# Kampüs Ağlarında Etkin Bant Genişliği Yönetimi V1.1

**Enis Karaarslan**

Muğla Üniversitesi, Bilgisayar Mühendisliği Bölümü / ULAK-CSIRT

**Vedat Fetah**

Ege Üniversitesi, BİTAM Kampüs Network Yönetim Grubu

**Gökhan Akın**

İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı / ULAK-CSIRT

**Sınmaz Ketenci**

İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı

# Giriş

- Kurumsal ağ – kampüs ağları
  - Farklı kullanıcı profilleri
  - Farklı ihtiyaçlar
- Hedef: Kısıtlı bant genişliğinin etkin kullanılması

# Etkinleştirme Çalışmaları

- Kampüs Ağının Tanımlanması
- Sistem Bilgilerinin Çözümlenmesi
- Kısıtlama/düzenlemelerin uygulanması

# Kampüs Ağının Tanımlanması

- Alt ağlar (subnet)
- Bilgisayar Sayısı
- Bant Genişliği (Bandwidth)
- Trafik Profili
- Kullanıcı Profili

# Sistem Bilgilerinin Çözümlenmesi

- Bant genişliği ihtiyaçlarının belirlenmesi

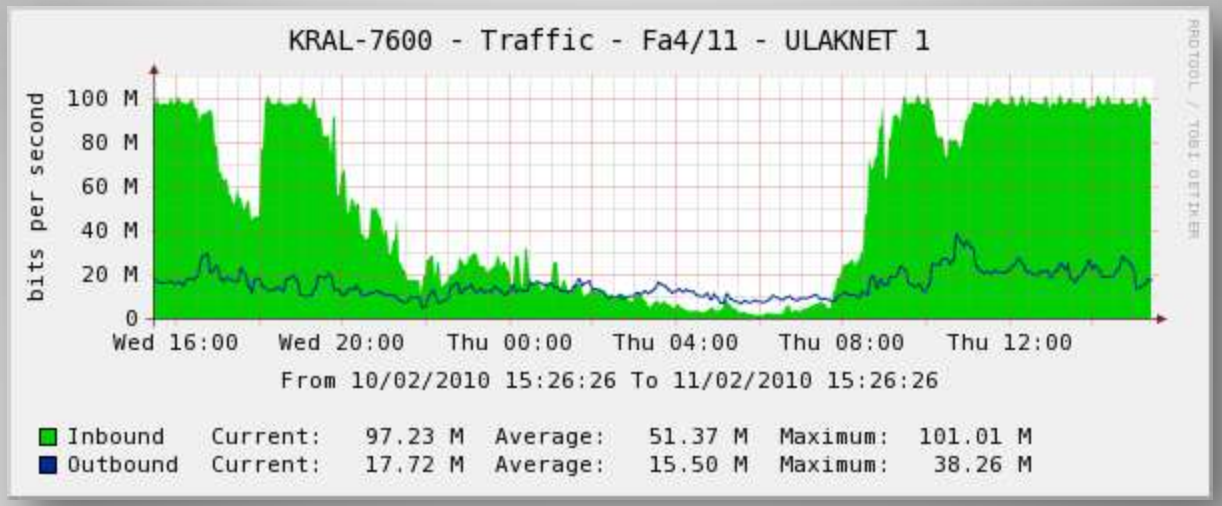
- Trafik profili incelenerek kurumun amacına uygun trafik tanımlanmalıdır. Örneğin:
  - YÜKSEK ÖNCELİK: Kurumun asıl öncelikli trafiği
    - Ör: hastane SGK erişimi
  - ORTA DERECE ÖNCELİK:
    - Ör: http web
  - DÜŞÜK ÖNCELİK: İstenmeyen Trafik
    - Ör: P2P

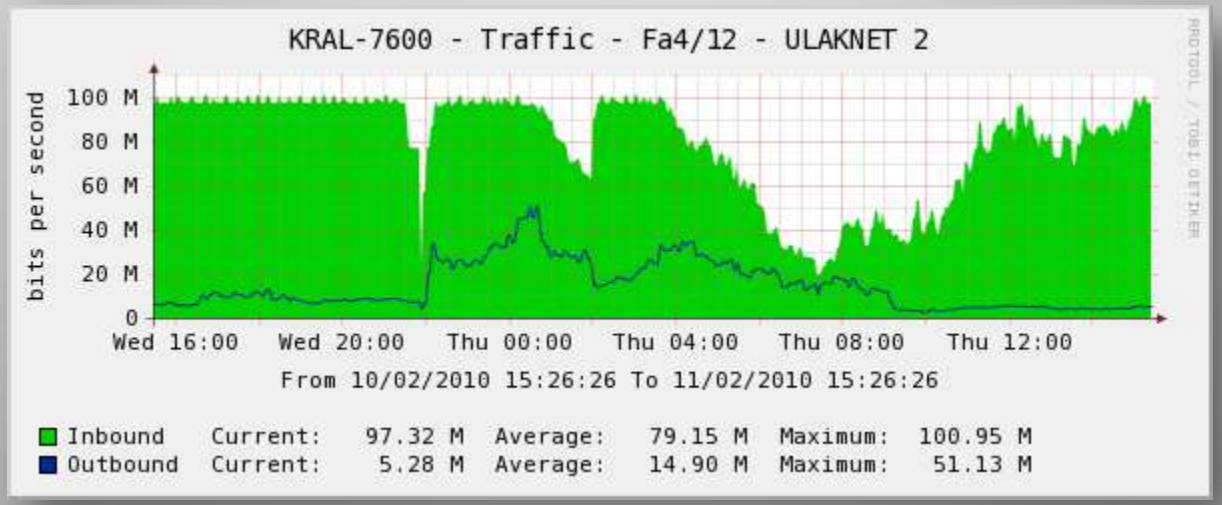
# Sistem Bilgilerinin Çözümlenmesi-2

**Kısıtlama Düzenleme Zamanının belirlenmesi. Örneğin:**

- **Hafta içi**
  - **Mesai içi**
  - **Mesai dışı**
- **Hafta Sonu**

# Sistem Bilgilerinin Çözümlenmesi-3



# Kısıtlama/Düzenleme

- Traffic shaping ile uygulama / alt ağ / host bazlı bant genişliğinin ayarlanması
- İhlal yaratan kullanıcıların belirlenmesi ve oluşturulacak bir karantina grubuna alınması - kısıtlanması

# Kısıtlama/Düzenleme-2

- P2P vb. protokollerin
  - Tamamen engellenmesi
  - Mesai saatlerinde tamamen engellenmesi
  - Mesai saatlerinde/sonrasında istenilen bant genişliğine sıkıştırılması.

