

PFSense PLATFORM İLE L7 FİLTRELEME VE QOS UYGULAMALARI

Vedat FETAH

**Ege Üniversitesi BITAM Network Yönetim Grubu UBE Binası Zemin Kat. 35100
Bornova – İzmir.**

İçindekiler Dizini

1. ÖZET.....	3
2. GİRİŞ.....	3
3. Açık Kaynak Kodlu Yazılım Kullanımının Önemi:.....	3
4. L7 Filtreleme:.....	4
5. Trafik Kontrolü ve QOS:.....	4
6. FreeBSD Seçiminin Nedenleri.....	4
7. PfSense Platformu.....	5
PFSENSE Arayüzü.....	6
Güvenlik Duvarı Özellikleri.....	7
State Tablosu Özelliği.....	8
8. UYGULAMA VE DİZAYN:	9
9. L7 UYGULAMA SONUÇLARI:.....	13
10. SONUÇ:.....	17
KAYNAKLAR:.....	17

1. ÖZET

Üniversiteler gibi büyük kurumsal ağlarda; çok sayıda kullanıcı farklı ihtiyaçları ile aynı anda internet hizmetini kullanmayı talep etmektedir. Kurumsal kullanıcı politikalarının kısıtlı olmaması veya uygulanamaması nedeniyle, bazı kullanıcılar tarafından aşırı band genişliği tüketimi gerçekleşmekte ve band genişliği yeterince etkin kullanılamamaktadır. Bu sebeple; peer to peer (P2P), Video Streaming, oyun vb. programların bağlantı/transfer ini, portlara bakmaksızın engelleyebilecek sistemlere ihtiyaç duyulmaktadır.

Kurum ağına girip çıkan paketler üzerinde daha etkin yaptırımlar uygulayabilmek ve ağ kullanımının etkinliğini arttırabilmek için OSI uygulama katmanı (L7) seviyesinde güvenlik duvarı (firewall) kullanımı önemli bir hal almıştır. Bu belgede bu tür bir çözüm için önerilen açık kaynak kodlu PFSENSE yazılımı ve nasıl kurulabileceği tanıtılmıştır.

2. GİRİŞ

Eskiden yapılan uygulamalarda kaynak, hedef adresi veya port bazlı kısıtlamalar yapılmaya çalışılmıştır. Ancak günümüzde yeni nesil uygulamalarda yapılan değişiklikler bu konuda engellemeleri ve politika dışı kullanımı engelleme amaçlı olarak policy tabanlı veya Qos protokolleri ile yeni uygulamalar geliştirilmiştir. Eski yöntemde yapılan uygulamalar da günümüzde etkisini kaybetmeye başlamıştır. Örnek olarak akademik ağlar bu konuda göz önünde olan uygulama birimleridir. Özellikle Türkiye şartlarında üniversitelerin birçoğunda kaynak ip adresi, hedef ip adresi ve port bazlı engelleme gibi yöntemler kullanılarak bu sorun çözülmeye çalışılmıştır. Ancak uygulama seviyesinde bazı uygulamalar ile kullanıcılar bu yöntemleri aşmayı başarmışlardır. Üniversitelerde birçok uygulamanın engellenmemesi, kullanıcıların özel firmalar yada askeri birimlerdeki gibi sıkı uygulama politikaları ile yaptırım uygulanması gibi yöntemlerle caydırılması mümkün olmamaktadır. Ancak bu uygulamaların olmaması uzun vadede bilgi işlem birimlerinde ciddi band genişliği kullanımı sorunlarına da yol açmaktadır. Özellikle sağlık hizmetlerini yürüten birimleri bulunan üniversitelerin ciddi sorunları ortaya çıkmaktadır. Bu sebeple L7 filtreleme veya Qos uygulamaları kullanılması zorunluluğu günden güne daha zorunlu hale gelmektedir.

3. Açık Kaynak Kodlu Yazılım Kullanımının Önemi:

Her ne kadar ticari ürünler kadar başarılı imzaları olmadığı söylene de açık kaynak kodlu yazılımlarla ciddi anlamda ağ trafiğinizi düzenleyebilmeniz mümkündür. Açık kaynak kodlu yazılımların önemi imza ücretinin olmaması, kendi imzalarınızı yazabilmeniz ve insan kaynağının masraf kapısı düşüncesinin ortadan kaldırılması olarak belirtilebilir. Ayrıca ticari ürünlerin bazı ciddi handikapları da bulunmaktadır. Yanlış yüklenen bir imzanın ağızda ciddi sıkıntılar ortaya çıkarması olası yaşanacak senaryolardandır. Bu gibi durumlarda kapalı kutunun üretici firmasının

sorunun neden kaynaklandığını bulup size uygun çözüm üretmesini beklemekten başka çareniz yoktur.

4. L7 Filtreleme:

Diğer trafik sınıflandırma araçlarından farklı olarak uygulama bazında trafiği inceleyerek işlem yapar. L7 filtreleme ile temelde yapılabilecek işlemleri 3 adımda genelleyebiliriz.

