

Kampüs Ağlarında Etkin Bant Geniřliđi Yönetimi V1.1

Enis Karaarslan

Muđla Üniversitesi, Bilgisayar Mühendisliđi Bölümü / ULAK-CSIRT

Vedat Fetah

Ege Üniversitesi, BITAM 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



Etkinleřtirme alıřmaları

- **Kampüs Ađının Tanımlanması**
- **Sistem Bilgilerinin özömlenmesi**
- **Kısıtlama/düzenlemelerin uygulanması**



Kampüs Ađının Tanımlanması

- **Alt ađlar (subnet)**
- **Bilgisayar Sayısı**
- **Bant Geniřliđi (Bandwidth)**
- **Trafik Profili**
- **Kullanıcı Profili**



Sistem Bilgilerinin Çözömlenmesi

- Bant genişliđi ihtiyaçlarının belirlenmesi
- Trafik profili incelenerek kurumun amacına uygun trafik tanımlanmalıdır. Örneđin:
 - YÜKSEK ÖNCELİK: Kurumun asıl öncelikli trafiđi
 - Ör: hastane SGK erişimi
 - ORTA DERECE ÖNCELİK:
 - Ör: http web
 - DÜŞÜK ÖNCELİK: İstenmeyen Trafik
 - Ör: P2P



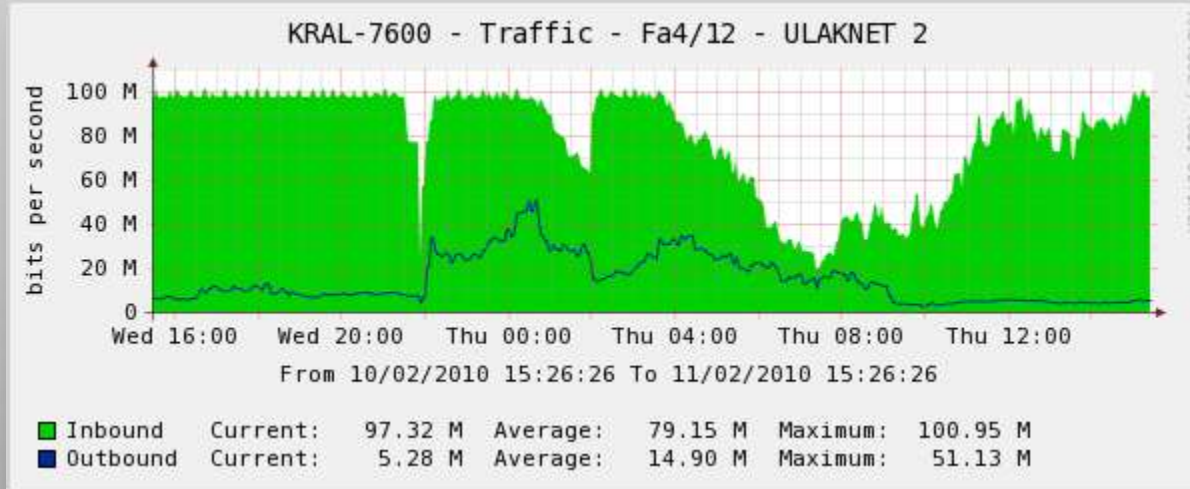
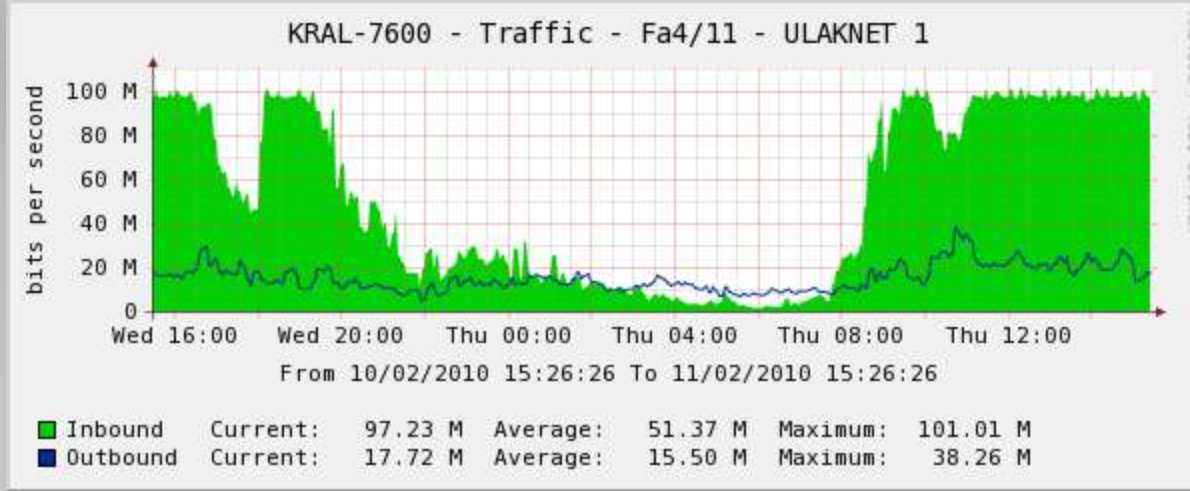
Sistem Bilgilerinin Çözömlenmesi-2

