AÇIK KAYNAK KODLU GÜVENLİK DUVARLARININ SANALLAŞTIRILMIŞ SİSTEMLER ÜZERİNDE KULLANILMASI

Harun TÜMER
201402205

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder ŞAHİNASLAN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Şubat, 2024

AÇIK KAYNAK KODLU GÜVENLİK DUVARLARININ SANALLAŞTIRILMIŞ SİSTEMLER ÜZERİNDE KULLANILMASI

Harun TÜMER
201402205
ORCID: 0000-0001-9300-0680

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder ŞAHİNASLAN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Şubat, 2024

JÜRİ VE ENSTİTÜ ONAYI

HARUN TÜMER'ın "Açık Kaynak Kodlu Güvenlik Duvarlarının Sanallaştırılmış Sistemler Üzerinde Kullanılması" başlıklı tezi 15.02.2024 tarihinde aşağıdaki jüri tarafından değerlendirilerek "Maltepe Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği" nin ilgili maddeleri uyarınca Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans/Doktora/Sanatta Yeterlik tezi oy birliğiyle/oy çokluğuyla, başarılı/başarısız olarak kabul edilmiştir.

	Unvanı. Adı ve Soyadı	İmza
Üye (Tez Danışmanı)	Dr. Öğr. Üyesi Önder ŞAHİNASLAN Maltepe Üniversitesi	.....
Üye	Dr. Öğr. Üyesi Hüseyin Fehmi Selim BAYRAKLI Milli Savunma Üniversitesi	.....
Üye	Dr. Öğr. Üyesi Erdal GÜVENOĞLU Üniversitesi	.....

Prof. Dr. Selva ERSÖZ KARAKULAKOĞLU
Enstitü Müdürü

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Hazırlamış olduğum tezde katkılarından ve desteklerinden ötürü Danışmanım Sn. Dr. Öğr. Üyesi Önder ŞAHİNASLAN'a çok teşekkür ederim. Tezimdeki düzenlemelerinden dolayı Kübra KAVALCI'ya, tezin test işlemlerini gerçekleştirdiğim Sümer Holding A.Ş.'ye teşekkürü bir borç bilirim. Hayatımın her alanında destek olan babam Abdullah TÜMER ve annem Gülhan TÜMER'e teşekkür ederim. Her zaman yanımda olan, tez yazım sürecimde gece gündüz birlikte çalıştığım canım eşim Öğr. Gör. Candan TÜMER'e, birlikte geçireceğimiz vakitlerinden çalmış olduğum canım oğlum Rüzgar TÜMER'e çok teşekkür ederim.

Harun TÜMER

Şubat, 2024

ÖZET

AÇIK KAYNAK KODLU GÜVENLİK DUVARLARININ SANALLAŞTIRILMIŞ SİSTEMLER ÜZERİNDE KULLANILMASI

Harun Tümer
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder Şahinaslan
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2024

Bilgi teknolojilerinin hayatın her alanına uyum sağlamasıyla, cihazların birbirleriyle ve insanlarla olan iletişiminin güvenli hale getirilmesi için büyük çaba, kaynak ve iş gücü gerekmektedir. Sanallaştırmanın sunduğu avantajlar ve kolaylıklar, günümüzde teknoloji üreticilerini daha fazla düşünmeye yönlendirmiştir. Bu talebe cevap verebilmek ve daha iyi çözümler üretebilmek adına birçok teknoloji üreticisi, sanallaştırmaya odaklanarak çalışmalarını sürdürmektedir. Sanallaştırılmış sistemler kullanılarak oluşturulacak güvenlik duvarlarında, donanım ihtiyacı fiziksel sunuculardan karşılanmaktadır. Bu sayede, güvenlik duvarı için gerekli olan tüm kaynaklar, sanallaştırma sistemi içindeki ihtiyaçlar ve gereksinimler doğrultusunda esnek bir şekilde yönetilebilmektedir. Açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanımı üzerine yapılan araştırma, modern bilgi teknolojilerindeki güvenlik ihtiyaçlarına daha etkili çözümler sunma amacını taşımaktadır. Bu çalışma, bilgilerin kaydedilmesi, işlenmesi ve değerlendirilmesi gibi kritik görevlerin gerçekleştirildiği sanallaştırılmış sistemlerde, güvenlik duvarlarının nasıl entegre edilebileceğini incelemektedir. Donanım maliyetleri, güvenlik standartları ve yazılımlara ödenen lisanslama ücretleri dikkate alınarak, açık kaynak kodlu güvenlik duvarlarının sağladığı avantajlar ve maliyet etkinliği araştırılmaktadır. Sanallaştırılmış sistemlerin esnek yapısı, güvenlik duvarlarının daha verimli bir şekilde yönetilmesine imkan tanıyarak, bilgi sistemlerinin güvenliğini artırabilmektedir. Çalışmanın sonuçları, açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde etkin bir biçimde kullanılabildiğini göstermekte, bu da hem

maliyet tasarrufu sağlamak hem de güvenlik önlemlerini güçlendirmek adına önemli bir potansiyel oluşturmaktadır.

Anahtar Sözcükler: Sunucu Sanallaştırma, Sanal Makineler, Güvenlik Duvarı, Açık Kaynak Kodlu Yazılım

ABSTRACT

USING OPEN SOURCE FIREWALLS ON VIRTUALIZED SYSTEMS

Harun Tümer
Master Thesis
Department of Computer Engineering
Master Program in Computer Engineering with Thesis
Thesis Advisor: Assist. Prof. Dr. Önder Şahinaslan
Maltepe University Graduate School, 2024

With information technologies adapting to every aspect of life, a great deal of effort, resources and manpower is required to secure the communication of devices with each other and with people. The advantages and conveniences offered by virtualization have led technology manufacturers today to think more. In order to respond to this demand and produce better solutions, many technology manufacturers continue their work by focusing on virtualization. In firewalls to be created using virtualized systems, the hardware requirement is met from physical servers. In this way, all the resources required for the firewall can be managed flexibly in line with the needs and requirements within the virtualization system. The research on the use of open source firewalls in virtualized systems aims to provide more effective solutions to the security needs in modern information technologies. This study examines how firewalls can be integrated in virtualized systems where critical tasks such as recording, processing and evaluating information are performed. Taking into account hardware costs, security standards and licensing fees paid for software, the advantages and cost effectiveness of open source firewalls are investigated. The flexible nature of virtualized systems allows firewalls to be managed more efficiently, which can improve the security of information systems. The results of the study show that open source firewalls can be used effectively in virtualized systems, which creates a significant potential for both cost savings and strengthening security measures.

Keywords: Server Virtualization, Virtual Machines, Firewall, Open Source Software

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

BSD : Berkeley Software Distribution

CPU : Merkezi İşlem Birimi

DHCP : Dinamik Ana Bilgisayar Yapılandırma Protokolü

DIFA : Dinamik Akıllı Güvenlik Duvarı Mimarisi

DMZ : Arındırılmış Bölge, Demilitarized Zone

DNS : Alan Adı Sistemi

FSF : Özgür Yazılım Vakfı

GNU : GNU, Unix Değildir

GPL : Genel Kamu Lisansı

HTTP : Güvenli Metin Aktarma Protokolü

IP : İnternet Protokolü

LAN : Yerel Alan Ağı

NAT : Ağ Adresi Çevirisi

RAM : Rastgele Erişimli Bellek

TCP/IP : Transmission Control Protocol/Internet Protocol

WAN : Geniş Alan Ağı

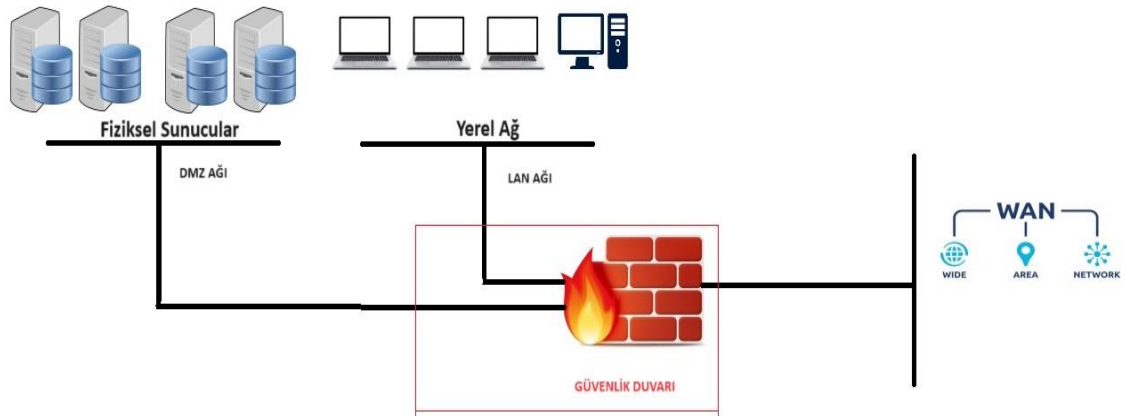
VPN : Sanal Özel Ağ

VM : Sanal Makine, Virtual Machine

1. GİRİŞ

Birçok ülkede bulunan binlerce bilgisayarın haberleşmesi internet sistemi olarak tanımlanmaktadır (İşler, Çiftçi, ve Yarangümelioğlu, 2013). Her geçen gün internet kullanımının yaygınlaşması ile birlikte internet sistemlerinde dolaşan bilginin güvenliği daha da önemli hale gelmiştir. Dünyada yaklaşık beş milyon kullanıcının internet sayesinde birbirlerine bağlı oldukları bilinmektedir (İnternet Kullanım İstatistikleri, 2023).

Bilgilerin kaydedilmesi, sunulması, işlenmesi ve değerlendirilmesi bilgi sistemleri tarafından yapılmaktadır. Oluşturulan bilgi sistemleri, sistemlerin büyüklüklerine bakılmaksızın sunucu sistemleri ve güvelik duvarları ile donatılmaktadır. Bu sistemlerde bulunan sunucular bilgilerin depolanması, işlenmesi, değerlendirilmesi ve sunulması gibi işlemleri yerine getirirken, güvenlik duvarları ise sunucu sistemlerinin güvenli şekilde çalışmalarına imkan sağlamaktadır. Söz konusu bu sistem tasarımları geleneksel sunucu tasarımı olarak Şekil 1'de gösterilmiştir. Oluşturulan bilgi sistemlerinde kullanılan bilgilerin ulaştırılması istenilen yerlere iletilmesi için birden fazla sunucu sistemine ihtiyaç duyulmaktadır.



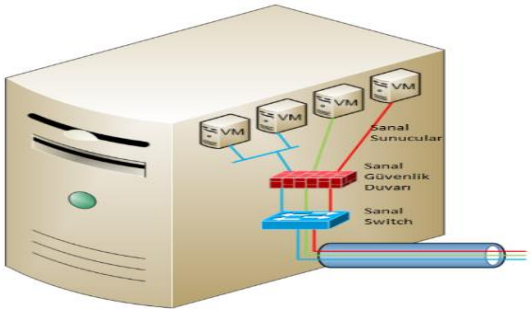
Şekil 1. Geleneksel Sistem Tasarımı

Bilgi ve bilişim teknolojilerinin her alanda kullanılmasıyla birlikte başkalarıyla veri paylaşımı yapabilmek için ağ ve web uygulamaları kullanılmaktadır. Bu uygulamalar ortak kullanım sağlayarak insanların ve sistemlerin ihtiyaçlarını karşılamaktadır.

İhtiyaçlar karşılanırken web uygulamaları farklı dillerde geliştirilebilirler. Web uygulamalarında kullanılacak veriler mssql, mysql, oracle, postgresql gibi veri tabanı sistemlerinde tutulmakta ve bu sistemlere çevrim içi olarak ulaşım sağlanabildiğinden dolayı istemcilerin ihtiyaçlarına cevap verebilmektedir. Diğer taraftan kullanılan yazılımların karmaşık yapılarda olmaları ve ilişkili olarak çalışmaları verileri güvende tutmayı zorlaştırmaktadır. Artan tehditlerin olaya dönüşmeden önlenebilmesi, risklerin önceden fark edilmesi ve kurum ve/veya birey bilgilerinin zarar görmeden korunmasını daha da önemli hale getirmiştir. Kurumlar tüm hizmet ve servisleri teknolojinin en son imkânlarını kullanarak kullanıcılarına uygun ve güvenli bir şekilde sunmak zorundadır (Şahinaslan, Razbonyalı, ve Şahinaslan, 2010).

Bilgi sistemleri; bilgi teknolojisi ve organizasyonların kesişimindeki sorunları çözmek için ekonomi, bilgisayar bilimi ve sosyal bilimler gibi diğer disiplinlerden birçok teoriyi sıklıkla kullandığı için uygulamalı bir araştırma disiplini olarak bilinmektedir (Peffers, Tuunanen, Rothenberger, ve Chatterjee, 2014). Bilgi sistemlerinin her geçen gün öneminin artması ile birlikte kullanılan sistemlerde bulunan sunucu maliyetlerinin çok olması ve her sistem için ayrı bir sunucu servisinin kullanılması sistem giderlerinin daha da artmasına neden olmaktadır. Maliyet olarak, sadece sunucu donanım maliyetlerini dikkate almak yeterli değildir. Aynı zamanda lisans, elektrik, soğutma, güvenlik, veri depolama ve diğer bilişim sistemleri de birer maliyet kalemi olarak sayılmaktadır. Bu maliyetleri olabildiğince aşağılara çekmek içinde sunucu sanallaştırma ve ağ sanallaştırma gibi sistemlerin önemi giderek artmaktadır.

Sanallaştırma sistemlerinin; sunucu, masaüstü, veri depolama, ağ ve uygulama sanallaştırma gibi türleri bulunmaktadır. Sunucu sanallaştırma bu sanallaştırma sistemlerinin temeli olarak kabul edilmektedir (Büyükyılmaz, 2016). Sanallaştırma 1960'lı yıllarda Manchester Üniversitesi'nin yapmış olduğu projede kullanılmış olsa da bir fikir olarak ilk kez Oxford Üniversitesi'nde ortaya çıkmıştır (Kervancı, 2017). Donanımsal kaynakların yüksek verimle kullanılması sanallaştırma ile sağlanabilmektedir. Yalnızca tek bir platform üzerinden farklı iş rollerinin yürütülmesi, yönetilmesi, kaynak paylaşımı yapılması maliyetlerin düşürülmesi için çok önemlidir. Sanallaştırılmış sunucu mimarisi Şekil 2'de gösterilmiştir (Hogg, 2023).



Şekil 2. Sanallaştırılmış Sistem Tasarımı

Donanım, güvenlik standartları ve yazılımlara ödenen lisanslama ücretlerinin yüksek olmasından dolayı maliyetlerin düşürülmesi amacıyla sanallaştırılmış sistemler üzerinde çalışılması gereklilik arz etmektedir. Bu nedenle çalışmada açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanımı araştırılmaktadır.

Araştırmalar sonucunda çalışmada bir test sunucusu yapılandırılmış, sanallaştırma için test sunucusu hazırlanmış, test sunucusunda sanal açık kaynak kodlu güvenlik duvarlarının kullanılabilmesi için gerekli olan kurulum ve yapılandırma işlemleri açıklanmıştır. Ayrıca sanal Pfsense güvenlik duvarı kurulmuş, test sunucusuna Windows sanal makineleri kurulmuş, kullanıcı bilgisayarlarının ağ yapılandırması gerçekleştirilmiş, sanal sunucularda trafik ve filtreleme testleri yapılmıştır. Son olarak bu testler kullanıcı bilgisayarlarında da uygulanmıştır.

1.1 Problem

Sanallaştırmanın sunduğu kolaylıklar ve faydalar günümüzde yoğun olarak kullanılan sanallaştırılmış sistemlere olan talebi artırmaktadır. Bu nedenle birçok teknoloji şirketi, endüstriye daha iyi çözümler sunabilmek ve talebi karşılayabilmek amacıyla sanallaştırma üzerinde yoğunlaşmıştır. Üreticiler performans kayıplarını sanallaştırma sistemleri ile en aza indirgeyerek daha basit, daha kararlı ve daha az yer tutacak çözümler üzerinde çalışarak kaynaklardan en fazla verimi üreten teknolojilere odaklanmışlardır (Doğru, 2019).

Sunucu sistemlerinde kullanılan sunucu donanımları teknolojinin gelişmesiyle her geçen gün değişmekte ve bu değişimlerle birlikte donanımların düzenli olarak güncelleştirilmesi gerekmektedir. İşletmelerin ve kurumların sistemlerinde kullanılan güvenlik duvarları;

sunucular üzerinde çalışan donanım ile yazılımın birleştirilmiş halde sunulduğu sistemlerdir. Üretici firmalara hem yazılım hem de donanım için ayrı ayrı fazla ücretler ödenmektedir. Hem donanım hem de yazılım için ayrı ayrı ödemeler yapılan güvenlik duvarlarında, donanımlar teknolojik gelişmelerin, sistemin gereksinimlerinin ve zamanın gerisinde kalmakta bu yüzdende ihtiyaçları karşılayamamaktadır.

Bilişim sistemlerinde kullanılan güvenlik duvarlarında donanım ve yazılım birbirine entegre şekilde kullanılmaktadır. Bütünleşik kullanılan güvenlik duvarlarının en büyük dezavantajı yazılımların upgrade (yazılım güncellemesi) edilirken donanımsal olarak kaynakların kullanılan süre içerisinde yetersiz kalması ve bunların upgrade edilememesidir.

Sanallaştırılmış sistemler kullanılarak oluşturulacak güvenlik duvarlarında kullanılacak donanım elimizde bulunan fiziksel sunucudan karşılanmaktadır. Bu sayede güvenlik duvarı için ihtiyaç duyulacak tüm kaynaklar sanallaştırma sistemi içerisinden ihtiyaçlar ve gereksinimlere bakılarak teknolojik olarak artırılıp azaltılabilmektedir.

Ticari yazılımlar için üreticilere yazılımın kullanım bedeli olarak lisans ücretleri ödenmekle birlikte teknik destek içinde belirli aralıklarla ödeme yapılmaktadır. Açık kaynak kodlu yazılımlar ise genellikle yazılım için ücret ödenmeden kullanılabilmektedir. Açık kaynak yazılımları, kullanıcılarının isteği doğrultusunda sadece teknik desteğe yapılan ödeme karşılığında kullanılabilmektedir.

Yapılan araştırmalar sonucu açık kaynak kodlu sanal güvenlik duvarları Türkiye'de neredeyse hiç çalışılmamış olup nispeten dünya genelinde de az çalışılmıştır. Çalışmamızda açık kaynak kodlu sanallaştırılmış güvenlik duvarlarının tanıtılması, yaygınlaştırılması ve çalışma olarak sunulması hedeflenmiştir.

1.2 Amaç

Bu araştırmada açık kaynak kodlu sunucu sanallaştırma teknolojilerinin güncel yazılım ve donanımlara gerek kalmadan çalıştırılabilmesi hedeflenmiştir.

Araştırmamızda açık kaynak kodlu güvenlik duvarlarının sanallaştırma sistemleri ile birlikte kullanılarak sistemlerin güvenli bir şekilde çalışması ve aynı zamanda da düşük

maliyetlerle kullanılabilmesi amaçlanmaktadır. Çalışmamızın diğer bir amacı da ülkemizde çalışılmamış olan bir konunun literatüre kazandırılmasıdır.

Bu araştırma, açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanımı konusunun anlaşılmasını ve kavramsallaştırılmasını kolaylaştırarak bundan sonra yapılacak çalışmalara ışık tutacaktır.

1.3 Önem

Bu çalışmada yapılan araştırmalar ışığında elde edilen verilerle, açık kaynak kodlu güvenlik duvarlarının var olan sistemlerimizde kaynak paylaşımı yapılarak kullanılması önem arz etmektedir. Oluşturulan sanallaştırma sistemi, kaynak paylaşımı ve açık kaynak kodlu güvenlik duvarı sayesinde lisans ve donanım ücreti ödemeden sistemleri güvenli hale getirebilmektedir.

Ayrıca güvenlik duvarları sistemlere dahil edilirken kullanıcı sayıları ve bant genişlikleri dikkate alınarak güvenlik duvarlarının donanım özellikleri belirlenmektedir. Bu belirlenen özelliklere göre güvenlik duvarlarının sistemde yöneteceği oturumlar hesaplanmaktadır. Ticari güvenlik duvarlarında lisanslamalar kullanıcı sayıları dikkate alınarak oluşturulmaktadır. Bu nedenle kullanıcı sayılarını belirleyen en önemli etken donanım özellikleridir. Güvenlik duvarı yazılımı değiştirilmeden farklı donanımlar üzerine yerleştirilerek kullanıcılara çeşitli ürünler sunulabilmektedir. Çalışmada sanallaştırma sistemlerinde oluşturulan sanal makineler ile kaynaklar istenildiği gibi kullanılabildiği için kullanıcı sayılarında ve güvenlik duvarlarında oluşturulmak istenen oturumların adedine göre istenilen donanıma sahip cihazlar elde edilmektedir. Yapılan çalışmanın önemlerinden biri de sistemlerde esneklik sağlayan bu özelleştirmelerle aynı yazılım ve donanımla yapılandırmalar yapılarak sistemlerin daha büyük ölçekli gereksinimlerinde de ihtiyacı karşılayacak durumda olabileceğinin gösterilmesidir.

Kurum ve işletmelere katkı sağlayacak olan bu araştırma yıllık ödenen lisans ve teknik destek ücretlerinin yanı sıra sistemlerde kullanılan bilgisayar donanımlarını güncellemek için katlanılan maliyetleri de ortadan kaldırmaktadır. Ayrıca kurum ve işletmeleri güvenlik için ödenen ekstra maliyetlerden de kurtarmaktadır.

1.4 Varsayımlar

Çalışma, yapılan literatür araştırması sonucunda elde edilen veriler ışığında uygulanmıştır. Uygulama için oluşturulan laboratuvar ortamlarından elde edilen ve teoride var olan veriler ile bu araştırma tamamlanmıştır. Araştırma sonuçları açık kaynak kodlu sistemlerin sanallaştırılmış sistemlerde kullanılabileceğini göstermektedir.

1.5 Sınırlıklar

Araştırmada; sanallaştırma sistemleri, güvenlik duvarları, ağ sistemleri, ağ güvenliği ve açık kaynak kodlu güvenlik duvarları gibi anahtar kelimelerin yer aldığı tez çalışmaları ve yayımlanmış makaleler incelenmiştir. Bu çalışma için YÖK Ulusal Tez Merkezi, Dergipark, Maltepe Üniversitesi ve Ardahan Üniversitesi'nin kütüphane veri tabanı sisteminde bulunan yayınlar içerisinden araştırmalar örnek alınarak çalışma yapılmıştır.

Hipervizör yazılımı olarak açık kaynak kodu Virtualbox, işletim sistemi olarak Windows Server 2022, açık kaynak kodlu güvenlik duvarı yazılımı olarak Pfsense kullanılmıştır.

1.6 Tanımlar

Sunucu sanallaştırma teknolojisi, en az bir fiziksel sunucu üzerinde birden fazla sanal makine çalıştırarak uygulama ve servislerin daha etkili bir şekilde yönetilmesini sağlamaktadır. Bu teknoloji, merkezi yönetim, otomatikleştirilmiş operasyonlar, yüksek erişilebilirlik ve hata toleransı gibi avantajlar sunmaktadır (Büyükyılmaz, 2016). Sunucu sanallaştırma, bir fiziksel sunucunun kaynaklarından CPU, RAM, Hard Disk ve Network Adapter gibi donanımların birden fazla sanal makineye paylaştırılarak aynı anda ve izole bir şekilde kullanılmasını sağlayan bir teknolojidir.

Günümüz bilişim dünyasında, bu yaklaşım geleneksel sistemlere göre maliyet, yönetim, erişilebilirlik ve esneklik konularında önemli avantajlar sunmaktadır (Yuusuf ve Vidalis, 2012). Özgür yazılım ve açık kaynaklı yazılım terimi, yazılımın kaynak kodunun incelenmesine, kullanılmasına, değiştirilmesine ve yeniden dağıtılmasına izin veren bir lisans altında yayınlanan yazılımı ifade etmektedir (Crowston, Wei, Howison, ve Wiggins, 2008). Sistemlerin güvenliğini artırmak için önemli bir unsuru oluşturan güvenlik duvarları, ağ güvenliğini sağlamak amacıyla kullanılan kritik bileşenlerden biri

olarak ifade edilmektedir. Güvenlik duvarları, bir ağı dışarıdaki ağlardan izole etmek ve bir tür duvar işlevi görmek üzere tasarlanmış ağ güvenlik sistemleridir. Genel olarak, donanımsal ve yazılımsal olmak üzere temelde iki farklı türde güvenlik duvarı bulunmaktadır (IBM, 2022).

2. LİTERATÜR ARAŞTIRMASI

Araştırma doğrultusunda yapılan literatür taraması sonucunda açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanılması hakkında literatürde sınırlı sayıda çalışmanın var olduğu gözlemlenmiş olmasına rağmen Türkiye'de yapılmış bir çalışmaya rastlanılmamıştır.

Xianqin ve diğerleri (2009) tarafından yapılan çalışmada, NSE-H tabanlı sanal bilgi işlem ortamında mevcut canlı geçiş uygulamasının tam olarak şeffaf canlı geçişi sağlamadaki yetersizliğine odaklanılmıştır. Araştırmada, mevcut uygulamanın sanal makinede kapsanan durumu tam olarak ele almadığı ve güvenlik bağlam kümesini ihmal ettiği belirtilmiştir. Bu eksiklikleri gidermek amacıyla, sanal makinenin durumu ve güvenlik bağlamı göz önüne alınarak bir çerçeve önerilmiştir. Önerilen çerçeve, mevcut açık kaynak araçlarını paketleyerek ve değiştirerek Linux ayrıcalıklı etki alanı tarafından yönetilen Xen hipervizörü üzerinde bir prototip sistem olarak uygulanmıştır. Çalışma, önerilen çerçevenin sorunları çözdüğünü işlev testleriyle göstermiş ve performans testleriyle ise kesinti süresinin yalnızca %15 civarında arttığını belirtmiştir (Xianqin, Han, Sumei, ve Xiang, 2009).

Basak ve diğerleri (2010), vShield Firewall ve Edge kullanarak güvenlik sanal gereçleri içindeki netsec işlevlerini sanallaştırmanın sektördeki eğilimini analiz etmişlerdir. VShield'in dağıtılmış ölçeklendirme mimarisine yeni güvenlik sanal gereçleri eklenmesi, performansın doğrusal olarak artabileceği veya azalabileceği bir durumu işaret ederken, aynı zamanda sanal makine klonlama, şablondan dağıtma ve sanal makine yüksek kullanılabilirliği gibi temel sanallaştırma ilkelerinden faydalanarak bu güvenlik sanal gereçlerinin yaşam döngüsü yönetimini basitleştirdiklerini göstermişlerdir. VShield Güvenlik Duvarı ve Edge'in veriminin fiziksel cihazlarla karşılaştırılabilir olduğunu, isteğe bağlı ölçek büyütme esnekliği ve CPU kaynaklarının yalnızca ihtiyaç duyulduğunda kullanıldığını belirtmişlerdir.

Ayrıca çalışmalarında, sanallaştırılmış netsec ile bulutta sanal bir veri merkezinin, fiziksel veri merkezlerinde günler/haftalar içinde kurulmasına kıyasla dakikalar içinde

kurulabileceğini göstermişlerdir. Araştırmada fiziksel dünyada mümkün olmayan ek güvenlik denetimlerinin sanal dünyada gerçekleştirilebileceğini sunmuşlardır. Sonuç olarak şu anda güvenlik duvarları gibi donanım aygıtları biçiminde olan güvenlik işlevlerinin sanallaştırılması ihtiyacını da çalışmalarında belirtmişlerdir. VMware vShield sanal güvenlik duvarının sanal makineyi güvence altına aldığını ve vMotion protokolünün koordinasyonu ile güvenli geçişin gerçekleştirilmesine yardımcı olduğunu göstermişlerdir (Basak, Toshniwal, Maskalik, ve Sequeira, 2010).

Wu ve diğerleri (2010) yapmış oldukları çalışmada, güvenliğin; bulut bilişimde kullanıcıların en önemli endişesi olduğunu belirterek bulut platformlarının kilit teknolojisi olan sanal ağın güvenliğine odaklanmışlardır. Çalışmalarında Xen analizine dayanarak, fiziksel makinelerde konuşlandırılan sanal makineler arasındaki iletişimin güvenliğini artırmak için yeni bir sanal ağ çerçevesi önermişlerdir. Önerdikleri güvenlik duvarının özellikleri, belirtilen alt ağlar ve yönlendirme tablosu, sanal makineleri teoride koklama ve yanıltma gibi saldırılara karşı etkili bir şekilde engelleyebilmesidir (Wu, Ding, Winer, ve Yao, 2010).