1. Sahip olunan band genişliğinin efektif kullanılabilmesi.
2. Ip yada network bazlı band genişliği yönetimi yapabilmeyi sağlaması.
3. İsteğe göre belirli uygulamalara garanti band genişliği ataması gerçekleştirilebilmesi.

Bir L7 güvenlik duvarının bu uygulamaları gerçekleştirebilmesinin yanında kural yazma bölümünün sade ve anlaşılabilir olması gerekmektedir.

5. Trafik Kontrolü ve QOS:

Ağ İletişimi Hizmet Kalitesi (İngilizce *Quality of Service*, kısaca **QoS**), Ağ üzerindeki uygulamaları önceliklendirerek zaman kaybını azaltmayı hedefleyen bir ağ servisi. Bir ağ bağlantısı üzerinden çalışan bir trafik veya program türüne öncelik veren çeşitli tekniklere karşılık gelir. İnternet hızı = band genişliğinin yüksek olması gibi yanlış bir kanı vardır günümüzde. Bu konuda şu örneği vererek açıklamak daha doğru olacaktır. Aynı otoyolda hareket eden araçlar içerisinde en hızlısı olan yükte hafif olandır. Yani yüklü bir kamyon yavaş hareket edeceği gibi trafikte de aksamalara yol açacaktır. Bu sebeple ağ üzerinde hareket eden paketlerin büyüklükleri sizin hızınızı belirleyen yapılar olmaktadır. Trafik şekillendirme ve Qos sayesinde ağ üzerinde hareket eden paketler sizin daha önce ağınız üzerinde analiz edip önceliklerini belirttiğiniz sırada bölünerek kuyruğa alınır. Bu sayede iletişimin hızlı olması kesintiye uğramaması gereken protokoller daha öncelikli ve belirli bir band genişliğine sahip olarak sorunsuz bir şekilde çalışmaktadır. Ağınızda kullanılan P2P uygulamaları sizin isteğiniz dışında band genişliğinizi ele geçirse bile Voip görüşmelerinizi kesintiye uğramaksızın gerçekleştirebilmenize olanak sağlar. [1]

6. FreeBsd Seçiminin Nedenleri

FreeBSD®, işletim sistemleri arasında en bilinen ticari işletim sistemleri de olmak üzere diğer işletim sistemlerinde halen bulunmayan ağ yapılandırma, performans, güvenlik ve uyumluluk özelliklerini bir arada sunar. Donanım kaynaklarını etkin ve verimli kullanarak binlerce simultane kullanıcı prosesi için tepki zamanlarını en iyi seviyede tutar, çok ağır yükler altında dahi güçlü ağ servisleri sunmaya devam eder. Yapılan karşılaştırmalı değerlendirmelerde Linux 2.6.22 veya 2.6.24 çekirdeklerine göre %15 daha fazla performansa sahip olduğu ortaya konulmuştur.

FreeBSD' nin Avantajları:

- Lisans gerektirmemesi
- Kullanıcı ve bağlantı (concurrent connection) bazlı lisans sınırlamasının olmaması
- Donanım kapasitesi ihtiyacı ve maliyetinin düşük olması
- Farklı işletim sistemlerine ve benzerlerine göre çok daha stabil, performanslı ve güvenli olması
- Uyumluluk probleminin bulunmaması
- İleri düzey yük paylaşımı ve (High Available) desteği [2]