# Çözümler

1- Internet Çıkış Noktasında Kullanılabilecek Ürünler
(Açık Kaynak Uygulama İşlenen Örneği: PFSENSE)

2- Proxy Sunucuları

3- Ağ Altyapısı Cihazları ile yapılabilecek Uygulama (İşlenen Örneği: Cisco cihazları)

# PFSENSE Çözümü

Pfsense özelleştirilmiş bir FreeBsd dağıtımıdır.

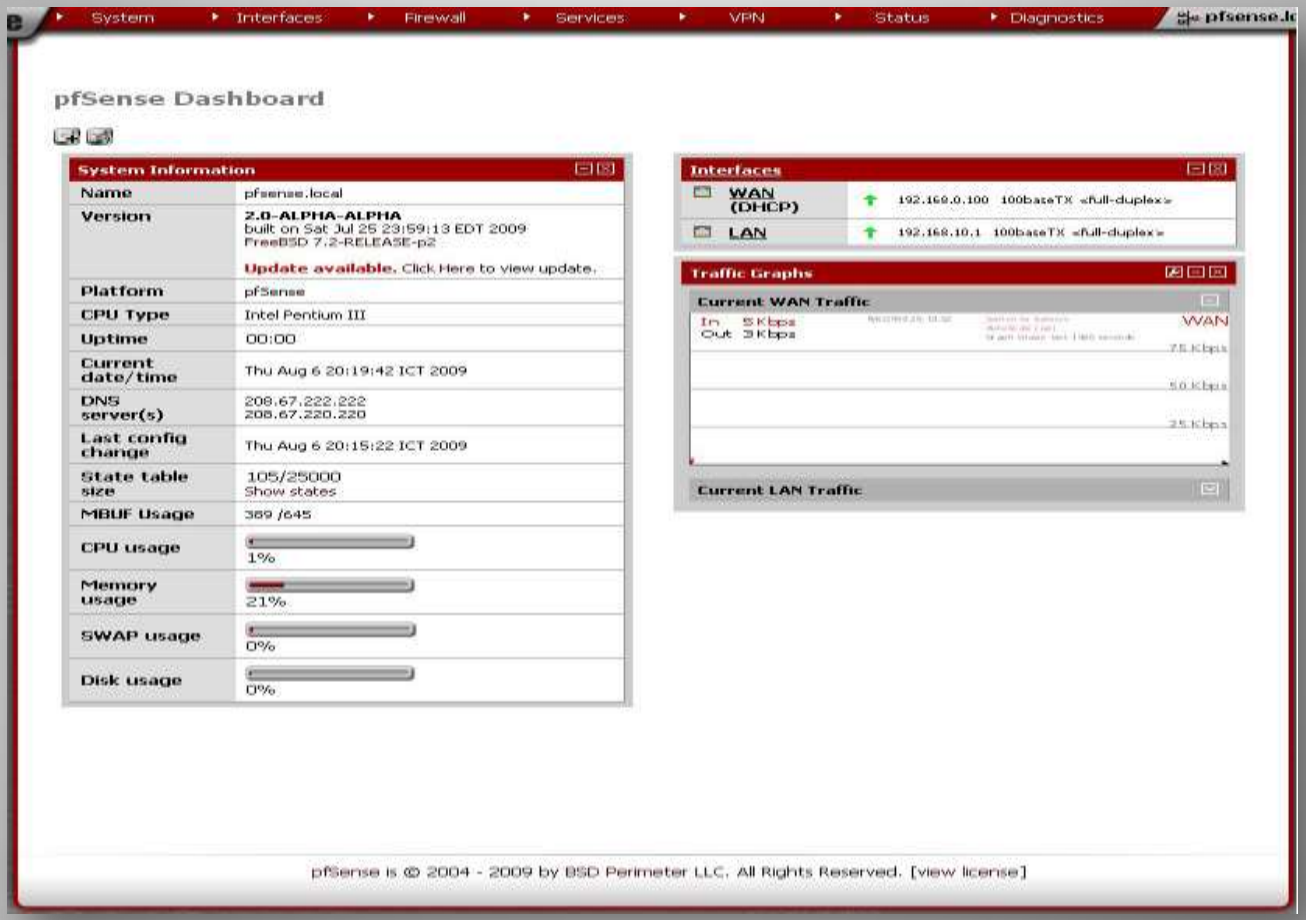
Esas olarak güvenlik duvarı ve router olarak çalışmak üzere tasarlanmıştır.

IDS, Antivirus Gateway, Squid Proxy, ntop, trafik şekillendirme ve Vpn gibi yazılımlar ekstra modül olarak eklenebilir.