Xu ve diğerleri (2011) tarafından gerçekleştirilen çalışmada, büyük ölçekli geniş alan ağı üzerinde IaaS'nin dinamik provizyonuna uyum sağlayabilen ve performans odaklı bir ağ sanallaştırma modeli olan WAVNet geliştirilmiştir. Araştırmada, WAVNet'in NAT/güvenlik duvarlarının arkasındaki tüm ana bilgisayarlar için uygulama paketlerini tünelleyen bir bağlantı katmanı sanal ağı sağladığı ve kullanıcıların mevcut fiziksel bant genişliğini minimum maliyetle kullanmalarına olanak tanıyan bir randevu katmanı (CAN katmanı) üzerinden keşfedilen kaynaklar arasında doğrudan ana bilgisayardan ana bilgisayara bağlantı sağladığı ifade edilmiştir.

Çalışmada, kullanıcıların WAVNet ile birlikte mevcut kaynakların sayısını artırabilecek veya azaltabilecek kendi sanal kümelerini oluşturabildikleri belirtilmiştir. Ayrıca, büyük ölçekli bulut sistemleri için önemli olan kesintisiz WAN (Geniş Alan Ağı) tabanlı sanal makine geçişinin, WAVNet üzerinde uygulanabildiği gösterilmiştir (Xu, Di, Zhang, Cheng, ve Wang, 2011).

Anwar (2013) yaptığı çalışmada, sanal makinelerin taşınması için ek bir güvenlik katmanı olarak açık kaynak paket filtreli güvenlik duvarını kullanarak sanal makine düzeyinde

sanal güvenlik duvarı oluşturmanın potansiyelini araştırmıştır. Çalışmada küçük ve büyük kuruluşlar, düşük işletme maliyetleri ve iş çevikliğindeki artış nedeniyle sanallaştırma sistemlerini kullandıklarından bahsetmektedir. Oluşturulan bu sistemler içerisinde sanallaştırılmış makinelerin birbirlerinin güvenliklerini tehdit etmemeleri için sanal güvenlik duvarı kullanmanın hatta açık kaynak kodlu sanal güvenlik duvarı kullanmanın öneminden bahsetmektedir. Çalışma, bulut bilişim'de sanal makine monitörü düzeyindeki güvenlik duvarına ek olarak sanal makine geçiş güvenliği ve genel olarak sanal makine güvenliği için sanal makine düzeyinde açık kaynak sanal güvenlik duvarı (virtual firewalls) kullanma anlayışını vurguladı. Böyle bir yaklaşımın kullanılmasının, ağ üzerinde ek bir güvenlik çevre katmanı ve özelleştirilmiş ve derin güvenlik sağlanması gibi sanal makineler için muhtemelen gelişmiş güvenlik sağlayacağı sonucuna varılmıştır. (Anwar, 2013).

Erdem ve Kocaoğlu (2014) tarafından geliştirilen DIFA (Dynamic Intelligent Firewall Architect), geleneksel güvenlik duvarı mimarilerinden tamamen farklı bir yaklaşım sunan bir güvenlik duvarı mimarisidir. DIFA, kendi kendisini yönetebilme yeteneğine dayanarak benzersiz bir yapı sunmaktadır. Bu mimari, trafiği analiz etmekte, yerel alan ağını taramakta ve erişim kurallarını otomatik olarak oluşturmaktadır. Korunan ağdaki yapısal değişiklikleri tespit ederek gerekli yapılandırmaları otomatik olarak gerçekleştirebilmektedir. Ağ yöneticisinin müdahalesine sadece kontrol amaçlı ihtiyaç duymaktadır. DIFA'nın verimliliği gerçek ağ ortamlarında test edilmiş ve elde edilen sonuçlar, DIFA'nın kural oluşturma işlemini başarılı bir şekilde gerçekleştirebildiğini göstermiştir (Erdem ve Kocaoğlu, 2014).

Bakker ve diğerleri (2016) tarafından yapılan çalışmada, geleneksel güvenlik duvarlarının ağ içindeki sınırlarda güvenlik ilkelerini uygulamak için kullanıldığı ve bu güvenlik duvarlarının, ana bilgisayarları parçası oldukları ağdan kaynaklanan saldırılara karşı savunmasız bırakabileceği vurgulanmaktadır. Çalışmada, ağ altyapısını sanal bir güvenlik duvarına dönüştürmek amacıyla yazılım tanımlı ağın esnekliğinden yararlanılmıştır. Araştırma, OpenFlow anahtarlarından oluşan bir ağdaki trafiği filtrelemek için OpenFlow protokolünü kullanan ve ağ genelinde güvenliği artırmak amacıyla tasarlanmış ACLSwitch adlı ağ çapında bir sanal güvenlik duvarının önemini

vurgulamaktadır. Bu yaklaşım, geleneksel güvenlik duvarlarının kısıtlamalarını aşarak ağ güvenliğini artırmayı hedeflemektedir. (Bakker, Welch, ve Seah, 2016).

Datta ve diğerleri (2018) yaptıkları çalışmalarında, P4Guard protokolden bağımsız ve platformdan bağımsız yazılım tabanlı güvenlik duvarını kullanarak sanallaştırılmış sistemlerde ağ işlevine dayalı bir güvenlik duvarı kullanarak nasıl tasarım yapılması gerektiğini anlatmaktadırlar. Tasarlamış oldukları yeni yazılım güvenlik duvarını, VNGuard ile karşılaştırmışlardır. Deneysel sonuçları, P4Guard'ın paket boyutu küçük olduğundan daha hızlı paket işleme süresi ve daha düşük ağ gecikmesi olduğunu göstermiştir (Datta, Choi, Chowdhary, ve Park, 2018).

3. MATERYAL ve YÖNTEM

Bu araştırmada literatür taraması yapılarak Türkiye'de ve dünyada açık kaynak kodlu güvenlik duvarlarının sanallaştırması sistemleri ile ilgili yapılmış çalışmalar içerik analizi yöntemiyle araştırılmıştır. Dijital teknoloji alanında yaygın olarak kullanılan, nicel ve nitel yöntemlerle gerçekleştirilen bir analizler topluluğu olan içerik analizi; Son yıllarda, dijital içeriklerin optimize edilmesi ve geniş bir kullanıcı kitlesine ulaştırılması konularında büyük fayda sağlayan bir yöntem olarak öne çıkmaktadır. İçerik analizi yöntemi kullanılarak ulaşılan bu veriler, ortaya çıkarılan içeriklerin başka kullanıcı ağılarına erişmesini sağlamaya yaramaktadır (Çalık ve Sözbilir, 2014). Ayrıca sanallaştırılmış sistemlerde kullanılabilen açık kaynak kodlu güvenlik duvarları ile alakalı bir araştırma eldeki sistem ve donanımlarla geliştirilmiştir. Elde edilen bulgular ışığında sanallaştırılmış sistemlerde kullanılan açık kaynak kodlu güvenlik duvarları ile ilgili ayrıntılı bir çalışma yapılmıştır.

3.1 Sunucu Sanallaştırma

Bulut bilişimin (Cloud Computing) temel prensibi, bilişimin tek bir yerel bilgisayar yerine çok sayıda dağıtılmış bilgisayara (sanal makineler) atanmasıdır. Sanal makine, donanım bileşenleri ile son kullanıcı arasındaki bir soyutlama katmanı veya ortamıdır (Kreuter, 2004). Son kullanıcı artık belirli bir fiziksel sistemin hazır olmasını beklemek zorunda değildir; tüm gereksinimleri desteklemek üzere yapılandırılmış çeşitli sanal makinelere, gerçek bir sistemin maliyetinin neredeyse beşte biri kadar bir maliyetle kolayca erişebilmektedir (Patel, Patel, ve Parmar, 2018). Her biri bir işletim sistemine sahip gerçek bir bilgisayar gibi davranan sanal makineler, temeldeki fiziksel makineler üzerinde oluşturulmaktadır. Bu tür bir sanallaştırmayla, kaynaklar ince ayrıntı düzeyiyle planlanabilmekte ve bu kaynak kullanımını önemli ölçüde artırılabilmektedir. Aynı zamanda, sanal makineler fiziksel kaynakları paylaşsa da, her sanal makine özel bir kaynakla ayrı ayrı çalışmakta ve bu şekilde sağlanan hizmetin kalitesini garanti etmeyi mümkün kılmaktadır (Li, Qian, Lu, ve Wu, 2013).

Sanallaştırma, bulut bilişimin ortaya çıkmasına yardımcı olan bulut bilişimin ana bileşenlerinden biridir. Sanallaştırma, yazılımın aynı sunucu üzerinde aynı anda birden fazla işletim sistemi ve birden fazla uygulama çalıştırmasını mümkün kılmaktadır. Sanallaştırma; sunucuların, iş istasyonlarının, depolama ve diğer sistemlerin fiziksel donanım katmanından bağımsız olmasını sağlamaktadır (Khajehei , 2014). Sunucu sanallaştırma, kullanıcılara internet veya özel ağlar üzerinden bilgi işlem kaynakları ve hizmetleri sağlayan bulut bilişim hizmetleri için de temel bir yapı taşı olarak kullanılmaktadır.

Bulut bilişim hizmetlerinin kullanıcıları, gerektiğinde sağlanan kullanıcı ara yüzleri aracılığıyla sanal makineleri kolayca talep edebilmekte ve kullanabilmektedir (Machida, Kim, ve Trivedi, 2013). Kaynak kullanımını artırmak için kullanılan önemli teknolojilerden biri sunucu sanallaştırmadır. Sunucu sanallaştırması, kaynak kullanımını artırmanın ve hizmet kalitesini artırmanın etkili bir yoludur (Li, Qian, Lu, ve Wu, 2013).

3.1.1 Sunucu sanallaştırma sistemleri

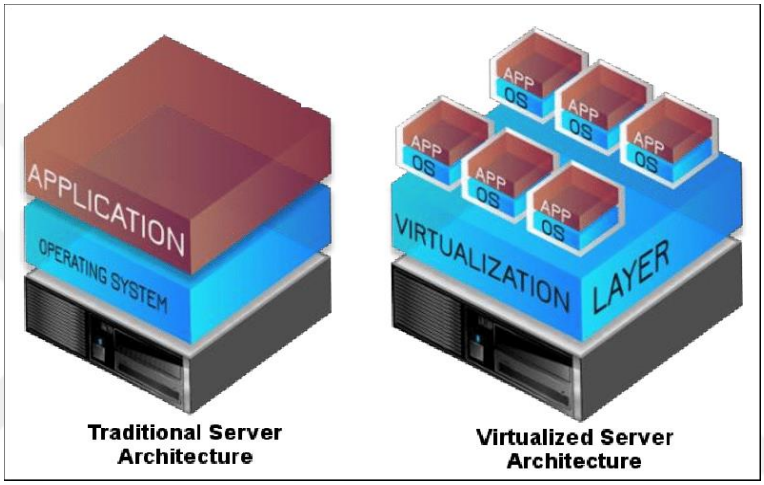
Sanallaştırma yazılımı, açık kaynak ve uygulamaları fiziksel ortamdan soyutlamakta, üzerinde çalıştığı donanımı ve kaynakları sanal makinelere tahsis etmekte, bu kaynakları sanal kaynaklar olarak yönetmekte ve paylaştırmaktadır. Bu yazılımlar hipervizör olarak bilinmektedir. Bilinen hipervizör yazılımlarından bazıları, KVM, ESX(i), Hyper-V, XenServer ve PowerVM'dir (Wikipedia, 2022).

Sanallaştırma yazılımları; açık kaynak kodlu ve ticari yazılımlar olmak üzere iki sınıfta incelenmektedir. Açık kaynak kod mantığı ve lisansı ile dağıtılan bu yazılımlar başlıca VirtualBox, Xen, Bochs, CoLinux, FAUmachine, Hercules emulator, KVM, LilyVM, QEMU, SheepShaver, Oracle VM Virtual Box olarak sıralanabilmektedir. Ticari anlamda başlıca kullanılan yazılımlar ise VMware, Microsoft Virtual PC, VM/CMS, Parallels Workstation, vThere, Parallels Desktop for Mac, SVISTA, Trango, Virtual Iron Software, Microsoft Hyper-V olarak gösterilebilmektedir (Demircioğlu, 2023).

3.1.2 Sunucu sanallaştırma yapılandırması

Sunucu sanallaştırma teknolojisi, bilgisayar sistemlerini fiziksel donanımlardan soyutlama prensibi üzerine kurulmaktadır. Bu teknoloji, donanımsal kaynaklardan en

etkin şekilde yararlanmayı amaçlamakta, böylece sistem odasında kullanılan donanım sayısını azaltılarak kullanılmasına ve azalan insan gücü ihtiyacına bağlı olarak maliyetlerin düşürülmesine olanak tanımaktadır (Büyükyılmaz, 2016). Sunucu sanallaştırma teknolojisi, hipervizör adı verilen bir yazılım katmanı aracılığıyla çalışmaktadır. Hipervizör, fiziksel donanım üzerinde sanal makinelerin oluşturulmasını ve yönetilmesini sağlamaktadır. Hipervizörün görevi, fiziksel sunucunun bir sanallaştırma ana bilgisayarı olarak işlev görmesini sağlamaktır. Bu sanal makineler, bağımsız işletim sistemleri ve uygulamaları çalıştırabilmektedirler (Posey, 2022).



Şekil 3. Geleneksel Sunucu Mimarisi ve Sanallaştırılmış Sunucu Mimarisi

Şekil 3'te görüldüğü gibi geleneksel sunucu mimarisinden farklı olarak bir fiziksel sunucu ile birden çok sunucu elde edilmesi amaçlanmaktadır (Patel, Patel, ve Parmar, 2018). Sanallaştırma yapısında bir adet fiziksel sunucu, fiziksel sunucu üzerine kurulacak bir adet sunucu işletim sistemi, hipervizör olarak bir adet sanallaştırma yazılımı ve sanal makinelerden kullanılacak işletim sistemi yazılımları bulunmaktadır.

3.1.3 Sunucu sanallaştırma avantajları

Sunucu sanallaştırma mimarisini oluşturmak ve elde edilen avantajları etkili bir şekilde kullanabilmek için, çeşitli unsurların entegre edilmesi ve doğru bir tasarımın yapılması gerekmektedir. Sunucu sanallaştırma mimarisi, temelde fiziksel donanımlardan ve bu donanımları sanallaştırarak kaynakların paylaşımını mümkün kılan yazılımlardan oluşmaktadır. Bu yaklaşım, sistemlerin daha verimli ve esnek bir şekilde yönetilmesine,

donanım kaynaklarının daha etkin kullanılmasına olanak sağlamaktadır (Büyükyılmaz, 2016).

Bulut hizmetlerine olan talebin artması nedeniyle, bulut sistemlerinin performansını, kullanılabilirliğini ve güvenilirliğini artırmak için kaynak tüketiminin optimizasyonu daha da önemli hale gelmektedir. Sanallaştırma teknolojilerinin bu gereksinimleri karşılamada oldukça faydalı olduğu kanıtlanmıştır (Çavdar, Korpeoglu, ve Ulusoy, 2024). Sunucu sanallaştırmanın avantajları arasında; kaynak kullanımı optimizasyonu, esneklik, maliyet tasarrufu, hızlı dağıtım, yedekleme ve kurtarma kolaylığı sayılabilmektedir. Kaynak kullanımı optimizasyonunda; fiziksel sunucunun kaynakları birden çok sanal sunucu arasında paylaştırılabilmektedir. Bu sayede donanım daha etkili bir şekilde kullanılmaktadır. Esneklik avantajında; sanal sunucuların dinamik olarak oluşturulması, kaldırılması veya taşınması mümkün olmaktadır. Bu, iş yüklerini daha iyi yönetmeyi sağlamaktadır. Maliyet tasarrufunda; fiziksel sunucuların sayısını azaltmak, enerji tüketimini düşürmek ve bakım maliyetlerini azaltmak gibi faktörler maliyetleri düşürebilmektedir. Hızlı dağıtımda ise; sanal makineler hızlı bir şekilde oluşturulabilmekte, bu da yeni uygulamaların veya hizmetlerin hızla dağıtılabilmesine olanak tanımaktadır. Yedekleme ve kurtarma kolaylığında; sanal makinelerin yedeklenmesi ve kopyalanması daha kolay olmakta, bu da veri koruma ve kurtarma süreçlerini iyileştirmektedir (Ersever, Doğru, ve Dörterler, 2017).

Önde gelen sunucu sanallaştırma platformları arasında VMware vSphere/ESXi, Microsoft Hyper-V, KVM (Kernel-based Virtual Machine) ve Xen bulunmaktadır. Bu teknolojiler, genellikle büyük veri merkezleri, işletmeler ve bulut hizmet sağlayıcıları tarafından yaygın olarak kullanılmaktadır.

3.2 Güvenlik Duvarı

Güvenlik duvarları (firewall) kurumsal güvenliğin temel dayanağıdır ve özel ağların korunmasında en yaygın olarak benimsenen teknolojidir. Güvenlik duvarları, özel ağlar ile dışarıdaki internet arasındaki giriş noktasına yerleştirilen güvenlik önlemleridir. Gelen ve giden tüm veri paketlerini denetleyen bir güvenlik görevlisi olarak işlev görmektedirler. Her bir paket, kaynak ve hedef IP (İnternet Protokol) adresleri, kaynak ve hedef bağlantı noktası numaraları ve protokol türü gibi sınırlı sayıda alana sahip bir

demet olarak ifade edilebilmektedir. Güvenlik duvarları, bu paketlerin içerdikleri alan değerlerini inceleyerek, kendi yapılandırmalarına uygun meşru paketleri kabul etmekte ve meşru olmayanları reddetmektedir. Bu yapılandırma, güvenlik duvarının politikalarını belirlemekte ve hangi tür trafiğin izin verildiğini, hangi türün engellendiğini belirlemektedir. Bu şekilde, güvenlik duvarları, ağın güvenliğini sağlamak ve yetkisiz erişimi önlemek için etkili bir kontrol noktası olarak görev yapmaktadır (Liu ve Gouda, 2008).

Güvenlik duvarları genellikle şu temel özellikleri sağlar:

- Paket Filtreleme (Packet Filtering): Ağ trafiğini paket seviyesinde inceleyerek, belirli kurallara göre paketleri kabul etme veya reddetme yeteneğine sahiptir.
- Durum Tabanlı İnceleme (Stateful Inspection): Paket filtrelemenin ötesine geçen, ağ trafiğini bir bağlantının durumunu izleyerek değerlendiren bir yöntemdir.
- Proxy Hizmetleri: İstemci ve sunucu arasında bir ara hizmet olarak çalışarak, iç ağdaki kullanıcıların doğrudan internete erişimini sınırlayabilmektedir.
- Ağ Adresi Çevirisi (NAT): İç ağdaki özel IP adreslerini dış ağdaki genel IP adresiyle eşleştirmek, ağdaki cihazların gerçek IP adreslerini gizlemek amacıyla kullanılmaktadır.
- Sanal Özel Ağ (VPN) Desteği: Güvenli bir şekilde uzaktan erişim sağlamak ve şifrelenmiş iletişim kurmak için kullanılan VPN protokollerini desteklemektedir.
- Günlükleme ve İzleme: Olayları kaydetme, izleme ve günlükleri inceleme yeteneği ile ağ güvenliği olaylarını tespit etmektedir.

3.2.1 Donanım tabanlı ve yazılım tabanlı güvenlik duvarı

Donanım tabanlı güvenlik duvarları, özel donanım cihazları olarak çalışmakta ve genellikle ağın giriş ve çıkış noktalarına konumlandırılmaktadırlar. Bu cihazlar, ağ trafiğini izlemek, filtrelemek ve yönlendirmek için tasarlanmış özel bir donanım üzerinde çalışan yazılımlar içermektedir. Bilgisayar işletim sistemine entegre değildir ve genellikle bağımsız bir cihaz olarak çalışmaktadır. Geleneksel donanım tabanlı güvenlik duvarları işleyebilecekleri maksimum trafik miktarına göre sabit bir kapasiteye sahiptirler (Li, ve diğerleri, 2017). Fakat özel tasarlanmış donanım parçalarını kullanarak ağ trafiğini hızlı bir şekilde işleyebilmektedirler. Modern güvenlik duvarları genellikle donanımsaldır ve

yazılım entegre edilmiştir. En büyük dezavantaj bu tür altyapıların en önemli özelliği donanıma bağımlılıkları nedeniyle sınırlıdır (Tümer ve Şahinaslan, 2022).

Yazılım tabanlı güvenlik duvarları, genellikle bilgisayar işletim sistemlerine entegre edilen veya ayrı olarak yüklenebilen yazılımlardır. Bu güvenlik duvarları, ağ trafiğini yazılım düzeyinde kontrol etmekte ve izin verilen veya engellenen bağlantıları belirleyen bir dizi kural setine dayanmaktadır. Yazılım tabanlı güvenlik duvarları genellikle daha esnek ve özelleştirilebilir olabilmektedir, böylece yazılım güncellemeleri veya konfigürasyon değişiklikleri kolaylıkla yapılabilmektedir. Düzenli olarak yazılımların güncellemeleri ve güvenlik açıklarına karşı güncel tutulmaları gerekmektedir (Li, ve diğerleri, 2017).

Yazılım tabanlı güvenlik duvarları, genel ağ güvenliği duvarının bir alt kümesidir. Ağ güvenlik duvarları; genellikle geniş bir kapsama sahiptir ayrıca donanım tabanlı, yazılım tabanlı veya her ikisini de içerebilecek bir dizi güvenlik önleminden oluşmaktadır.

3.2.2 Açık kaynak kodlu ve ticari güvenlik duvarları

Açık kaynak kodlu güvenlik duvarları genel kamu lisansına sahip yazılımlardır. Bu yazılımları kullanmak genellikle ücretsiz olup geliştirmek istenildiğinde geliştirilmeye açık olmaları nedeniyle kullanıcılara avantajlar sunmaktadırlar. Bilişim teknolojilerinde kullanılan açık kaynak kodlu güvenlik duvarlarının popüler olanları Tablo 1'de listelenmiştir.

Tablo 1. Açık Kaynak Kodlu Güvenlik Duvarları

Güvenlik Duvarı	Platform	Öne Çıkan Özellikler	Desteklediği Protokoller
pfSense	FreeBSD tabanlı	Web tabanlı ara yüz, paket filtreleme, NAT, VPN desteği	TCP/IP, UDP, ICMP, GRE, IPsec, OpenVPN
OPNsense	FreeBSD tabanlı	Artırılmış Web GUI, Intrusion Detection/Prevention (IDS/IPS)	TCP/IP, UDP, ICMP, IPsec, OpenVPN
iptables	Linux tabanlı	Paket filtreleme, NAT, bağlantı izleme, güçlü komut satırı ara yüzü	TCP/IP, UDP, ICMP, GRE
Smoothwall	Linux tabanlı	Web tabanlı ara yüz, trafik analizi, içerik filtreleme, VPN desteği	TCP/IP, UDP, ICMP, IPsec, PPTP, L2TP
Untangle	Linux tabanlı	Web tabanlı ara yüz, güvenlik uygulamaları, raporlama, içerik filtreleme	TCP/IP, UDP, ICMP, OpenVPN, IPsec
Endian Firewall	Linux tabanlı	Web tabanlı ara yüz, güvenlik uygulamaları, VPN desteği	TCP/IP, UDP, ICMP, IPsec, OpenVPN
FirewallD	Linux tabanlı	Dinamik kurallar, yönetilebilir profil seçenekleri	TCP/IP, UDP, ICMP
VyOS	Linux tabanlı	Yönlendirme, VPN, Firewall, QoS, MPLS	TCP/IP, UDP, ICMP, GRE, IPsec, OpenVPN
Security Onion	Linux tabanlı	Ağ güvenliği, IDS, NSM, paket analizi, SIEM	TCP/IP, UDP, ICMP
IPFire	Linux tabanlı	Web tabanlı ara yüz, güvenlik uygulamaları, VPN desteği	TCP/IP, UDP, ICMP, IPsec, OpenVPN

Ticari güvenlik duvarları bir firma tarafından oluşturulmuş sistemlerdir. Geliştirme ve destek hizmetleri oluşturulan firma tarafından verilen bu yazılımlar lisans ücretleri alınarak sistemlerde kullanımına izin verilen yazılım ve donanımlar bütünüdür. Bilişim sistemlerinde kullanılan popüler ticari güvenlik duvarları Tablo 2'de listelenmiştir.

Tablo 2. Ticari Güvenlik Duvarları

Güvenlik Duvarı	Platform	Öne Çıkan Özellikler	Desteklediği Protokoller
Cisco Firepower NGFW	Cisco ASA/Firepower Threat Defense	IPS, VPN, Uygulama Kontrolü, Tehdit İstihbaratı	TCP/IP, UDP, ICMP, IPsec, SSL VPN
Fortinet FortiGate	Bağımsız Donanım/FortiGate VM	UTM, IPS, VPN, Antivirüs, Antispam, Uygulama Kontrolü	TCP/IP, UDP, ICMP, IPsec, SSL VPN
Palo Alto Networks NGFW	Palo Alto Networks Hardware	Uygulama Kontrolü, Tehdit İstihbaratı, VPN	TCP/IP, UDP, ICMP, IPsec, SSL VPN
Check Point Security Gateway	Check Point Hardware	UTM, IPS, VPN, Tehdit İstihbaratı	TCP/IP, UDP, ICMP, IPsec, SSL VPN
Sophos XG Firewall	Sophos Hardware/XG VM	UTM, IPS, VPN, Uygulama Kontrolü, Web Filtreleme	TCP/IP, UDP, ICMP, IPsec, SSL VPN
Juniper Networks SRX Series	Juniper SRX Series	VPN, IPS, Güvenlik Hizmetleri, Yüksek Performans	TCP/IP, UDP, ICMP, IPsec, SSL VPN
SonicWall NSA Series	SonicWall Hardware	UTM, VPN, IPS, Güvenlik Hizmetleri	TCP/IP, UDP, ICMP, IPsec, SSL VPN
WatchGuard Firebox	WatchGuard Hardware	UTM, VPN, Güvenlik Hizmetleri	TCP/IP, UDP, ICMP, IPsec, SSL VPN
Barracuda NextGen Firewall F-Series	Barracuda Hardware	UTM, VPN, Güvenlik Hizmetleri	TCP/IP, UDP, ICMP, IPsec, SSL VPN

3.2.3 Güvenlik duvarları ile çalışmak

Güvenlik duvarları, bilgisayar ağlarındaki veri trafiğini denetleyerek istenmeyen ve zararlı içeriklere karşı koruma sağlarlar. Temel amacı, ağa giren ve çıkan veri paketlerini analiz etmek ve bu paketlere dayalı olarak belirlenen güvenlik politikalarını uygulamaktır. Ağ güvenlik duvarları, farklı güvenlik seviyelerine sahip ağlar arasındaki

trafiği kontrol eden cihazlar veya sistemlerdir. Genellikle internet bağlantısı ve TCP/IP protokol paketleri bağlamında ele alınsa da, güvenlik duvarlarının kullanımı sadece internet içeren ortamlarla sınırlı değildir. Örneğin, birçok kurumsal işletme, muhasebe veya personel departmanları gibi hassas işlevlere hizmet veren iç ağlara güvenlik duvarları ekleyerek, bu alanlara yetkisiz erişim önlenmektedir.

Güvenlik duvarları, ağ güvenliğini artırmak amacıyla bağlantıları kontrol ederek ve belirli güvenlik politikalarını uygulayarak işlev gören cihazlar veya sistemlerdir. Bir güvenlik duvarı eklemek, ağın daha hassas bölgelerinde yetkisiz erişimi engelleyerek ek bir güvenlik katmanı sağlamaktadır. Temel güvenlik duvarları genellikle daha az sayıda katman üzerinde çalışmakta, daha gelişmiş güvenlik duvarları daha fazla sayıda katmanı kapsamaktadır. Daha kapsamlı katmanlar, genellikle daha gelişmiş ve etkili bir güvenlik sağlama potansiyeline sahiptir. Kapsamlı ek katmanlar, güvenlik duvarının içerdiği yapılandırma ayrıntı düzeyini artırmaktadır. Böylece güvenlik duvarının daha fazla uygulama ve protokolü inceleyebilmesine olanak tanımaktadır. Katman farkındalığı eklemek, güvenlik duvarının daha gelişmiş uygulamaları ve protokolleri tanıyabilmesine olanak sağlamaktadır. Bu, özellikle günümüzdeki karmaşık ağ trafiği ve tehdit ortamında daha etkili bir koruma sağlamak için önem arz etmektedir. Ayrıca, güvenlik duvarlarının inceleyebileceği katmanları artırmak, kullanıcı kimlik doğrulaması gibi çok kullanıcılı hizmetleri de destekleyebilmektedir. Bu, ağdaki kullanıcıların güvenlik duvarının üzerinden geçerken kimliklerinin doğrulanmasını sağlamaktadır. Uluslararası bilgi güvenliği standardına göre bilgi, kuruluşlar için en değerli varlıktır ve sürekli olarak korunması gerekir (Şahinaslan E. , 2023). Sonuç olarak, çeşitli güvenlik duvarı platformları bulunmaktadır ve bu platformlar ağ ihtiyaçlarına ve güvenlik politikalarına göre farklı seviyelerde katmanlı güvenlik sağlama kapasitesine sahiptir (Wack, Cutler, ve Pole, 2002).