7. PfSense Platformu

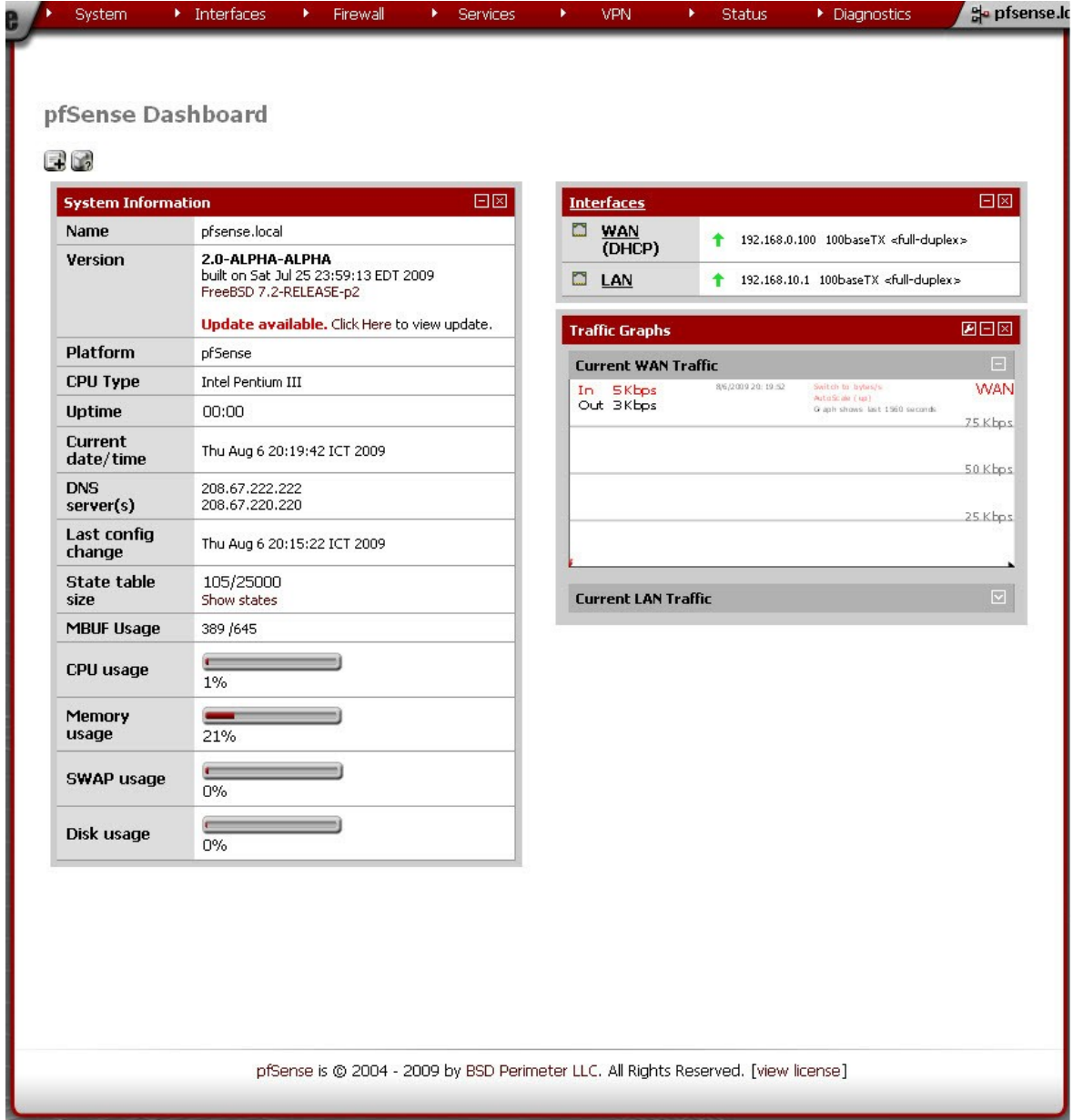
Pfsense dağıtımı neden tarafımızdan seçildi? L7 seviyesinde güvenlik duvarı olarak çalışan birkaç dağıtım daha vardır. Bunları sayacak olursak IPCop, OpenBSD PF, ebttables ve Bandwidth Arbitrary gibi yazılımlar listelenebilir. Pfsense dağıtımı bu dağıtımlar arasından ön plana çıkaran temel özellikleri şu şekilde sıralayabiliriz:

1. L7 filtrelemede application pattern girebilir ve bu sayede dağıtımın desteklemediği patternler için paket filtreleme özelliğini kullanır.
2. Grafik arayüzünün basitliği sayesinde kullanıcı isterse ekstra modüller kurabilir.
3. Kurulabilecek modüller arasında IDS, Antivirus Gateway, Squid Proxy, ntop, trafik şekillendirme ve Vpn gibi yazılımlar sayılabilir.
4. Modülleri web arayüzden aktive edebilir yada deaktive edebilirsiniz.
5. Yüksek boyutlu disklere kurulumu sırasında diski görmeme gibi sorunlar yaşamazsınız.
6. Diğer Linux dağıtımlarındaki gibi kurulum sırasında grafik kartının tanınmaması gibi bir sorun ile uğraşmak zorunda kalmazsınız.
7. Vlan desteği vardır.
8. Birden fazla Wan ve Lan arayüzünü destekler.
9. NAT, CARP, Load Balance, Packet Capture ve Bogon networkleri tanıma özellikleri ayrıca bulunmaktadır.

Pfsense özelleştirilmiş bir FreeBSD dağıtımdır. Esas olarak güvenlik duvarı ve router olarak çalışmak üzere tasarlanmıştır. Pfsense, yüksek throughput senaryoları düşünülerek (500 Mbps) tasarlanmış bir dağıtımdır. Bu hızlarda çalışabilmesi için kullanacağınız yüksek kapasiteli bir donanım mimarisi kullanmanız gerekmektedir.

PFSENSE Arayüzü

Arayüzü oldukça basit tasarlanmış kullanımı kolay bir dağıtımdır. Bu dağıtımın 2.0 Alpha Alpha versiyonu ile birlikte L7 seviyesinde Qos ve paket filtreleme yapılabilmektedir. Önceki sürümlerinde sadece snort ve squid kullanılarak bandgenişliği kontrolü sağlanırken yeni versiyonu ile birlikte trafik şekillendirme özelliği güçlendirilmiştir. Uygulama seviyesinde bir çok uygulamanın imzası kendi içerisinde olduğu için ekstra bir çabaya gerek yoktur. Ancak var olan imzalar dışında herhangi bir uygulama için bu işlemi yürütecekseniz onun içinde paket yüklemenize ve imzayı tanıma özelliği de eklenmiş durumdadır. Pfsense kurulumunuzu bitirdikten sonra birçok değişikliği web arayüzden yapabilirsiniz. Sizi sisteminize girişle birlikte karşılayan ilk ekran aşağıdaki gibi olacaktır.



