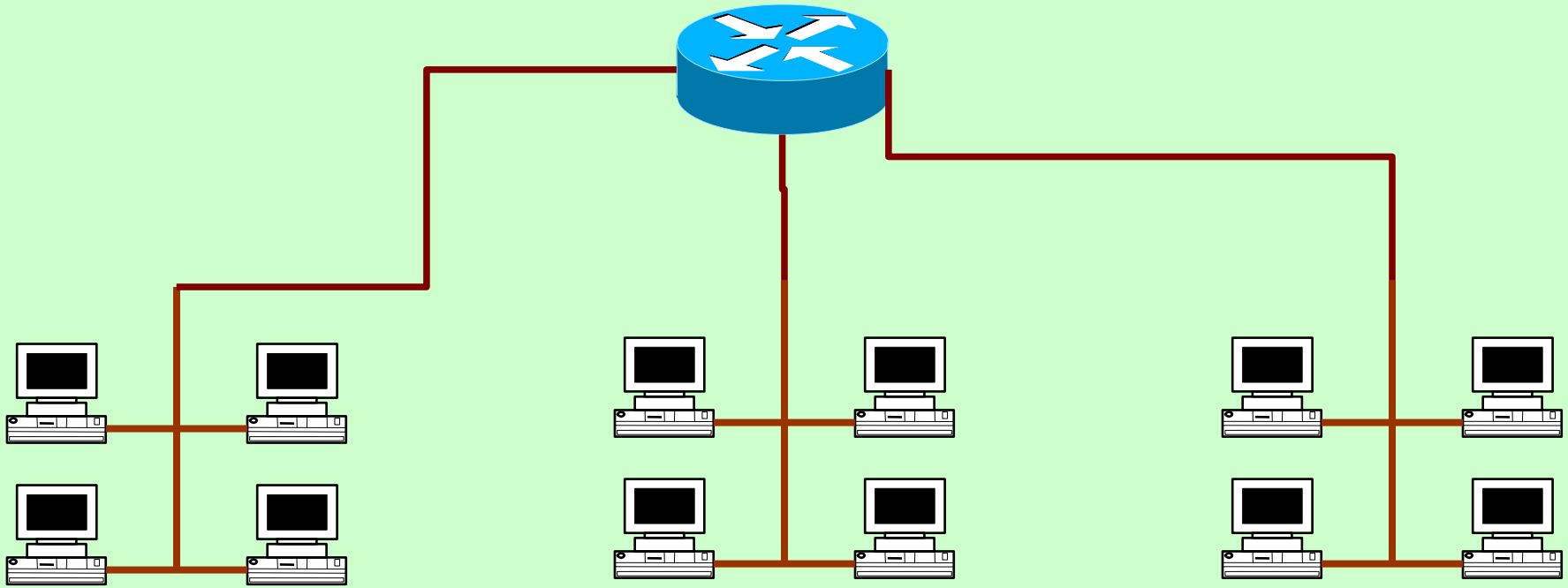
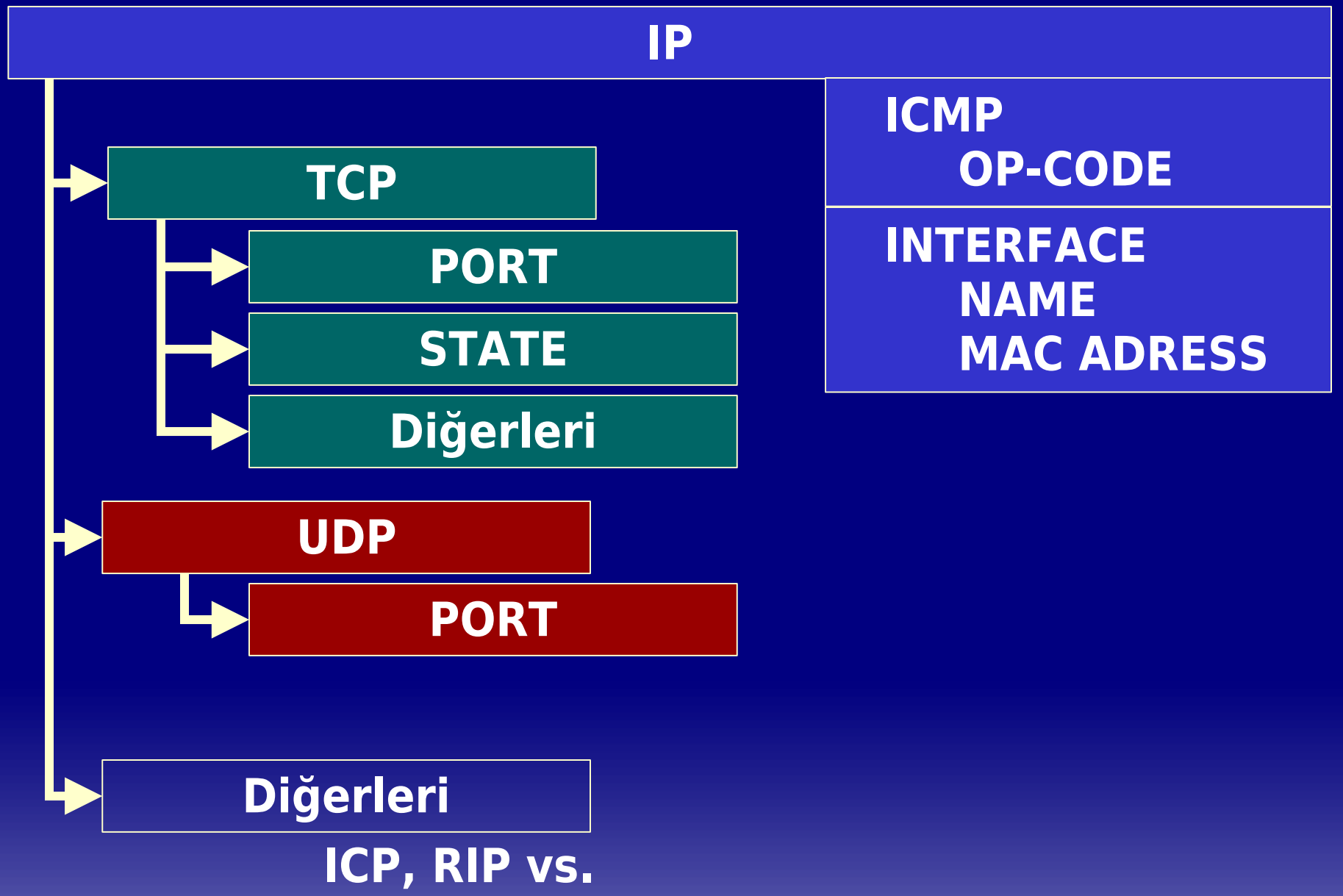
Netfilter + IPTables Güvenlik Duvarı

Firewall Nedir ?



Ağlar arasında yalıtımı sağlayan düzeneklerdir.

Bilinmesi gerekenler..



Netfilter + IPTables...

Netfilter;

Linux 2.4+ serisi kerneller için firewall altsistemi..

IPTables;

Bu altsistemi yönetmeyi sağlayan kullanıcı seviyesi program..

Netfilter’in kabiliyetleri

Packet filter;

IP paketlerinden istenilen kriterlere uygun olanlar durdurulabilir.

Full NAT;

Gelen paketler, orijinal hedeflerinden farklı yerlere yönlendirilebilir.

Connection Tracking;

Paketler bağlantı bazında izlenebilir. Böylece bağlantının sürmesi için gerekli olan işlevler otomatikman yerine getirilir.