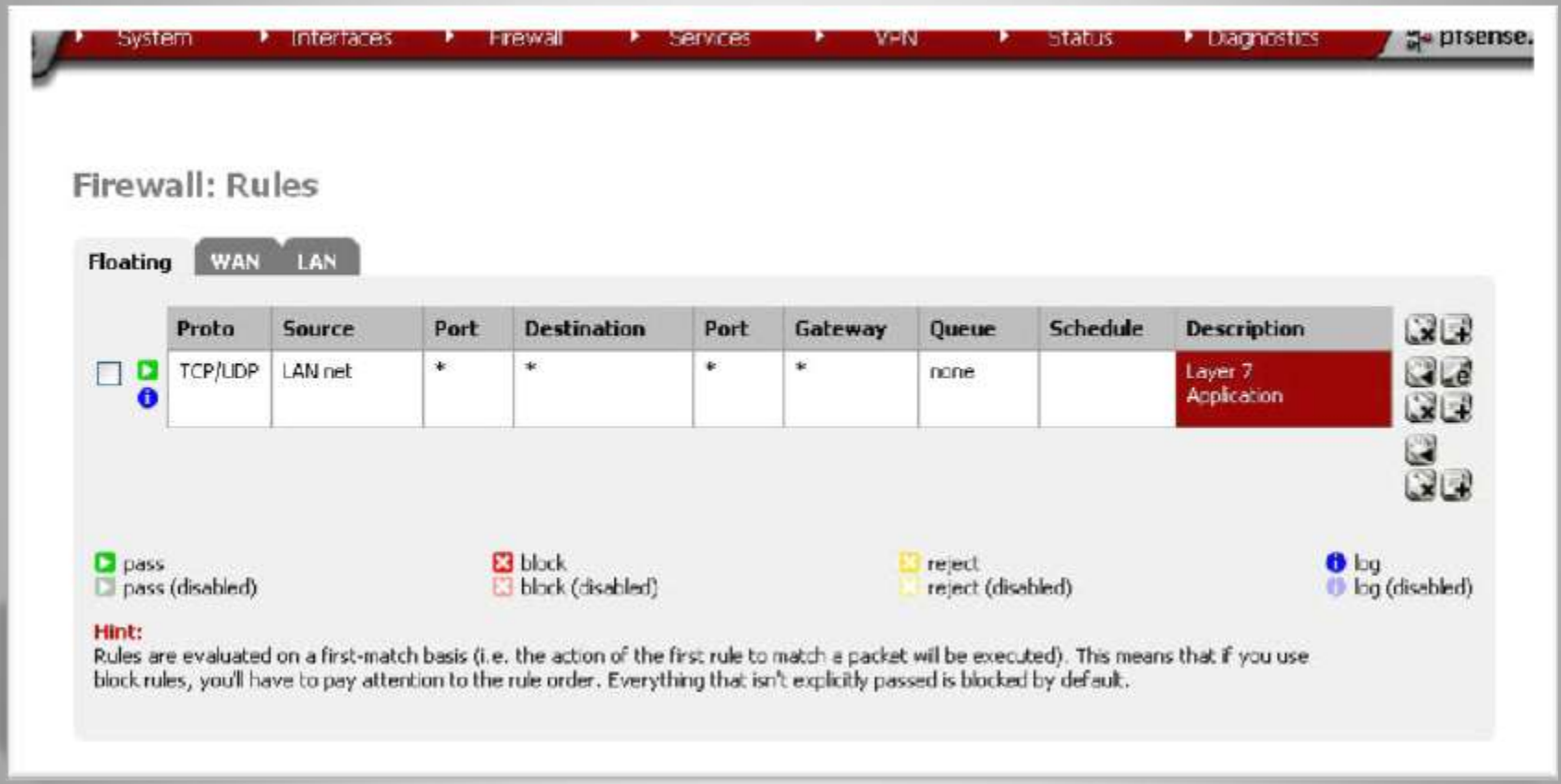
# PFSENSE'in Özellikleri

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.