3.2.4 Sanal güvenlik duvarları

Sanal güvenlik duvarları, özellikle bulut bilişim ortamlarında, sanallaştırılmış ağlarda ve genel olarak sanal ortamlarda çalışan sistemlerin güvenliğini sağlamak için yaygın olarak kullanılan bir güvenlik önlemidir. Geleneksel güvenlik duvarları gibi, sanal güvenlik duvarları da ağ trafiğini izleyerek, filtreleyerek ve yönlendirerek ağ güvenliğini sağlamaktadır; ancak bu işlevleri, sanal ortamlardaki sanal makineler, bulut altyapıları ve

sanallaştırılmış ağlar için optimize edilmiştir. Aynı zamanda güvenlik politikaları daha esnek bir şekilde uygulanabilmekte, kaynaklar daha iyi izole edilmekte ve ağ güvenliğinin sanal ortamlara özgü ihtiyaçlara uygun bir şekilde cevap vermesini sağlamaktadır. Sanal güvenlik duvarları, sanal ağlarda veya bulut ortamlarında farklı uygulama katmanları veya kullanıcı grupları arasında trafik izolasyonu sağlamak için kullanılabilmektedir. Ağdaki saldırıların yayılması sınırlandırılmakta ve güvenlik seviyeleri artırılmaktadır. Böylelikle ağ trafiği analiz edilerek, belirli protokol ve portlar kullanılarak iletişim kurmaya çalışan trafik filtrelenebilmektedir. Belirli kurallara dayanarak, izin verilen ve engellenen trafik belirlenebilmektedir. Her bir sanal makine için ayrı ayrı güvenlik politikalarını uygulanabilmektedir. Her bir sanal kaynağın izole bir güvenlik seviyesine sahip olması sağlanmaktadır. Sanal güvenlik duvarları, otomasyon yetenekleri ve esnek konfigürasyon seçenekleri ile entegre edilebilir sistemlerdir. Böylelikle dinamik sanallaştırılmış ortamlarda hızlı ve otomatik tepkiler verebilme yeteneği kazanmıştır. Güvenlik olaylarını izleyebilmekte, günlükleyebilmekte ve raporlar oluşturabilmektedir. Tüm bunlar güvenlik tehditlerini tespit etmede, olayları incelemede ve uyumluluk gereksinimlerini karşılamada önem arz etmektedir (Bakker, Welch, ve Seah, 2016). Sanal güvenlik duvarlarının avantajlarının yanı sıra bazı zorlukları da bulunmaktadır. Potansiyel performans yükü, çok kullanıcılı ortamları yönetme yükü, büyük ölçekli dağıtımlardaki karmaşıklıklar ve güvenlik etkileri bu zorluklar arasında sayılabilmektedir.

3.2.5 Sanal güvenlik duvarları ortamları

Güvenlik duvarı ortamı, ağ üzerinde belirli bir noktada tüm güvenlik duvarı işlevselliğini sağlamaya veya desteklemeye dahil olan sistemler ve bileşenler kümesini tanımlamak için kullanılan bir terimdir. Basit bir güvenlik duvarı ortamı sadece bir paket filtresi güvenlik duvarından oluşabilmektedir. Güvenlik duvarı ortamı daha karmaşık ve güvenli bir ortam sağlamak, sistemleri ve güvenliği desteklemek için birkaç güvenlik duvarı, proxy ve belirli topolojilerden oluşturulmaktadır.

Güvenlik duvarları aynı zamanda VPN ağ geçidi olarak da kullanılabilmektedir. Bu sayede, bir kurum veya organizasyon güvenlik duvarının ardındaki sistemlerden işbirliği yapan bir VPN ağ geçidi üzerinden diğer uzak sistemlere şifrelenmemiş ağ trafiği iletebilmektedir. Güvenlik duvarı, trafiği şifrelemekte ve ardından şifresini çözerek hedef

sistemlere ileten uzak VPN ağ geçidine yönlendirmektedir. Günümüzde, birçok popüler güvenlik duvarı bu tür bir işlevselliği desteklemektedir (Wack, Cutler, ve Pole, 2002).

3.2.6 Sanal olarak kurulabilecek güvenlik duvarları

Güvenlik duvarları kullanımı bütçelere göre değişmektedir. Ticari veya ücretli güvenlik duvarları tamamen gelişmiş özelliklere sahiptir. Bu güvenlik duvarları herhangi bir kullanıcı tarafından kullanabilmektedir, ancak bu hizmetleri kullanmak için ödeme yapılması gerekmektedir. Ticari veya ücretli güvenlik duvarlarına örnek olarak cyberoam ve SonicWALL-Dell gösterilebilir. Ücretsiz veya açık kaynaklı güvenlik duvarları ise serbestçe herkes tarafından kullanılabilen güvenlik duvarıdır. Kullanıcılar kaynak kodunu değiştirebilmekte, hataları bulabilmekte ve raporlayabilmektedirler. Ücretsiz veya açık kaynaklı güvenlik duvarlarına örnek olarak IPFire, IPCop, PFSense, Opsense, Endian, Smoothwall, VyOS, OpenWrt, Untangl ve Shorewall gösterilebilir (Sharma ve Parekh, 2017).

pfSense, FreeBSD (Free Berkeley Software Distribution) tabanlı bir açık kaynak güvenlik duvarı ve yönlendirme platformudur. Güvenlik duvarlarının tüm temel olanaklarını içermektedir. Ayrıca kullanıcıların pfSense içine üçüncü taraf paketleri yüklemelerine izin vermektedir (Kiratsata, ve diğerleri, 2022). PfSense; Netgate tarafından geliştirilmiş olup, ağ güvenliği alanında uzmanlaşmış bir şirket tarafından desteklenmektedir. İlk olarak 2006 yılında m0n0wall projesinin bir çatalı olarak ortaya çıkmıştır ve günümüze kadar aktif olarak geliştirilmiştir. BSD lisansı altında dağıtılan pfSense; kullanım, değiştirilme ve dağıtılma açısından ücretsizdir (Pfsense, 2023).

PfSense, küçük ve orta ölçekli işletmeler ve ev ağları için kapsamlı ağ güvenliğinin yanında yönlendirme işlevselliği de sunmak üzere tasarlanmıştır. Web tabanlı bir GUI aracılığıyla; güvenlik duvarı kuralları, yönlendirme ve ağ hizmetleri gibi konuları yönetmeyi kolaylaştırmaktadır. Çeşitli güvenlik özelliklerini desteklemektedir; bu özellikler arasında paket denetimi, VPN bağlantıları, saldırı tespiti ve önleme, içerik filtreleme gibi fonksiyonlar bulunmaktadır. PfSense'in esnek ve genişletilebilir olması, üçüncü taraf paketler ve eklentilerle DNS, DHCP sunucuları, web proxyleri ve yük dengeleyicileri gibi ek işlevlerin eklenmesine olanak tanımaktadır. Ayrıca gelişmiş yönlendirme protokollerini destekleyerek karmaşık ağ topolojilerinin oluşturulmasına

imkan vermektedir. Bu sayede, pfSense çeşitli ağ güvenliği ve yönlendirme ihtiyaçlarına uygun şekilde yapılandırılabilmekte ve özelleştirilebilmektedir (Ford, Arnold, ve Saniie, 2023).

3.2.7 Sanallaştırılmış bir ortamda sanal güvenlik duvarının rolü

Geleneksel donanım tabanlı güvenlik duvarları genellikle sabit ağ giriş noktalarına konumlandırılmakta ve belirli bir zaman biriminde işleyebilecekleri maksimum trafik miktarına bağlı olarak sabit bir kapasiteye sahip olmaktadırlar. Ancak günümüzdeki yaygın sanallaştırılmış ortamlar, akışkan ağ çevreleri ve önemli ölçüde değişken ağ trafiğine sahiptirler. Bu durum, geleneksel donanım tabanlı güvenlik duvarlarının kullanılmasını zorlaştırmaktadır. Bu nedenle, sanallaştırılmış ortamları korumak için donanım tabanlı güvenlik duvarları kullanmak pratikte zor olmaktadır. Çünkü bu tür ortamlar, sürekli değişen ve büyüyen bir şekilde kaynakları paylaşan sanal makineleri içermektedir. Geleneksel donanım tabanlı güvenlik duvarları, bu dinamik yapıya etkili bir şekilde uyum sağlayamamakta ve ağ trafiğini dinamik bir şekilde yönetmekte zorlanabilmektedir. Bu nedenle, sanallaştırılmış ortamların gereksinimlerini karşılamak için genellikle daha esnek ve ölçeklenebilir sanal güvenlik çözümleri tercih edilmektedir (Li, ve diğerleri, 2017).

Sanallaştırılmış ortamda sanal güvenlik duvarlarının rolü, sanal makine tabanlı ortamlarda ağ güvenliğini sağlamak ve yönetmektir. Bu duvarlar, özellikle sanallaştırılmış altyapılar ve bulut ortamlarında, geleneksel ağ güvenlik duvarlarının yerine geçerek veya onları tamamlayarak görev yapmaktadırlar. Sanal güvenlik duvarları, sanal ağlarda segmentasyonu kolaylaştırarak farklı kullanıcı grupları veya uygulama katmanları arasında trafik izolasyonu sağlamaktadırlar. Protokol, port ve IP adresi tabanlı kurallarla trafiği filtreleyebilmekte, güvenliği artırabilmekte ve istenmeyen erişimleri engelleyebilmektedir. Belirli güvenlik politikalarını uygulayarak sanal ortamdaki kaynakların güvenliğini sağlamaktadır. Sanallaştırma ortamlarındaki dinamik yapıya uyum sağlamak ve taleplere hızlı cevap verebilmek için esnek konfigürasyon seçenekleri sunmaktadırlar. Ayrıca, ağ trafiğini izleyerek olay günlükleri ve raporlar oluşturmaktadırlar. Günümüzde yaygın olarak bulut altyapılarında ve sanallaştırılmış ortamlarda kullanılarak, esnek, etkili ve ölçeklenebilir bir ağ güvenliği sağlamaktadırlar.

3.3 Açık Kaynak Kodlu Yazılım

Açık kaynak yazılım veya özgür ve açık kaynak yazılım, yazılım endüstrisinde ve araştırma topluluğunda yaygın olarak kullanılmaktadır. Çok sayıda geliştirici açık kaynak yazılım projelerine katkıda bulunmakta ve birçok kuruluş açık kaynak yazılım kitaplıklarını yeniden kullanmakta veya ürünlerini açık kaynak olarak sunmaktadırlar (Kapitsak, Tselikas, Kyriakou, ve Papoutsoglou, 2022).

Açık kaynak kodlu yazılım, yazılımın kaynak kodunun genel olarak kamuya açık bir şekilde paylaşıldığı ve kullanıcılara özgürce erişim imkanı tanıyan, telif hakkı sahibinin, yazılımı ve kaynak kodunu kullanıcılara herhangi bir amaç için inceleme, değiştirme, kullanma ve dağıtma izni verdiği bir lisans altında yayınlanan bilgisayar yazılımıdır (IBM, 2022). Bu sayede kullanıcıların yazılımın içyapısını inceleme, değiştirme, geliştirme ve dağıtma özgürlüğüne sahip olmalarına olanak tanınmaktadır. Açık kaynak kodlu yazılımların yayılmasını sağlayan özgür yazılım lisansları, bu özgürlükleri korumak ve yazılımın özgür kalmasını sağlamak amacıyla kullanılmaktadır. Açık kaynak kodlu yazılım modeli, işbirliği, şeffaflık ve özgürlüğü vurgulamaktadır. Öne çıkan örnekler arasında Linux İşletim Sistemi, Apache HTTP Server (Güvenli Metin Aktarma Protokolü), Mozilla Firefox, ve GNU Bash (GNU, Unix Değildir) gibi pek çok yazılım bulunmaktadır.

Özgür yazılımın ilk resmi tanımı FSF (Free Software Foundation) tarafından Şubat 1986'da yayımlanmıştır. Bilgisayar bilimci Richard Stallman, yazılıma erişme, yazılımı değiştirme ve geliştirme becerilerine getirilen sınırlamalardan endişe duyarak özgür yazılım hareketini başlatmıştır (Bessen, 2002). Özgür yazılımlarda programı herhangi bir amaç için çalıştırma özgürlüğü, programın nasıl çalıştığını inceleme ve onu istenildiği gibi yapacak şekilde değiştirme özgürlüğü, çalışma arkadaşlarına yardım edebilmek için yeniden dağıtma ve kopya çıkarma özgürlüğü, programı geliştirme ve iyileştirmelerde (ve genel olarak değiştirilmiş versiyonlarını) tüm topluluğun yararlanacağı şekilde kamuya yayınlama özgürlüğü bulunmaktadır (Anand, Krishna, Tiwari, ve Sharma, 2018).

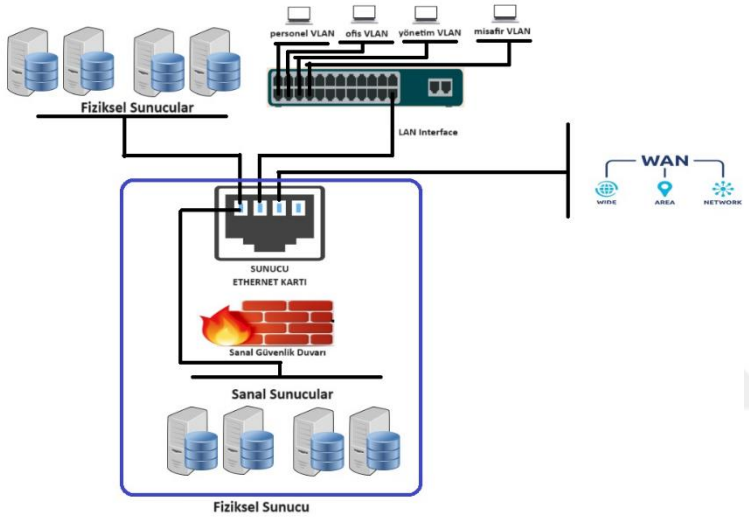
Açık kaynak kodlu yazılım ve özgür yazılım, genellikle benzer kavramlar olarak algılansa da, aralarında bazı temel farklar bulunmaktadır. Açık kaynak kodlu yazılım ile özgür yazılım arasındaki ana farklar:

- Kullanım Özgürlüğü: Kullanıcılar açık kaynak kodlu yazılımı inceleme, değiştirme ve paylaşma özgürlüğüne sahiptir, ancak kullanımını sınırlayan lisanslar da bulunmaktadır. Özgür yazılımda ise, kullanıcıların yazılımı özgürce kullanma, değiştirme, paylaşma ve geliştirme özgürlüğü bulunmaktadır. Özgür yazılım lisansları genellikle kullanıcılara bu özgürlükleri garanti etmektedir.
- Lisanslar: Açık kaynak kodlu yazılım genellikle birçok farklı lisans altında yayınlanabilmektedir. Bu lisanslar, yazılımın nasıl kullanılabileceği ve dağıtılabileceği konularını düzenlemektedir. Özgür yazılım ise genellikle özgür yazılım tanımına uyan lisanslar altında yayınlanmaktadır. FSF'nin GNU Genel Kamu Lisansı (GPL) özgür yazılım için bilinen bir lisans örneğidir.
- Felsefi Yaklaşım: Açık kaynak, genellikle yazılımın kalitesini ve işlevselliğini artırmak için bir geliştirme modeli olarak vurgulanmaktadır. Özgür yazılım ise genellikle kullanıcı özgürlüklerini ve etik konuları vurgulamaktadır. FSF'nin özgür yazılım tanımına göre, özgür yazılım kullanıcıların özgürlüklerini savunmakta ve topluluk dayanışmasını önemsemektedir.
- Topluluk Katılımı: Topluluk katılımı açık kaynak projeleri için önemlidir, ancak projenin yönetimi ve katkıların kabul edilme süreci daha esnek olabilmektedir. Özgür yazılım projelerinde topluluk katılımı genellikle merkezi bir organizasyon tarafından daha sıkı bir şekilde yönetilmekte ve belirli bir felsefi yaklaşımı paylaşan katkıda bulunanları teşvik etmektedir.

Linux'un ilk yaratıcısı Linus Torvalds, yüzlerce gönüllü programcının internet üzerinden ortak yazılım geliştirmeye katılmasını mümkün kılan yeni organizasyon şemalarına öncülük etmiştir. Bu geniş katılımdan, GPL ve diğer lisans anlaşmaları altında geliştirilen yazılımları içeren açık kaynak hareketi ortaya çıkmıştır.

4. BULGULAR VE TARTIŞMA

Araştırmada güvenlik duvarlarının sanallaştırılmış sistemlerde kullanımının mümkün olduğu ve birçok ticari firmanın çalışma yürüttüğü tespit edilmiştir. Ayrıca açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanılabildiği de görülmüştür. Test ortamı Şekil 4'teki gibi planlanmış ve tüm yapılandırma bu plana göre dizayn edilmiştir.



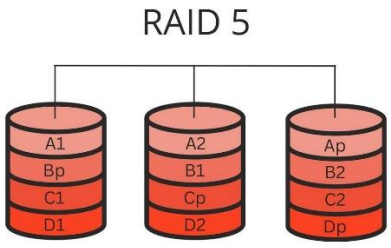
Şekil 4. Sanallaştırılmış Sistemlerde Açık Kaynak Güvenlik Duvarı Kullanımı

Test ortamı sisteminde kullanılan sunucu, 28 çekirdekli CPU (Intel E5 2680) ve 256 GB DDR4 RAM'e sahip olup Hp Dl380 Gen9'dur. Ağ için cisco 2960 layer 2 switch, işletim sistemi olarak Windows Server 2022 Standart Edition ve Windows Server 2022 Datacenter Edition sürümü kullanılmıştır. Sanallaştırma yazılımı olarak Virtualbox 7.0.12 versiyonu ve açık kaynak kodlu güvenlik duvarı olarak Pfsense kullanılmıştır.

4.1 Test Sunucusunun Yapılandırılması

Test sunucusu; özellikleri Şekil 6'da gösterildiği gibi 28 çekirdekli CPU (Intel E5 2680) ve 256 GB DDR4 RAM'e sahiptir. Hp Dl380 Gen9 sunucusunda üç adet 480 GB sas disk RAID 5 yapılarak sunucu işletim sistemi için ortam uygun hale getirilmiştir. Sunucuda

bulunan disk kapasitesi 1440 GB iken Şekil 5'te gösterilen RAID 5 yapılandırması sonucunda 894 GB olarak kullanılmıştır.



Şekil 5. Raid 5 Mimarisi

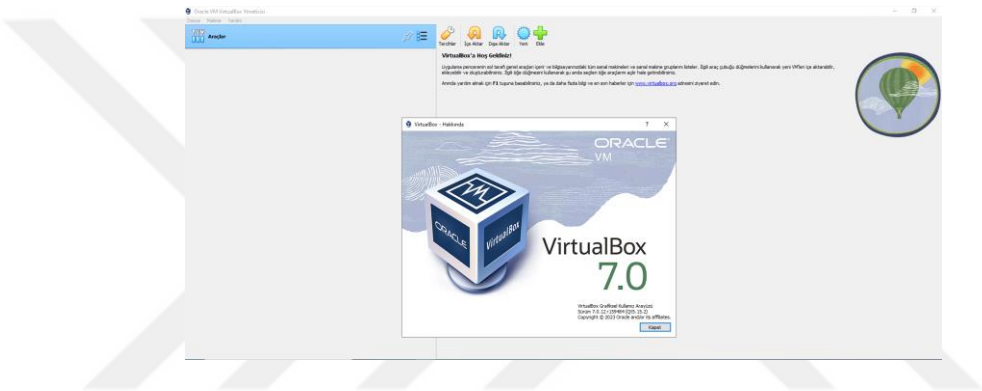
Yapılandırmalardan sonra Windows Server 2022 Datacenter Edition sürümü kurulumu tamamlanmıştır.

Şekil 6. Test Sunucusu Özellikleri

İşletim sistemi kurulumundan sonra gerekli tüm güncellemeler tamamlanmış ve test sunucusu sanallaştırma istemi için gerekli kurulumlar için hazır hale getirilmiştir.

4.2 Sanallaştırma İçin Test Sunucusunun Hazırlanması

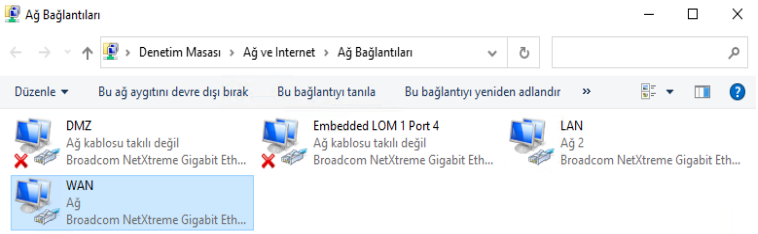
Sanallaştırma sistemi için hipervizör yazılımı kullanılması gerekmektedir. Bu işlem için birçok seçenek bulunmaktadır. Windows sunucularda HyperV tercih edilirken, bilişim sektöründe ücretli ve açık kaynak olarak kullanılabilecek ücretsiz birçok hipervizör yazılımı bulunmaktadır. Hipervizör yazılımlar birbirinden farklı özelliklere sahiptirler. Test ortamında kullanılmaya karar verilen ücretsiz ve açık kaynak kodlu hipervizör yazılımı olan Virtualbox'ın 7.0.12 son versiyonu https://www.virtualbox.org/ sitesinden indirilerek test sunucusuna kurulmuştur. Şekil 7'de. kurulumu gerçekleştirilen hipervizör yazılım ekranı gösterilmiştir.



Şekil 7. Kurulumu Gerçekleştirilen Hipervizör Yazılımı

Kurulum işlemlerinin ardından oluşturulması planlanmış yapıda açık kaynak kodlu güvenlik duvarı kurulumu, güvenlik duvarı yapılandırması, sanal sunucuların oluşturulması, layer2 switch yapılandırması ve son olarak kullanıcı bilgisayarların ağa dahil edilmesi gerçekleştirilmiştir.

Hipervizör yazılımının ağ yapılandırılması Şekil 8'deki isimlendirmelerle WAN, LAN ve DMZ olarak yapılandırılması yapılmıştır. Bu yapılandırma için hipervizör yazılımların sanal anahtar özelliği kullanılmıştır. Sanal anahtar özelliği ile 1. Ethernet port WAN, 2. Ethernet port LAN ve 3. Ethernet portu DMZ olarak yapılandırılmıştır. Bu yapılandırmada test sunucusu WAN portundan ağa bağlanmış, LAN portu ile kullanıcı bilgisayarları için sanal ağlar oluşturulmuş ve DMZ portu ile sanal sunucular için ağ yapılandırılması yapılmıştır.



Şekil 8. Test Sunucusunun Ağ Yapılandırması

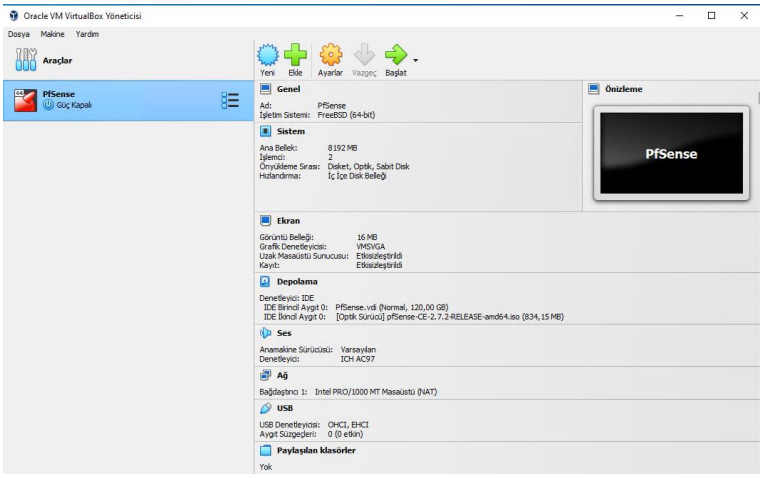
4.3 Test Sunucusuna Sanal Açık Kaynak Kodlu Güvenlik Duvarının Kurulması

Çalışma içerisinde hangi güvenlik duvarı yazılımlarının hangi amaçlarla kullanılabileceği araştırılmıştır. Açık kaynak kodlu güvenlik duvarı yazılımlarından bazıları: Pfsense, Opsense, Iprop, Endian, OpenWrt, IPFire, Untangl, Smoothwall, Shorewall, IPCop ve VyOS'dur. Bu yazılımlar web tabanlı, fiziksel donanım tabanlı ve sanal sistem tabanlı çalışabilmektedir (IBM, 2022).

Bu açık kaynak kodlu yazılımlardan Pfsense güvenlik duvarı yazılımı freeBSD bir yazılımdır. Açık kaynak kodlu bir güvenlik duvarı yazılımı olan freeBSD ticari olarak kullanılabileceği gibi ücretsiz olarak da kullanılabilmektedir.

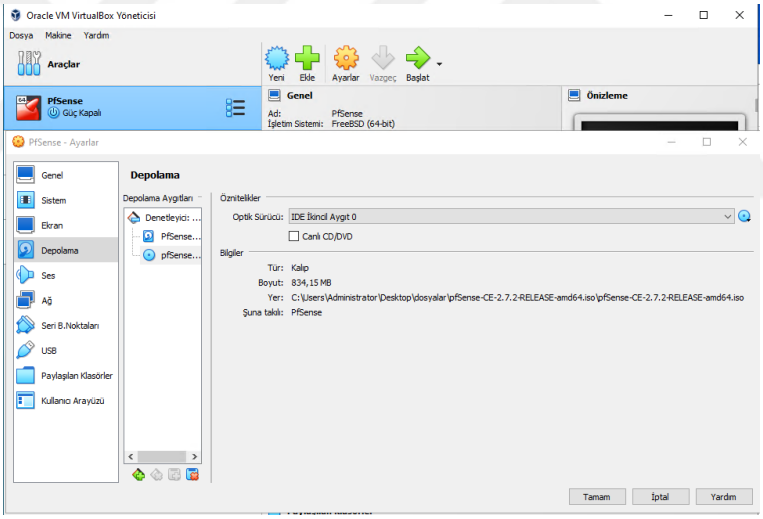
Pfsense yazılımı bir donanıma entegre edilerek çalışabildiği gibi sanal sistemlerde de sorunsuz çalışabilmektedir. Bu çalışma içerisinde kullanım yaygınlığı, sanallaştırılmış sistemlerde kullanılabilirliği ve sorun yaşandığı zaman destek alarak kullanılabilecek güvenlik duvarları araştırılmıştır. Araştırmada Pfsense ile birlikte birkaç güvenlik duvarının sanallaştırılmış sistemlerde kullanılmasının mümkün olduğu anlaşılmıştır. Pfsense yazılımı açık kaynak yazılım olarak bir firma bünyesinde bulunan hem ticari hem de ücretsiz bir yazılımdır. Bu nedenle de destek olarak daha az sorun yaşanacak açık kaynak kodlu güvenlik duvarlarındandır.

Pfsense'in en son kararlı sürümü (topluluk sürümü) 2.7.2 resmi web sayfası https://www.pfsense.org/download/ adresinden ISO formatında indirilmiş ve sanal makine olarak kurulum aşamasına geçilmiştir. Sistem gereksinimleri çok düşük olan bir yazılım olan PfSense için Şekil 9'da test sunucusunda bir sanal makine oluşturulmuştur.



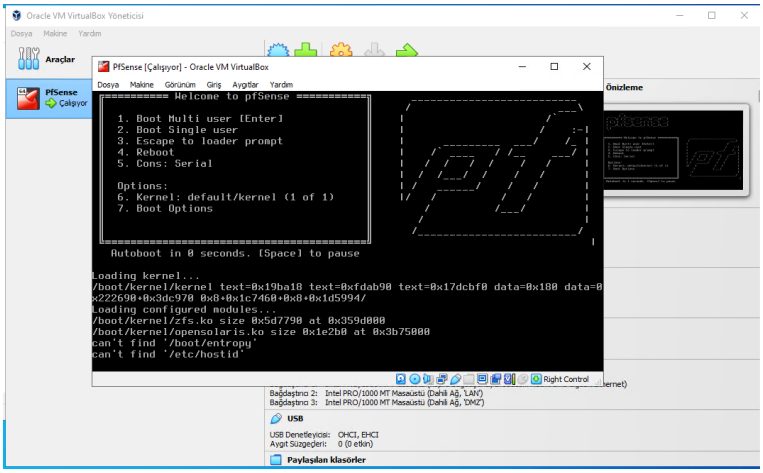
Şekil 9. Pfsense Sanal Güvenlik Duvarının Sistem Konfigürasyonu

Sanal makine 2 çekirdekli işlemciye, 8 GB RAM belleğe, 120 GB disk alanına sahip olacak şekilde yapılandırılmıştır.