Kısıtlama Düzenleme Zamanının belirlenmesi. Örneđin:

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



Sistem Bilgilerinin Çözömlenmesi-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

The screenshot displays the pfSense Dashboard with a navigation menu at the top: System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The dashboard is divided into several sections:

- System Information:** A table providing details about the system, including name, version, platform, CPU type, uptime, current date/time, DNS servers, last config change, state table size, and resource usage (MBUF, CPU, Memory, SWAP, Disk).
- Interfaces:** A list of network interfaces, showing WAN (DHCP) and LAN with their respective IP addresses and capabilities.
- Traffic Graphs:** A section for monitoring network traffic, currently showing WAN traffic with In and Out rates.

At the bottom of the dashboard, a copyright notice reads: "pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]"



Firewall Arayüzü

System Interfaces Firewall Services VPN Status Diagnostics pfSense

Firewall: Rules

Floating WAN LAN

	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	TCP/LDP	LAN net	*	*	*	*	none		Layer 7 Application	

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

Kuralların Belirlenmesi

-firewall: Traffic Shaper: Layer7

By Interface By Queue Limiter **Layer7** Wizards

wizard
Test
webLim
block_p2p
misc

Create new L7 rules group

Enable/Disable	<input checked="" type="checkbox"/> Enable/Disable layer7 Container																					
Name	block_p2p																					
Description	Block P2P traffic You may enter a description here for your reference (not parsed).																					
Rule(s)	<div style="border: 1px dashed gray; padding: 5px;">Add one or more rules</div> <table><thead><tr><th>Protocol</th><th>Structure</th><th>Behaviour</th></tr></thead><tbody><tr><td>bittorrent</td><td>action</td><td>block</td></tr><tr><td>gnutella</td><td>action</td><td>block</td></tr><tr><td>edonkey</td><td>action</td><td>block</td></tr><tr><td>sonibada</td><td>action</td><td>block</td></tr><tr><td>napster</td><td>action</td><td>block</td></tr><tr><td>fasttrack</td><td>action</td><td>block</td></tr></tbody></table>	Protocol	Structure	Behaviour	bittorrent	action	block	gnutella	action	block	edonkey	action	block	sonibada	action	block	napster	action	block	fasttrack	action	block
Protocol	Structure	Behaviour																				
bittorrent	action	block																				
gnutella	action	block																				
edonkey	action	block																				
sonibada	action	block																				
napster	action	block																				
fasttrack	action	block																				

Save Cancel Delete

Kuralların Arayüze Uygulanması

In/Out

none / none

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.

Ackqueue/Queue

none / none


Choose the Acknowledge Queue only if you have selected Queue.

Layer7

block_p2p

Choose a Layer7 container to apply application protocol inspection rules. This rule are valid for tcp and udp protocols for now.

Description

 Layer7 block P2P

You may enter a description here for your reference.

Save

Cancel

Save

Cancel

You may enter a description here for your reference.

Layer7 block P2P



Trafik Şekillenmesi

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.

