Paganini, P. SOHO pharming attack hit more that 300,000 devices worldwide. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsecurityaffairs.co%2Fwkordpress%2F22743%2Fcyber-crime%2Fsoho-pharming-attack.html&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

59. İnternet: Largent, W. New VPNFilter malware targets at least 500K networking devices worldwide. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fblog.talosintelligence.com%2F2018%2F05%2FVPNFilter.html&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

60. İnternet: Heffner, C. and Yap, D. Security Vulnerabilities in SOHO Routers. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.exploit-db.com%2Fdocs%2Fenglish%2F13000-security-vulnerabilities-in-soho-routers.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

61. Maheshwari, N. and Dagale, H. (2018). Secure communication and firewall architecture for IoT applications. *International Conference on Communication Systems Networks,* 328-335.

62. Asghari, V., Amiri, S. and Amiri, S. (2015). Implementing UTM based on PfSense platform. *2nd International Conference on Knowledge-Based Engineering and Innovation,* 1150-1152.

63. Arunwan, M., Laong, T. and Atthayuwat, K. (2016). Defensive performance comparison of firewall systems. *Management and Innovation Technology International Conference,* 221-224.

64. İnternet: 2016-2019 Ulusal Siber Güvenlik Stratejisi. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.udhb.gov.tr%2Fdoc%2Fsiberg%2F2016-2019guvenlik.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

65. İnternet: Bilgi Güvenliği ne demektir? URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilgimikoruyorum.org.tr%2F%3Fb121_bilgi-guvenligi-ne-demektir&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

66. Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği,* 27(3), 451-471.

67. Zhao, K. and Ge, L. (2013). A Survey on the Internet of Things Security. *Ninth International Conference on Computational Intelligence and Security,* 663-667.

68. Risteska Stojkoska, B. L. and Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production,* 140, 1454-1464.

69. Billure, R., Tayur, V. M. and Mahesh V. (2015). Internet of Things - a study on the security challenges. *International Advance Computing Conference,* 247-252.

70. İnternet: ENISA - Baseline Security Recommendations for IoT. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fbaseline-security-recommendations-for-iot&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

71. İnternet: National Cybersecurity Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.sbs.ox.ac.uk%2Fcybersecurity-capacity%2Fcontent%2Fnational-cybersecurity-strategies-setting-course-national-efforts-strengthen-security&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

72. İnternet: Cryptolocker virüsü hakkında bilgi notu. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.udhb.gov.tr%2Fimages%2Fduyurular%2F74bc0128f065b41.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

73. Silic, M. (2013). Dual-use Open Source Security Software in Organizations - Dilemma: Help or Hinder? *Computer Security*, 39, 386-395.

74. Çavuş, M. F. ve Kurt, H. S. (2017). Kamu Kurumlarında Açık Kaynak Kodlu Yazılımların Kullanımı. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, 5(3).

75. Miranda, J. M., Mtz, F. A. P. and Mata, M. A. M. (2017). Next generation systems — Scope and application of intrusion detection and prevention systems (IDPS) a systematic literature review. *12th Iberian Conference on Information Systems and Technologies,* 1-7.

76. Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C. and Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16-24.

77. Vasiliadis, G., Antonatos, S., Polychronakis, M., Markatos, E. P. and Ioannidis, S. (2008). Gnort: High Performance Network Intrusion Detection Using Graphics Processors. R. Lippmann, E. Kirda and A. Trachtenberg (Eds.), *Recent Advances in Intrusion Detection*, Springer Berlin Heidelberg, 116-134.

78. Patchava, V., Kandala, H. B. and Babu, P. R. (2015). A Smart Home Automation technique with Raspberry Pi using IoT. *International Conference on Smart Sensors and Systems*, 1-4.

79. İnternet: NSA Information Assurance. Best Practices for Keeping Your Home Network Secure. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fdodcio.defense.gov%2FPortals%2F0%2FDocuments%2FCyber%2FSlicksheet_BestPracticesForKeepingYourHomeNetworkSecure_Web_update.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

80. İnternet: pfSense vs OPNsense: technical comparison. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fopnsense.firewallhardware.it%2Fen%2Fpfsense_vs_opnsense.html&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

81. Albin, E. (2011). *A comparative analysis of the snort and suricata intrusion-detection systems,* Doctoral Thesis, Naval Postgraduate School, Monterey, California, 49.

82. Day, D. (2011). A performance analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines. *The Fifth International Conference on Digital Society,* 187-192.

83. Brumen, B. and Legvart, J. (2016). Performance analysis of two open source intrusion detection systems. *39th International Convention on Information and Communication Technology, Electronics and Microelectronics*, 1387-1392.

84. White, J. S., Fitzsimmons, T. and Matthews, J. N. (2013). Quantitative analysis of intrusion detection systems: Snort and Suricata. *Society of Photographic Instrumentation Engineers: Defense, Security, and Sensing*, (8757).

85. Aslan, Ö. and Samet, R. (2017). Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs. *International Conference on Cyberworlds*, 222-225.

86. İnternet: APU2C0 IPFire throughput test. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fteklager.se%2Fen%2Fknowledge-base%2Fapu2c0-ipfire-throughput-test-much-faster-pfsense%2F&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

87. İnternet: Forwarding performance lab of a PC Engines APU. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fbsdrp.net%2Fdocumentation%2Fexamples%2Fforwarding_performance_lab_of_a_pc_engines_apu&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

88. Segars, S. (2011). ARM processor evolution: Bringing high performance to mobile devices. *IEEE Hot Chips 23 Symposium*, 1-37.

89. Taleck, G. (2003). Ambiguity Resolution via Passive OS Fingerprinting. G. Vigna, C. Kruegel and E. Jonsson (Eds.), *Recent Advances in Intrusion Detection*, Springer Berlin Heidelberg, 192-206.

90. İnternet: Suricata User Guide. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fmedia.readthedocs.org%2Fpdf%2Fsuricata%2Fsuricata-3.2%2Fsuricata.pdf&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

91. İnternet: Extending and consolidating hosts files from several well-curated sources. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fgithub.com%2FStevenBlack%2Fhosts&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

92. İnternet: Ultimate hosts blacklist. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fgithub.com%2Fmitchellkrogza%2FUltimate.Hosts.Blacklist&date=2018-12-30, Son Erişim Tarihi: 30.12.2018.

93. Say, T., Alkan, M., Dörterler, M., and Doğru, İ. A. 2018. CPU Performance Test of A Home Firewall. *3rd International Conference on Computer Science and Engineering*, 509-513.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : SAY, Tamer
Uyruğu : T.C.
Doğum tarihi ve yeri : 04.12.1991, Ankara
Medeni hali : Bekâr
Telefon : 0 (506) 933 89 94
E-mail : tamersay777@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilgi Güvenliği Müh.	Devam ediyor
Lisans	Karabük Üniversitesi / Bilgisayar Müh.	2015
Lise	Dr. Şerafettin Tombuloğlu Lisesi	2009

İş Deneyimi

Yıl	Yer	Görev
2016-Halen	Yurdum Yayıncılık ve Yazılım Ltd.	Sistem ve Güvenlik Müh.

Yabancı Dil

İngilizce

Yayınlar

1. Say, T., Alkan, M., Dörterler, M., and Doğru, İ. A. 2018. CPU Performance Test of A Home Firewall. *3rd International Conference on Computer Science and Engineering*, 509-513.

Hobiler

Kitap okuma, Sinema, Doğa fotoğrafçılığı

GAZİ GELECEKTİR..