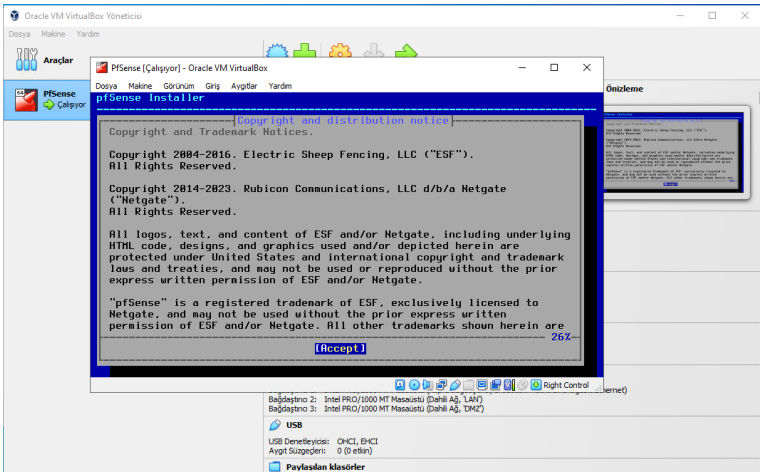
Şekil 10. ISO Dosyasının Sanal Makineye Bağlanması

Oluşturulan sanal makine içerisine kurulum yapmak için Şekil 10'da indirilen Pfsense 2.7.2 sürümünün disk görüntü dosyası sanal makinenin optik sürücüsüne yerleştirilip ardından kurulum başlatılmıştır.



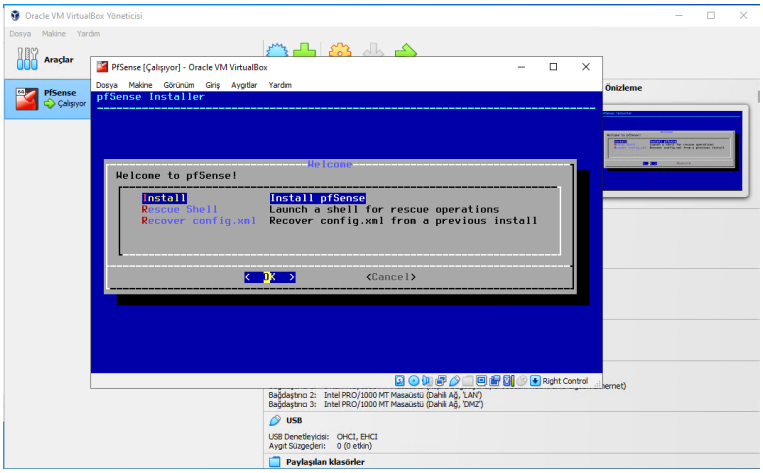
Şekil 11. Pfsense Kurulum Seçenekleri

Kurulum ilk aşamasında Şekil 11'de ekrana gelen ilerleme iletişim penceresi 5 saniye gözükmektedir, sonrasında ise varsayılan ayar olarak kurulum aşamaları başlamaktadır. Bu alandaki 1. Seçenek çoklu kullanıcı için kurulum yapmayı, 2. Seçenek tek bir kullanıcı için kurulum yapmayı, 3. Seçenek kurulumdan çıkmayı, 4. Seçenek sistemi yeniden başlatmayı ve 5. Seçenek ise sisteme seri porttan bağlantı yapmayı sağlamaktadır. Çoklu kullanıcı için kurulum yapmayı sağlayan 1. Seçenekle devam edilmiş ve sistemin kernel yapısı ve driverları RAM belleğe yüklenmeye başlamıştır.



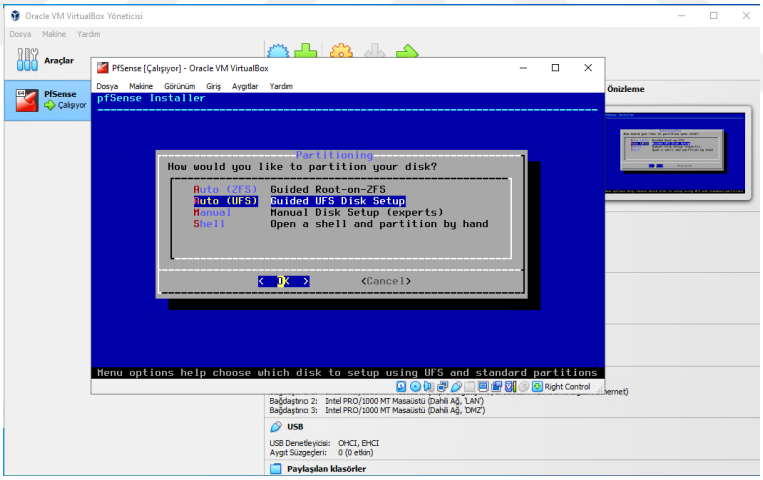
Şekil 12. Pfsense Sözleşmesi

Tüm kurulumlarda olduğu gibi Pfsense'in kurulumunda da Şekil 12'de olduğu gibi sözleşme iletişim kutusu ekrana çıkmaktadır, kabul edilip devam edilmiştir.



Şekil 13. Pfsense Yükleme ve Kurtarma Ekranı

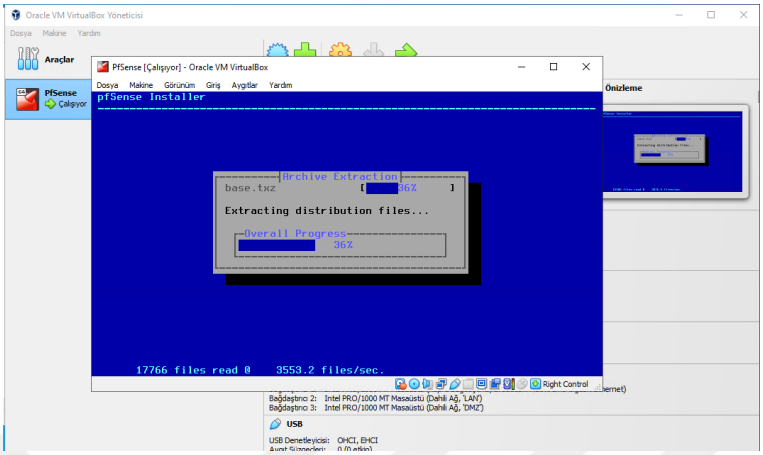
Şekil 13'te ekranda Install seçeneği kuruluma devam etmeyi, Rescure Shell seçeneği Pfsense'de meydana gelen bir sorunda kurtarma özelliğini kullanarak güvenlik duvarını düzeltmeyi ve Recover config.xml ise sistemi oluşturulan yedek xml dosyasından yüklemeyi sağlamaktadır.



Şekil 14. Pfsense Dosya Biçimi Seçme

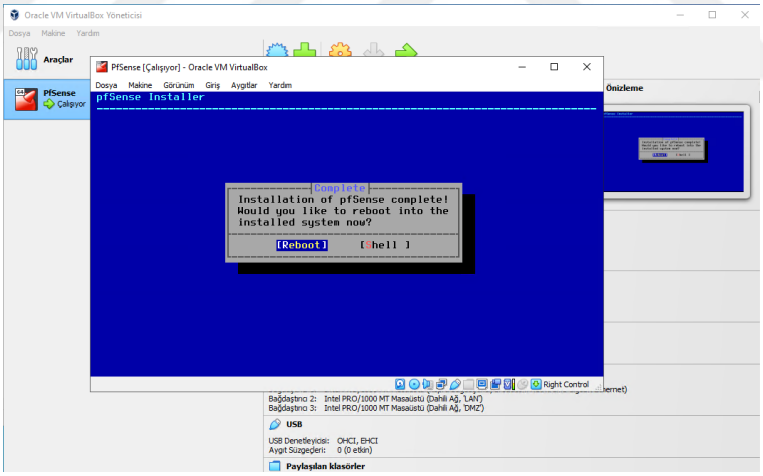
Kurulumun bir sonraki aşamasında Şekil 14'te sabit diskin hangi formatta biçimlendirileceğinin belirlendiği ekranda; otomatik ve elle yapılandırma

seçeneklerinden ZFS veya UFS otomatik yapılandırmalarından Auto (UFS) seçeneğini seçilerek kuruluma devam edilmiştir.



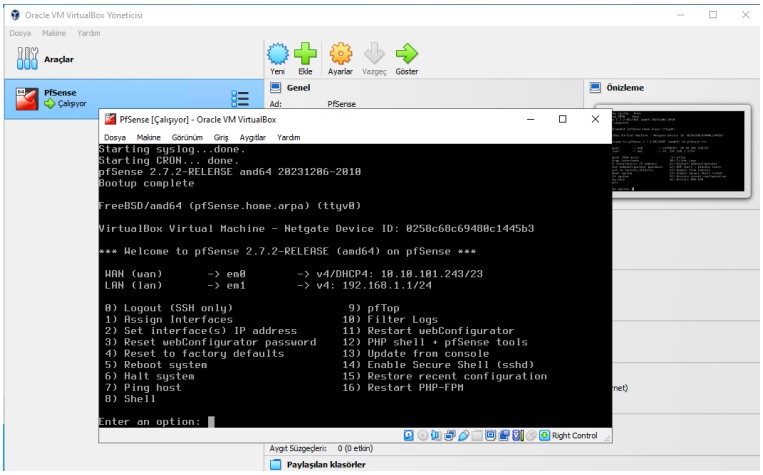
Şekil 15. Pfsense Dosyalarının Diske Aktarılması

Disk biçimlendirmesinden sonra Şekil 15'te RAM belleğe yüklenen tüm dosyaların kısa sürede diske aktarılması ile kurulum tamamlanmaktadır.



Şekil 16. Pfsense Kurulum Bilgi Ekranı

Kurulumun tamamlanmasının ardından Şekil 16'da sistemin yeniden başlatılması ya da sistemde değişiklik yapılmasının mümkün olduğu iletişim kutusundan Reboot seçeneği seçilerek güvenlik duvarının kurulum aşaması tamamlanmış olmaktadır.

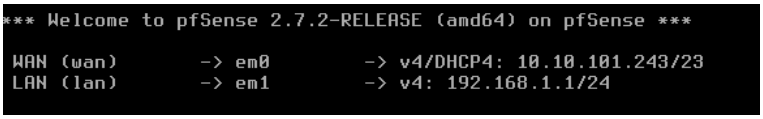


Şekil 17. Pfsense Konsol Ekranı

Sistemin yeniden başlamasının ardından monitöre yansıyan ekranda sistemin yapılandırılması işlemleri yapılabilmektedir. Şekil 17'de bulunan Pfsense ekranından interface yapılandırması, sistem şifre sıfırlamaları, fabrikasyon ayarlarına dönülmesi, sistem testleri, log filtrelemeleri ve konsol bağlantıları gibi birçok işlem yapılabilmektedir. WAN ve LAN IP'leri bu ekranda varsayılan olarak görünmektedir. LAN IP'si "192.168.1.1" web ara yüzüne LAN portuna bağlı bir bilgisayar ile giriş yapılmasını sağlamaktadır. Pfsense yapılandırmaların hepsinin, web ara yüzünden gerçekleştirilmesini sağladığı için arızaların olması durumu dışında bu bölümden ayar yapmasına gerek kalmamaktadır.

4.4 Pfsense Güvenlik Duvarı Ağ Yapılandırması

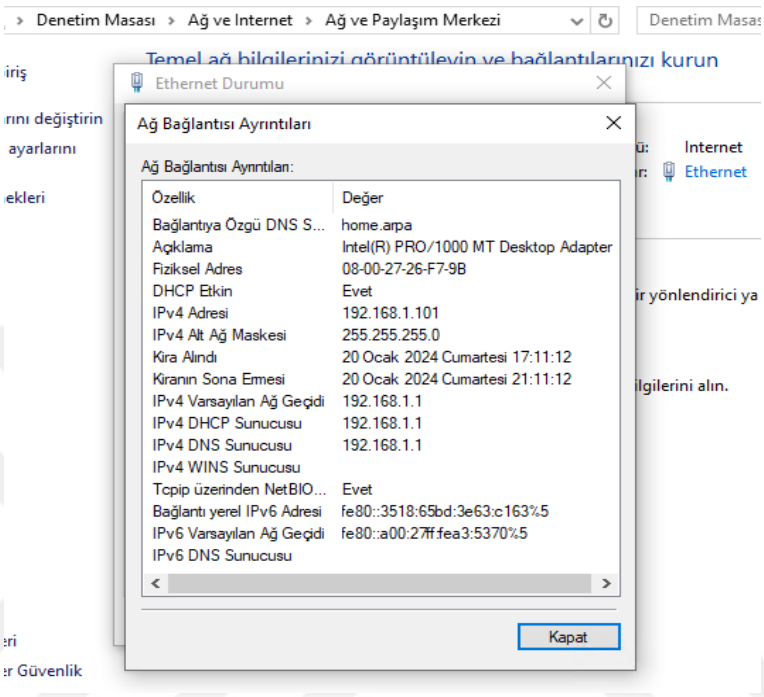
Pfsense güvenlik duvarı kurulumu tamamlandıktan sonra oluşturulan WAN ve LAN portları Şekil 18'de gösterilmiştir. Güvenlik duvarının WAN IP'si 10.10.101.134 ve LAN IP'si ise 192.168.1.1 varsayılan olarak atanmıştır.



Şekil 18. Pfsense Ethernet Uç Bilgileri

Güvenlik duvarının web ara yüzüne erişmek için LAN portuna bir bilgisayar bağlanabilmekte veya sanal bir makineden ağ kartına LAN portu tanımlanabilmektedir.

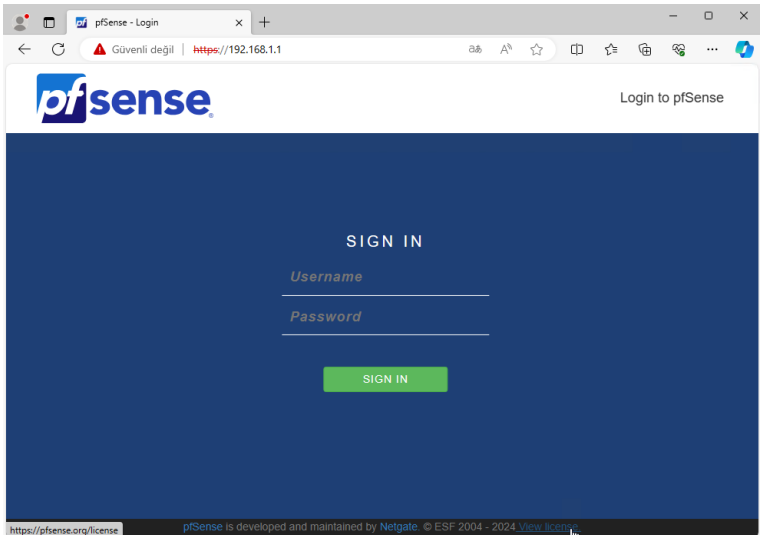
Şekil 19'da gösterilen LAN ağına dahil olduktan sonra bilgisayarın IP yapılandırması incelediğinde varsayılan ağ geçidinin güvenlik duvarının, varsayılan IP'si olan 192.168.1.1 adresi olduğu görülmektedir. Bu IP aynı zamanda web ara yüz erişim IP'sidir.



Şekil 19. Lan Ağına Bağlı Bilgisayarın Ağ Bilgileri

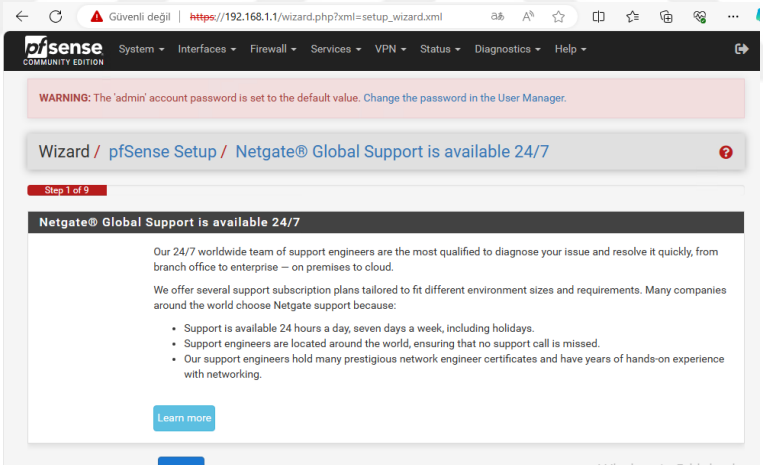
4.5 Pfsense Güvenlik Duvarı Web Ara Yüzü ve Kurulum Sihirbazı

Varsayılan kullanıcı adi "admin" parolası da "pfsense" dir. Şekil 20'de bu bilgiler kullanılarak web ara yüzüne erişim sağlanmaktadır. Pfsense'in tüm yapılandırma ve kurulum işlemlerinin tamamı web ara yüzünden yapılmaktadır. Konsol ekranından sadece sisteme ulaşım sağlanmamaktadır. Ara yüz ekranından çözülemeyecek büyük sorunlarla karşılaşıldığında erişim sağlanıp işlem gerçekleştirilmektedir.



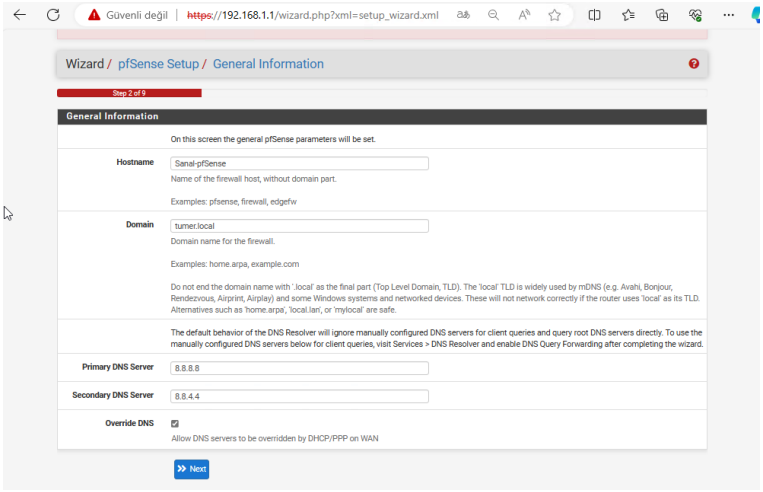
Şekil 20. Pfsense Web Ara Yüzü

Giriş işleminden sonra Şekil 21'de gösterilen ekranda setup wizard bulunmaktadır ve bu bölümden hızlı bir şekilde güvenlik duvarının ilk yapılandırma ayarları gerçekleştirilmektedir.



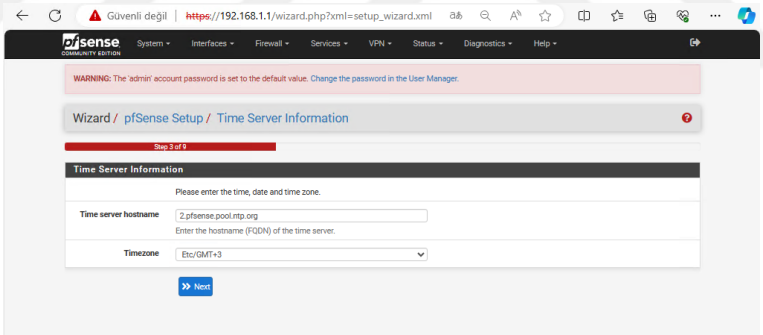
Şekil 21. Pfsense İlk Kurulum Sihirbazı 1/9

Şekil 22'de dokuz bölümden oluşan bu hızlı kurulumda; 1/9 sayfasında (ilk sayfada) ihtiyaç halinde Netgate firmasının 7/24 destek verebildiği anlatılmaktadır. Çalışmada cominity versiyonunun kurulumu yapılmıştır. Herhangi bir hata durumunda Netgate firmasından ücretli yardım alınabilmekte veya cominity forumlarından destek alınabilmektedir.



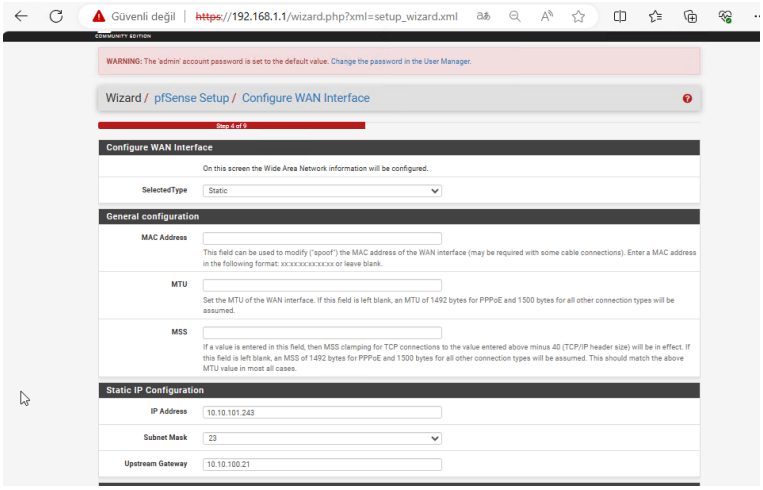
Şekil 22. Pfsense İlk Kurulum Sihirbazı 2/9

İlk kurulum ayarlarının ikinci sayfası Şekil 22'de hostname, domain ve DNS bilgilerinin girilmesi istenmektedir. Bu bilgilerin girildikten sonra düzenlenme işlemleri system menüsünden gerçekleştirilebilmektedir. Sonraki yapılandırma; Şekil 23'te sistem saati yapılandırması ayarı ile tamamlanmıştır.



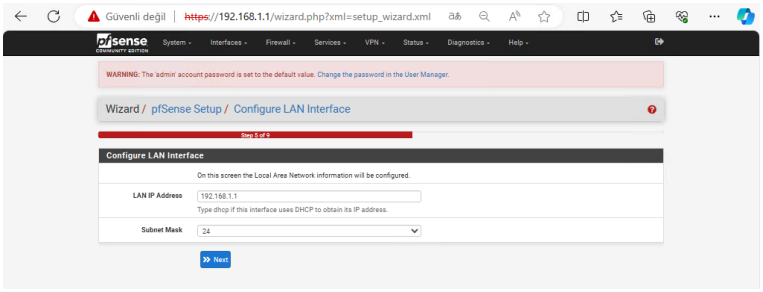
Şekil 23. Pfsense İlk Kurulum Sihirbazı 3/9

Güvenlik duvarına bağlı cihazların WAN ağına çıkabilmeleri için sistemin durumuna göre WAN yapılandırmasının yapılması gerekmektedir. Kurulan sistemde sabit IP kullanıldığı için Şekil 24'te olduğu gibi static seçeneği seçilip IP bilgileri doğru bir şekilde girilerek WAN yapılandırması sonlandırılmıştır.



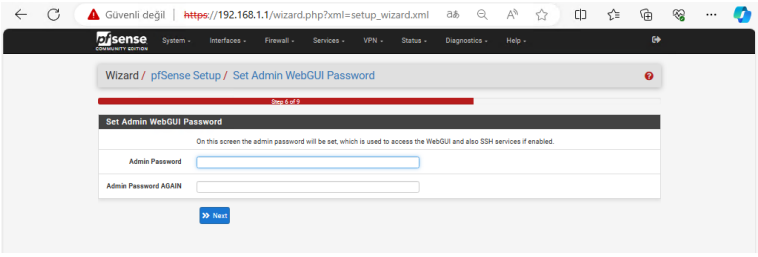
Şekil 24. Pfsense İlk Kurulum Sihirbazı 4/9

Güvenlik duvarları gateway görevi gören cihazlardır. LAN interfacenin IP yapılandırması varsayılan olarak 192.168.1.1 ağı belirlenmiştir. Eğer kullanılmak istenen farklı bir ağ yapılandırması var ise bu kısımdan firewall IP'sinin Şekil 25'te gösterilen ekrandan değiştirilerek devam edilmesi gerekmektedir. Yapılandırılmak istenilen güvenlik duvarında VLAN kullanılması planlandığı için çalışmada bu bölüm değiştirilmeden devam edilmiştir.



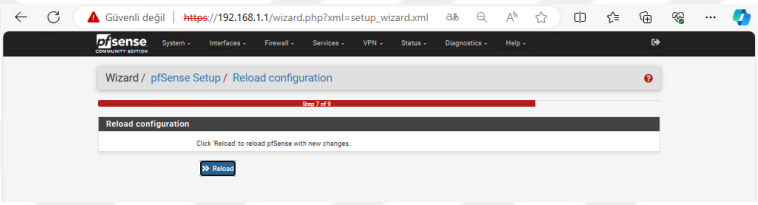
Şekil 25. Pfsense İlk Kurulum Sihirbazı 5/9

Güvenlik duvarları, sistemin güvenliği için dışarıdan erişime açık olmamalıdır. Sistemin varsayılan olarak gelen parolalarının değiştirilmesi gerekmektedir. Son yapılandırma olarak Şekil 26'da parola değiştirildikten sonra ilk kurulum ayarları yapılmış olmaktadır.



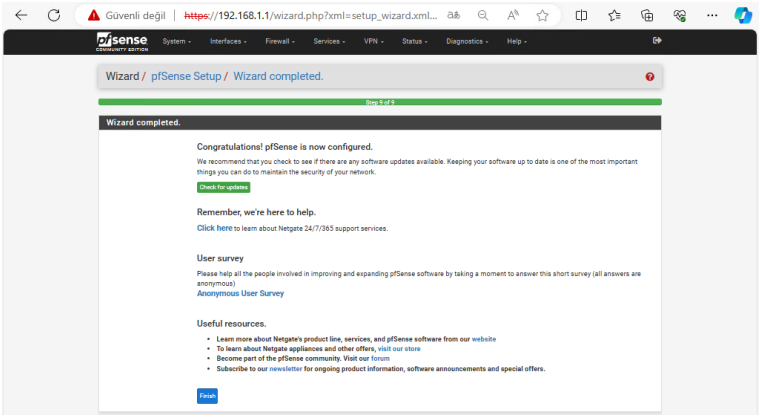
Şekil 26. Admin Kullanıcısı Parola Belirleme Pfsense İlk Kurulum Sihirbazı 6/9

Pfsense kurulumu tamamlandıktan sonra varsayılan kullanıcı adı "admin" parolası ise "pfsense" olarak belirlenmiştir. Bu durum güvenlik açıklarına yol açacağından ilk kurulum sihirbazında parola değiştirme işlemi yapılarak devam edilmiştir.



Şekil 27. Pfsense İlk Kurulum Sihirbazı 7/9

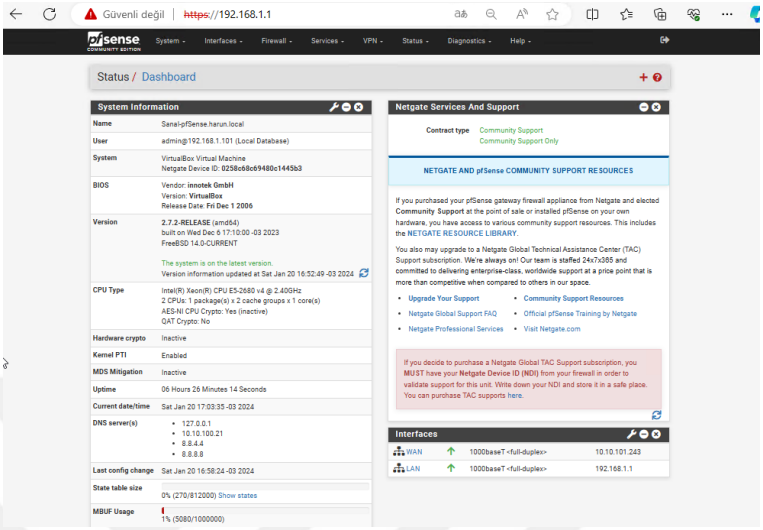
Sistem kurulumu tamamlandıktan sonra diğer aşamada Pfsense ayarlarının etkinleştirilmesi gerekmektedir. Sistemin yeniden başlatılması bilgisinin verildiği Şekil 27'deki ekranda reload butonuna basılarak kuruluma devam edilmiştir.



Şekil 28. Kurulum Tamamlandı Ekranı

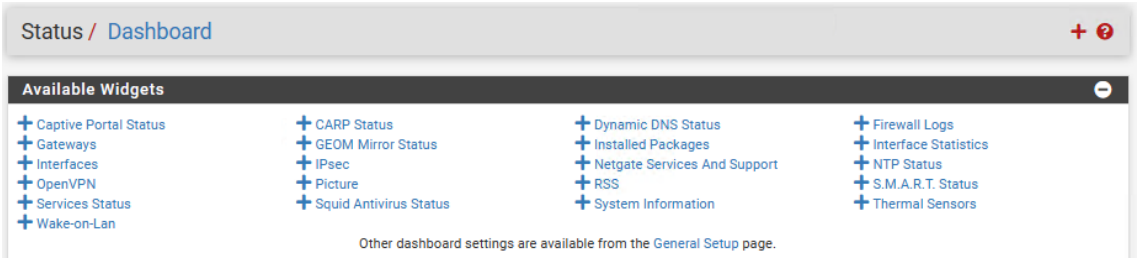
Pfsense güvenlik duvarının kurulumu tamamlanmıştır. Şekil 28'de görüldüğü gibi ekranda Pfsense kullanılırken 7/24/365 destek için yazılım geliştiricisi olan Netgate

firmasından istenirse destek alınabileceği bilgisi verilmektedir. Pfsense yazılımı açık kaynak kodlu bir yazılım olmasına rağmen ücretsiz versiyonu haricinde 7/24/365 desteği ve fiziksel olarak bir cihaz ile sunulan versiyonu mevcuttur.