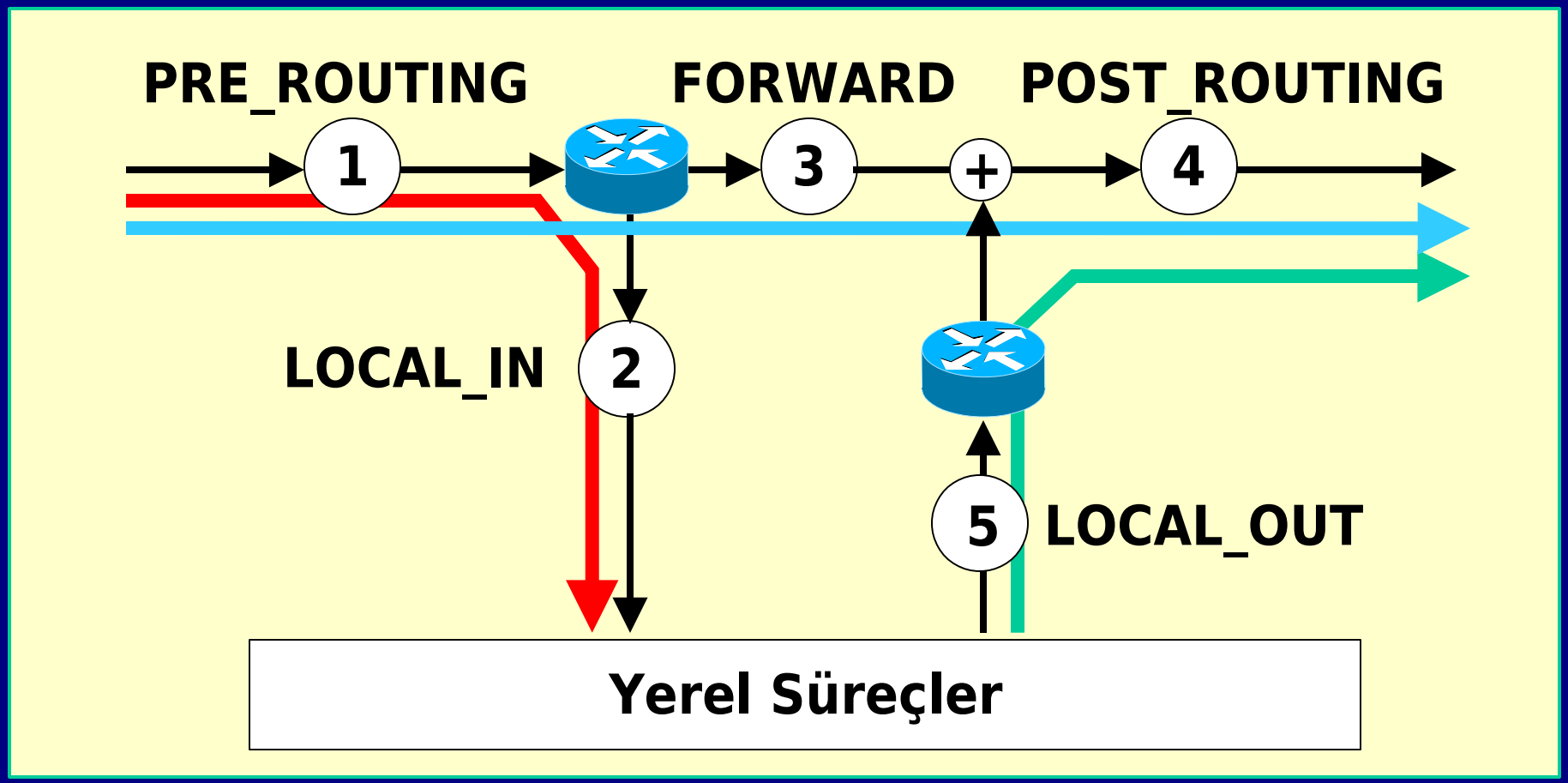
IPTables.. Kullanıcı arabirimi..

 # iptables --help

Iptables parametreleri ilk bakışta çok karmaşık görünür.

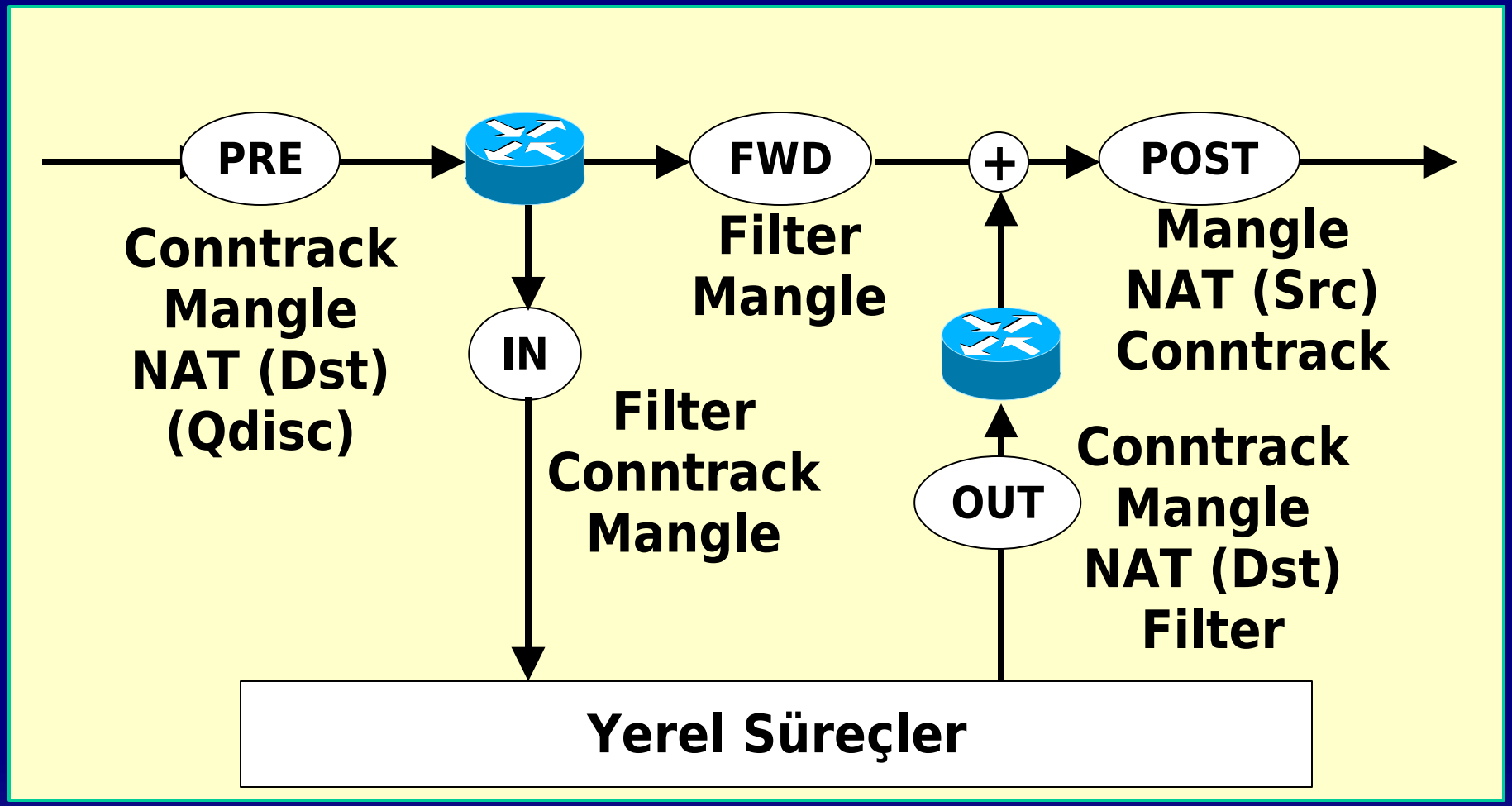
Halbuki Iptables'i anlamak o kadar zor değildir

Kernel'deki uzantılar (HOOKS)..



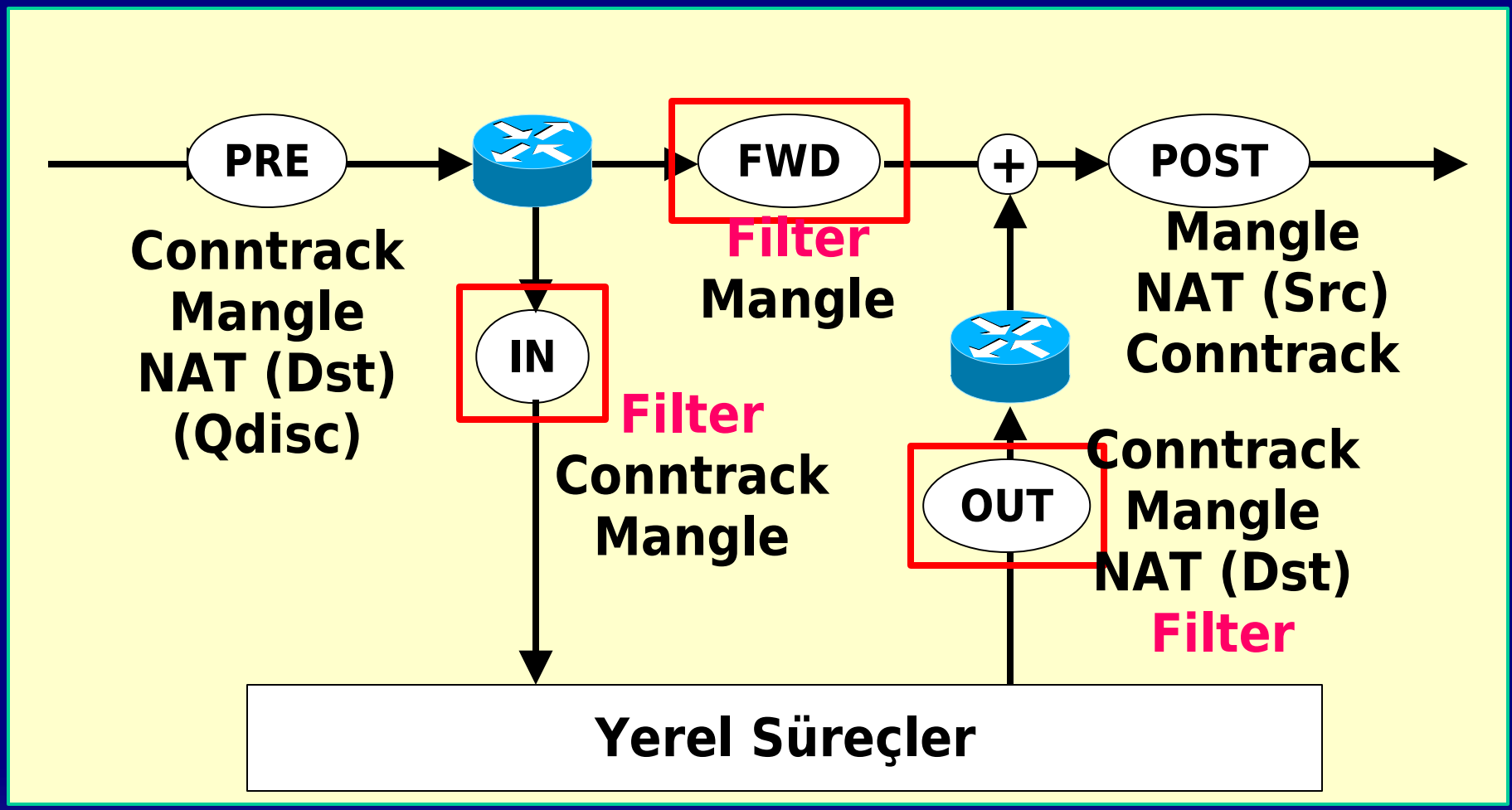
Netfilter, farklı noktalardan Protokol yığınına bağlanır