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:	<input type="checkbox"/> Aimster and other P2P using the Aimster protocol and ports
BitTorrent:	<input checked="" type="checkbox"/> Bittorrent and other P2P using the Torrent protocol and ports
BuddyShare:	<input type="checkbox"/> BuddyShare and other P2P using the BuddyShare protocol and ports
CuteMX:	<input type="checkbox"/> CuteMX and other P2P using the CuteMX protocol and ports
DCplusplus:	<input checked="" type="checkbox"/> DC++ and other P2P using the DC++ protocol and ports
DCC:	<input type="checkbox"/> irc DCC file transfers
DirectConnect:	<input checked="" type="checkbox"/> DirectConnect and other P2P using the DirectConnect protocol and ports
DirectFileExpress:	<input type="checkbox"/> DirectFileExpress and other P2P using the DirectFileExpress protocol and ports
eDonkey2000:	<input checked="" type="checkbox"/> eDonkey and other P2P using the eDonkey protocol and ports



L7 Limitleme Uygulanması

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; text-align: center;">Add one or more rules</div> <table><thead><tr><th>Protocol</th><th>Structure</th><th>Behaviour</th><th></th></tr></thead><tbody><tr><td>http</td><td>limiter</td><td>Lim_2mb</td><td></td></tr><tr><td>pop3</td><td>limiter</td><td>Web</td><td></td></tr><tr><td>smtp</td><td>limiter</td><td>Web</td><td></td></tr><tr><td>cvs</td><td>limiter</td><td>Others</td><td></td></tr></tbody></table> 	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"/>																					

Yeni L7 Pattern'lerin Yüklenmesi

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!

Upload

File to upload:

Browse

Upload



Cisco Cihazlarda Bant Geniřliđi Yönetimi Teknikleri

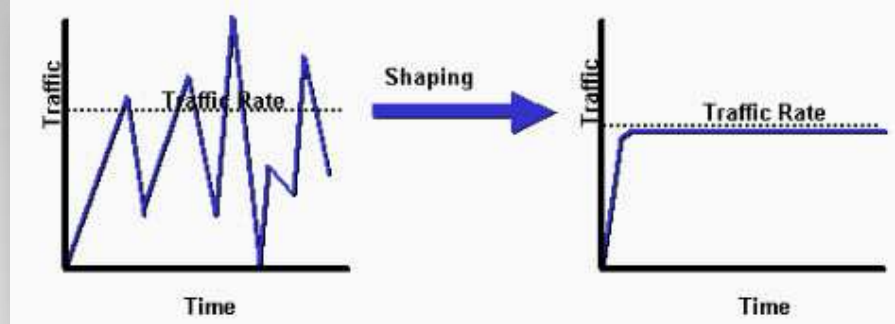
Cisco yönlendirici ve anahtar cihazlarında bant geniřliđi yönetimi iki farklı metot ile gerçekleştirilebiliyor:

1- Traffic Shaping (Trafik Şekilleme)

2- Traffic Policing(Trafik Sınırlandırılması)



Traffic Shaping (Trafik Şekilleme)

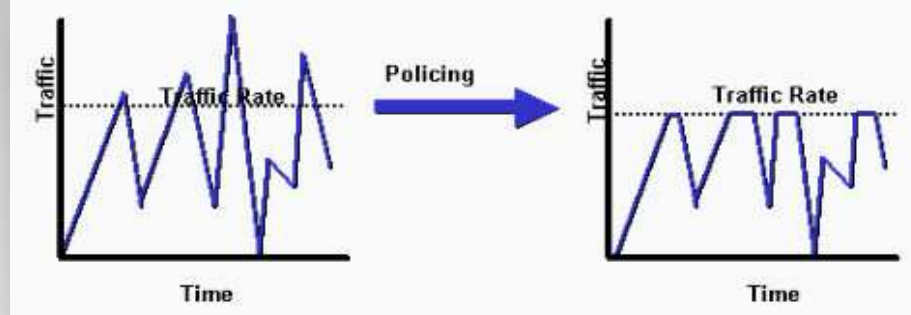


Kaynak: www.cisco.com

“Traffic Shaping” tekniğinde belirlenen limiti aşan trafik yönlendiricinin tampon belleğinde 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 belirlemede 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 genişliği politikası belirlenir. (Policy-map)

(örnek: kullanıcılar maksimum 10Mb kullanabilsin.)