Şekil 29. Pfsense Ana Ekran (Dashboard)

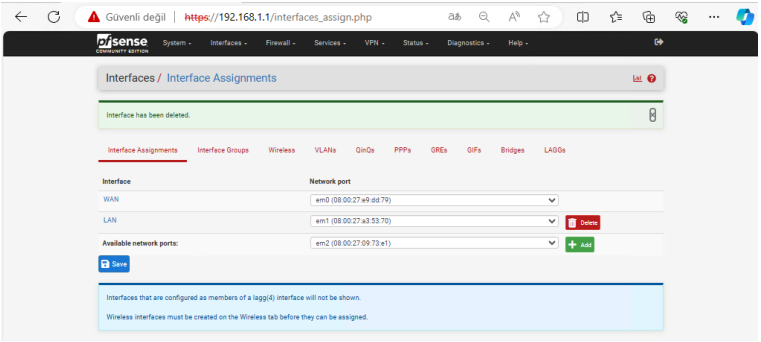
Pfsense kurulumundan tamamlandıktan sonra Şekil 29'da web ara yüzüne ilk girişte ekrana Pfsense ana sayfası gelmektedir. Bu sayfada donanım bilgileri, sistemin genel durumu ve desteğin nasıl alınabileceğine ilişkin bilgilerin olduğu tablolar bulunmaktadır. Şekil 30'da gösterilen ekranın sağ üst kısmında bulunan "+" işaretine tıklanarak dashboarda kullanım kolaylığı sağlayan widgetler eklenebilmektedir.



Şekil 30. Dashboard Ekranına Eklenebilecek Özellikler

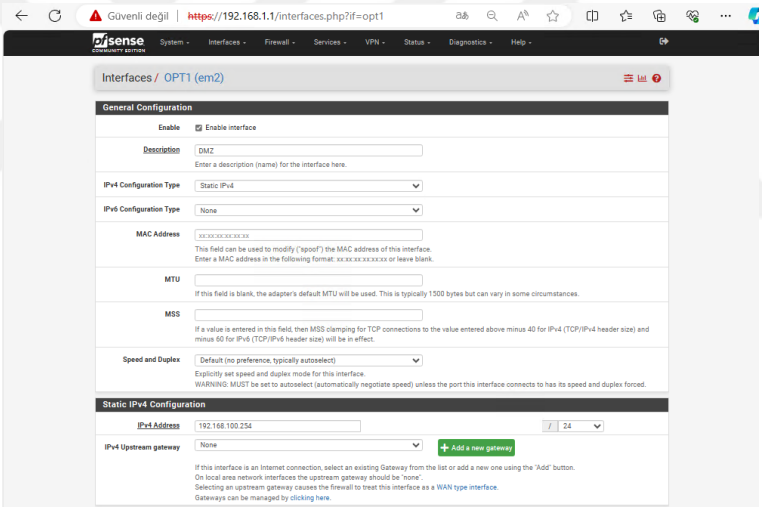
4.6 Pfsense Güvenlik Duvarı VLAN Yapılandırması

Sistemin tasarımı WAN, LAN ve DMZ olarak planladığı için öncelikle Şekil 31'de DMZ interfacenin aktifleştirilmesi ile kuruluma devam edilmiştir.



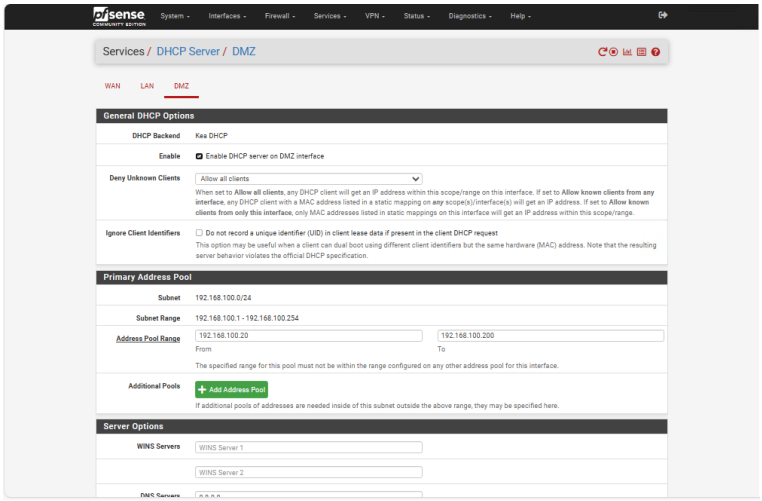
Şekil 31. Interface Tanımlama Ekranı

Pfsense'e tanımlanan tüm ara yüzler ve VLAN'lar Interface Assignments ekranından bir ara yüze bağlandıktan sonra çalışabilmektedir. Oluşturulan VLAN'ların kullanılabilmesi için bu menüden "Add" butonuna basılarak sisteme dahil edilmeli sonrasında konfigürasyonları yapılmalıdır.



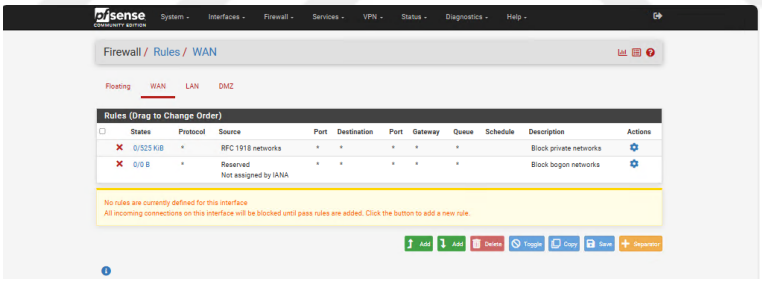
Şekil 32. DMZ Interface Konfigürasyon Ekranı

Şekil 33'te DMZ interfacenin yapılandırmasından sonra DMZ VLAN'nın DHCP ayarları yapılmıştır. IP aralığı tanımlanmış ve IP alan istemcilerin ağa dahil olmaları sağlanmaktadır.



Şekil 33. DMZ Interface DHCP konfigürasyonu

DMZ ağının DHCP yapılandırmasından sonra yapılması gereken ilk ayar güvenlik kuralı yazmaktır. Güvenlik kuralı bulunmayan ağlar WAN ağına çıkış yapamamaktadırlar. Güvenlik kurallarının izin ve engelleme kuralları olarak bilinen iki türlü bulunmaktadır. Güvenlik duvarlarının en önemli özelliklerinden biri kurulumu gerçekleştiren kişiler tarafından hedef ve kaynak göstererek ağın davranışının belirlenebilmesidir.

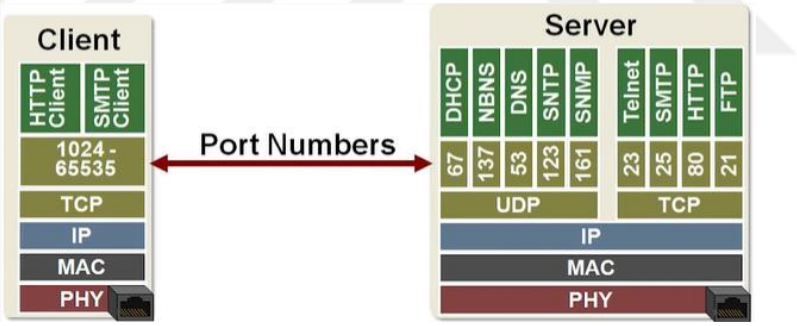


Şekil 34. Güvenlik Kuralları Ekranı

Şekil 34'te Rules menüsünde DMZ interfacesinin kurallarına bakmadan önce Pfsense'te kural yazma mantığı ve işleyişini bilmek gerekmektedir. Güvenlik duvarında kurallar yukarıdan aşağıya doğru işletilmektedir. En üstte buluna kural ilk çalıştırılacak kuraldır. Alt bölümde "Add" butonları ile istenilen sıraya kural eklenebilmektedir. "Delete" butonu kullanarak istenilmeyen kural silinebilmekte, "Toggle" butonu ile kurallar geçici olarak devre dışı bırakılabilmekte, "Copy" butonu ile seçili kural kopyalanarak diğer interfacelere aktarılabilmekte, "Save" butonu ile kural kaydı gerçekleştirilebilmekte ve son olarak "Seperator" butonu kullanarak kurallar arasına açıklama yazılabilmektedir.

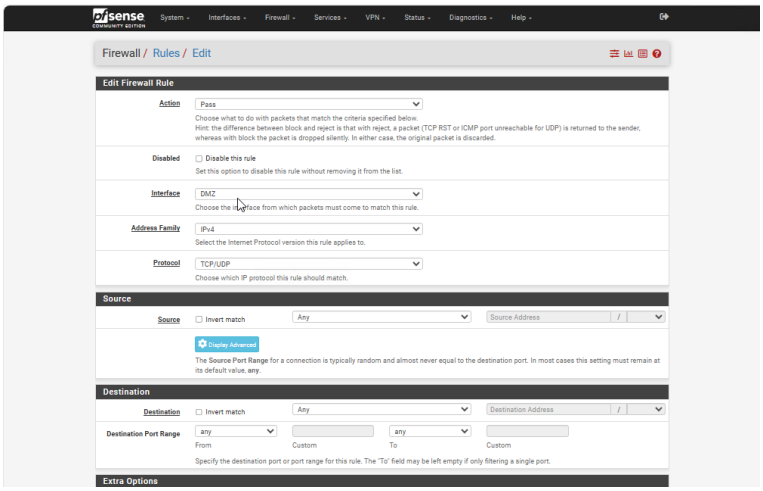
Kurallar listesinde kurallar yazılırken önce izinlerin sonra engelleme kurallarının yazılmasına dikkat edilmesi gerekmektedir.

WAN interface için otomatik olarak oluşturulan iki adet kural bulunmaktadır. Alt kısımda bilgi olarak "Henüz tanımlanmış bir kural yoktur. Yeni bir kural tanımlanana kadar dışardan gelen tüm bağlantılar engellenir." yazmaktadır. Varsayılan olarak gelen kurallar sadece WAN ağı için tanımlanması gereken kurallardır. Bu kurallarda rezerve edilmiş ağ IP'lerinden gelen trafik engellenmekte ve internet yönlendirme tablosunda görülmemesi gereken IP'lerin engellemesi sağlanmaktadır. WAN ağına bir kural yazılması planlanıyorsa dikkat edilerek kaynak ve hedef adresler belirlenmelidir. Aynı zamanda sadece ihtiyaç olan port numarasına izin verilmelidir. Kuralları doğru yazmak için hangi portun hangi işlemler için kullanıldığını bilmek gerekmektedir. Örnek olarak HTTP portu 80'dir. Ağda 80 potundan bir IP ile çıkış veya giriş yapılacaksa kural özelliklerine dikkat edilerek yazılmalıdır. Hangi istemcinin hangi protokolle sisteme giriş veya çıkış yapacağı bu kurallarla belirlenmektedir. Şekil 35'te istemci ve sunucu tarafında en çok kullanılan protokollerin port numaraları verilmiştir.



Şekil 35. İstemci ve Sunucu Tarafında Kullanılan Port ve Protokoller

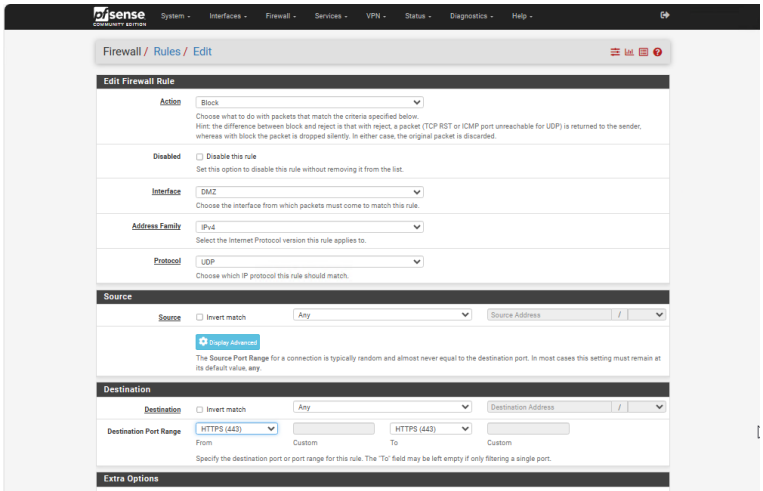
Kurulan güvenlik duvarında WAN, LAN ve DMZ olarak üç adet interface bulunmaktadır. Oluşturulan yeni interface için yazılması gereken ilk kural izin kuralıdır. İzin kuralı yazarken mevcut interface ağından her yere çıkış izni verilebileceği gibi istenilen kısıtlamalar yapılarak engelleme kuralları da yazılabilmektedir. Çalışmaya Şekil 36'da gösterildiği gibi Pfsense güvenlik kurallarına her interface için Any-Any kuralı yani her yerden her yere erişime izin veren bir kural yazılarak başlanmıştır.



Şekil 36. DMZ Interface WAN Ağına Çıkış Kuralı

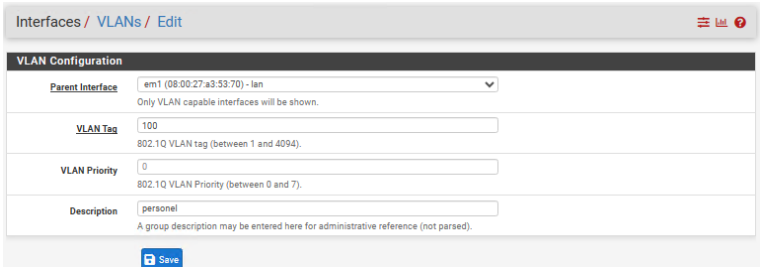
Bu kuralın yazılması ve kaydedilmesinden sonra DMZ ağında bulunan istemciler WAN ağına çıkış yapabilmektedirler.

LAN ve sonradan oluşturulacak tüm VLAN'lar içinde izin kuralı yazılmış ve oluşturulan kurallar ile tüm ağların WAN'a çıkışları sağlanmıştır. Şekil 37'de örnek olarak verilen engelleme kuralında UDP protokolü kullanılarak DMZ ağına HTTPS(443) protokolüyle yapılacak tüm bağlantıları bloklama işlemi gerçekleştirilmiştir.

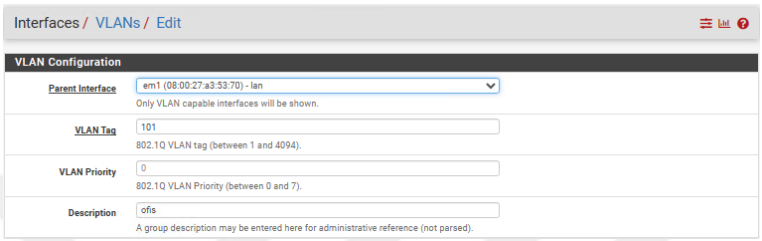


Şekil 37. DMZ Interface HTTPS Protokolünün Kısıtlama Kuralı

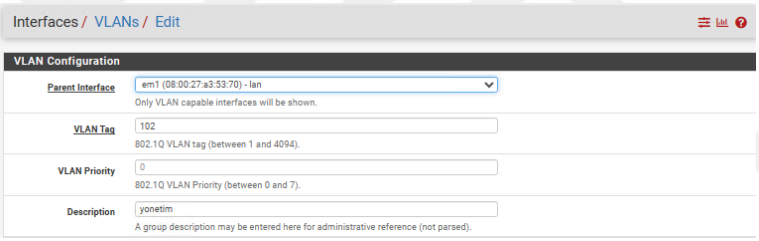
Ağda kullanılması planlanan VLAN tanımlamaları gerçekleştirilmiştir. VLAN tanımlamalarından sonra oluşturulmuş olan VLAN'lar için interface tanımlamaları ve her interface için ağ tanımlamalarının yapılması gerekmektedir.



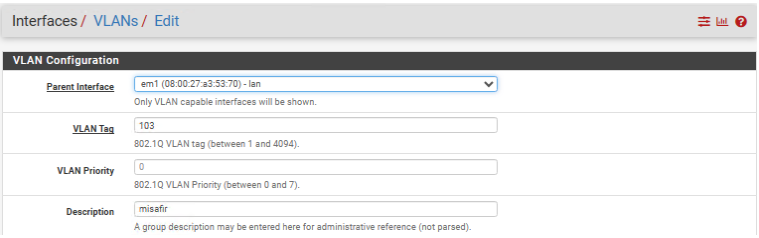
Şekil 38. VLAN Ekleme "personel"



Şekil 39. VLAN Ekleme "ofis"



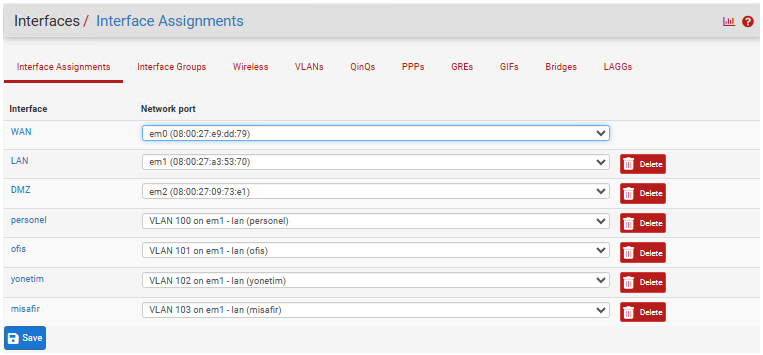
Şekil 40. VLAN Ekleme "yonetim"



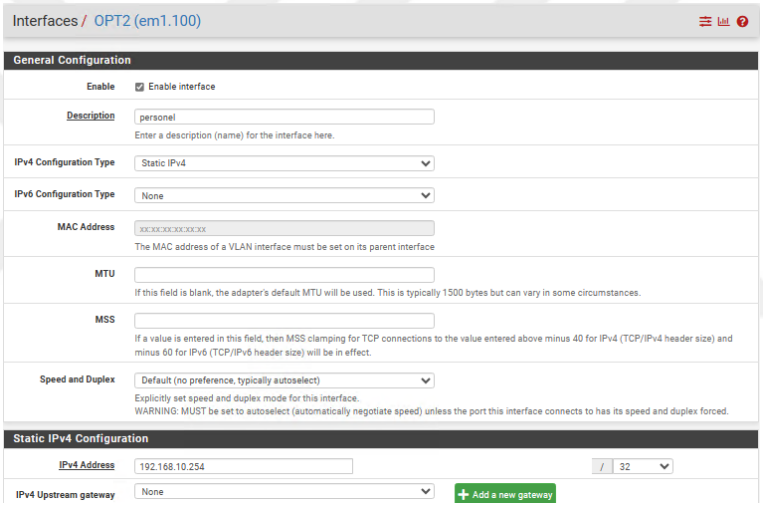
Şekil 41. VLAN Ekleme "misafir"

Interface assignments bölümünden eklenen VLAN'ların genel ayarlarının yapılması Şekil 38, 39, 40, 41'de gösterildiği gibi gerçekleştirilmiştir. VLAN tanımlamaları yapılırken en önemli nokta VLAN id bölümüdür. Tanımlanan VLAN id'ler switch yapılandırması sırasında VLAN oluştururken aynı id ile oluşturulmalıdır. Yapılan bu

ayarlamalarda her VLAN'ın tanımlanması, IP yapılandırılması ve aktif/pasif durumu belirlenmektedir.

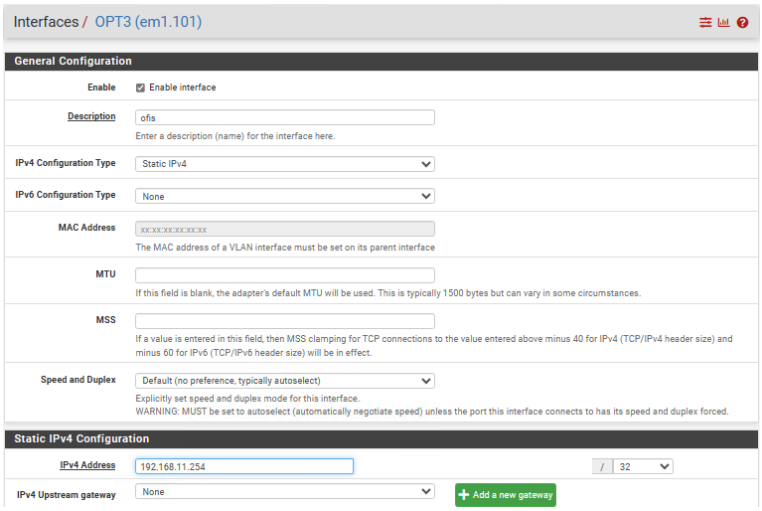


Şekil 42. VLAN Ara yüz Atamaları Ekranı



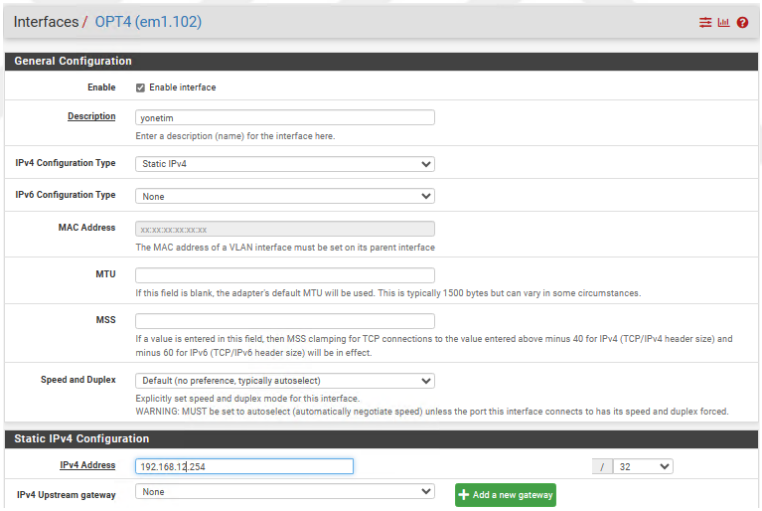
Şekil 43. VLAN Ara Yüz Ekranı "personel"

Şekil 43'te oluşturulan personel VLAN'ının IPv4 adresinin, durumunun ve diğer özelliklerinin belirlenerek aktif edilmesi sağlanmıştır.



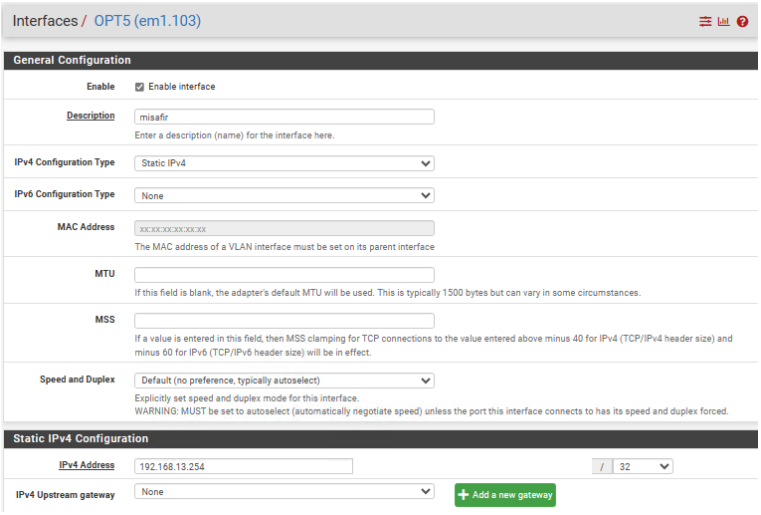
Şekil 44. VLAN Ara yüz Ekranı "ofis"

Şekil 44'te oluşturulan ofis VLAN'ının IPv4 adresinin, durumunun ve diğer özelliklerinin belirlenerek aktif edilmesi sağlanmıştır.



Şekil 45. VLAN Ara yüz Ekranı "yönetim"

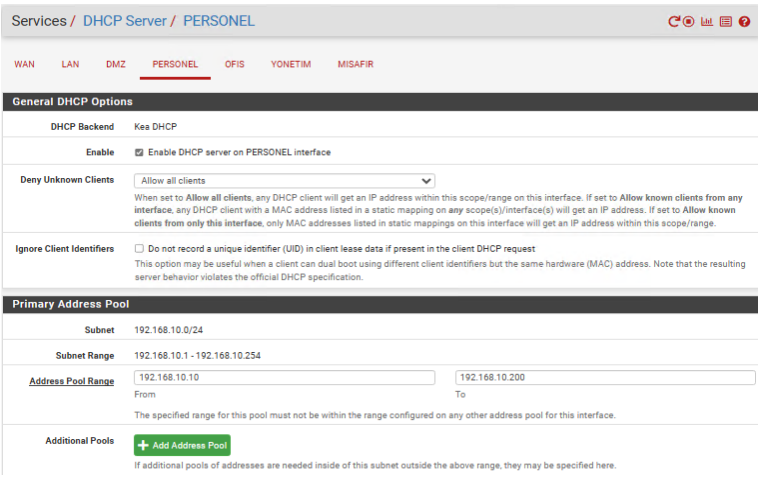
Şekil 45'te oluşturulan yonetim VLAN'ının IPv4 adresinin, durumunun ve diğer özelliklerinin belirlenerek aktif edilmesi sağlanmıştır.



Şekil 46. VLAN Ara yüz Ekranı "misafir"

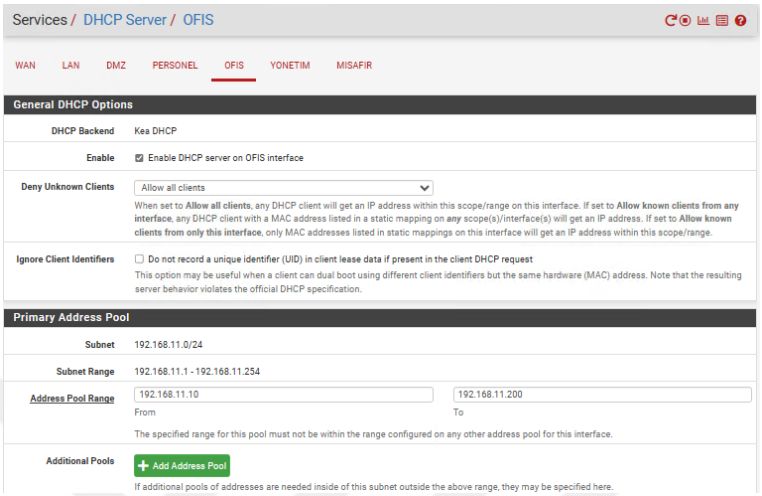
Şekil 46'da oluşturulan misafir VLAN'ının IPv4 adresinin, durumunun ve diğer özelliklerinin belirlenerek aktif edilmesi sağlanmıştır.

Oluşturulan VLAN'lar LAN interface üzerinden tanımlanmış ve tüm VLAN'ların tanımlamaları sistem de kullanılan Cisco 2960 model switche LAN interface üzerinden tagged olarak aktarılmıştır. Swicth yapılandırması yapıldıktan sonra VLAN tanımına göre port atamaları yapılması gerekmektedir. Güvenlik duvarından tanımladığımız VLAN'ların otomatik IP dağıtma ayarları services menüsünün altında bulunan DHCP bölümünden gerçekleştirilerek ağa bağlanan tüm cihazların bağlandığı porta tanımlı VLAN'dan IP almaları sağlanmıştır.



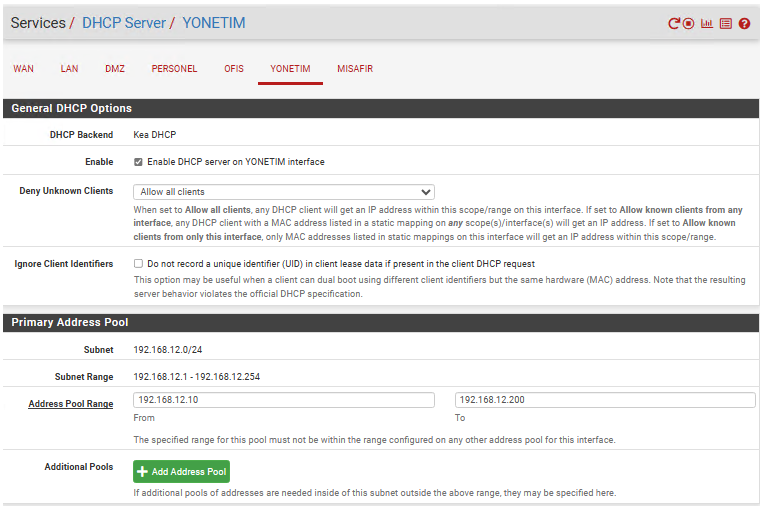
Şekil 47. VLAN DHCP Yapılandırması "personel"

Şekil 47'de personel VLAN için 192.168.10.0/24 ağı tanımlanmış ve 192.168.10.10-200 IP aralığında IP dağıtması için gerekli yapılandırma yapılmıştır. Varsayılan ağ geçidi personel VLAN tanımında 192.168.10.254 olarak verilmiştir.