Resim 1. Pfsense Dashboard.

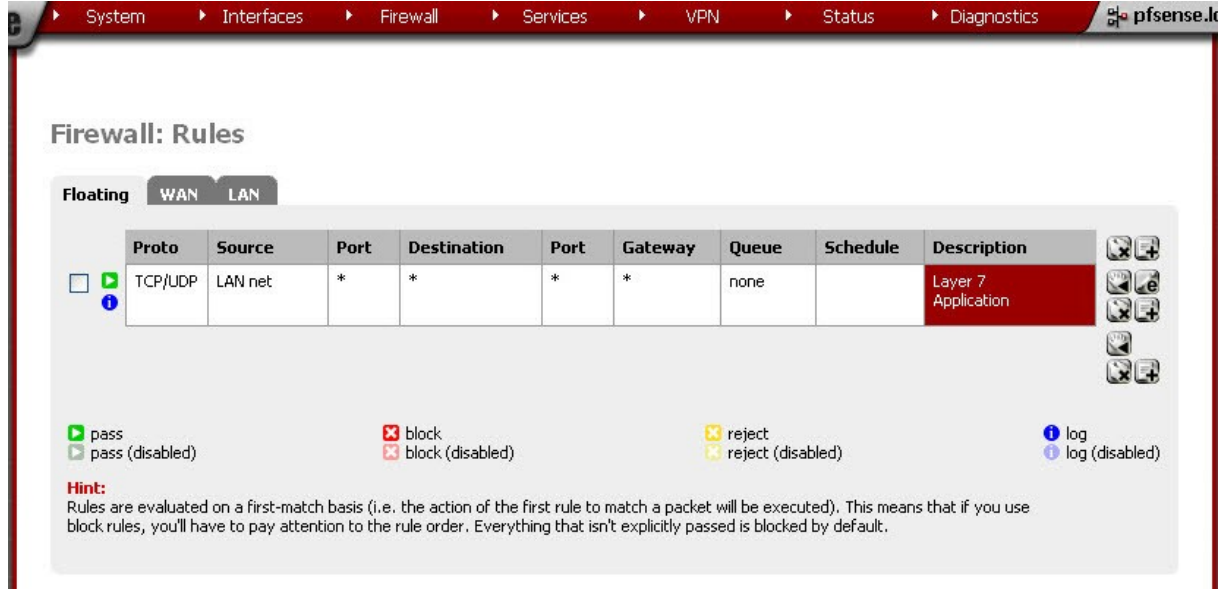
Ekran görüntüsünden de anlaşılacağı gibi dashboard ekranı özelleştirilebilmektedir. Burada CPU durumunu, ethernet arayüzlerinin durumunu, CARP durumunu gösteren ek paneller konulabilmektedir. Yukarıda bulunan kırmızı şerit üzerindeki menüler sayesinde bütün özelliklerini kullanabilmemiz mümkündür. Pfsense'i ön plana çıkaran en temel özellikleri yüklenmelerde gösterdiği performansın yanı sıra kolay paket kurulumu, forum ile ücretsiz desteği ve komut bazlı müdahale imkanı tanınmasıdır. Bu özelliklerin yanısıra ayrıca web arayüzünden seri portla bağlanılıp kontrol edilebilen bir kutu çözümü olarakta kullanılabilmesi özelliği diğer çözümler arasında ön plana çıkmasını sağlar. Kurulumla birlikte kullanabileceğiniz hazır olarak gelen özellikleri trafik şekillendirme, güvenlik duvarı ve CARP ilk olarak göze çarpanlardır.

Güvenlik Duvarı Özellikleri

Güvenlik duvarı özelliğine hızlı bir bakış atacak olursak [5]:

1. Floating, Wan ve Lan arayüzleri için ayrı kural yazma alanı vardır.
2. Yazdığınız kurallar için tanımlama (Description) yapabiliyorsunuz.
3. Kural yazarken alias tanımlama özelliği sayesinde gruplar oluşturabilir Ya da belirli bir ip adresine bir isim atanarak kullanılması sağlanabilir.
4. L7 seviyesinde kural tanımlanabilir.
5. Tanımlanan kurala belirli bir zaman dilimi için çalışması söylenebilir. Örnek verecek olursak mesai tanımı yapılabilir. Sabah 08:00 ile akşam 17:00 arasında torrent imzaları aktif olsun ya da aktif olmasın şeklinde bir girdi yazılabilir.
6. Kaynak ve hedef ip, ip protokolü, kaynak ve hedef port için TCP/UDP protokollerin tanımlanması işleri.
7. Kural bazlı olarak belirli kullanıcılar için limit belirleyebilirsiniz.
8. Her kural için loglama yaptırabilir veya iptal edebilirsiniz.