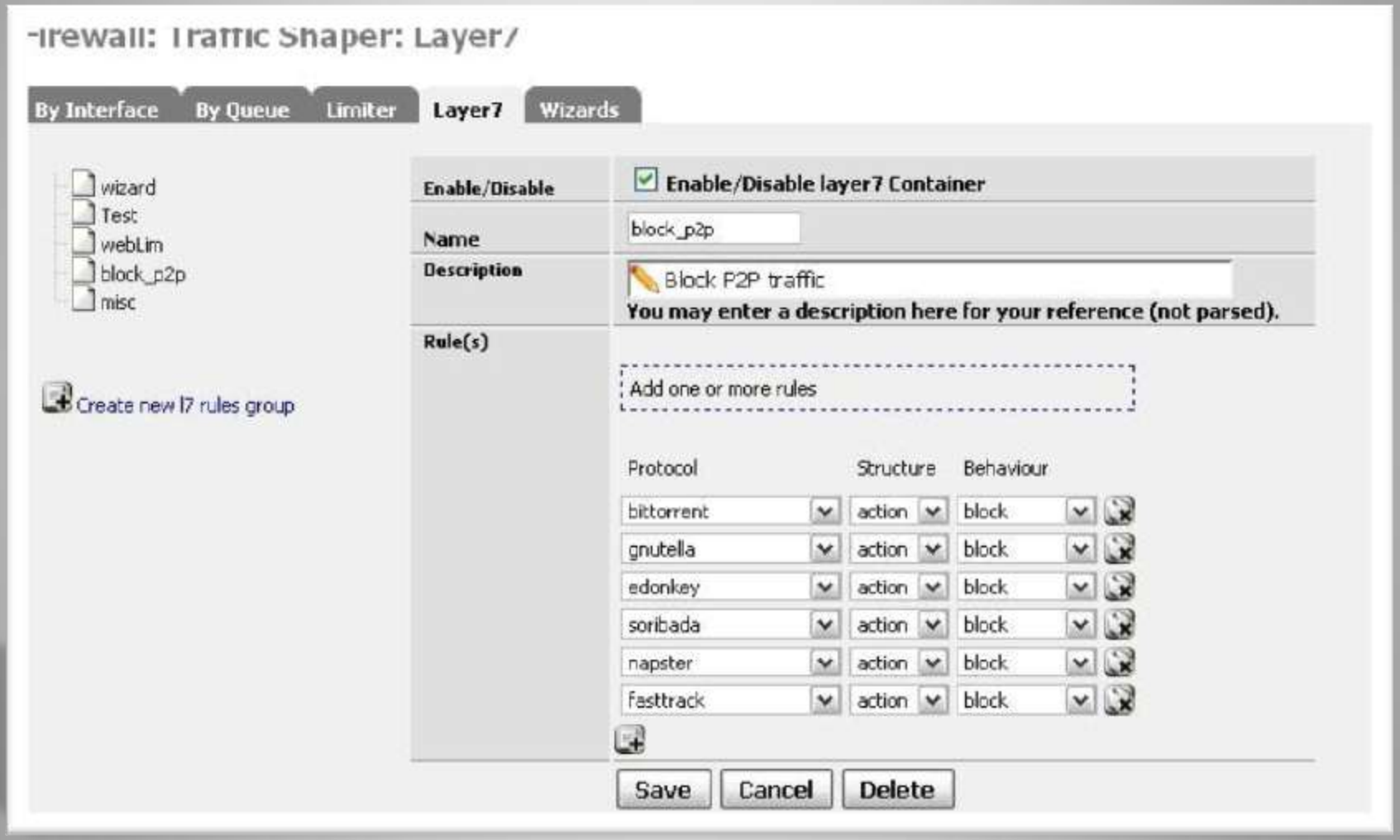
# PFSENSE Dashboard



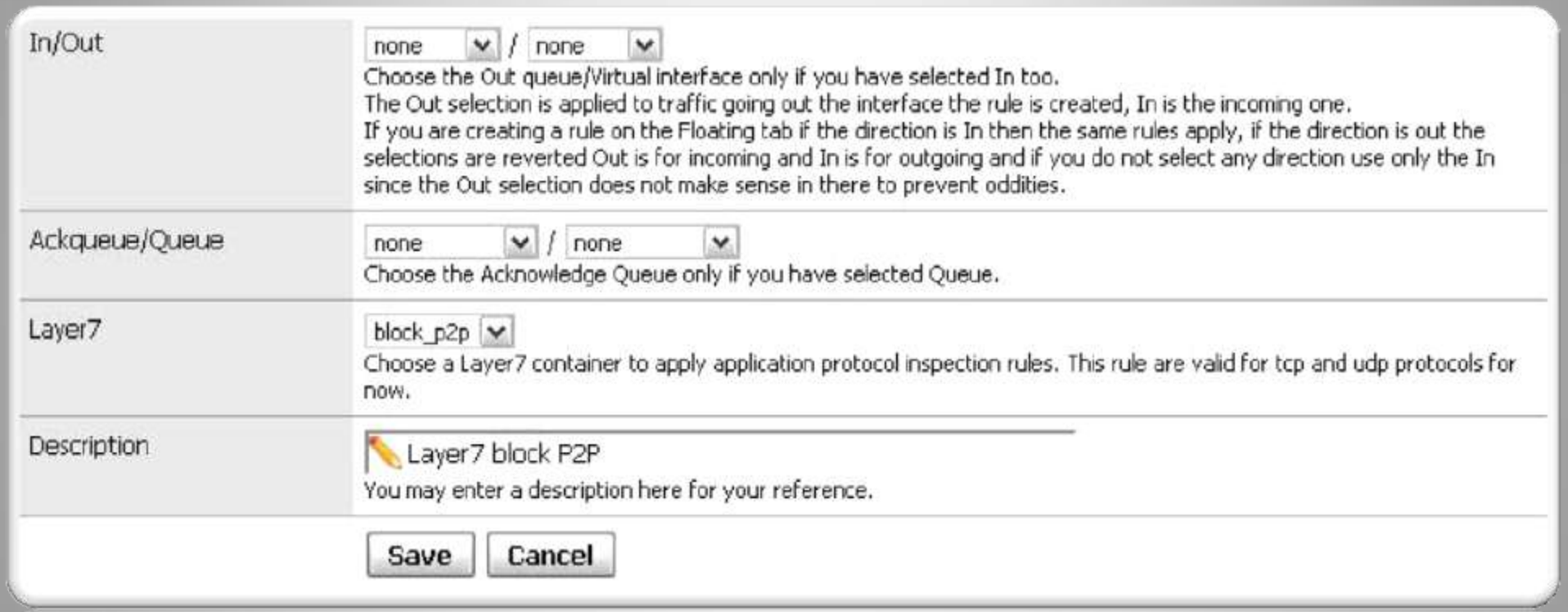
# Firewall Arayüzü



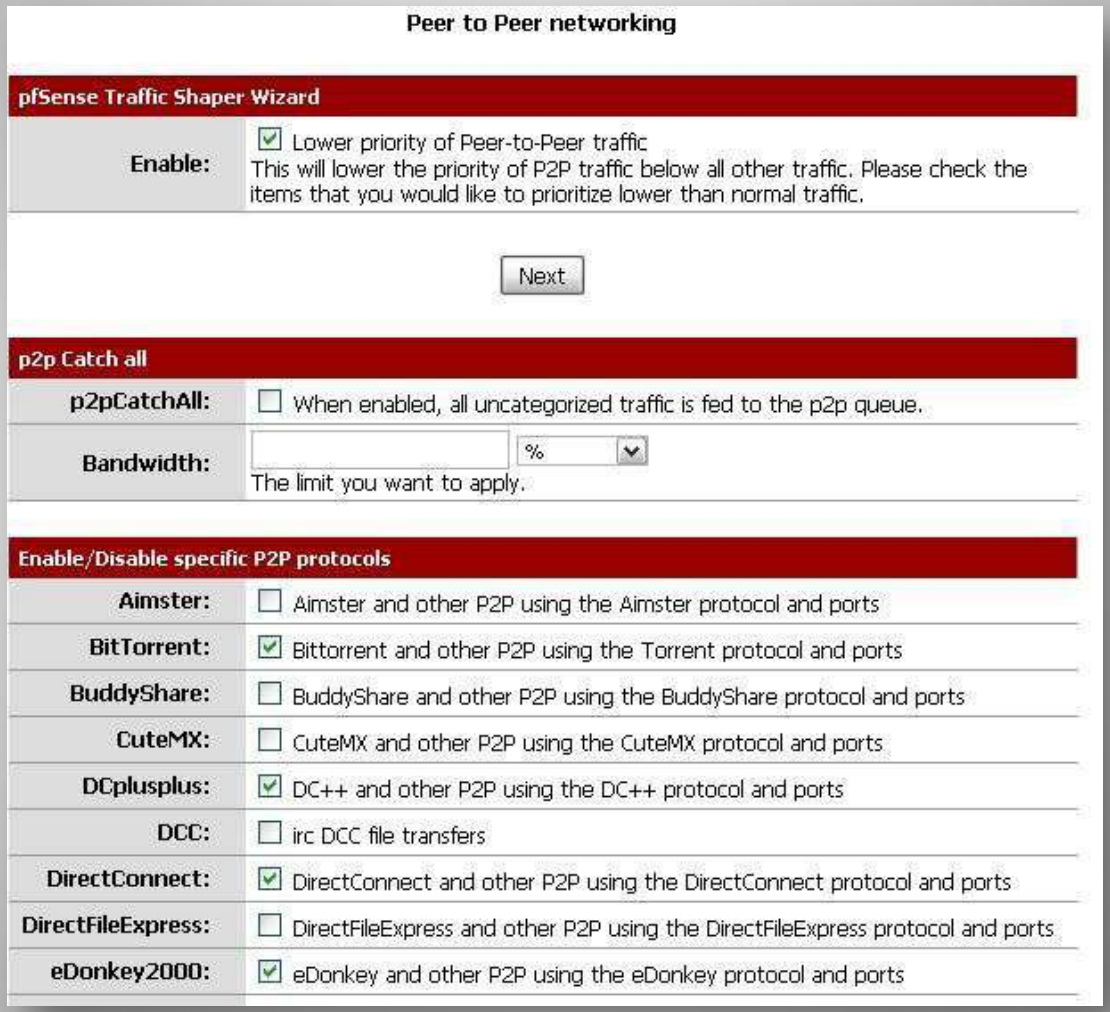
# Kuralların Belirlenmesi



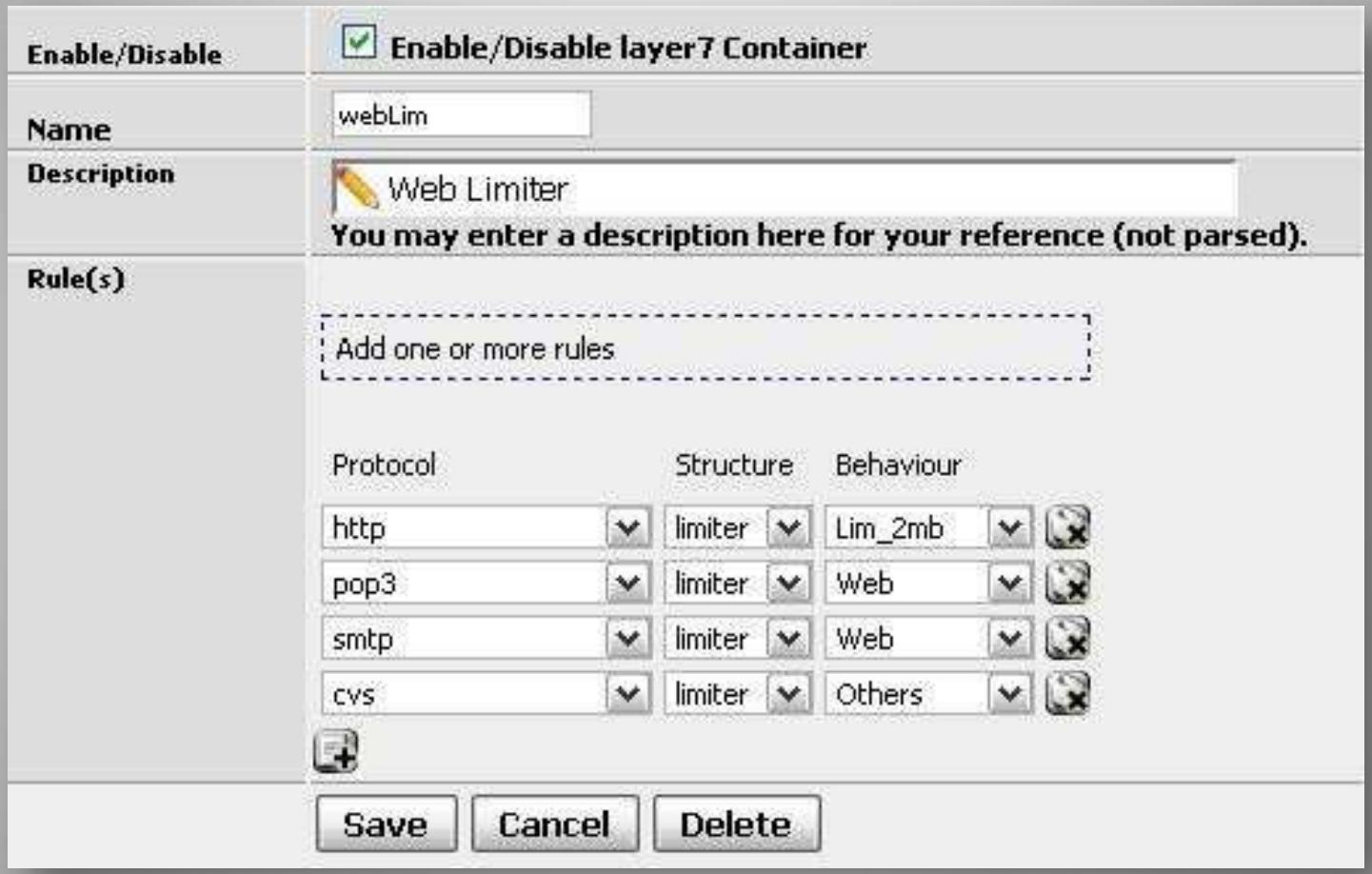
# Kuralların Arayüze Uygulanması



# Trafik Şekillenmesi



# L7 Limitleme Uygulanması



# Yeni L7 Pattern'lerin Yüklenmesi

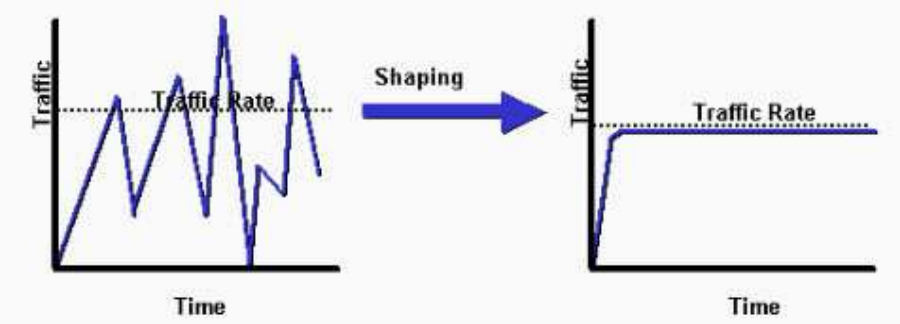
# Cisco Cihazlarda Bant Genişliği Yönetimi Teknikleri

**Cisco yönlendirici ve anahtar