Kernel'deki uzantılar (TABLES)..



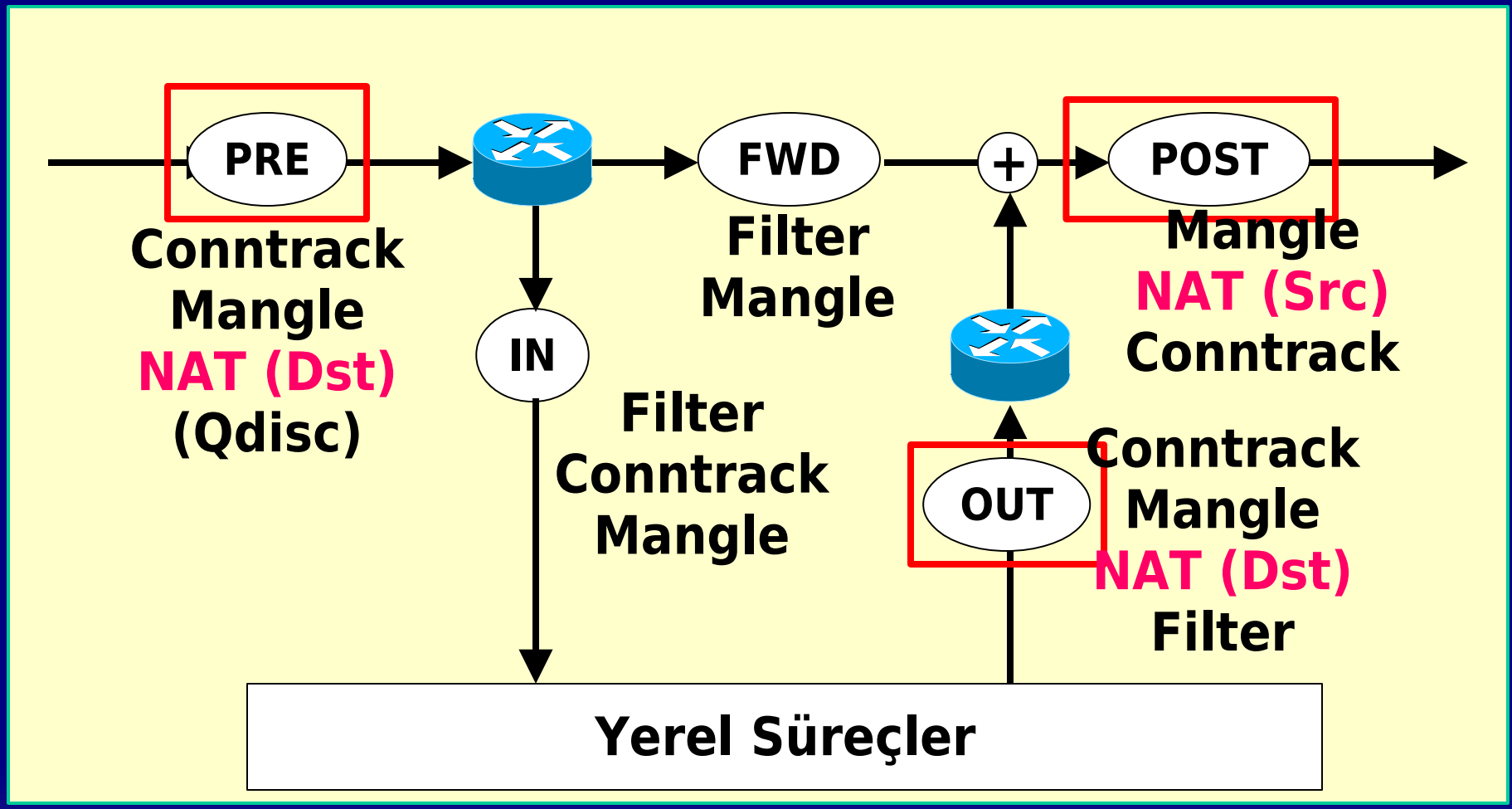
Tablolar, zincirlerdeki paketler üzerinde işlem yapan modüllerdir.
Kendilerini ilgili zincirlere bağlarlar.

Standart tablolar (FILTER)..



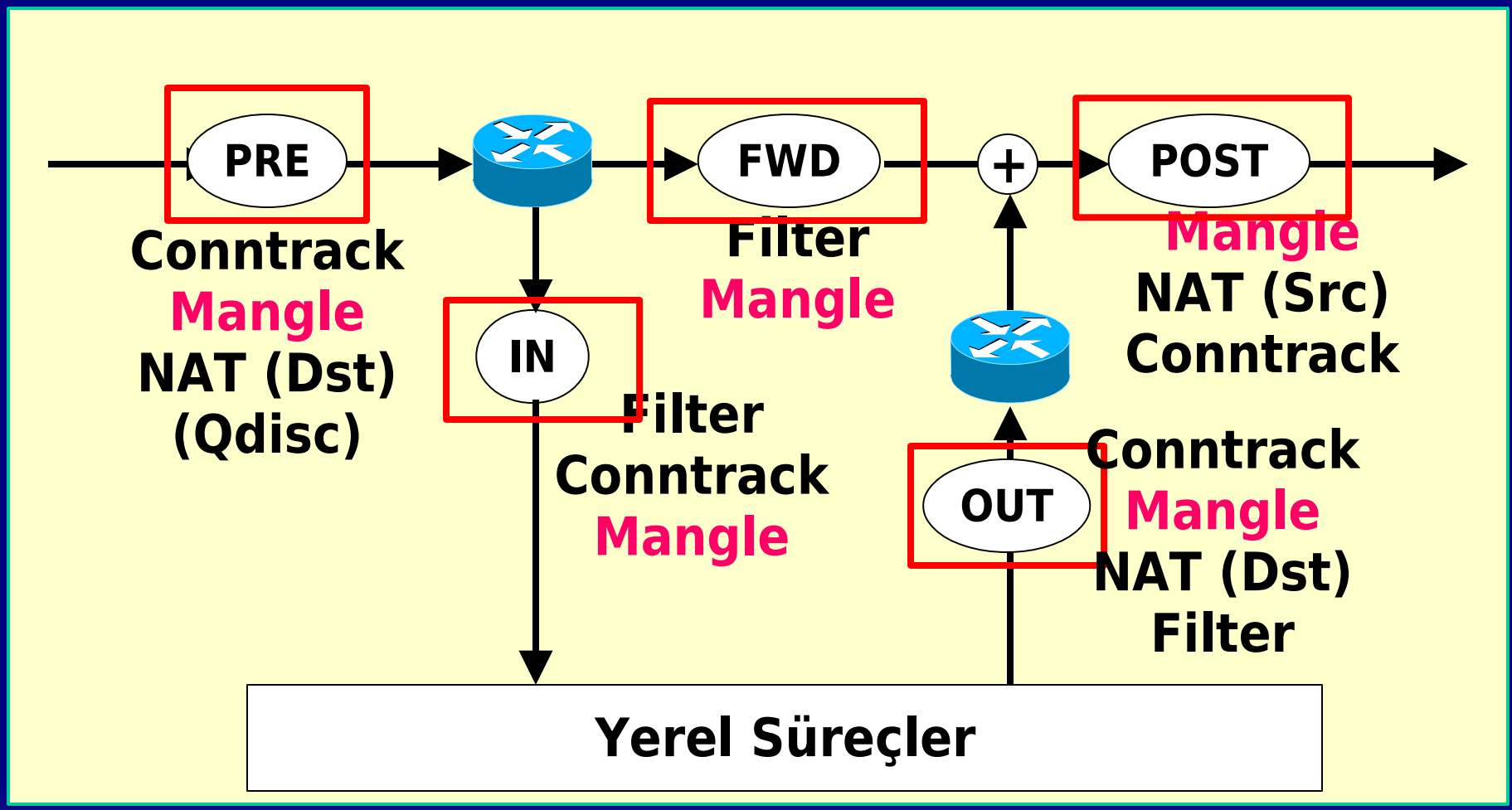
Filter, paketlerin buradan geçip yoluna devam edip edemeyeceğini belirler.
DROP ACCEPT STOLEN

Standart tablolar (NAT)..