Örnek bir kural yazım tablosu görüntüsü aşağıdaki gibidir:



System > Interfaces > Firewall > Services > VPN > Status > Diagnostics pfsense.it

Firewall: Rules

Floating WAN LAN

Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
TCP/UDP	LAN net	*	*	*	*	none		Layer 7 Application

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Resim2. Güvenlik duvarı Kural Yazım Tablosu

State Tablosu Özelliği

Birçok güvenlik duvarının aksine Pfsense state tablosunu kontrol edebilme özelliğine sahiptir. Ayrıca Pfsense stateful özelliğine sahip olduğu için ilk kurulumda tüm kuralları stateful özelliğine göre çalışmaktadır.

State tablosunun temel özellikleri:

1. Kural bazlı özellikleri

- a. Eş zamanlı client bağlantılarının sayısını belirleyebilirsiniz
- b. Host başına state belirleyebilirsiniz.
- c. Yeni kurulacak bağlantıları/saniye sınırlayabilirsiniz.
- d. State zaman aşımı süresini belirleyebilirsiniz.
- e. State türünü belirleyebilirsiniz.

2. State Türleri

- a. Keep state – Bütün protokoller ile çalışır. Tüm kurallar için varsayılan olarak atanmıştır.
- b. Modulate state – Sadece TCP paketleri ile çalışır. Pfsense host adına ISN'leri kendisi üretir.
- c. Synproxy state – Proxyler gelen TCP bağlantılarını, sunucuyu olası spoof edilmiş TCP SYN saldırılarına karşı tutar. Bu seçenek keep state ve synproxy state'in karma halidir.
- d. Hiçbiri – Herhangi bir state girdisi tutulmaz. Genelde bu tür bir yapı kullanılmaz ancak bazı özel durumlar için tutulmaktadır.

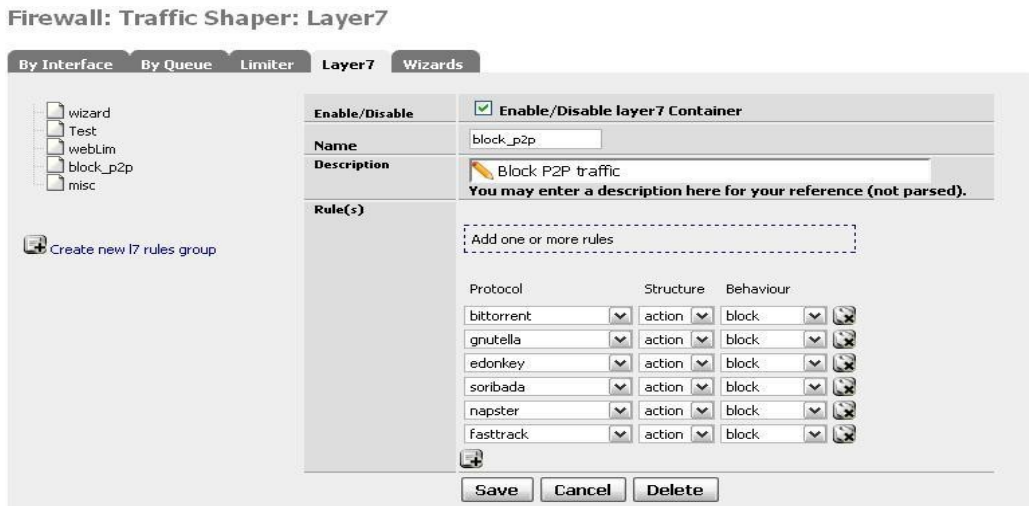
3. State tablosunun optimize edilmesi:

- a. Normal – Varsayılan olarak ayarlı algoritma.
- b. High latency – Uydu bağlantıları için çok kullanışlıdır. Idle durumuna düşmüş bağlantılar Normal'den daha geç düşmektedir.
- c. Aggressive – Idle duruma düşen bağlantılar çok hızlı bir şekilde düşürülür. Donanım performansını arttırmak için kullanılacak bir özellik.
- d. Conservative – Bu türde bağlantıların hali hazırda kullanılacak bağlantılar olduğu ihtimaline karşın bazılarının düşürülmemesidir. Bunun sonucunda memory ve CPU kullanım değerleri daha yüksek olacaktır.

Yukarıda bahsedilen özelliklerin dışında birçok özellik detaylı olarak incelenebilir. Ancak pfsense güvenlik duvarı üzerinde L7 filtreleme özelliklerini daha detaylı bir şekilde inceleyeceğiz.