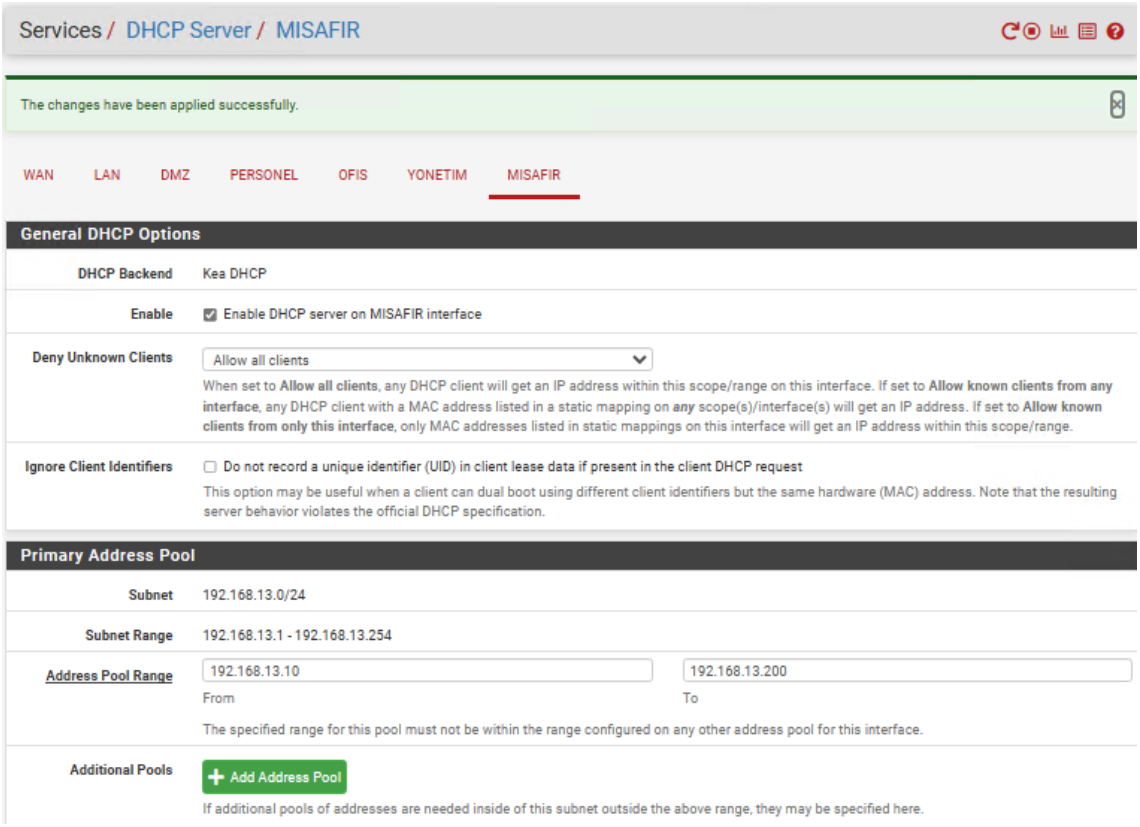
Şekil 48. VLAN DHCP Yapılandırması "ofis"

Ofis VLAN için Şekil 48'de gösterildiği gibi 192.168.11.0/24 ağı tanımlanmış ve 192.168.11.10-200 IP aralığında IP dağıtması için gerekli yapılandırma yapılmıştır. Varsayılan ağ geçidi ofis VLAN tanımında 192.168.11.254 olarak verilmiştir.



Şekil 49. VLAN DHPC Yapılandırması "yönetim"

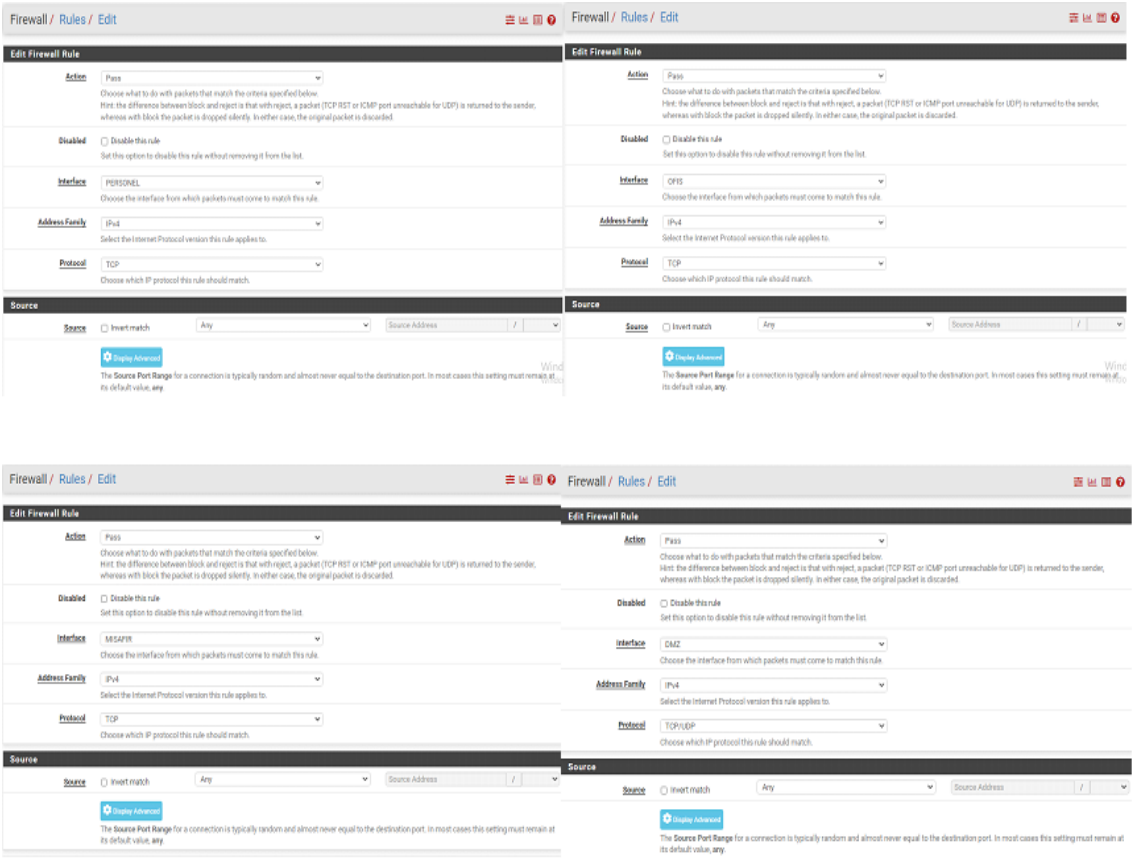
Şekil 49'da gösterilen ekranda yonetim VLAN için 192.168.12.0/24 ağı tanımlanmış ve 192.168.12.10-200 IP aralığında IP dağıtması için gerekli yapılandırma yapılmıştır. Varsayılan ağ geçidi yonetim VLAN tanımında 192.168.12.254 olarak verilmiştir.



Şekil 50. VLAN DHPC Yapılandırması "misafir"

Şekil 50'de gösterilen ekranda misafir VLAN için 192.168.13.0/24 ağı tanımlanmış ve 192.168.12.13-200 IP aralığında IP dağıtması için gerekli yapılandırma yapılmıştır. Varsayılan ağ geçidi misafir VLAN tanımında 192.168.13.254 olarak verilmiştir.

VLAN'ların oluşturulmasından ve DHCP ayarlamalarından sonra bu her bir VLAN için Şekil 51'de gösterildiği gibi birer izin kuralı oluşturularak WAN ağına çıkışları sağlanmıştır.

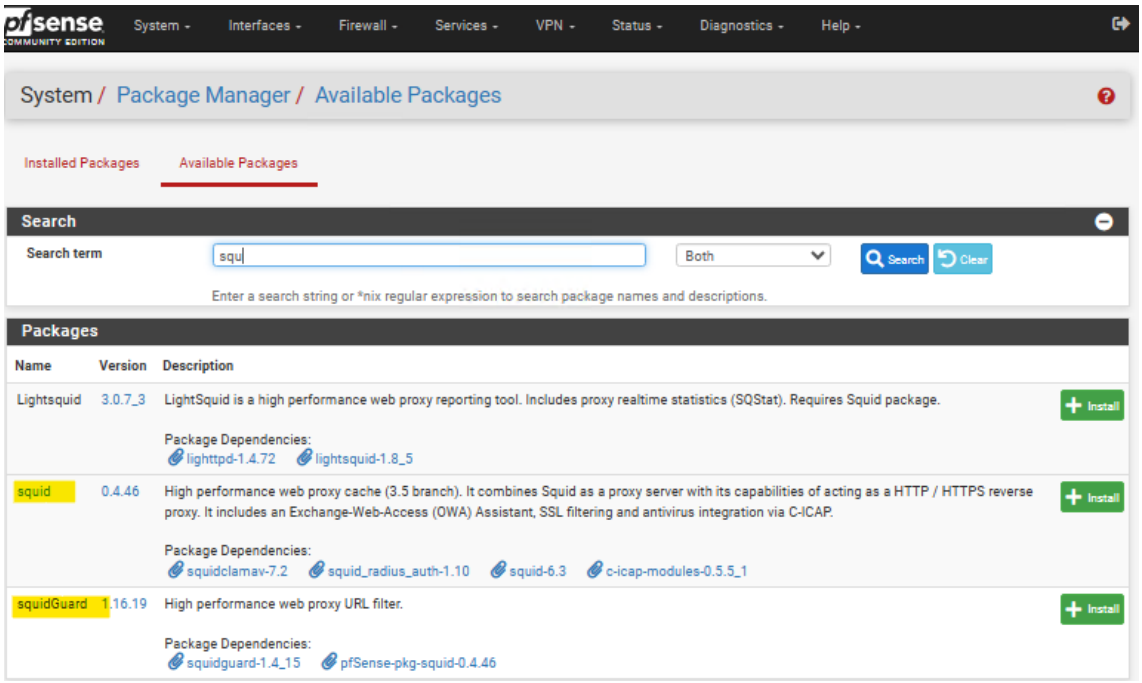


Şekil 51. VLAN'ların WAN Ağına Çıkmaları İçin Yazılan Kurallar

İstemci bilgisayarların oluşturulan ağlara bağlantılarının sağlanabilmeleri ve WAN ağına çıkmaları için switch yapılandırması yapılmalıdır. Bu yapılandırmada Cisco 2960 model test switchine consol kullanılarak bağlantı sağlanmış ve gerekli ayarlamalar yapılmıştır. 100 nolu VLAN için Gi1/0/1-2, 101 nolu VLAN için Gi1/0/3-4, 102 nolu VLAN için Gi1/0/5-6 ve 103 nolu VLAN için Gi1/0/7-8 nolu portlar "Accessport" olarak tanımlanmış Gi1/0/24 nolu port ise Trunk port olarak tanımlanmıştır. Bu tanımlamaların ardından Hp test sunucusunun LAN portundan alınan patch kablo ile switchin Gi1/0/24 port bağlantısı yapıldıktan sonra Pfsense güvenlik duvarından tagged olarak gönderilen VLAN'ların switche aktarılması tamamlanmıştır. Tanımlanan portlara bağlanan istemci bilgisayarların bağlı oldukları VLAN'dan IP almaları ve WAN ağlarına çıkışları sağlanmıştır.

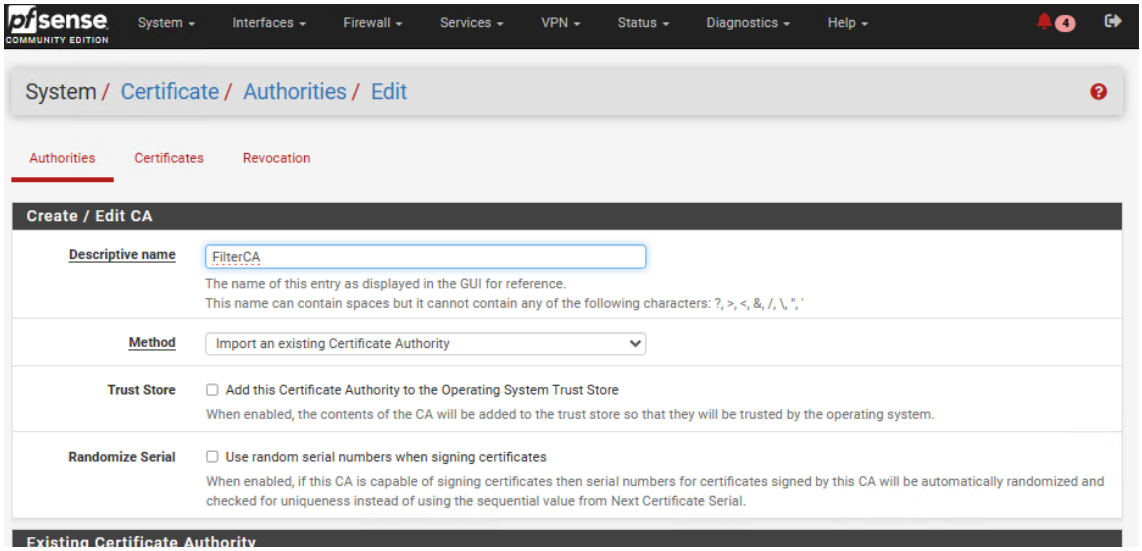
4.7 Pfsense Güvenlik Duvarında Filtreleme Servisi

Pfsense paket yöneticinden kullanmak istenilen paketler indirilerek güvenlik duvarının özellikleri artırılabilmektedir. Squid ve squidguard paketleri güvenlik duvarının filtreleme işlemleri yapabilmesi için gerekli olan paketlerdir. Bu paketlerin kurulumları gerçekleştirildikten sonra yapılandırma işlemleri yapılmalıdır.



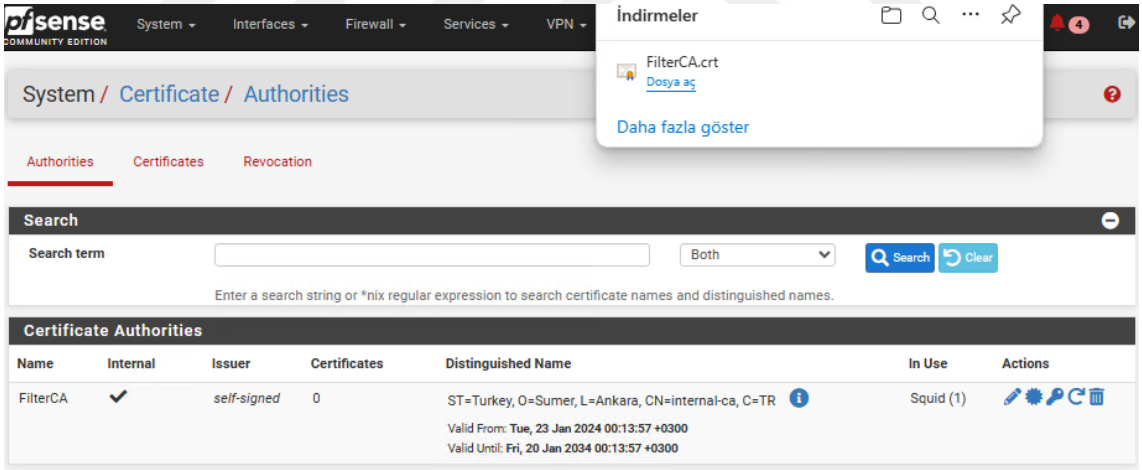
Şekil 52. Paket Yöneticisi Ekranı

Şekil 52'de gösterilen ekrandan Pfsense güvenlik duvarına istenilen paketler install butonun basarak kurulmuştur.



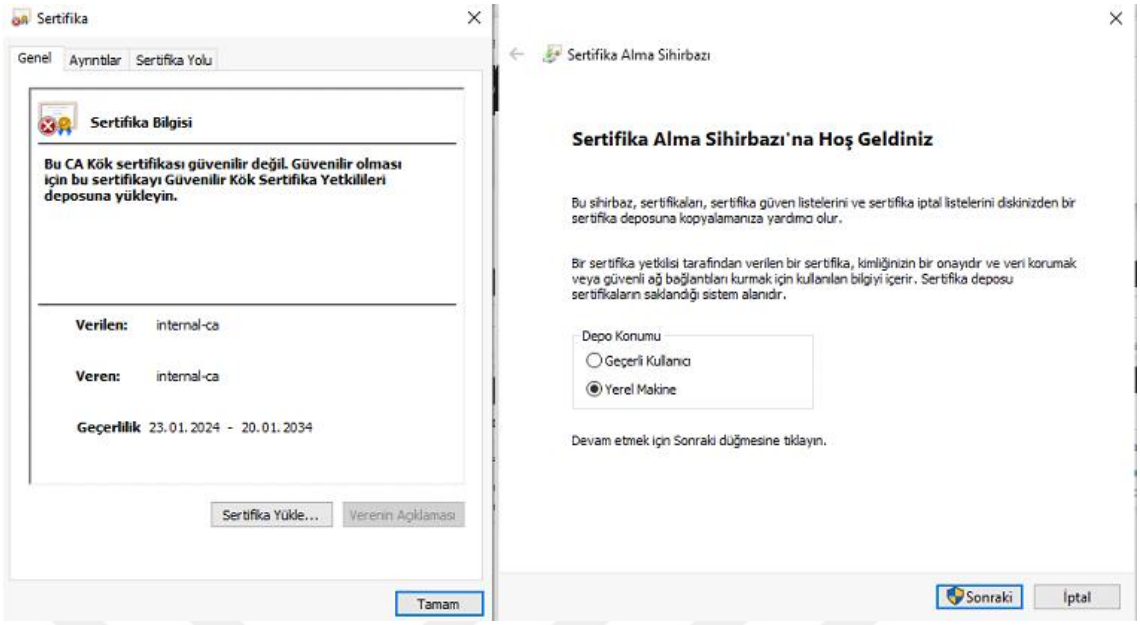
Şekil 53. Paket Filtreleme İçin Sertifika Oluşturma Ekranı

Filtreleme servisinin HTTPS protokolüne sahip sitelerde de çalışabilmesi için yerel makineye bir güvenilir sertifika yüklenmesi gerekmektedir. Şekil 53'te gösterilen ekrandan Pfsense de bir sertifika oluşturulmuş ve yerel makinede çalışması sağlanmıştır.



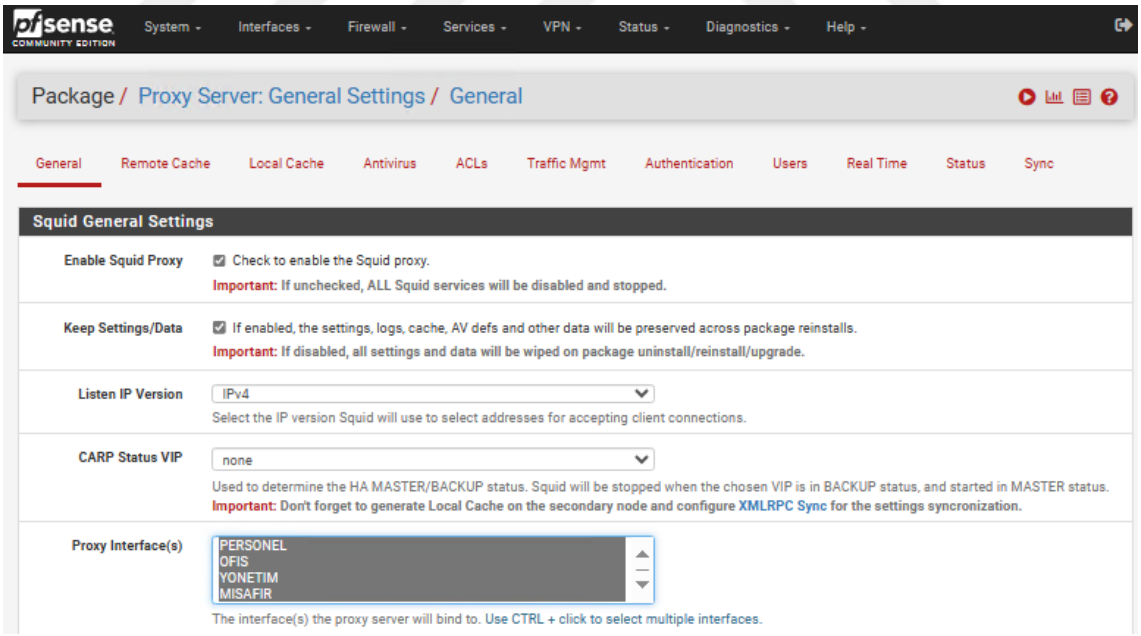
Şekil 54. Sertifika İndirme ve Ayar Ekranı

Oluşturulan sertifika Şekil 54'te indir butonu ile istemci bilgisayara indirilmiş ve bu sertifikanın istemci bilgisayara kurulumu Şekil 55'de gösterildiği gibi yapılmıştır.



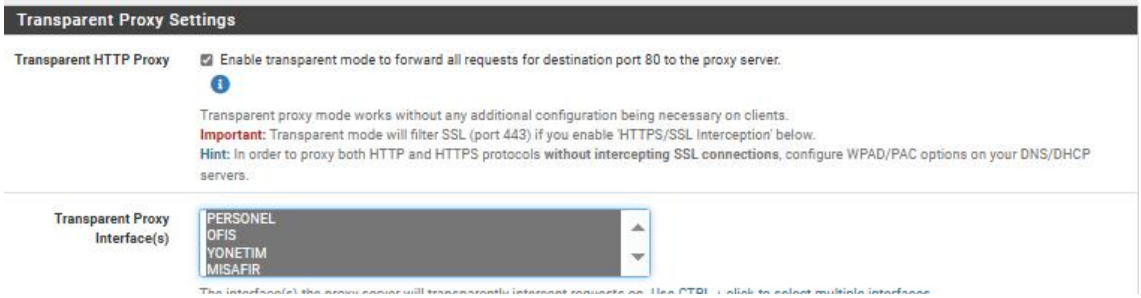
Şekil 55. İndirilen Sertifikanın Yerel Makineye Yüklenmesi

Kurulum tamamlandıktan ve güvenli sertifika olarak yerel makineye yüklendikten sonra engellenen sitelerin hata mesajı vermeleri sağlanmıştır.



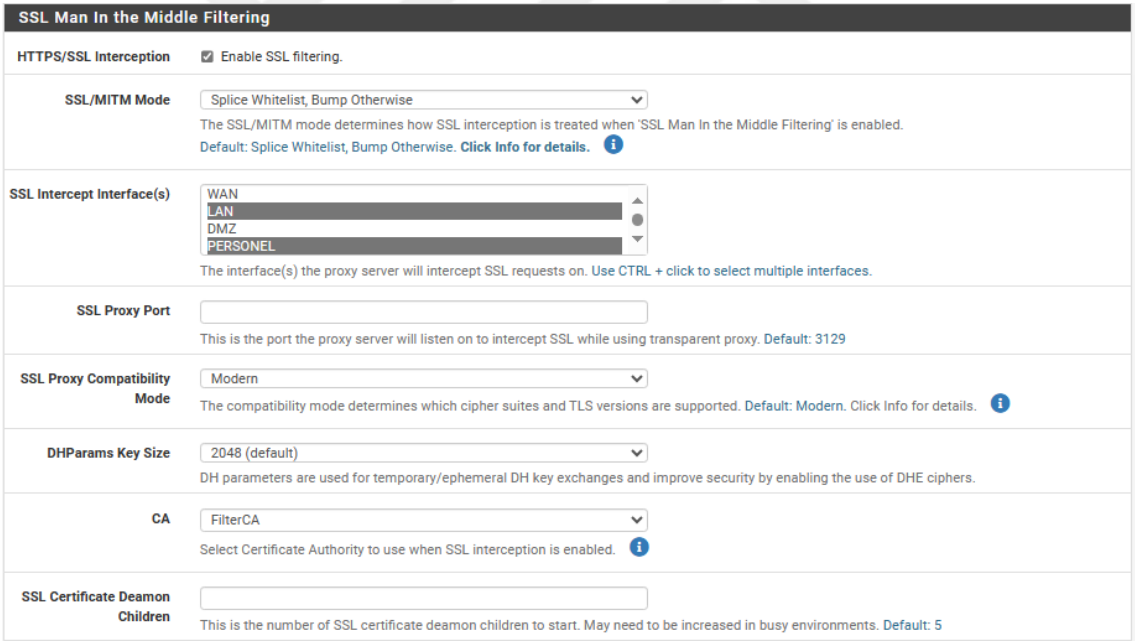
Şekil 56. Paket Filtreleme Proxy Server Ayar Ekranı

Sertifika oluşturulduktan sonra Şekil 56'da gösterilen ekrandan Proxy server yapılandırması ile işlemlere devam edilmiştir. Bu konfigürasyonda servisin aktif edilmesi ve hangi ağlarda çalışması gerektiği belirlenmiştir.



Şekil 57. Paket Filtreleme Proxy Server Ayar Ekranı

Şekil 57'de gösterilen ekranda Transparent HTTP Proxy özelliğinin aktif edilmesi ile 80 portundan yapılacak tüm filtrelemelerin çalışması sağlanmıştır.

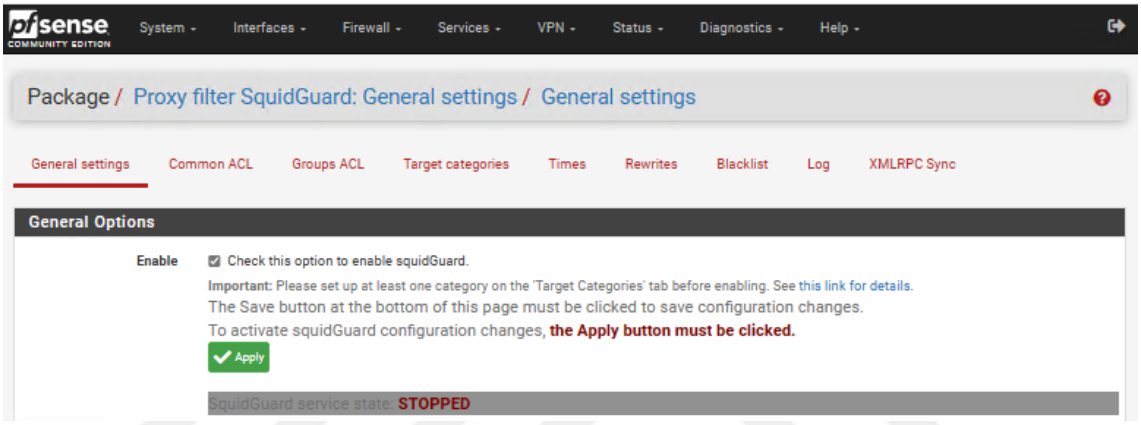


Şekil 58. Paket Filtreleme Proxy Server Ayar Ekranı

Transparent HTTP Proxy aktif edildikten sonra https/ssl interseption ayarı aktif edilerek 443 portu filtrelemeye dahil edilmiştir.

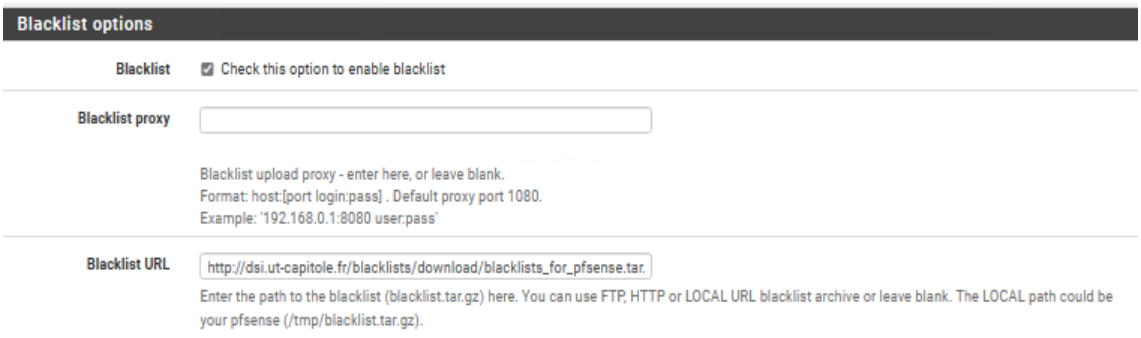
Şekil 59. Paket Filtreleme Proxy Server Ayar Ekranı

Yapılan filtrelemelerin kayıtlarının tutulması için Şekil 59'da gösterilen ekrandan loglama servisi aktif edilmiştir. Bu işlemden sonra squid Proxy ayarları tamamlanmıştır.