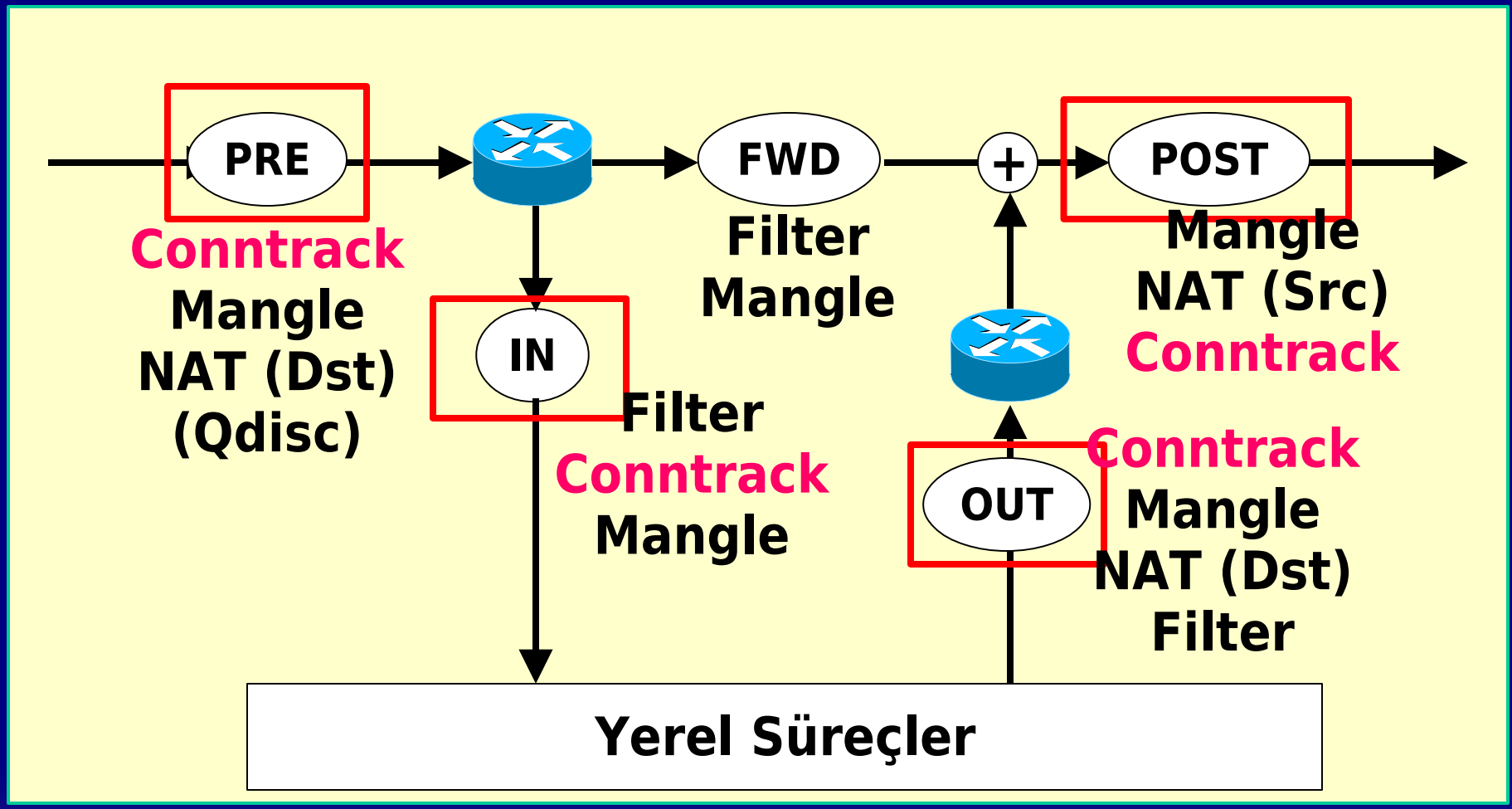
NAT, Network Adress Translation
IP paketinin nerden geldiğini ve nereye gittiğini farklı göstermek için yapılır.

Standart tablolar (MANGLE)..



MANGLE, paketlerin ceşitli özelliklerini değiştirebilmeyi sağlar.
TOS, TTL, MARK

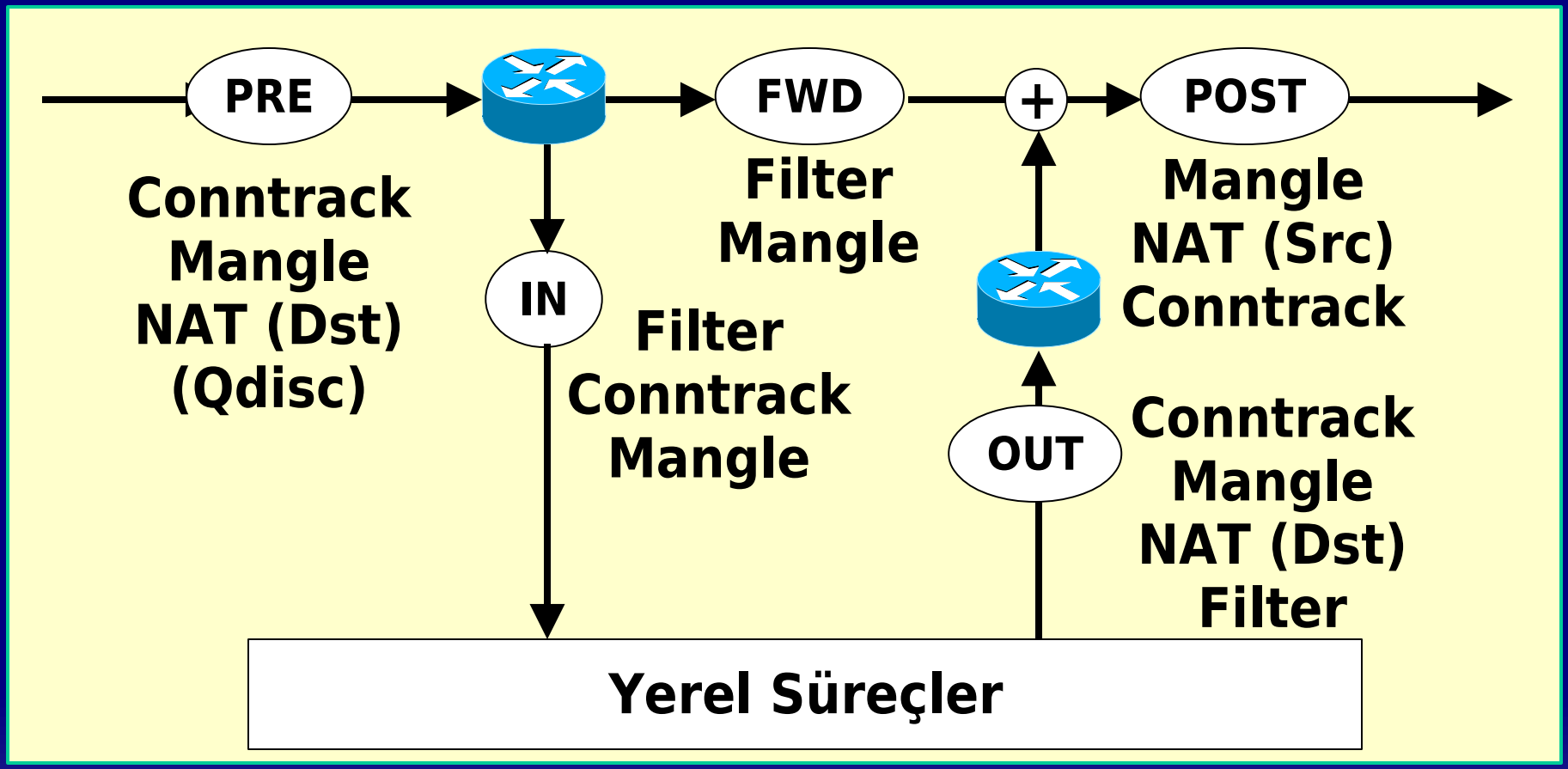
Standart tablolar (MANGLE)..



Conntrack, bağlantıları takip ederek gerekli işlevleri yerine getirir. Özellikle NAT için gereklidir.

Kernel'deki uzantılar (TABLES)..