8. UYGULAMA VE DİZAYN:

Daha önceki tanımlarımızda bahsettiğimiz üzere L7 filtreleme yapabilmek için öncelikli olarak uygulama olarak ipfw-classifyd konusunda bilgi vermemiz gerekmektedir. Bu uygulamanın neler yapabileceğine göz atacak olursak: (i) gelen trafik için bloklama kuralı oluşturabilir, (ii) Gelen ip paketleri veya belirlenen akışlar traffic shaper sayesinde AltQ kuyruğuna atılır. Peki bu işlemler pfsense tarafından nasıl basitleştirilmiştir? Bir L7 kuralı oluşturulduğu zaman bu işlemin sonunda pf otomatik olarak ipfw-classifyd ile arka planda kuyruğa atma işlemi için gerekli kuralları oluşturur. Burada dikkat edilmesi gereken husus, ipfw-classifyd uygulamasının sadece TCP ve UDP paketleri destekler. Bu yüzden işlemleri yapacağınız paketlerin protokolleri çok önemlidir. Pfsense kutumuzda bu kuralların nasıl yazıldığına göz atacak olursak:



Resim 3. Traffic Shaper: L7 Kural Yazma Alanı

Herhangi bir işlem yapmadan önce kendi ağımızda ne tür protokoller ile işlemler yürütülecek ve ağımızın satüre olmasına sebep olan protokollerin neler olduğu belirlenmelidir. Örnek olarak Ege Üniversitesi ağın ile ilgili bilgiler verilecek olursa şu şekilde bir sıralama ortaya çıkar:

- 1- http download
- 2- ftp download
- 3- flash video streaming
- 4- video streaming şeklinde bir sıralama ortaya çıkar.

Bu sorunun önüne geçebilmek için yapılabilecekler:

1. trafik şekillendirme ile toplam bandgeniřlięi belirlenmesi
2. İhlal yaratan kullanıcıların belirlenmesi ve oluşturulacak bir karantina grubuna alınması
3. P2P vb. Protokollerin mesai saatlerinde tamamen engellenmesi, mesai sonrasında ise istenilen bandgeniřlięine sıkıřtırılması.

Resim 3' te belirlenen protokollere göre yapılacak işlemlerde protokolün bloklanması dışında Limiter sekmesinde belirli bir limit dahilinde çalışması sağlanabilir. Yani video streaming işlemi için verilecek değerin üzerine çıkılması durumunda işlemin kuyruęa atılması özellięi de kullanılabilir. Bu işlemleri tanımladıktan sonra güvenlik duvarı tablosunda kural yazabileceğimiz alanda nasıl özellikler kullanabileceğimizi daha net görebiliriz.

In/Out	<input type="text" value="none"/> / <input type="text" value="none"/> <small>Choose the Out queue/virtual interface only if you have selected In too. The Out selection is applied to traffic going out the interface the rule is created, In is the incoming one. If you are creating a rule on the Floating tab if the direction is In then the same rules apply, if the direction is out the selections are reverted Out is for incoming and In is for outgoing and if you do not select any direction use only the In since the Out selection does not make sense in there to prevent oddities.</small>
Ackqueue/Queue	<input type="text" value="none"/> / <input type="text" value="none"/> <small>Choose the Acknowledge Queue only if you have selected Queue.</small>
Layer7	<input type="text" value="block_p2p"/> <small>Choose a Layer7 container to apply application protocol inspection rules. This rule are valid for tcp and udp protocols for now.</small>
Description	<input type="text" value="Layer7 block P2P"/> <small>You may enter a description here for your reference.</small>

Resim 4. Güvenlik duvarı kural yazım alanı

Yukarıda da görülebileceęi üzere güvenlik duvarında yazılması gereken kurala atayabileceğiniz L7 kuralı ve kuyruk işlemleri görülmektedir. Bloklama işlemi yapılabildięi gibi kuyruęa atma işlemi de gerçekteşebilmektedir.

Yukarıda belirlenen şekilde protokoller hakkında işlem yapılacaęı gibi pfsense'in kendi üzerinde bulunan sihirbazlar sayesinde belirli bazı protokol gruplar özel yaptırımlar uygulanabilir. Mesela p2p uygulamalar için atanacak bandgeniřlięini belirleyebilirsiniz bazı p2p uygulamalarını bu gruptan çıkarabilir veya hepsi için bütün bu kuralları uygulayabilirsiniz. Bu uygulamalar sadece p2p uygulamaları için geçerli deęildir. Aynı zamanda oyun networkleri için de aynı özellikleri kullanabilmeniz mümkün kılınmıştır.

Peer to Peer networking

pfSense Traffic Shaper Wizard

Enable: Lower priority of Peer-to-Peer traffic
This will lower the priority of P2P traffic below all other traffic. Please check the items that you would like to prioritize lower than normal traffic.

Next

p2p Catch all

p2pCatchAll: When enabled, all uncategorized traffic is fed to the p2p queue.

Bandwidth: %
The limit you want to apply.