cihazlarında bant genişliği yönetimi iki farklı metot ile gerçekleştirilebiliyor:**

**1- Traffic Shaping (Trafik Şekilleme)**

**2- Traffic Policing(Trafik Sınırlandırılması)**

# Traffic Shaping (Trafik Şekilleme)

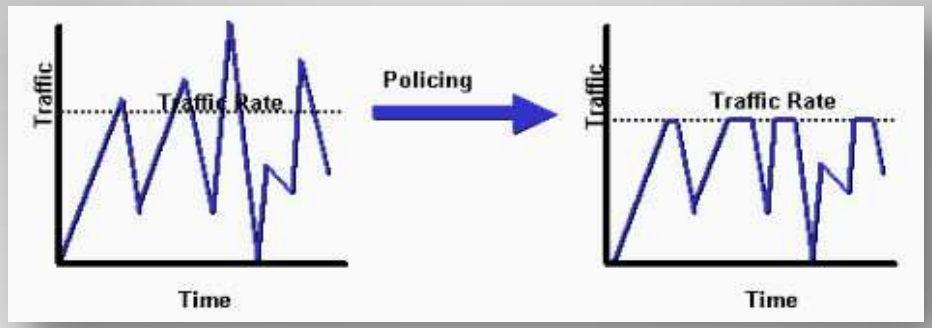



Kaynak: www.cisco.com

**"Traffic Shaping" tekniğinde belirlenen limiti aşan trafik yönlendiricin tampon belliğinde tutulur ve akışın sürekli aynı bant genişliğinde kalması sağlanacak şekilde bant genişliğinin akışına izin verilir.**