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



Per-interface Aggregate Policing

Personel Grubu

Bütün gruba toplam : 60 Mbit



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
```



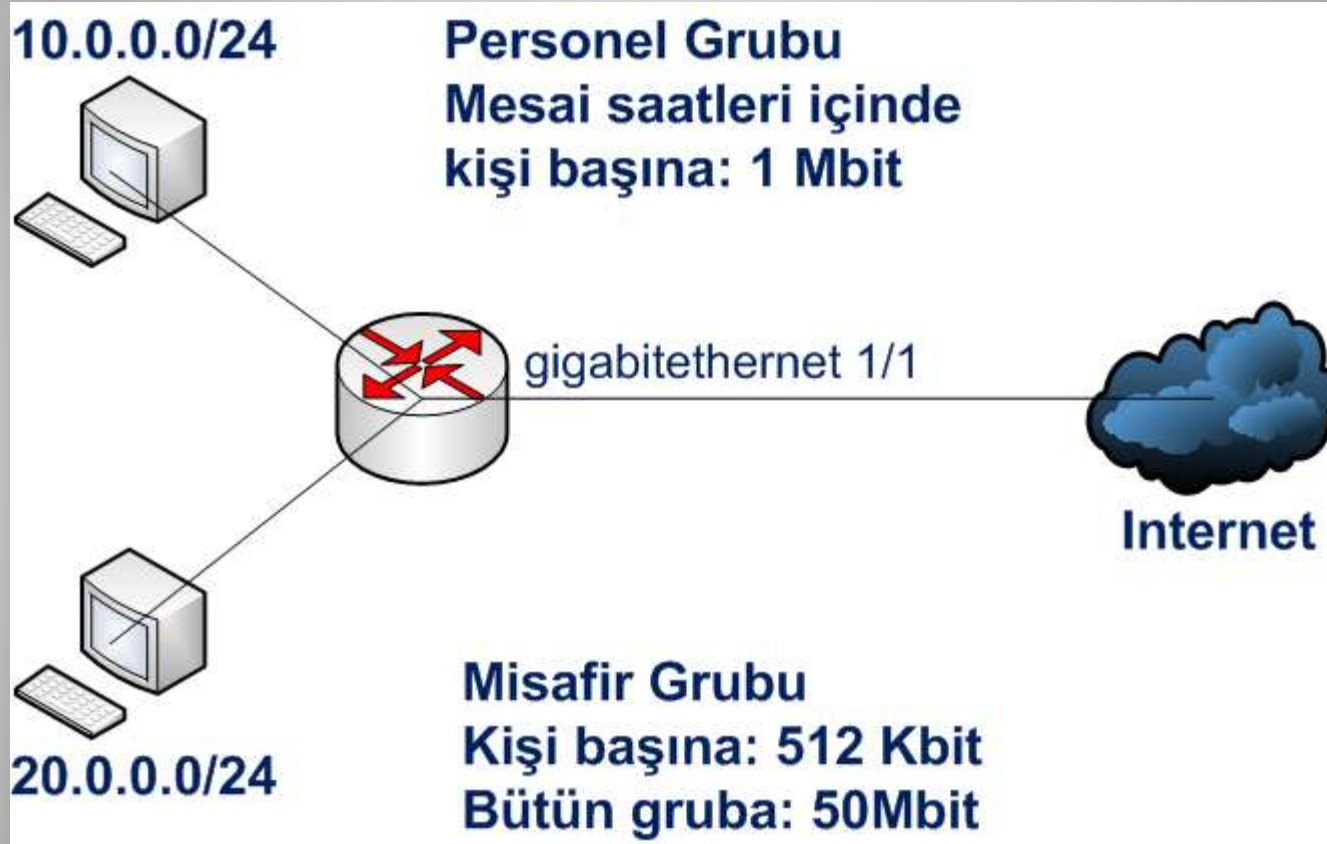
Politikanın Belirlenmesi ve Uygulanması

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

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



Zamana Baęlı Bant Geniřlięi 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
```