Enable/Disable specific P2P protocols

Aimster: Aimster and other P2P using the Aimster protocol and ports

BitTorrent: Bittorrent and other P2P using the Torrent protocol and ports

BuddyShare: BuddyShare and other P2P using the BuddyShare protocol and ports

CuteMX: CuteMX and other P2P using the CuteMX protocol and ports

DCplusplus: DC++ and other P2P using the DC++ protocol and ports

DCC: irc DCC file transfers

DirectConnect: DirectConnect and other P2P using the DirectConnect protocol and ports

DirectFileExpress: DirectFileExpress and other P2P using the DirectFileExpress protocol and ports

eDonkey2000: eDonkey and other P2P using the eDonkey protocol and ports

Resim 5. trafik şekillendirme sihirbazı ile uygulama gruplarına belirli bandgeniřliđi atanması

Network Games

pfSense Traffic Shaper Wizard

Enable: Prioritize network gaming traffic
This will raise the priority of gaming traffic to higher than most traffic.

Next

Enable/Disable specific games

BattleNET:	<input type="checkbox"/> Battle.net - Virtually every game from Blizzard publishing should match this. This includes the following game series: Starcraft, Diablo, Warcraft. Guild Wars also uses this port.
Battlefield2:	<input type="checkbox"/> Battlefield 2 - this game uses a LARGE port range, be aware that you may need to manually rearrange the resulting rules to correctly prioritize other traffic.
CallOfDuty:	<input type="checkbox"/> Call Of Duty (United Offensive)
Counterstrike:	<input type="checkbox"/> Counterstrike. The ultimate 1st person shooter.
DeltaForce:	<input type="checkbox"/> Delta Force
DOOM3:	<input checked="" type="checkbox"/> DOOM3
EmpireEarth:	<input type="checkbox"/> Empire Earth
Everquest:	<input type="checkbox"/> Everquest - this game uses a LARGE port range, be aware that you may need to manually rearrange the resulting rules to correctly prioritize other traffic.
Everquest2:	<input type="checkbox"/> Everquest II
GunZOnline:	<input type="checkbox"/> GunZ Online
FarCry:	<input type="checkbox"/> Far Cry

Resim 6. trafik şekillendirme sihirbazı ile uygulama gruplarına belirli bandgeniřlięi atanması – 2

9. L7 UYGULAMA SONUÇLARI:

Bütün bu bahsedilen işlemler, basit bir web arayüzünden yönetilebilmektedir. Bu yöntemlerin çalışma şekli basitçe açıklanabilir. Bir L7 protokol grubu hakkında yapılacak olan işlemler önce config.xml dosyasında kayıtlı bulunan özellikler sayesinde web arayüzünden yapılır.

```

<container>
  <name>block_p2p</name>
  <enabled>on</enabled>
  <description>Block P2P traffic</description>
  <divert_port>47244</divert_port>
  <17rules>
    <protocol>bittorrent</protocol>
    <structure>action</structure>
    <behaviour>block</behaviour>
  </17rules>
  <17rules>
    <protocol>gnutella</protocol>
    <structure>action</structure>
    <behaviour>block</behaviour>
  </17rules>

```

Resim 6.1. config.xml

Resim 6.1'de belirtilen config.xml dosyasının bir parçasında p2p prokolleri ile ilgili bir kısım bulunmaktadır. Bu xml dosyası basitçe ipfw-classifyd uygulamasını harekete geçirecek temel verileri içermektedir. Web arayüzünden yapılan işlemler sonucunda arka planda gerçekleşen işlemler aşağıda listelenmiştir.

```

Bittorrent = action block
Gnutella = action block
E-Donkey = action block
Fasttrack = action block

```

Eğer belirlenen yöntem action block ise yukarıdaki gibi bir çıktıyı ipfw-classifyd çıktısı olarak alırız. Eğer web arayüzünden güvenlik duvarı kuralı olarak işlersek aşağıdaki gibi bir çıktı alacağız.

```

pass in quick on $LAN proto { tcp udp }
from { 192.168.160.2 } to 192.168.87.2 divert 47244
keep state ( max-packets 5, overload action
diverttag ) label "USER_RULE: Layer7 block P2P"

```



Bu çıktılar protokol bloklama işlemi sırasında gerçekleşen işlemlerin çıktılarıdır. Eğer bloklama yerine qos işlemi uygulayacaksa uygulamaların arka plandaki davranışları farklıdır. Bu işlemleri gerçekleştirmek için Dummynet pipe yapısı kullanılmaktadır. Bu durumda L7 container şu şekilde oluşacaktır:

```
http = dnpipe 2
pop3 = dnqueue 2
smtp = dnqueue 2
cvs = dnqueue 1
```

Bu konfigürasyon dosyasını anlayabilmek için dosyanın içerisindeki Dummynet yapısına bir göz atmamız gerekmektedir.

```
dnpipe 1 bandwidth 1Mb
dnqueue 1 dnpipe 1 weight 1
dnqueue 2 dnpipe 1 weight 3
dnpipe 2 bandwidth 2Mb
```

Yukarıdaki gibi bir konfigürasyon dosyasında dnpipe' ın 2 Mb ile sınırlı olduğunu açıkça görebilmekteyiz. Kuyruğa atma işlemini en kolay açıklama yöntemi aşağıda verilmiş olan ekran görüntüsünün arka planda ipfw-classifyd tarafından nasıl kuyruğa atıldığını incelemekle ortaya çıkacaktır.