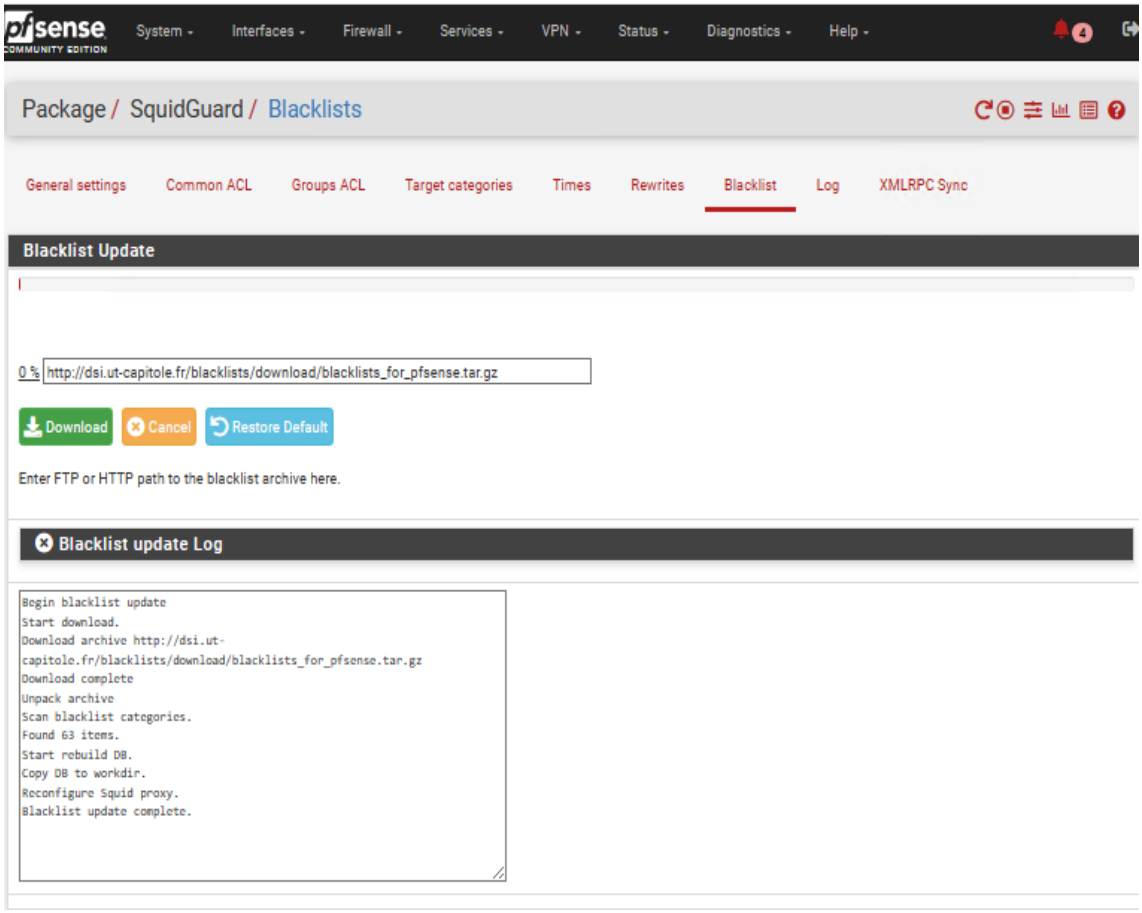
Şekil 60. Proxy Filtrelemede Kullanılacak SquidGuard Ekranı

Şekil 60'ta gösterilen ekran Proxy filter squidguard ayarlamaları filtreleme işleminin yapılması için gerekli ayrıntıların yapıldığı menüdür. Bu bölümde filtreleme kategorileri eklenmiş ve filtrelenmesi gereken sitelerin belirlenmesi işlemi gerçekleştirilmiştir.



Şekil 61. SquidGuard Ekranı Blacklist Ekranı

Squidguard ayarlarından en önemli olan kısım kara listenin belirlenmesidir. Kara liste filtreleme işlemlerinin yapılacağı kategorileri barındıran bir listedir. Şekil 61'de gösterilen ekranın Blacklist URL kısmına bir kara liste URL'si girilmiştir.



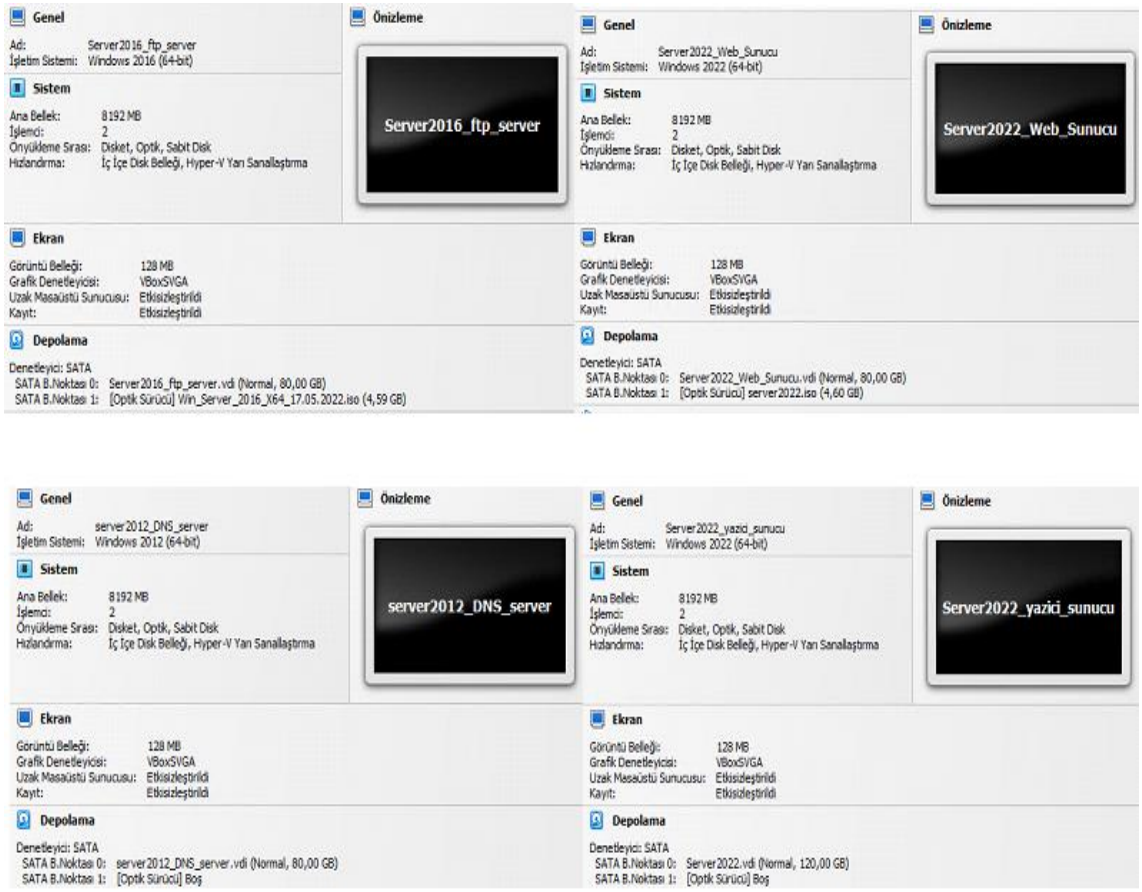
Şekil 62. SquidGuard Ekranı Blacklist Yükleme Ekranı

Şekil 62'de gösterilen ekranda Squidguard menüsünde girilen kara liste sisteme indirilmiş ve kara liste içerisinde bulunan tüm kategoriler Pfsense target kategoriler bölümünde görüntülenmiştir. Filtreleme servisinin aktifleştirme işlemi tamamlandıktan sonra hangi kategorilere filtreleme yapılması isteniyorsa onların seçilmesi yeterli olacaktır.

4.8 Test Sunucusuna Sanal Makinelerin Kurulması

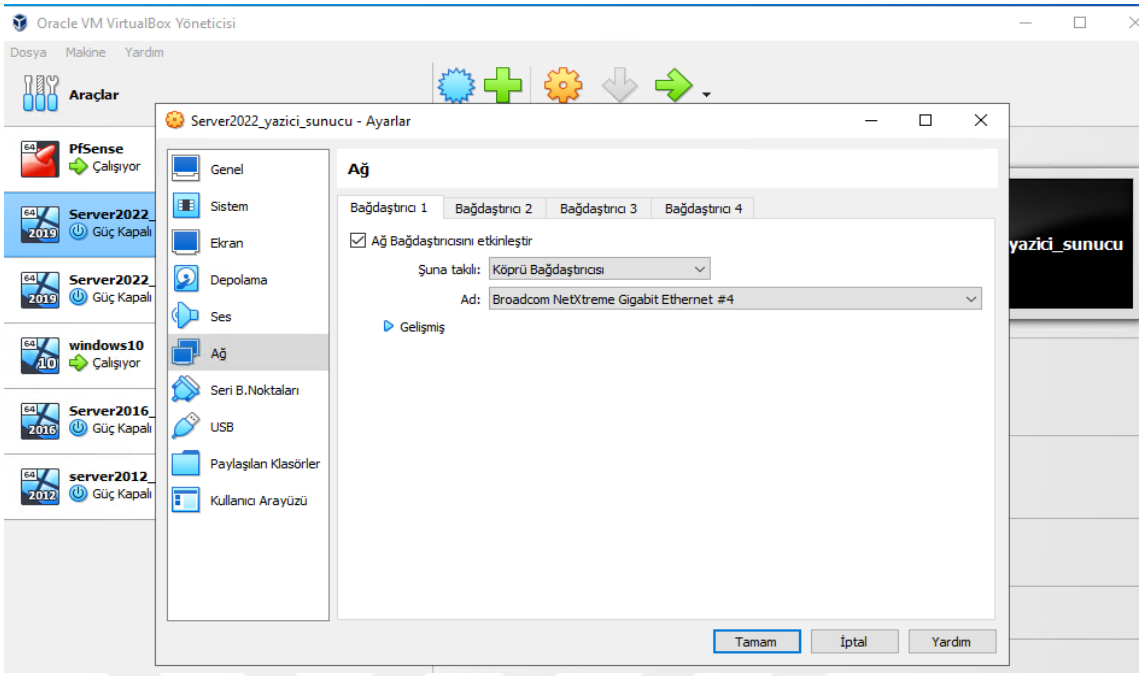
Test sunucusunun içerisine birden fazla işlem yapmak için Şekil 63'te gösterildiği gibi Server 2022, Server 2016, Server 2012 kurulumu yapılmıştır. Sanal sunucular oluşturulmuş ve sunuculara roller verilmiştir. Web sunucusu, yazıcı sunucusu, veri tabanı sunucusu ve DNS sunucusu isimli dört adet sanal sunucu, Pfsense güvenlik duvarının da

kurulumunu yapılan test sunucusuna kurulmuştur. Oluşturulan sanal sunuculara iki çekirdek işlemci, 8192MB RAM ve 80 GB HDD donanımları ayarlanmıştır.



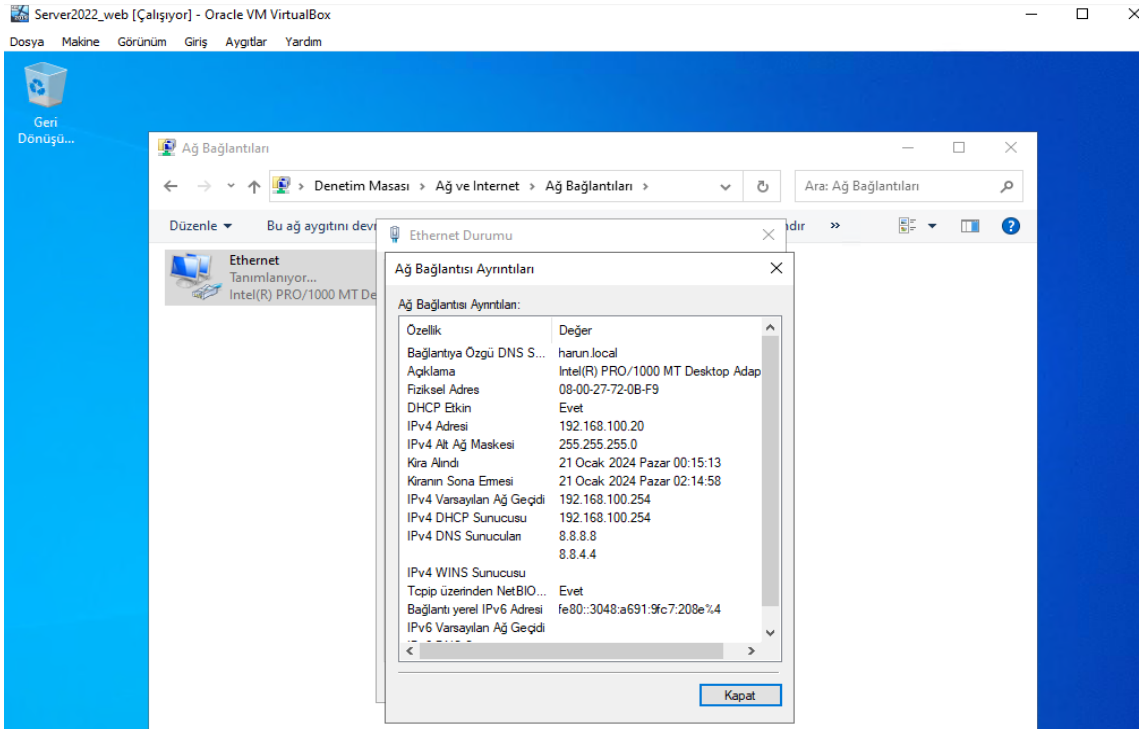
Şekil 63. Sanal Sunucuların Donanım Bilgileri

Sunucuların DMZ ağına bağlanmaları için ağ kartı seçimi DMZ portu olarak tanımlanan Broadcom NetXtreme Gigabit Ethernet #3 seçilmiştir. Pfsense güvenlik duvarında yapılan DHCP yapılandırmasına göre IP almaları sağlanmıştır.



Şekil 64. Sanal Sunucu Ağ Yapılandırması

Sanal sunucuların ağ yapılandırması için Şekil 64'te gösterildiği gibi Pfsense'de DMZ için belirlenen ethernet portu, sunucuların ağ kartlarına köprü bağdaştırıcısı olarak seçilmiştir.



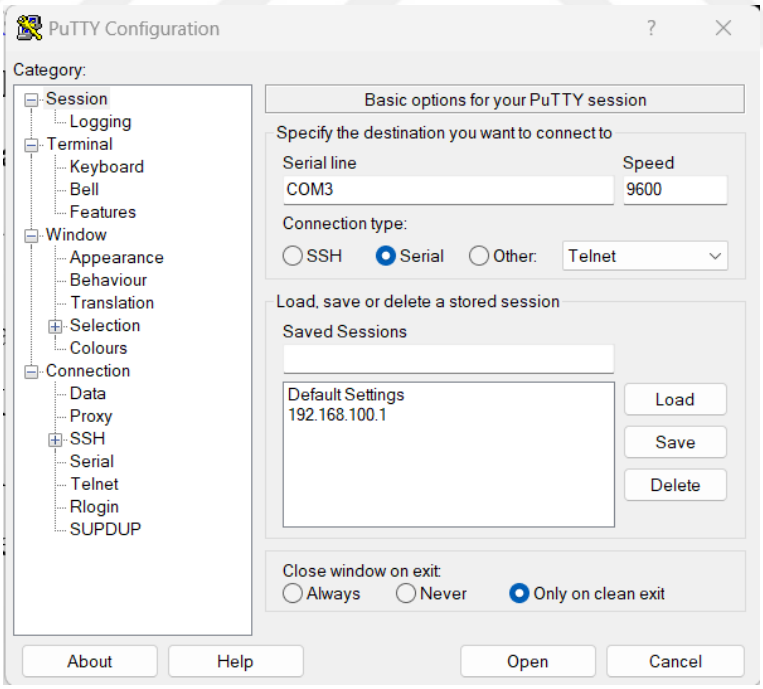
Şekil 65. Oluşturulan Sanal Sunucu Ağ Bilgileri

Ağ kartı sanal sunucuda seçildikten sonra sunucuların Şekil 65'te gösterildiği gibi 192.168.100.0/24 DMZ ağından IP almaları sağlanmaktadır.

4.9 Kullanıcı Bilgisayarlarının Ağ Yapılandırması

Kullanıcı bilgisayarların test ağına dahil olabilmeleri için Hp test sunucusunun Pfsense'e tanımlanmış ethernet portlarından LAN portu kullanılmıştır. Pfsense'e tanımlanan VLAN'lar LAN ara yüzü üzerinden WAN ağına çıkış yapabilecek şekilde ayarlanmışlardır. Yapılan konfigürasyonda oluşturulan dört adet VLAN LAN portu üzerinden Tagged olarak gönderilmiştir. Test switchi olarak kullanılan Cisco 2960 model cihaz üzerinden gerekli tanımlamalar yapıldıktan sonra kullanıcının bağlandığı ağ hangi port tanımlı ise o port üzerinden WAN ağına çıkışı sağlanmıştır.

VLAN tanımlamalarının layer 2 switch üzerinden yapılabilmesi için bir adet konsol kablosunun olması gerekmektedir. Konsol kablosu ile konfigürasyonu gerçekleştirilen bilgisayar switche bağlandıktan sonra konsol üzerinden işlemleri yapmak için "putty" isimli programla switch ara yüzüne bağlantı sağlanmıştır.



Şekil 66. Putyy Programı

Şekil 66'da gösterildiği gibi Putty ile bağlantıyı seri port üzerinden yaptıktan sonra switch ara yüzüne ulaşım sağlanmıştır. Bu bölümde yapılan işlemler için switch kod yazma bilgisi gerekmektedir.

```
Switch#configure terminal
Enter configuration commands, one per line.  End wit
Switch(config)#vlan 100
Switch(config-vlan)#name personel
Switch(config)#interface range gi1/0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config)#vlan 101
Switch(config-vlan)#name ofis
Switch(config)#interface range gi1/0/3-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 101
Switch(config)#vlan 102
Switch(config-vlan)#name yonetim
Switch(config)#interface range gi1/0/5-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 102
Switch(config)#vlan 103
Switch(config-vlan)#name misafir
Switch(config)#interface range gi1/0/7-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 103
```

Şekil 67. Switch VLAN Tanımlama İşlemleri

Switch üzerinde Şekil 67'de yapılan yapılandırmada personel, ofis, yonetim ve misafir VLAN'ları 1-2. Portlar personel, 3-4. Portlar ofis, 5-6. Portlar yonetim ve 7-8. Portlar misafir VLAN'ı olacak şekilde tanımlamalar yapılmıştır.

```
Switch(config)#interface gi1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100,101,102,103
```

Şekil 68. Trunk Port Olarak Tanılama Yapma

Pfsense güvenlik duvarının LAN portu switchde 24. porta bağlandığı zaman, Pfsense tarafında tanımlanmış olan VLAN'ların switch üzerinde tanımlı portlardan IP dağıtabilmesi için gerekli ayarlamalar tamamlanmıştır.

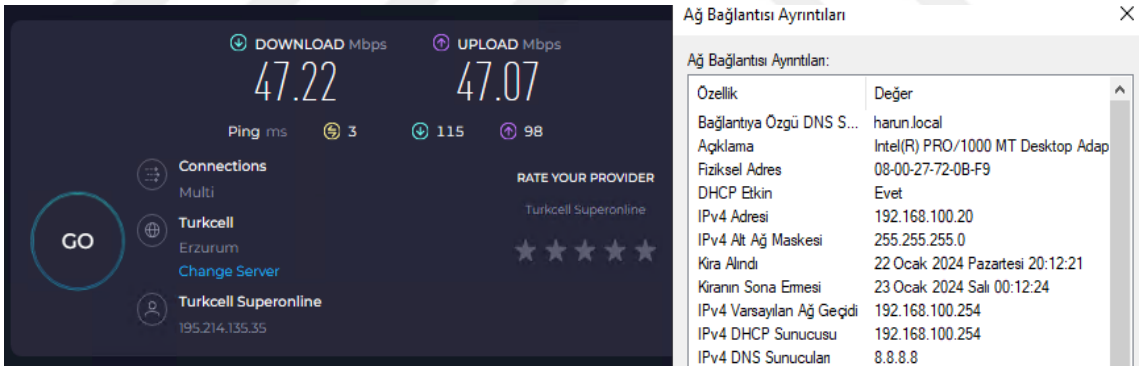
```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/9, Gi1/0/10, Gi1/0/11
                                                Gi1/0/12, Gi1/0/13, Gi1/0/14
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24, Gi1/0/25, Gi1/0/26
                                                Gi1/0/27, Gi1/0/28
100  personel                         active    Gi1/0/1, Gi1/0/2
101  ofis                             active    Gi1/0/3, Gi1/0/4
102  yonetim                          active    Gi1/0/5, Gi1/0/6
103  misafir                          active    Gi1/0/7, Gi1/0/8
```

Şekil 69. Swicth VLAN Yapılandırması

Yapılan bu işlemlerden sonra switch üzerine takılan patch kablo ile bilgisayarların 1-2. Portlardan 192.168.10.0, 3-4. Portlardan 192.168.11.0, 5-6. Portlardan 192.168.12.0 ve 7-8. Portlardan 192.168.13.0 ağlarından IP almaları sağlanmıştır.

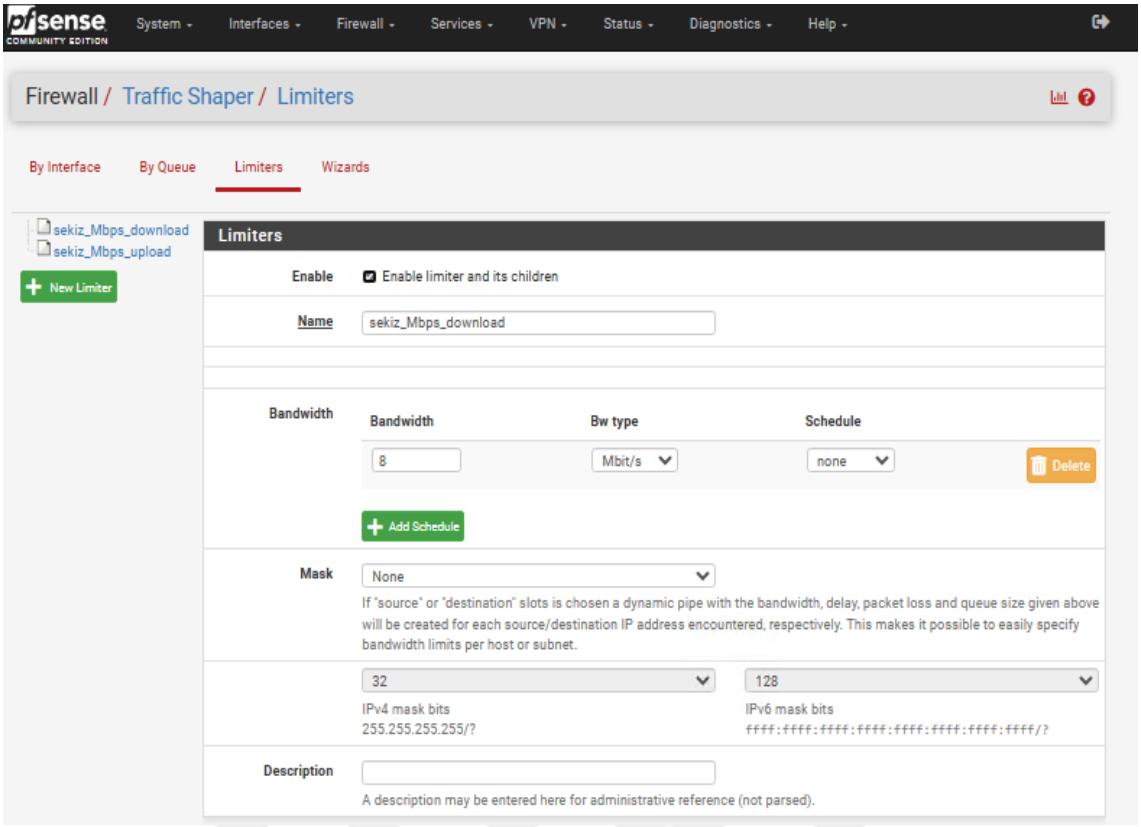
4.10 Trafik Testleri Ve Filtreleme Testleri

Pfsense kurulumu ve ayarlamaları yapıldıktan sonra DMZ ağından IP alan sanal sunucuda bant genişliği testi için https://www.speedtest.net/ adresi kullanılarak indirme ve yükleme hızları incelenmiştir. Test sisteminin kurulduğu ağ 50Mbps indirme ve yükleme hızına sahiptir.



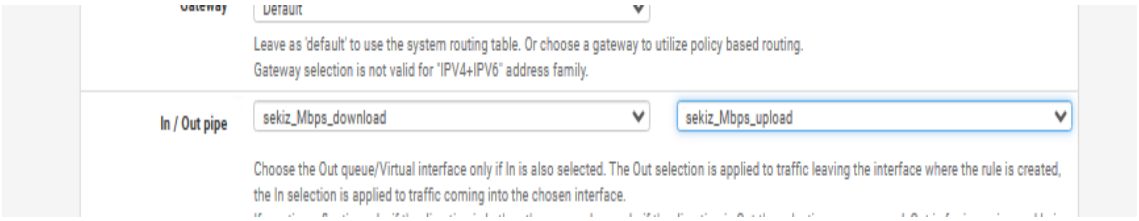
Şekil 70. Sanal Sunucu Ağında İlk kurulumdan Sonra İnternet Hız Testi

Test sonucunda alınan hız verileri Şekil 70'te gösterildiği gibi 47Mbps indirme ve yükleme hızındadır. Pfsense güvenlik duvarından yazılacak kurallar ile bu hız sınırlarında limit işlemi gerçekleştirilebilmektedir. Adil kullanım için yapılan bu işlemler Traffic shapper menüsünden limitleyici oluşturduktan sonra Rules menüsünden kural yazılarak yapılmaktadır.



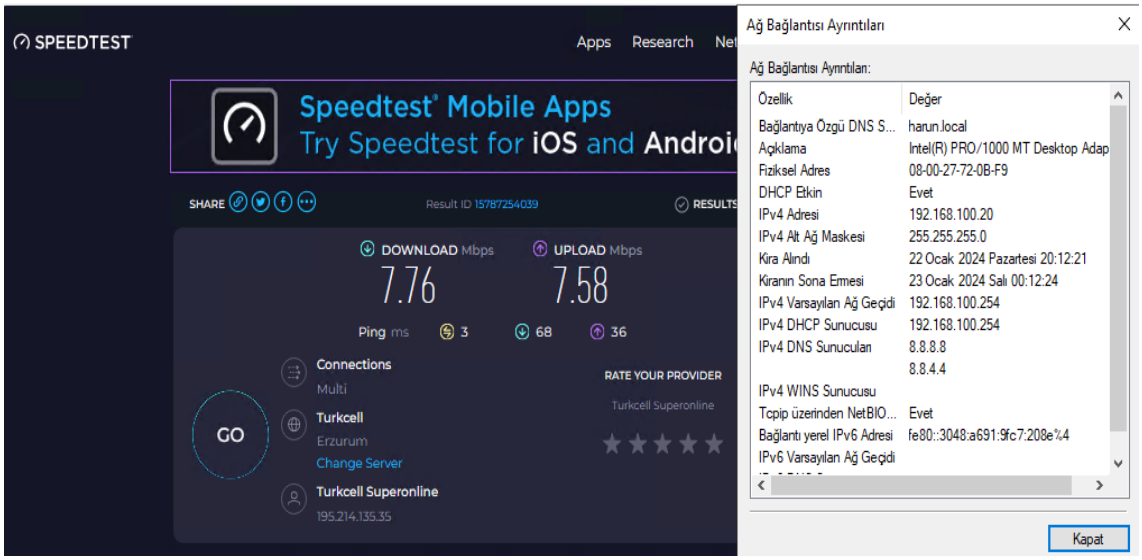
Şekil 71. Traffic Shapper Ekranında Limitleyiciler

8Mbps indirme ve yükleme hız limitleyicileri Şekil 71'de gösterildiği gibi oluşturulduktan sonra kullanılması için aktif moda alınmıştır. Burada yapılan tanımlamalar istenilen VLAN'da kullanılabilmektedir.



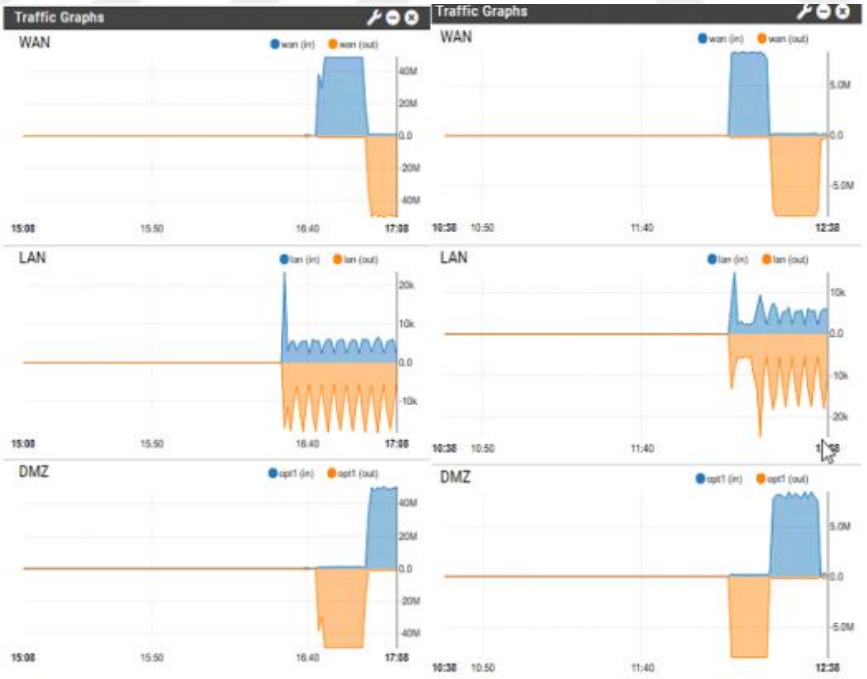
Şekil 72. Limitleyicilerin Güvenlik Kuralına Eklenmesi

Oluşturulan kuralın Şekil 72'de gösterilen gelişmiş yapılandırma seçeneklerinden In/Out Pipe bölümünde birinci bölüme indirme ikinci bölüme yükleme limitleyicisi seçilerek hız limitleme işlemi gerçekleştirilmiştir.