**Yaygın olarak Frame-Relay, ATM gibi birbirinden farklı hızlar ile bağlantı sağlanabilen WAN linklerinde kullanılmaktadır.**

# Traffic Policing (Trafik Sınırlandırılması)




Kaynak: www.cisco.com

**"Traffic Policing" metodunda belirlenen bant genişliği miktarının üstündeki trafik ya çöpe atılır (drop) yada bu trafiğin IP başlığında bulunan ToS kısmındaki paket önceliğini belirleyen sayı değerleri değiştirilir.**

# Traffic Policing Teknikleri

**1- Aggregate Policing:**

**Bu teknik bir grup kullanıcının tamamı için toplam bir üst sınır belirlemekte kullanılır.**

**2- Microflow Policing:**

**Bir trafik akışına (flow) bant genişliği sınırlaması uygulanabilir. Doğru bir yapılandırma ile bir kullanıcının anlık erişebileceği bant genişliği üst sınırı belirlenebilir.**

# Aggregate Policing Türleri

**1- Per-interface aggregate policing (arayüz bazlı)**

**Arayüz bazlı aggregate policer uygulandığı her arayüz için ayrı ayrı sınırlandırma yapar.**

**2- Named aggregate policing (isimlendirilmiş)**

**İsimlendirilmiş aggregate policer ise uygulandığı tüm arayüzlerdeki trafiğin toplamına sınırlandırma getirir.**

# Per-interface Aggregate Policing

**Konfigurasyon adımları:**
**1- Erişim kontrol listeleri ile trafik tarif edilip bir trafik sınıfı oluşturulur. (Class-map)**
**(örnek: kaynak IP adresi 10.0.0.1 olan gibi)**

**2- Oluşturulan sınıfa uygulanacak bant genişiliği politikası belirlenir. (Policy-map)**
**(örnek: kullanıcılar maksimum 10Mb kullanabilsin.)**

**3- Bu politika ilgili interface'e giren veya çıkan trafiğe uygulanır.**

# Per-interface Aggregate Policing

# Erişim Kontrol Listeleri ile Trafiğin Tarifi

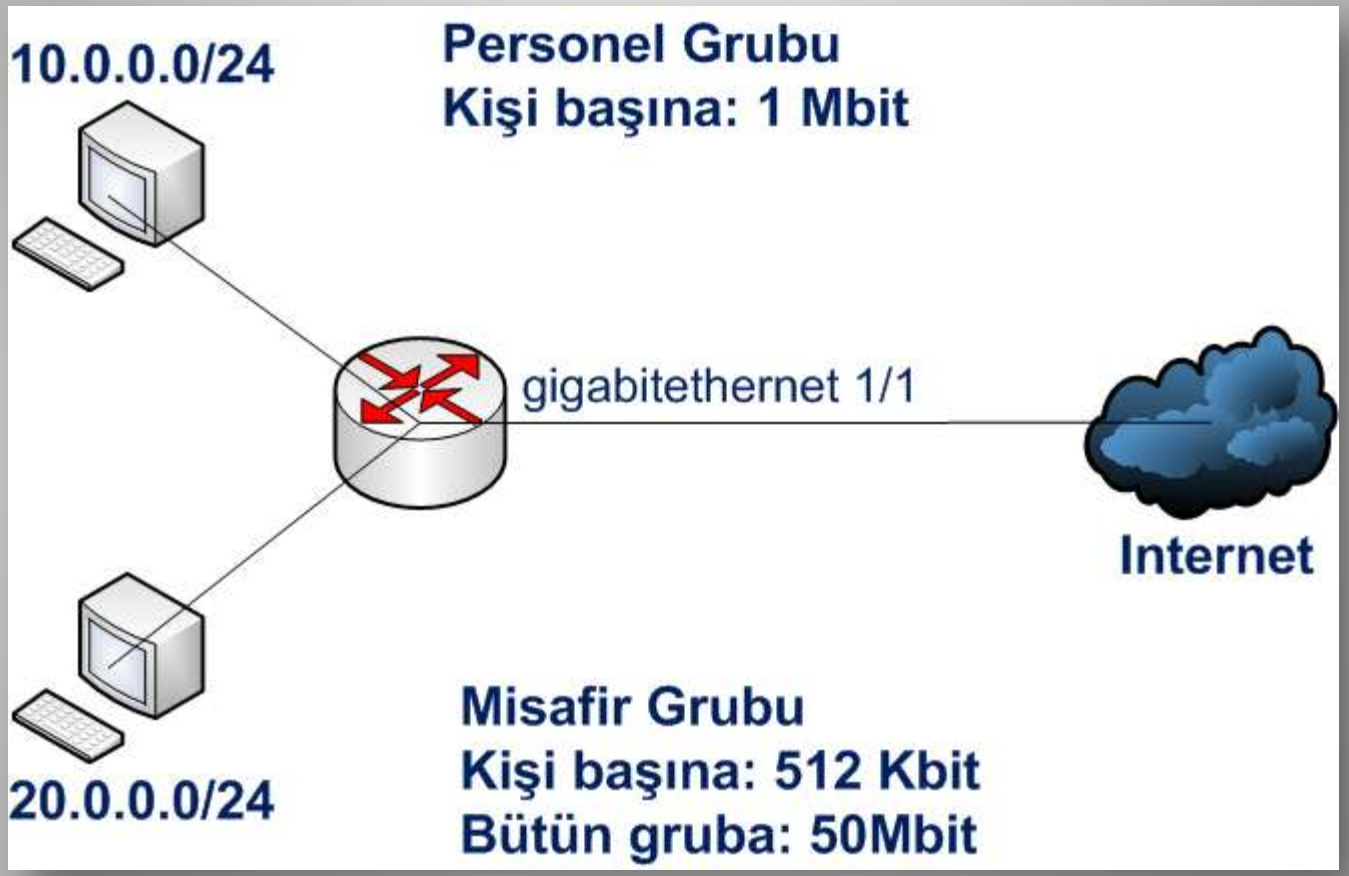
```
6500(config)#mls qos
6500(config)#access-list 160 permit ip any 10.0.0.0
    0.0.0.255

6500(config)#class-map 60Mb_Sinifi
6500(config-cmap)#match access-group 160
6500(config-cmap)#exit
```

# Politikanın Belirlenmesi ve Uygulanması

```
6500(config)# policy-map 60Mb_toplam
6500(config-pmap)# class 60Mb_Sinifi
6500(config-pmap-c)# police 60000000
6500(config-pmap-c)# exit
6500(config-pmap)# exit

6500(config)# interface gigabit 2/1
6500(config-if)# service-policy input 60Mb_toplam
```

Not: L3 Interface'ine giren ve çıkan trafiğe (Input ve Output) uygulanabilir.