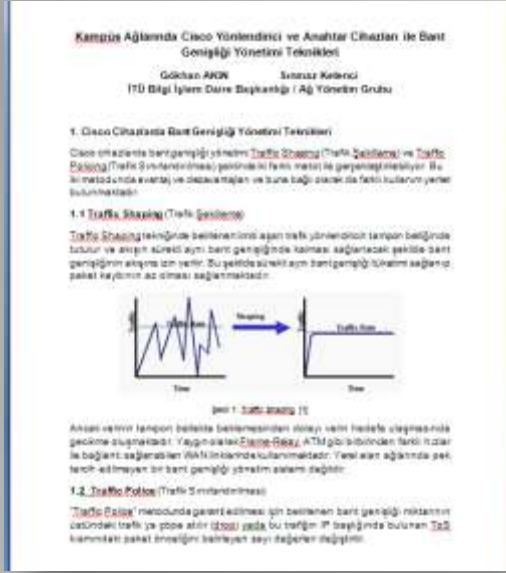
2- Protokol analizi yaparak: Yönlendiricilerde NBAR özelliği ile gerçekleştirilebilir.

```
Router(config)# class-map match-any WEB_TRAFIGI  
Router (config-cmap)#match protocol http
```

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



Reklamlar-1



Cisco Cihazlarda Bandgenişliği Yönetimi Detaylı Dökümanı

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

veya

<http://www.gokhanakin.net>



ULAK/CSIRT Güvenlik Blogu

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

Reklamlar-2



The screenshot shows the Agciyiz.net website with a blog post titled "SNMP v3 (Bölüm2)". The post discusses the security levels of SNMPv3, comparing them to previous versions and highlighting the importance of authentication and encryption. The website has a navigation menu with "ANASAYFA", "ARŞİV", "YAZARLAR", and "İLETİŞİM". There is also a search bar and a sidebar with a subscription form and various advertisements.

AGCIYIZ.NET
NETWORK KONTROL ALTINDA

ANASAYFA ARŞİV YAZARLAR İLETİŞİM

20 MAY/18

SNMP v3 (Bölüm2)

SNMPv3 önceki versiyonlara göre ve güvenli açısından daha gelişmiştir. SNMPv3'te güvenlik düzeyi kavramı ortaya çıkmıştır. Bu düzeyler noAuthNoPriv (kimlik denetimi ve şifreleme yok), authNoPriv (kimlik denetimi var, şifreleme yok) ve authPriv (kimlik denetimi ve şifreleme var) şeklindedir. Bu düzeylerin özellikleri şöyledir.

- noAuthNoPriv: v1 ve v2'ye karşılık gelen güvenli düzeydir. Sadece kullanıcı adı başı şifreleme yapar.
- authNoPriv: Önceki versiyonlara göre daha üst seviyede bir güvenlik sağlar çünkü kimlik denetimini kullanıcı adı ve şifre başı yapmanın yanı sıra MD5 veya SHA algoritmalarını kullanarak veri bütünlüğü de sağlar.
- authPriv: Uygulanması tavsiye edilen güvenli düzeydir çünkü bir önceki seviyeye ek olarak DES, 3DES ya da AES algoritmaları kullanarak sadece aynı anahtarla sahip alıcılara çözülebileceği bir şekilde veriyi şifeler.

Yani SNMPv3 güvenli modeli authPriv güvenli düzeyinde kullanıldığında güvenliğin 3 temel bileşeni olan kimlik denetimi, veri bütünlüğü ve gizliliği sağlar. Bu nedenle SNMPv3 IETF tarafından 2004 yılından itibaren güncel SNMP standardı olarak kabul edilmiş, önceki versiyonlar "denetim" olarak nitelendirilmiştir.

Kategori: Genel [Dünya'da Önemli](#)

18 MAY/18

SNMP v3 (Bölüm1)

SNMP (Simple Network Management Protocol) ile cihazların yönetimi ve bilgilendirilmesi.

Agciyiz.NET Abone Formu

Kullanıcı adı:

E-posta:

Ölümün yakından haberdar olabilmek için diğer ilgili alanları doldurarak kayıt olunuz.

Kayıt ol

İnternet Dükkanı

Voice & Qos

vitcfining

Mizah

Radikal Yayıncılık

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>