* **Paketlerin hangi tabloda işleneceğini belirleyin**




```
# iptables -t nat
# iptables -t filter
```

IPTables.. Kullanıcı arabirimi..

* **Hangi Tabloyu kullanacağınızı belirleyin.**

Sistemdeki belli servislere erişimi kontrol etmek istiyorsanız,

* **Dahili bilgisayarların, ana sistemlere erişimini denetlemek,**
* **Ana sistemlere Internet'ten erişimi sınırlamak..**
* **Dahili bilgisayarların, Internet'e erişimini kısıtlamak..**

FILTER

IPTables.. Kullanıcı arabirimi..

* **Hangi Tabloyu kullanacağınızı belirleyin.**

Public IP'leriniz yetersizse,

Server hostlar için ekstra güvenlik istiyorsanız,

Yük dengeleme gerekiyorsa,

Bir hostun diğer hostlara erişimi gerekirken, diğerlerinin bu hostu görmesini istemiyorsanız

NAT

IPTables.. Kullanıcı arabirimi..

* **Hangi Tabloyu kullanacağınızı belirleyin.**

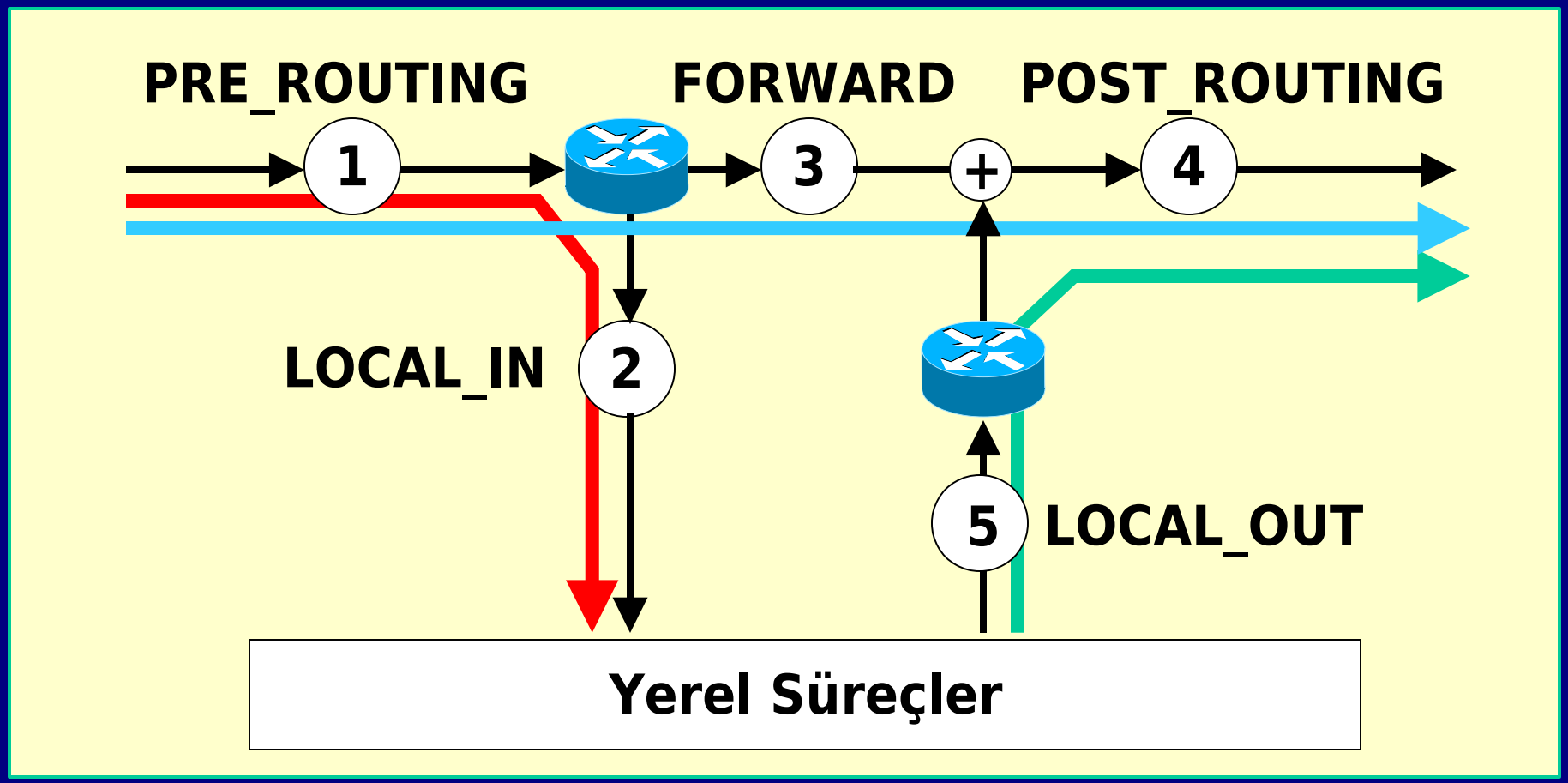
QoS kontrolu,

Bandwith balancing,

IP paket özelliklerinde tam hakimiyet,

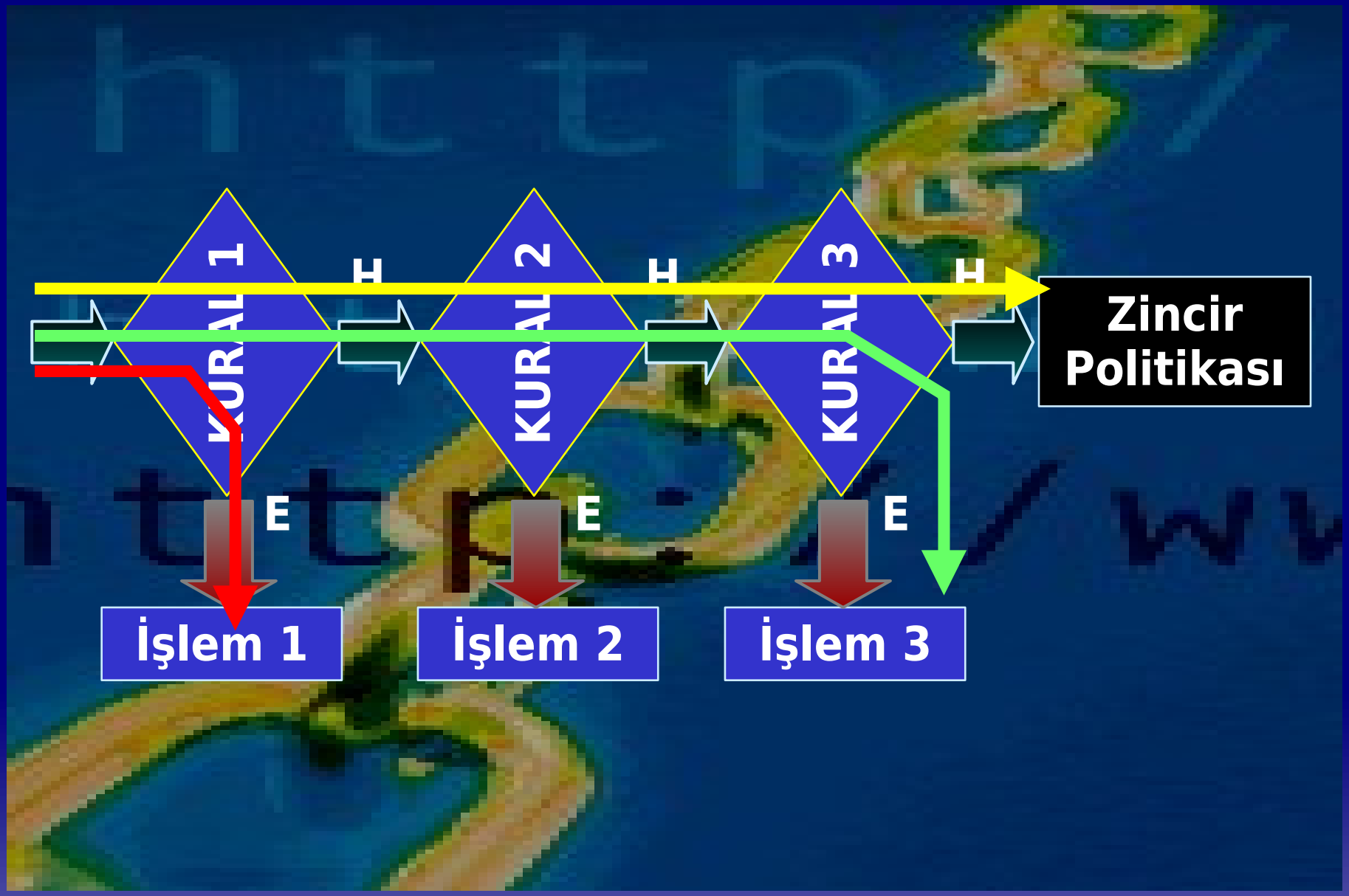
MANGLE

Kernel'deki uzantılar (CHAINS)..