# Microflow Policing



# Erişim Kontrol Listeleri ile Trafiğin Tarifi

```
6500(config)# access-list 101 permit ip any 10.0.0.0 0.0.0.255
```

```
! Personel sınıfının tanımlanması
6500(config)# class-map personel_sinifi
6500(config-cmap)# match access-group 101
6500(config-cmap)# exit
```

# Erişim Kontrol Listeleri ile Trafiğin Tarifi - 2

```
6500(config)# access-list 102 permit ip any 20.0.0.0 0.0.0.255

! Misafir sınıfının tanımlanması
6500(config)# class-map misafir_sinifi
6500(config-cmap)# match access-group 102
6500(config-cmap)# exit
```

# Politikanın Belirlenmesi ve Uygulanması

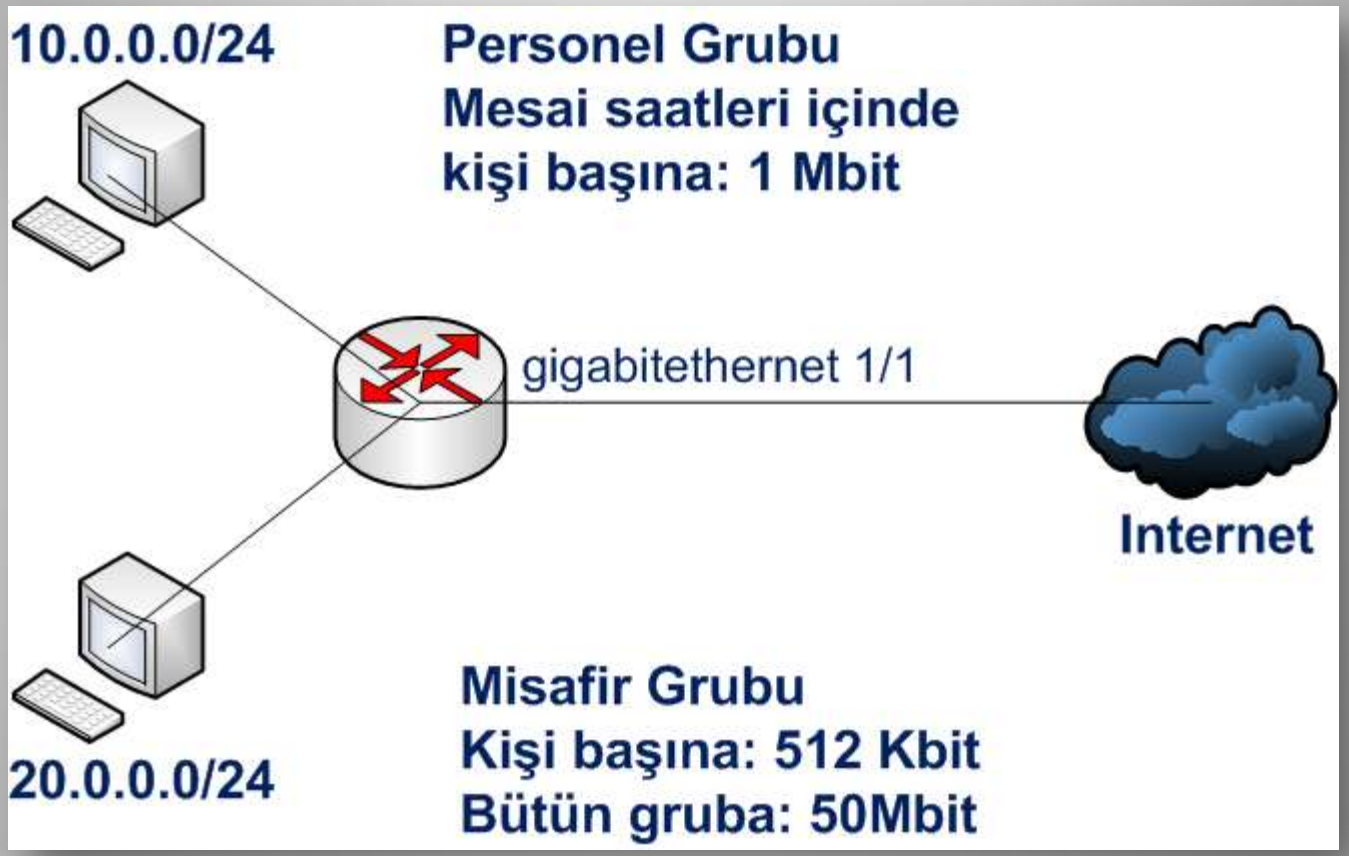
```
6500(config)# policy-map Personel_Misafir_sinirla
6500(config-pmap)# class personel_sinifi
6500(config-pmap-c)# police flow mask dest-only 1024000
256000 conform-action transmit exceed-action drop
6500(config-pmap-c)# exit

6500(config-pmap)# class misafir_sinifi
6500(config-pmap-c)# police flow mask dest-only 512000
128000 conform-action transmit exceed-action drop
6500(config-pmap-c)# police 50000000
6500(config-pmap-c)# exit
```

# Politikanın Belirlenmesi ve Uygulanması

**6500(config)# interface gigabitEthernet 1/1**
**6500(config-if)# service-policy input Personel_Misafir_sinirla**

**Not: Sadece interface'e giren trafiğe (input) uygulanabilir.**

# Zamana Bağlı Bant Genişliği Yönetimi



# Zaman Aralığı Belirtilmesi

**1- Periyodik tekrar eden zaman aralığı tarifi:**

**Router(config)# time-range time_range_name**
**Router(config-time)# periodic [istenen günler] [hh:mm] to [hh:mm]**
**Monday, Tuesday, Wednesday, Thursday, Friday, Saturday ,**
**Sunday, Daily (hergün), Weekdays (haftaiçi), Weekend (hafta sonu)**

**2- Sadece belirli tarih için:**

**Router(config)# time-range time_range_name**
**Router(config-time)# absolute [Başlangıç saat-dakika-saniye-gün-ay-yıl] [bitiş saat-dakika-saniye-gün- ay-yıl]**

# Erişim kural listesine zaman aralığının tanımlanması

**Mesai saatleri aralığının tarifi:**

```
Router(config)# time-range mesai
Router(config-time-range)# periodic weekdays 09:00 to 18:00
Router(config-time-range)# exit

Router(config)# access-list 101 permit ip any 10.0.0.0 0.0.0.255 time-range mesai
```