Enable/Disable	<input checked="" type="checkbox"/> Enable/Disable layer7 Container															
Name	webLim															
Description	 Web Limiter You may enter a description here for your reference (not parsed).															
Rule(s)	<div style="border: 1px dashed gray; padding: 5px; margin-bottom: 10px;">Add one or more rules</div> <table border="1"><thead><tr><th>Protocol</th><th>Structure</th><th>Behaviour</th></tr></thead><tbody><tr><td>http</td><td>limiter</td><td>Lim_2mb</td></tr><tr><td>pop3</td><td>limiter</td><td>Web</td></tr><tr><td>smtp</td><td>limiter</td><td>Web</td></tr><tr><td>cvs</td><td>limiter</td><td>Others</td></tr></tbody></table> <div style="text-align: right;"></div>	Protocol	Structure	Behaviour	http	limiter	Lim_2mb	pop3	limiter	Web	smtp	limiter	Web	cvs	limiter	Others
Protocol	Structure	Behaviour														
http	limiter	Lim_2mb														
pop3	limiter	Web														
smtp	limiter	Web														
cvs	limiter	Others														
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Delete"/>																

Resim 7. Web limiter kuralının web arayüzünde işlenişi

Resim 7'de belirtildiği gibi bir kural işlenişi gerçekleştiğinde arka planda oluşacak çıktılar şu şekilde olacaktır:


```
pass in quick on $LAN proto { tcp udp } from { 192.168.160.1 }  
to 192.168.87.2 divert 51391 keep  
state ( max-packets 5, overload dummy net diverttag )  
label "USER_RULE: Layer7 webLim"
```

Bütün bu işlemler tanımlı olan uygulama pattern' leri için geçerlidir. Eğer kendinizin kullandığı hali hazırda verilmiş olan pattern dışında bir pattern kullanmak istiyorsanız örnek pattern dosyanızı aşağıdaki gibi web arayüzünden sisteme dahil edebilirsiniz. **[6]**

Layer7: Add pattern

You can upload new patterns to your system!

Note: The patterns won't be verified and if they already exist, they will be replaced!

Use it at your own risk!



The image shows a web form for uploading a pattern. At the top, there is a grey button labeled "Upload". Below it, the text "File to upload:" is followed by a text input field and a "Browse" button. Below the input field, there is another "Upload" button.

Resim 8. Pattern ekleme menüsü

10. SONUÇ:

Günümüzde ihtiyaçlar yön değiştirmeye başlamıştır. Trafik düzenlemesi için önceleri IPS'ler kullanılıyordu ancak bu donanımlarla yapılan yanlış bloklamalar kurumları başka çözümlere doğru yöneltmiştir. Günümüzde http download protokolleri çok yüksek band genişlikleri tüketmeye başlamıştır. Bununla beraber kullanıcılar p2p uygulamaları ile çekemedikleri filmleri web üzerinden HD yayın olarak kesintisiz bir şekilde izlemeye başlamışlardır. Bu ise ağ yöneticilerinin karşısında ciddi sorunlar olarak çıkmaya başlamıştır. Bloklamanın bir çözüm olmaktan çıkmıştır, aksine insanları başka arayışlara yönlendirmekte ve ticari ürünlerin kullanımını yaygınlaştırmaktadır.

Çözüm ise engellemek yerine belirli protokolleri ve ihlalleri en çok yaratan kullanıcıları belirlemek ve bunlara özel bandgenişliği tanımlamaktır. L7 filtreleme ise bu süreçte kullanılacak en önemli araçlardan birisidir.

Bu belgede, bu süreçte kullanılacak PFSENSE yazılımı ayrıntılı olarak ele alınmıştır. Pfsense dağıtımı 2.0 sürümü ile L7 filtreleme özelliğini desteklemeye başlamıştır. Sistem oldukça esnektir ve kısa sürede yaygın bir kullanıma ulaşmıştır. Henüz test sürümü bulunmasına rağmen, 2010 yılı içerisinde tam sürüm dağıtımının olacağı belirtilmektedir.

Dökümanın en güncel sürümüne <http://csirt.ulakbim.gov.tr/dokumanlar> adresinden ulaşabilirsiniz.

KAYNAKLAR:

[1] 2009, <http://alper.web.tr/2009/03/16/qos-quality-of-service/>

[2] 2009, <http://www.secretflow.com/icerik.asp?tur=1&aid=90&agac=,35,90,>

[3] 2009, Huzeyfe ÖNAL, OpenBsd Packet Filter(PF) ile güvenlik duvarı Uygulamaları

[4] 2009, <http://roadtoqos.wordpress.com/2008/11/13/ipfw-classifyd/>

[5] 2009, http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43

[6] 2009, L7 Classification and Policing in the pfSense Platform