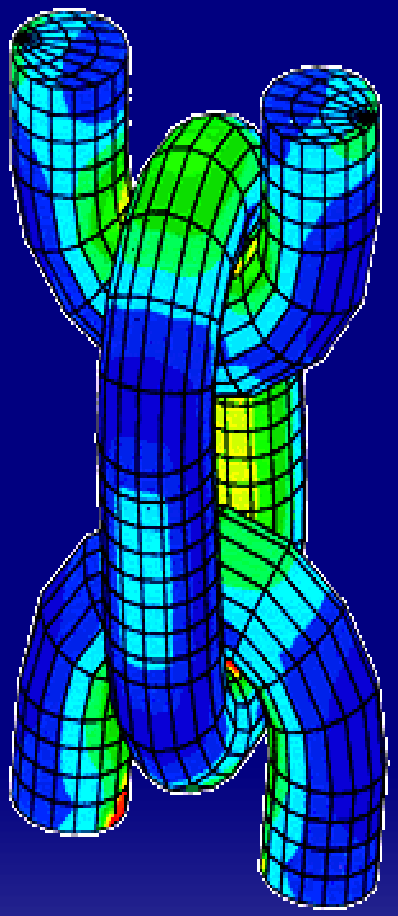


Netfilter, farklı noktalardan Protokol yığınına bağlanır

IPTables.. Zincirlerde paket işlemleri.



IPTables.. Zincirlerde paket işlemleri.



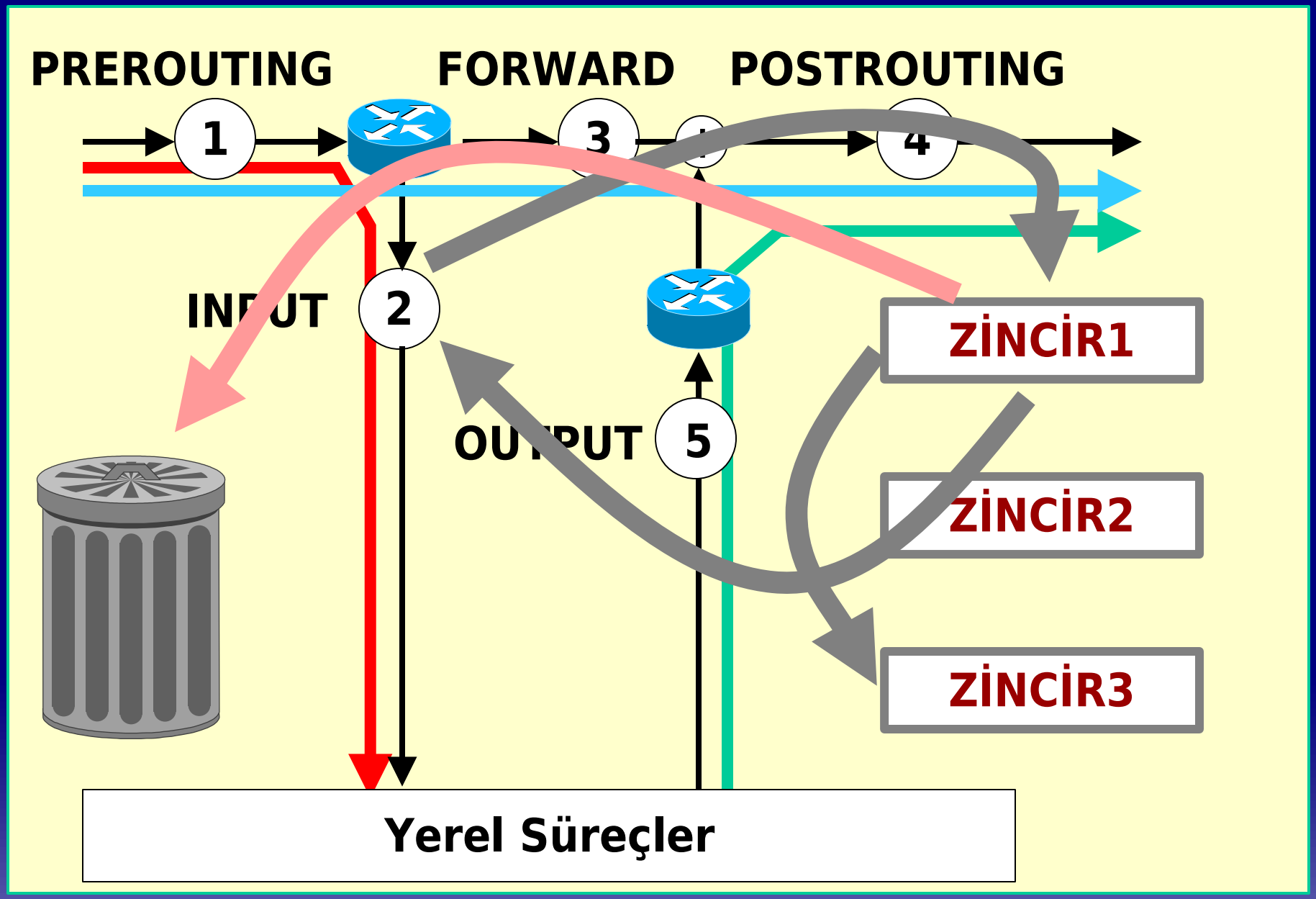
Paketin bizim aradığımız kritere uygunluğunu tarif eden özellikleri

KURAL

Uygun paketi bulunca onu ne yapacağımıza dair komut

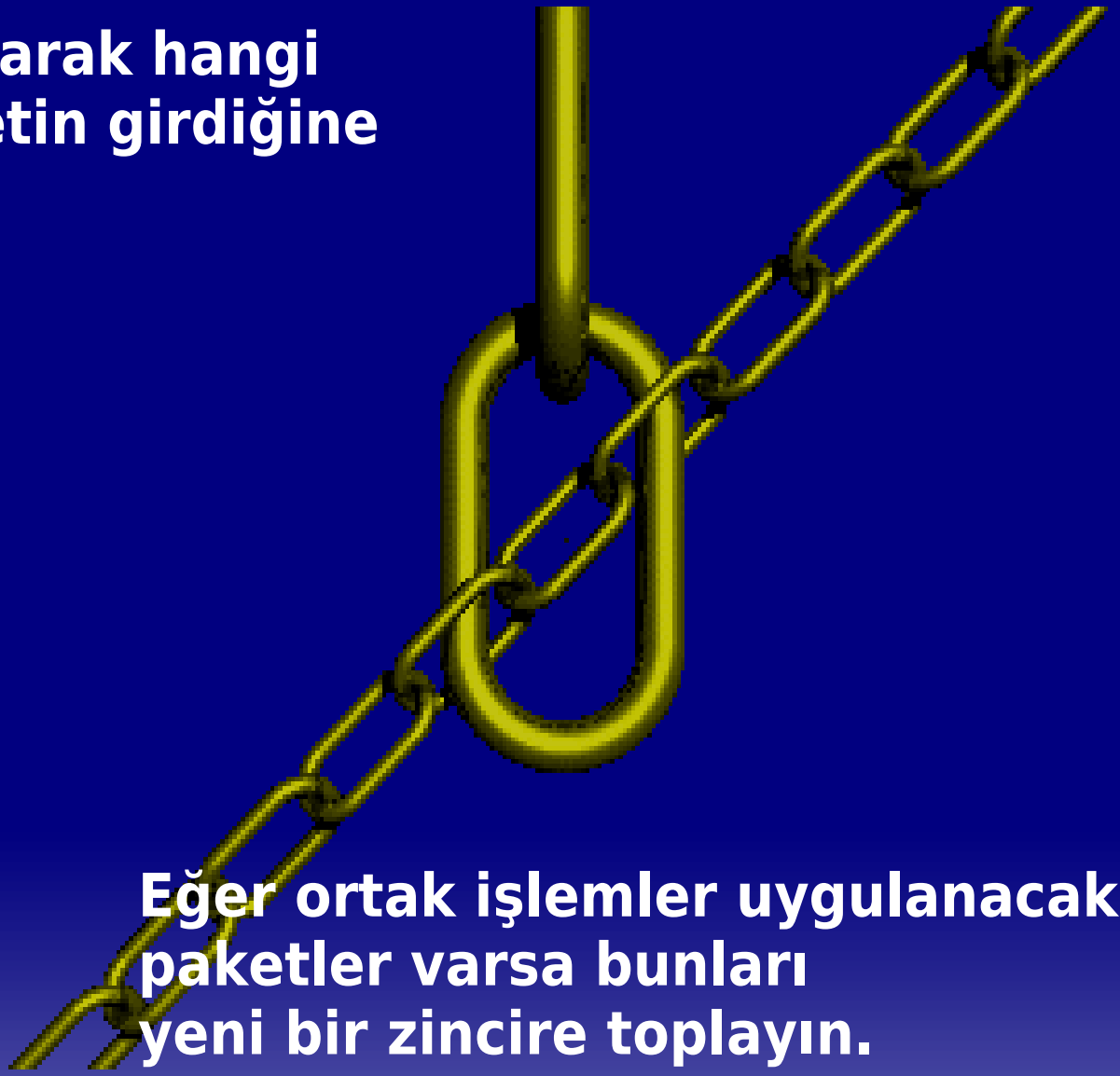
YAPTIRIM

IPTables.. Zincirlerde paket işlemleri.