# Uygulamanın Belirtilmesi

**1- Port numarası belirterek:**
**Router(config)# access-list 101 permit tcp 10.0.0.0 0.0.0.255 eq 80 any time-range mesai**

**2- Protokol analizi yaparak: Yönlendiricilerde NBAR özelliği ile gerçekleştirilebilir.**
**Router(config)# class-map match-any WEB_TRAFIGI**
**Router (config-cmap)#match protocol http**

**Detay : P2P Engellemek için QoS ile Cisco NBAR Kullanılması**
**http://www2.itu.edu.tr/~akingok/etkinlikler.php**
**(Akademik Bilişim 2006)**

# Reklamlar-1 ☺

Kampüs Ağlarında Cisco Yönlendirici ve Anahtar Cihazları ile Bant Genişliği Yönetimi Teknikleri

Gökhan AKIN — Sınırsız Kelenci
İTÜ Bilgi İşlem Daire Başkanlığı / Ağ Yönetim Grubu

1. Cisco Cihazlarda Bant Genişliği Yönetimi Teknikleri

Cisco cihazlarda bant genişliği yönetimi Traffic Shaping (Trafik Şekillendirme) ve Traffic Policing (Trafik Sınırlandırılması) yöntemleri ile farklı metotlar ile gerçekleştirilebiliyor. Bu iki metodun avantaj ve dezavantajları ve bunlara bağlı olarak da farklı kullanım yerleri bulunmaktadır.

1.1 Traffic Shaping (Trafik Şekillendirme)

Traffic Shaping tekniğinde belirlenen limit aşan trafik yönlendirici tamponunda bekletilir ve akışın süresini aynı bant genişliğinde kalması sağlanacak şekilde bant genişliğinin aşılmasına izin verilir. Bu şekilde sürekli aşırı bant genişliği tüketimi sağlanır ve paket kaybının az olması sağlanmaktadır.



Şekil 1: Traffic shaping [1]

Ancak verinin tampon belleğe beklemesinden dolayı veri hedefe ulaşmasında gecikme oluşmaktadır. Yaygın olarak Frame-Relay, ATM gibi bölütten farklı hızlar ile bağlantı sağlanabilen WAN linklerinde kullanılmaktadır. Yerel alan ağlarında pek tercih edilmeyen bir bant genişliği yönetim sistemi değildir.

1.2 Traffic Police (Trafik Sınırlandırılması)

Traffic Police metodunda garanti edilmesi için belirlenen bant genişliği miktarının üstündeki trafik ya düşe atılır (drop) veya bu trafiğin IP başlığında bulunan ToS kısmındaki paket önceliğini belirleyen sayı değerleri değiştirilir.

Cisco Cihazlarda Bandgenişliği Yönetimi Detaylı Dökümanı

http://web.itu.edu.tr/akingok

veya

http://www.gokhanakin.net

ULAK-CSIRT

Ulusal Akademik Ağ ULAKNET Bilgisayar Olaylarına Müdahale Birimi ULAK-CSIRT Blogu

Home Hakkında

Terabit Ethernet!

May 3rd, 2010 No comments

Bu yıl içinde 40Gbit ve 100Gbit Ethernet'in standart haline gelmesi bekleniyor. 100Gbit'lik kartların Juniper ve Cisco tarafından üretimene başlandı bile. 100Gbit Ethernet var olan altyapının 10 kat hıza çıkabilmesi anlamına geliyor. Bunun da ne gibi yenilikler getirebileceğini şu anda hayal edemiyorum. Yakın gelecekte istemci portlarının 100mb olması bile yetersiz hale gelecek gibi. 802.11n standart olduğunda şu dönemde, kablosuz ağ erişimi iki kanalla 300mbit hızlara ulaşabiliyor, kablodan vazgeçip cümbür cemaat kablosuza geçecez belkide

Şöki durum, asıl şaşırdığım haber bunlar değil. Şaşırdığım ifade TERABIT Ethernet'in 2015 gibi gelecoğinin söylenmesi. Bu ifadeyide bizzat Bob Metcalfe'in bir konferansta çekilmiş videosundan kendi ağzından duydum. Fazla değil 5 yıl sonrasından bahsediliyor. Bırakın şu andaki PC'lerin harddisk veri yazma hızlarını, bizim teknolojiye yetişme hızımız bunlara yetişcek mi ? Umut ederim

Kalın sağlıcakla.

Gökhan AKIN

http://www2.itu.edu.tr/~akingok

Tagın: ethernet, terabit

Netfilter connlimit yapısı.

Feb 22nd, 2010 No comments

Iptables veya Netfilter yapısı içerisinde bulunan connlimit ile bağlantı sayısını sınırlandırabiliyoruz. Connlimit modülü standart netfilter yapısında uzun zamandır bulunmaktadır.

```
# iptables -m connlimit -h
```

Anket

CSIRT Blog un bu arayüzü sizce nasıl?

İyi, kullanışlı

Kötü, kullanışsız

İdare eder

Oy Ver

Sonuçları Göster

Kategoriler

Ağ Cihazları - Cisco (15)
Ağ Güvenliği (53)
DNS (9)
eduroam (1)
Genel Bilgiler (21)
Güvenlik Açıkları (22)
İşletim Sistemleri - Debian (2)
İşletim Sistemleri - FreeBSD (5)
İşletim Sistemleri - Genel (3)
İşletim Sistemleri - Linux (14)
İşletim Sistemleri - Microsoft (3)
İşletim Sistemleri - Unix (1)

ULAK/CSIRT Güvenlik Blogu

http://blog.csirt.ulakbim.gov.tr

# Reklamlar-2


**Agciyiz.net**
**Ağ Yönetimi Blogu**

**http://www.agciyiz.net**

# Reklamlar-3


**“WALKBEE” SNMPWalk Yazılımı**
**http://www.walkbee.com**

**Walkbee ile merkez L3 cihazlarının ARP tablolarını çok kolay kayıt altına alabilirsiniz.**

**Walkbee hakkındaki sunum için:**
**http://web.itu.edu.tr/akingok/inettr09/guvenlik_amacli_walkbee_yazilimi_sunumu.pdf**

**Walkbee hakkında makale için:**
**http://web.itu.edu.tr/akingok/inettr09/guvenlik_amacli_walkbee_yazilimi.pdf**

# Sorular

Teşekkürler.

**Sunum ve Dökümanlar için:**

**http://csirt.ulakbim.gov.tr/dokumanlar**