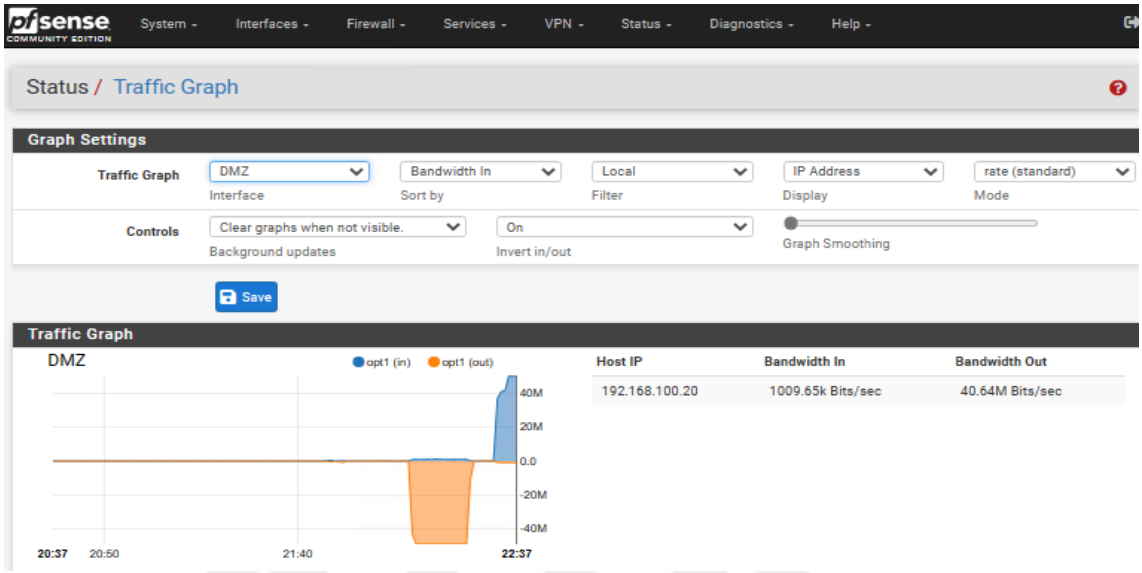
Şekil 73. Sanal Sunucu Ağında Limitleyiciden Sonra İnternet Hız Testi

Yeniden test yapıldığında hız verileri 7.76Mbps ve 7.58Mps olarak Şekil 73'teki gibi görülmüştür. Oluşturulan limitleyiciler görevlerini yerine getirmiştir. Bu limitleyicilerden ihtiyaçlar doğrultusunda istenildiği kadar oluşturabilir ve tanımlı VLAN'lara uygulanabilir.



Şekil 74. Limitleyiciden Önce ve Sonra Dashboard Trafik Grafikleri

Trafik limitleyici devreye alındıktan sonra limitleyicide tanımlanan 8Mbps değerinde indirme ve yükleme işleminin yapılabildiği görülmüştür. Hem speettest sitesinde hem de Pfsense trafik grafiğinde aynı değerler alınmıştır.

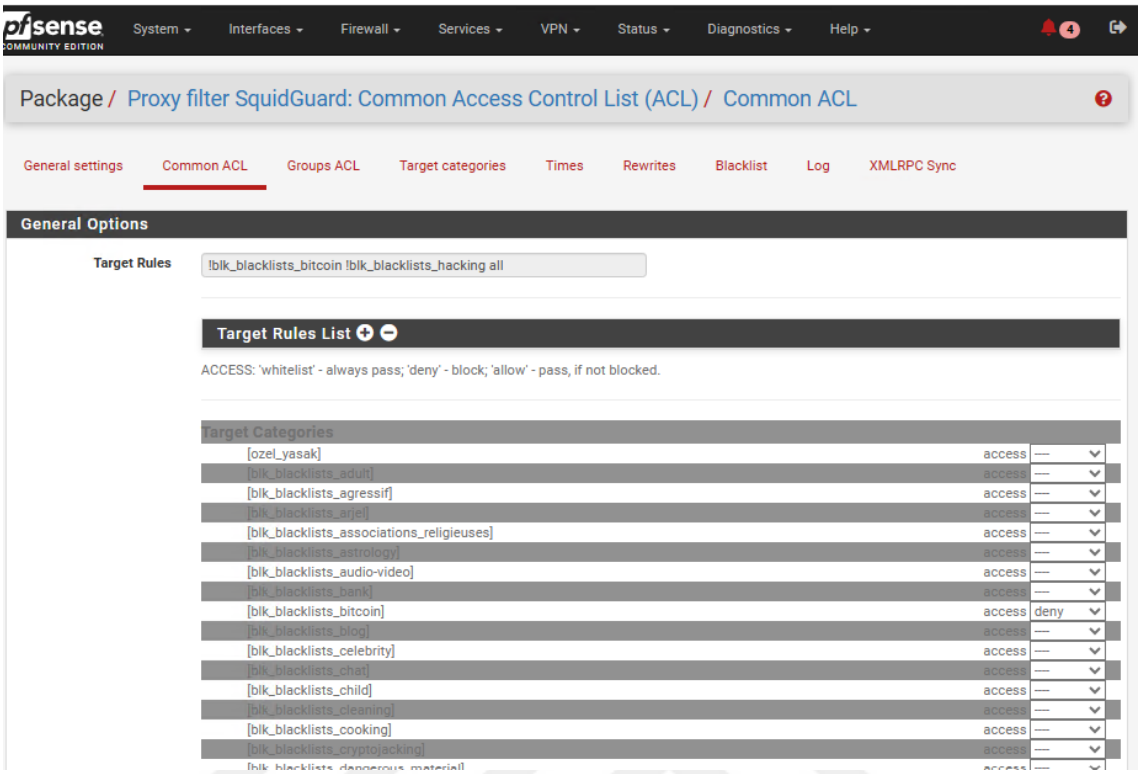


Şekil 75. VLAN Bazlı Kullanıcı Trafik Ekranı

Ağa bağlı tüm kullanıcıların dahil oldukları VLAN'lar da trafik oluşturdukları zaman anlık olarak bant genişliklerinin kullanıcı bazlı olarak listelendiği ve bulundukları ağın bant genişliğinin görülebildiği ekran Şekil 75'teki gibidir. Bu menünün dashboardda bulunan trafik grafiği bölümünden farkı o ağdaki kullanıcılarında görüntülenebilmesidir.

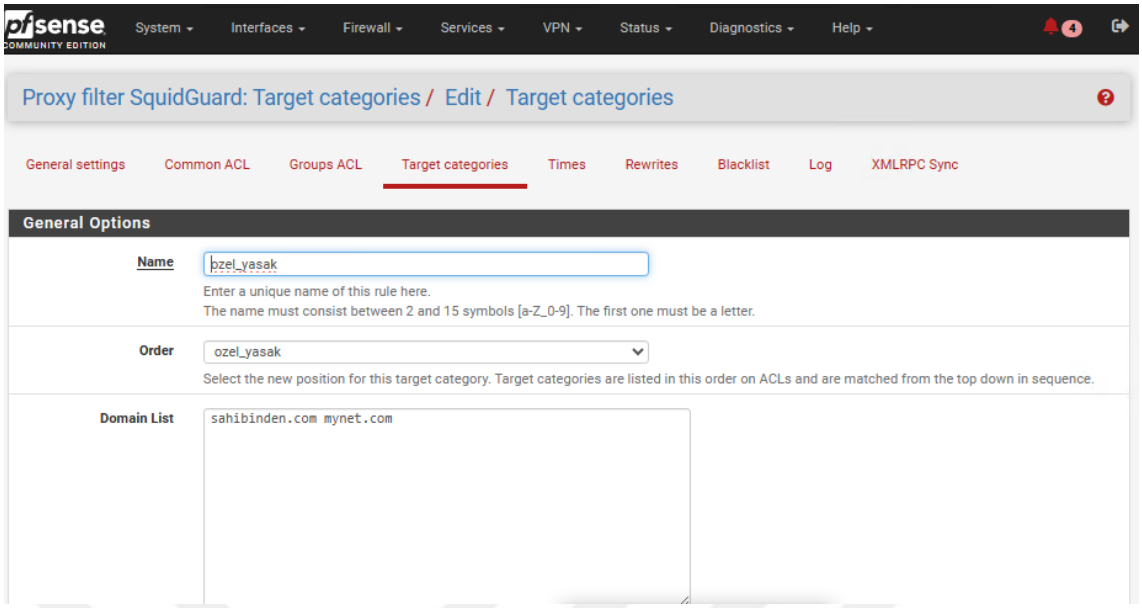
Trafik testlerinden sonra filtreleme servislerinin çalışması için hangi tür site kategorilerinin veya sitelerin filtreleneceği belirlenmiştir.

,



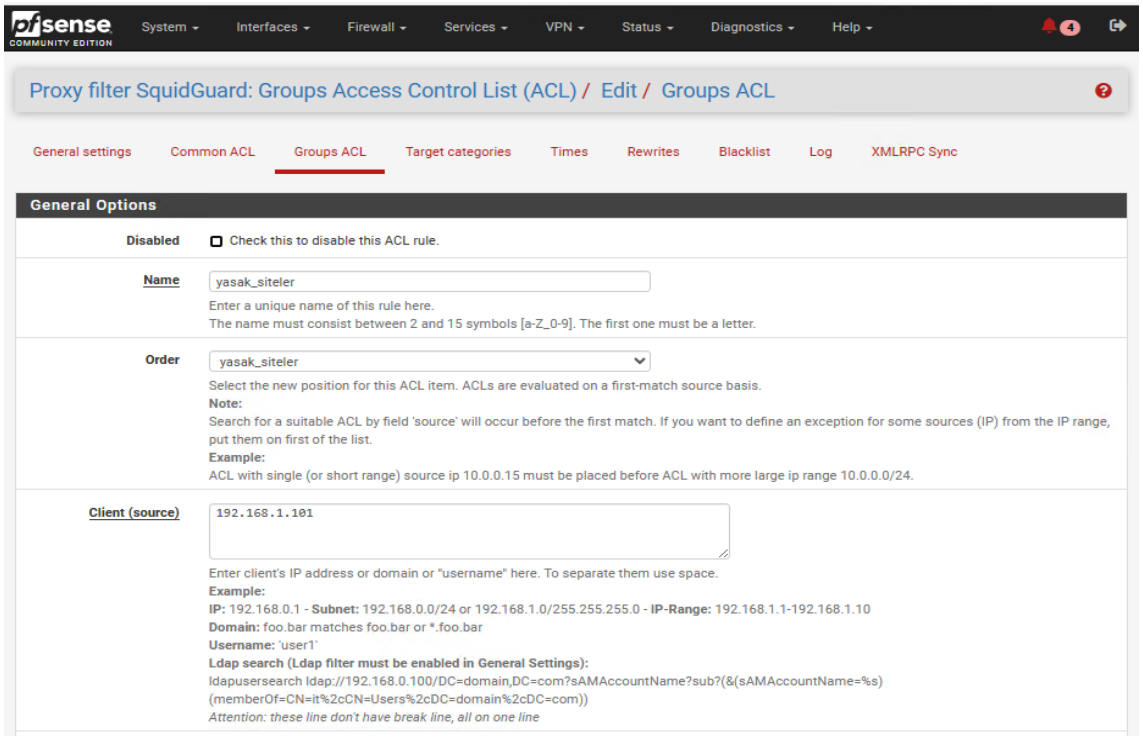
Şekil 76. Filtreleme Kategorileri

Şekil 76’ da görünen Comman Acl menüsü filtreleme işlemleri için kara listeden çekilen kategorilerin görüldüğü bölümdür. Bu Menüden “bitcoin” kategorisi “deny” olarak seçilmiştir.



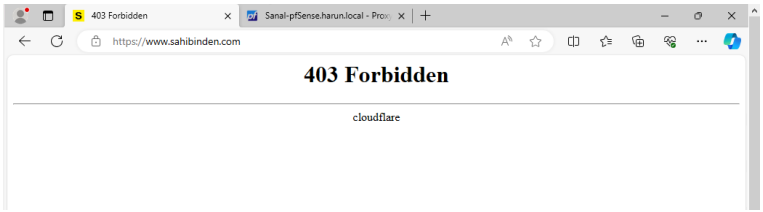
Şekil 77. Hedef Kategoriler

Hedef kategorilerin belirlenmesi bir grup olarak tanımlanan kategorilerin kullanım kolaylığı sağlaması ve ağ bazlı olarak filtreleme işlemlerinin kullanımı kolaylaştırmak için önemlidir. Türkiye'de çok ziyaret edilen iki adet site Şekil 77'de gösterildiği gibi özel_yasak kategorisinde filtrelenerek erişim engeli konulmuştur.



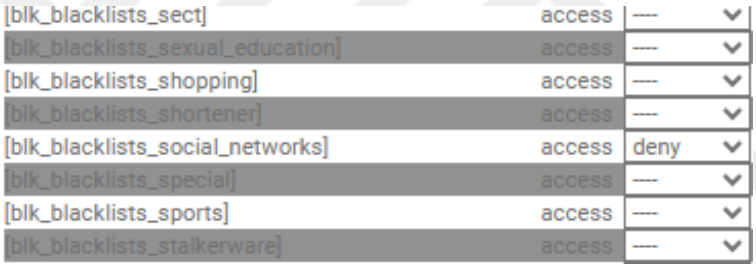
Şekil 78. Filtreleme Yapılacak Gruplar

Grup Acl menüsü ile filtreleme işlemine tabi tutulacak ağ veya istemcilerin gruplarının oluşturulduğu bölümdür. Bu bölümde 192.168.1.101 IP adresine sahip istemci yasak isteler isimli gruba dahil edilmiştir ve belirlenen sitelere erişim yapması engellenmiştir. Clint alanına istenilen IP veya ağ adresi yazılarak gruplar oluşturulabilmektedir.



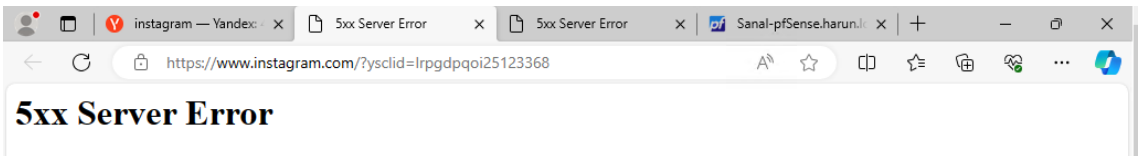
Şekil 79. Eklenen Siteye Erişimin Engellenmesi

Şekil 79'da gösterildiği gibi Target categories bölümünde ozel_yasak olarak belirtilen siteye erişim engellendiği için browser'da 403 hatası gelmektedir. Engelli listesinde eklenecek olan sitelere erişim engeli bu menüden yapılabilmektedir.



Şekil 80. Kategori Olarak Engelleme

Pfsense squidguard ile site bazlı olarak engelleme yapılabileceği gibi kategori bazlıda engelleme yapılabilmektedir. Şekil 80'de social_networks kategorisi "deny" olarak belirlendikten sonra tanımlı kara listede bulunan tüm sosyal ağ sitelerine giriş engellenmiştir.



Şekil 81. Sosyal Ağ Engeli

Şekil 81'de görüntülenen browser sayfasında social network kategorisi "deny" olarak tanımlandığı için sosyal ağ sitelerine giriş yapılmak istendiği zaman "5XX Server Error" hatası alınmıştır.

5. SONUÇ ve ÖNERİLER

Araştırmada sistemlerin daha güvenli hale getirilmesi için mevcut sistemlere alternatif olabilecek öneriler verilmektedir. Problemin çözüme ulaşması için sanallaştırma sistemlerinin içerisinde açık kaynak kodlu güvenlik duvarları kullanılarak işletme ve kurumlara hatta bireysel kullanıcılara yeni öneriler sunulmuştur. Bu öneriler sanallaştırılmış sistemlerde açık kaynak kodlu güvenlik duvarları kullanılarak kaynaklardan, lisans ücretlerinden ve zamandan tasarruf edilebileceğini göstermiştir.

Yapılan araştırmada açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanılmasının mümkün olduğu fakat kurum ve işletmelerin bu yazılımları kullanmakta kararsız kalmalarındaki en önemli durumun teknik destek ile ilgili olduğu görünmektedir. Ayrıca sistemlerinde oluşabilecek bir güvenlik açığında karşılaşacakları durumlar göz önüne alındığında kurumlar ve işletmeler karşılarında garantör olarak bir firma istemektedirler. Bu durum açık kaynak kodlu yazılımların bilgisayar sistemlerinde hak ettiği değeri ve kullanılabilirliğini çok etkilemektedir.

Özellikle açık kaynak kodlu yazılımların kurum ve işletmelerde kullanılmasının ne kadar faydalı olacağı çok iyi irdelenmelidir ve bunun için sisteme özel bir çalışma yapılmalıdır.

Ticari olarak kullanılan güvenlik duvarları sistemlerine uygun donanımları ile birlikte satılmaktadır. Son yıllarda ise bu firmalar sanallaştırılmış sistemlerde kullanılmak üzere kendi güvenlik duvarlarını hazırlamıştırlar. Açık kaynak kodlu güvenlik duvarları teknolojik anlamda gelişmelerin gerisinde kalmadan sanallaştırılmış sistemlerde güvenli bir şekilde çalışabilmektedir. Bu araştırmada elde edilen verilerle açık kaynak kodlu sistemlerinin sanallaştırılmış sistemlerde güvenli ve sorunsuz bir şekilde kullanılabileceği görülmüştür.

Açık kaynak kodlu güvenlik duvarlarından Pfsense sanallaştırılmış sistemde çalıştırılmış ve bilişim sistemlerinde kullanılan genel yapılandırmaları yapılarak testleri gerçekleştirilmiştir. Yapılan çalışmalar neticesinde stabil olarak çalıştığı görülmüştür. Genel olarak kullanılan kural yazma, bant genişliği limitleme ve trafik filtreleme işlemleri sorunsuz bir şekilde gerçekleştirilmiştir.

Toplanan bilgiler ve yapılan araştırmalar sonraki çalışmalara ışık tutacaktır. Daha sonra yapılacak çalışmalarda açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanılmasının uygulaması gerçekleştirilebilir. Açık kaynak kodlu güvenlik duvarlarının sanallaştırılmış sistemlerde kullanılarak performansları kıyaslanabilir. Ayrıca sistemlerde kullanılabilecek açık kaynak ve ticari tüm güvenlik duvarlarının performans ve kaynak kullanım karşılaştırılması da yapılabilir.

KAYNAKLAR

Anand, A., Krishna, A., Tiwari, R., ve Sharma, R. (2018). Comparative Analysis between Proprietary Software VS. Open-Source Software VS. Free Software. *5th IEEE International Conference on Parallel, Distributed and Grid Computing*, 144-147.

Anwar, M. (2013, Aralık). Virtual firewalling for migrating virtual machines in cloud computing. *5th International Conference on Information and Communication Technologies*, (s. 1-11). Karachi, Pakistan.

Bakker, J., Welch, I., ve Seah, W. (2016, Kasım). Network-wide virtual firewall using SDN/OpenFlow. *In 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks*, s. 62-68.

Basak, D., Toshniwal, R., Maskalik, S., ve Sequeira, A. (2010). Virtualizing Networking and Security in the Cloud. *ACM SIGOPS Operating Systems Review, 44(4)*, 86-94.

Bessen, J. (2002). What good is free software. *Government policy toward open source software, 12*, 27.

Büyükyılmaz, E. (2016). *Sunucu sanallaştırma Teknolojili veri merkezi ve bir uygulaması*. (Tez No. 434251) [Haliç Üniversitesi, İstanbul]. Yükseköğretim Kurulu Ulusal Tez Merkezi. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Crowston, K., Wei, K., Howison, J., ve Wiggins, A. (2008). Free/Libre open-source software development: What we know and what we do not know. *ACM Computing Surveys (CSUR), 44(2)*, 1-35.

Çalık, M., ve Sözbilir, M. (2014). Parameters of Content Analysis. *Eğitim ve Bilim, 39(174)*, 33-38.

Çavdar, M. C., Korpeoglu, I., ve Ulusoy, Ö. (2024). A Utilization Based Genetic Algorithm for virtual machine placement in cloud systems. *Computer Communications,* 136-148.

Datta, R., Choi, S., Chowdhary, A., ve Park, Y. (2018). P4Guard: Designing P4 based Firewall. *MILCOM 2018-2018 IEEE Military Communications Conference,* (s. 64-69). Los Angeles.

Demircioğlu, B. (2023, 10 15). *Sanallaştırma Nedir?* 15 Eylül 2023 tarihinde sudo.ubuntu-tr.net: https://sudo.ubuntu-tr.net/sanallastirma adresinden alındı

DMZ Configuration in OpenWrt Routers. (t.y.). BK Web Tasarım:10 Ekim 2023 tarihinde https://www.bkwebtasarim.com/dmz-nedir/ adresinden alındı

Doğru, A. (2019). *Sunucu sanallaştırma ve uygulama sanallaştırma teknolojileri performans karşılaştırması*. (Tez No. 538721) [Maltepe Üniversitesi, İstanbul]. Yükseköğretim Kurulu Ulusal Tez Merkezi. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Erdem, A., ve Kocaoğlu, R. (2014). Yeni Bir Ağ Güvenliği Yaklaşımı: Dinamik Zeki Güvenlik Duvarı Mimarisi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 29(4)*.

Ersever, B., Doğru, İ. A., ve Dörterler, M. (2017). Büyük Ölçekli Veri Merkezleri İçin Bulut Bilişim Kullanarak Sunucu Sanallaştırma. *Gazi Mühendislik Bilimleri Dergisi, 3(1),* 20-26.

Ford, J., Arnold, D., ve Saniie, J. (2023). Environment Provisioning and Management for Cybersecurity Education. *2023 IEEE International Conference on Electro Information Technology (eIT),* 368-372.

Hogg, S. (2023, 09 2). *Death to Firewalls; Long Live Firewalls*. Networkworld: 02 Eylül 2023 tarihinde https://www.networkworld.com/article/738768/cisco-subnet-death-to-firewalls-long-live-firewalls.html adresinden alındı

IBM. (t.y.). What is open source software? :10 Ocak 2023 tarihinde https://www.ibm.com/tr-tr/topics/open-source adresinden alındı

IBM. (t.y.). Ocak 5, 2022 tarihinde Açık kaynak ve kapalı kaynak kodlu yazılım: https://www.ibm.com/tr-tr/topics/open-source adresinden alındı

İnternet Kullanım İstatistikleri. (2023, Ocak 5). Ocak 5, 2022 tarihinde Internet World Stats: https://www.internetworldstats.com/stats.htm adresinden alındı

İşler, D. B., Çiftçi, M., ve Yarangümelioğlu, D. (2013). Halkla İlişkiler Aracı Olarak: Sosyal Medyanın Kullanımı ve Yeni Stratejiler. *Sosyal ve Beşeri Bilimler Dergisi, 5(1),* 174-185.

Kapitsak, G. M., Tselikas, N. D., Kyriakou, K.-I. D., ve Papoutsoglou, M. (2022). Help me with this: A categorization of open source software problems. *Information and Software Technology, 152*, 107034.

Kervancı, İ. (2017). *Açık kaynak kodlu sanallaştırma bir üniversite örneği: Gaziantep Üniversitesi*. (Tez No. 493773) [Kahramanmaraş Üniversitesi, Kahramanmaraş]. Yükseköğretim Kurulu Ulusal Tez Merkezi. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Khajehei , K. (2014). Role of virtualization in cloud computing. *International Journal of Advance Research in Computer Science and Management Studies, 2(4),* 15-23.

Kiratsata, H. J., Raval, D., Viras, P. K., Lalwani, P., Patel, H., ve Panchal, S. D. (2022). Behaviour Analysis of Open-Source Firewalls Under Security Crisis. *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET),* 105-109.

Kreuter, D. (2004). Where server virtualization was born. *Virtual Strategy Magazine*.

Li, H., Deng, J., Hu, H., Wang, K.-C., Ahn, G.-J., Zhao, Z., vd. (2017). Poster: On the Safety and Efficiency of Virtual Firewall Elasticity Control. *In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, (s. 129-131).

Li, X., Qian, Z., Lu, S., ve Wu, J. (2013). Energy efficient virtual machine placement algorithm with balanced and improved resource utilization in a data center. *Mathematical and Computer Modelling, Volume 58, Issues 5–6*, 1222-1235.

Liu, A. X., ve Gouda, M. G. (2008). Diverse firewall design. *EEE Transactions on Parallel and Distributed Systems, 19(9),* 1237-1251.

Machida, F., Kim, D. S., ve Trivedi, K. S. (2013). Modeling and analysis of software rejuvenation in a server virtualized system with live VM migration. *Performance Evaluation 70.3*, 212-230.

Patel, V., Patel, D., ve Parmar, S. (2018). Arcus Cloud: A Private Cloud Establishment. *International Journal of Computer Sciences and Engineering, 6(3)*, 283-291.

Peffers, K., Tuunanen, T., Rothenberger, M. A., ve Chatterjee, S. (2014). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24(3),* 45-77.

Pfsense. (t.y.). Open Source Securıty 12 Ekim 2023 tarihinde https://www.pfsense.org/ adresinden alındı

Posey, B. (2022, 8 9). *What is a Server?* TechTarget:08 Eylül 2023 tarihinde https://www.techtarget.com/whatis/definition/server adresinden alındı

Sharma, R., ve Parekh, C. (2017). Firewalls: A Study and Its Classification. *International Journal of Advanced Research in Computer Science, Volume 8, No. 4,* 1979-1983.

Şahinaslan, E. (2023). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ve Uygulaması.* LAP Lambert Academic Publishing, Editör:Vetrici Luminita, Basım sayısı:1, Sayfa sayısı:176, ISBN:978-620-5-64044-9.

Şahinaslan, Ö., Razbonyalı, M., ve Şahinaslan, E. (2010). Open Source Administration Software and Implementation Results for ensuring Electronic Communication and Information Security. *Gediz Üniversitesi İSCSE Dergisi*

Tümer, H., ve Şahinaslan, Ö. (2022). Configüration Open Source Firewalls on Virtual Systems. *Third International Şişli Science Congress*, (s. 52-53). Istanbul.

Wack, J., Cutler, K., ve Pole, J. (2002). *Guidelines on Firewalls and Firewall Policy.* Gaithersburg: National Institute of Standards and Technology .

Wikipedia. (2022, Aralık 25). "Hypervisor" https://en.wikipedia.org/wiki/Hypervisor adresinden alındı

Wu, H., Ding, Y., Winer, C., ve Yao, L. (2010). Network security for virtual machine in cloud computing. *In 5th International conference on computer sciences and convergence information technology. IEEE*, 18-21.

Xianqin, C., Han, W., Sumei, W., ve Xiang, L. (2009). Seamless virtual machine live migration on network security enhanced hypervisor. *In 2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology, IEEE.*, (s. 847-853).

Xu, Z., Di, S., Zhang, W., Cheng, L., ve Wang, C.-L. (2011). WAVNet: Wide-Area Network Virtualization Technique for Virtual Private Cloud. *In 2011 International Conference on Parallel Processing, IEEE*, (s. 285-294).

Yuusuf, H., ve Vidalis, S. (2012). On The Road To Vırtualızed Envıronment . *In 2012 Third International Conference on Emerging Intelligent Data and Web Technologies*, s. 270-275.

ÖZGEÇMİŞ

Harun TÜMER

Eğitim

Lisans	2020 Namık Kemal Üniversitesi, Mühendislik Fakültesi Bilgisayar Mühendisliği (3,55/4)
Lisans	2009 Gazi Üniversitesi, Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği (2,84/4)

İş/İstihdam (Varsa)

2023 - Devam	Başuzman. Hazine ve Maliye Bakanlığı, Sümer Holding AŞ., Bilgi İşlem
2015 – 2023	Öğretim Görevlisi. Ardahan Üniversitesi Teknik Bilimler MYO
2013- 2015	Bilgisayar Öğretmeni, İkiteknik Bilişim, Eğitim ve Danışmanlık Hizmetleri
2010- 2013	Yazılımcı, Teknik Servis, CEO-TEK Bilgisayar
2009- 2010	Veritabanı Yöneticisi, Part-time Yazılımcı Stajyer, METEKSAN

Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler

Şahinarslan Ö., Tümer H., (2022) "*Configuration Open Source Firewalls On Virtual Systems.",* Third International Şişli Science Congress, 26-27 Mayıs 2022, Sayfa 52.