IPTables.. Hangi Zincir ?

Şekillere uygun olarak hangi zincire hangi paketin girdiğine göre zinciri seçin.



Eğer ortak işlemler uygulanacak paketler varsa bunları yeni bir zincire toplayın.

IPTables.. Hangi Zincir ?

```
# iptables -P INPUT ACCEPT
# iptables -F FORWARD
# iptables -t nat -Z OUTPUT
```

```
# iptables -A INPUT  ..........
# iptables -I  FORWARD 2 ..........
# iptables -R OUTPUT 2 ..............
# iptables -D PREROUTING 2
```

```
# iptables -N WEBDATA
# iptables -X WEBDATA
# iptables -E WEBDATA WEBCHAIN
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- **Kaynak ve hedef adresleri**
- **TTL değeri**
- **Parçalanmış olma durumu**
- **Hangi arabirimden alındığı**
- **Hangi arabirimden çıkacağı**
- **Ethernet için, MAC Adresleri**
- **Paket alınma/yollanma sıklığı**

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- **Kaynak ve hedef adresleri**
- **TTL değeri**
- **Parçalanmış olma durumu**
- **Hangi arabirimden alındığı**
- **Hangi arabirimden çıkacağı**
- **Ethernet için, MAC Adresleri**
- **Paket alınma/yollanma sıklığı**

```
# iptables -s a.b.c.d -d e.f.g.h
# iptables -s a.b.c.d/n.n.n.n -d a.b.c.d/n.n.n.n
# iptables -s a.b.c.d/n.n.n.n -d ! a.b.c.d/n.n.n.n
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- Kaynak ve hedef adresleri
- **TTL değeri**
- Parçalanmış olma durumu
- Hangi arabirimden alındığı
- Hangi arabirimden çıkacağı
- Ethernet için, MAC Adresleri
- Paket alınma/yollanma sıklığı

```
# iptables -m ttl --ttl-eq 128
# iptables -m ttl --ttl-lt 128
# iptables -m ttl --ttl-gt 128
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- Kaynak ve hedef adresleri
- TTL değeri
- **Parçalanmış olma durumu**
- Hangi arabirimden alındığı
- Hangi arabirimden çıkacağı
- Ethernet için, MAC Adresleri
- Paket alınma/yollanma sıklığı

```
# iptables -f
# iptables  ! -f 128
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- Kaynak ve hedef adresleri
- TTL değeri
- Parçalanmış olma durumu
- **Hangi arabirimden alındığı**
- Hangi arabirimden çıkacağı
- Ethernet için, MAC Adresleri
- Paket alınma/yollanma sıklığı

```
# iptables -i eth0
# iptables -i ppp+
# iptables -i ! eth+
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- Kaynak ve hedef adresleri
- TTL değeri
- Parçalanmış olma durumu
- Hangi arabirimden alındığı
- **Hangi arabirimden çıkacağı**
- Ethernet için, MAC Adresleri
- Paket alınma/yollanma sıklığı

```
# iptables -o eth0
# iptables -o ppp+
# iptables -o ! eth+
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- Kaynak ve hedef adresleri
- TTL değeri
- Parçalanmış olma durumu
- Hangi arabirimden alındığı
- Hangi arabirimden çıkacağı
- **Ethernet için, MAC Adresleri**
- Paket alınma/yollanma sıklığı

```
# iptables -m mac --mac-source 01:02:03:04:05:06
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

Tüm IP paketleri için ortak olan değerler..

- Kaynak ve hedef adresleri
- TTL değeri
- Parçalanmış olma durumu
- Hangi arabirimden alındığı
- Hangi arabirimden çıkacağı
- Ethernet için, MAC Adresleri
- **Paket alınma/yollanma sıklığı**

```
# iptables -m limit --limit 30/second
# iptables -m limit --limit 10/hour
# iptables -m limit --limit-burst 5
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

TCP için değerler..

- **Geldiği port**
- **Gittiği Port**
- **Paketin durum bilgileri**
  - **SYN, ACK, FIN, URG, PSH, ALL, NONE**

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

TCP için değerler..

- **Geldiği port**
- **Gittiği Port**
- **Paketin durum bilgileri**
  - **SYN, ACK, FIN, URG, PSH, ALL, NONE**

```
# iptables -p tcp --source-port 80
# iptables -p tcp --sport ftp
# iptables -p tcp --sport  6600:7700

# iptables -p tcp -m multiport --sport  25,110
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

TCP için değerler..

- **Geldiği port**
- **Gittiği Port**
- **Paketin durum bilgileri**
  - **SYN, ACK, FIN, URG, PSH, ALL, NONE**

```
# iptables -p tcp --destination-port 80
# iptables -p tcp --dport ftp
# iptables -p tcp --dport  6600:7700

# iptables -p tcp -m multiport --dport  80,21
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

TCP için değerler..

- **Geldiği port**
- **Gittiği Port**
- **Paketin durum bilgileri**
  - **SYN, ACK, FIN, URG, PSH, ALL, NONE**
  - **NEW, ESTABLISHED, INVALID, RELATED**

```
# iptables -p tcp --tcp-flags  SYN,ACK,FIN SYN
# iptables --syn
# iptables -p tcp -m state --state NEW,RELATED
# iptables -p tcp -m state --state ESTABLISHED
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

UDP için değerler..

- **Geldiği port**
- **Gittiği Port**

```
# iptables -p udp --source-port 80
# iptables -p udp --sport ftp
# iptables -p udp --sport  6600:7700

# iptables -p udp --destination-port 80
# iptables -p udp --dport ftp
# iptables -p udp --dport  6600:7700
```

IPTables.. Kuralların tespiti..

* **Hangi paketlerin işleme tabi tutulacağını belirleyin.**

ICMP için değerler..

ICMP Op-code..

```
# iptables -p icmp --icmp-type  echo-reply

# iptables -p icmp -h
```

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

FILTER tablosu, hangi paketin geçebileceği..

DROP

ACCEPT

QUEUE

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

FILTER tablosu, hangi paketin geçebileceği..

DROP

ACCEPT

QUEUE

```
# iptables (kural) -j DROP
```

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

FILTER tablosu, hangi paketin geçebileceği..

DROP

ACCEPT

QUEUE

 # iptables (kural) -j ACCEPT

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

FILTER tablosu, hangi paketin geçebileceği..

DROP

ACCEPT

QUEUE

```
# iptables (kural) -j QUEUE
```

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

NAT Tablosu geliş /gidiş adreslerini değiştirme için.

DNAT

SNAT

REDIRECT

MASQUERADING

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

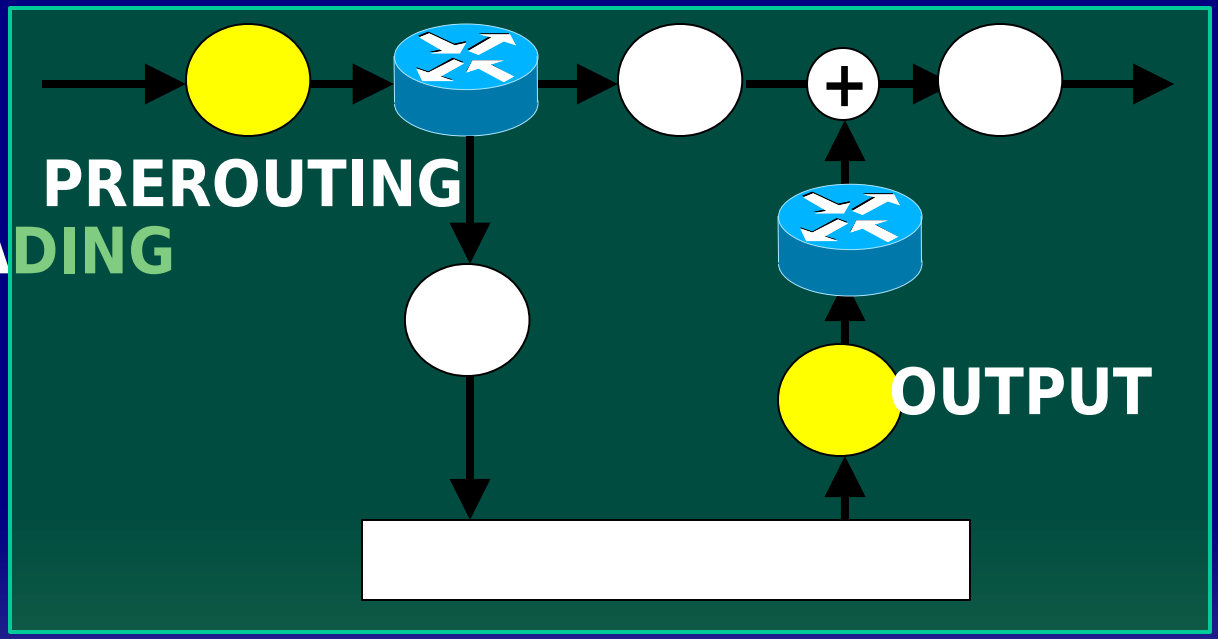
NAT Tablosu geliş /gidiş adreslerini değiştirme için.

DNAT

SNAT

REDIRECT

MASQUERADING



 # iptables -t nat -? ZİNCİR -j DNAT --to a.b.c.d:xx

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

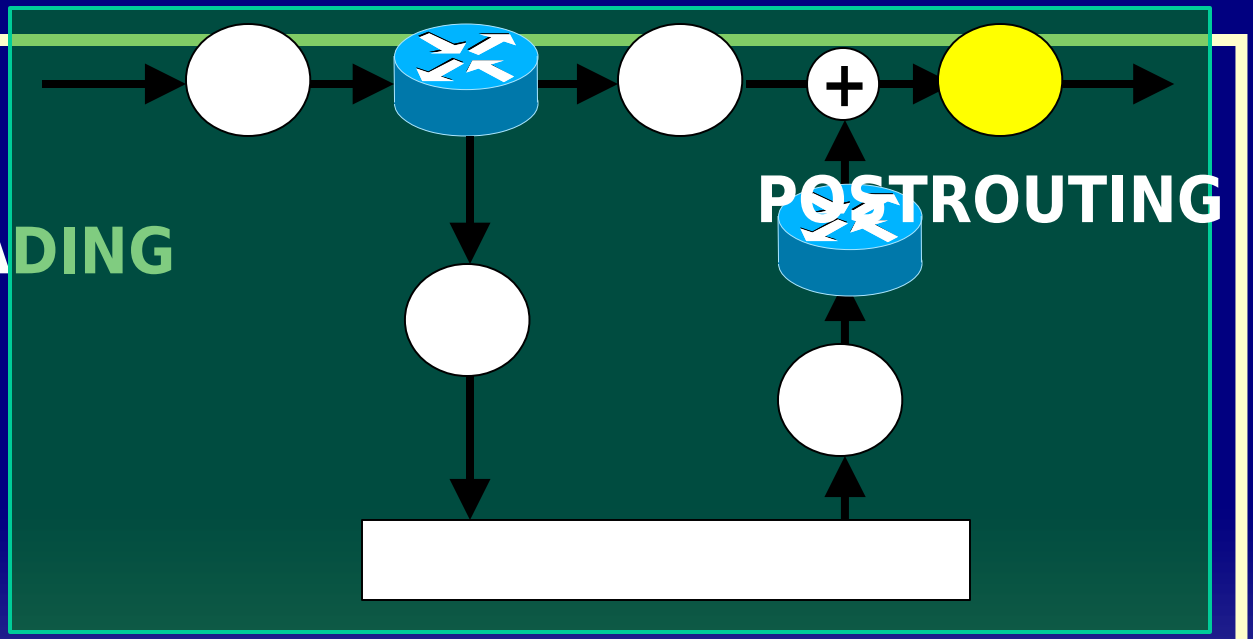
NAT Tablosu geliş /gidiş adreslerini değiştirme için.

DNAT

SNAT

REDIRECT

MASQUERADING




```
# iptables -t nat -POSTROUTING -j SNAT --to a.b.c.d:xx
```

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

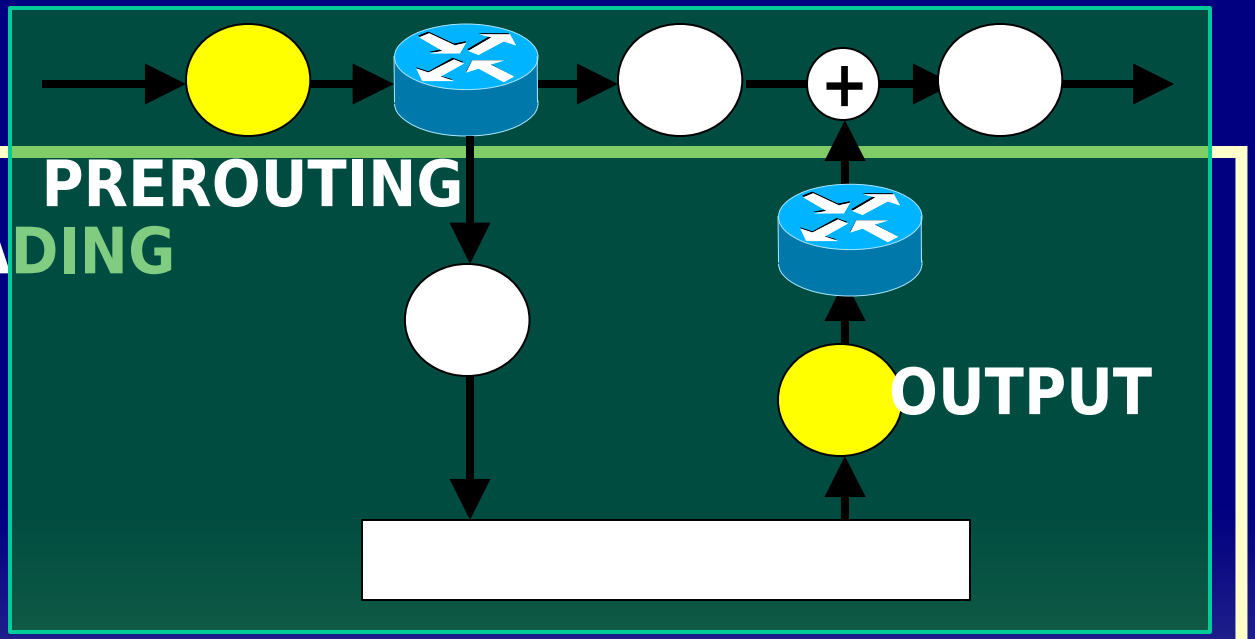
NAT Tablosu geliş /gidiş adreslerini değiştirme için.

DNAT

SNAT

REDIRECT

MASQUERADING



 # iptables -t nat -? ZİNCİR -j REDIRECT --to xx

IPTables.. Kullanıcı arabirimi..

* **Paketlere ne yapacağınızı belirleyin..**

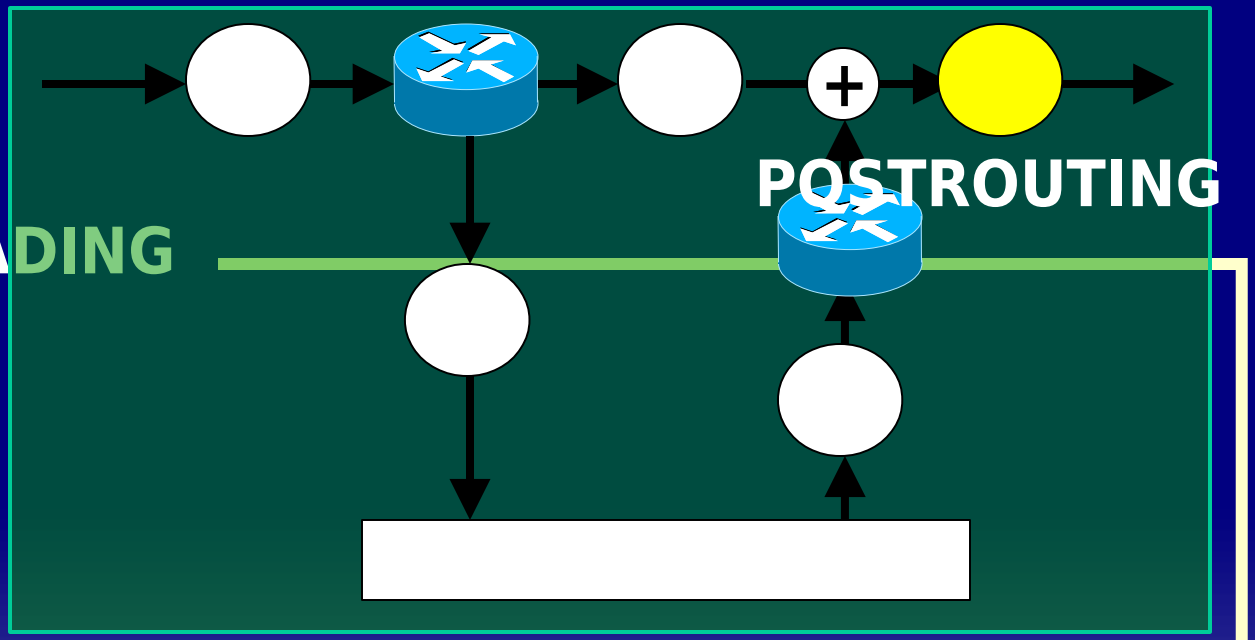
NAT Tablosu geliş /gidiş adreslerini değiştirme için.

DNAT

SNAT

REDIRECT

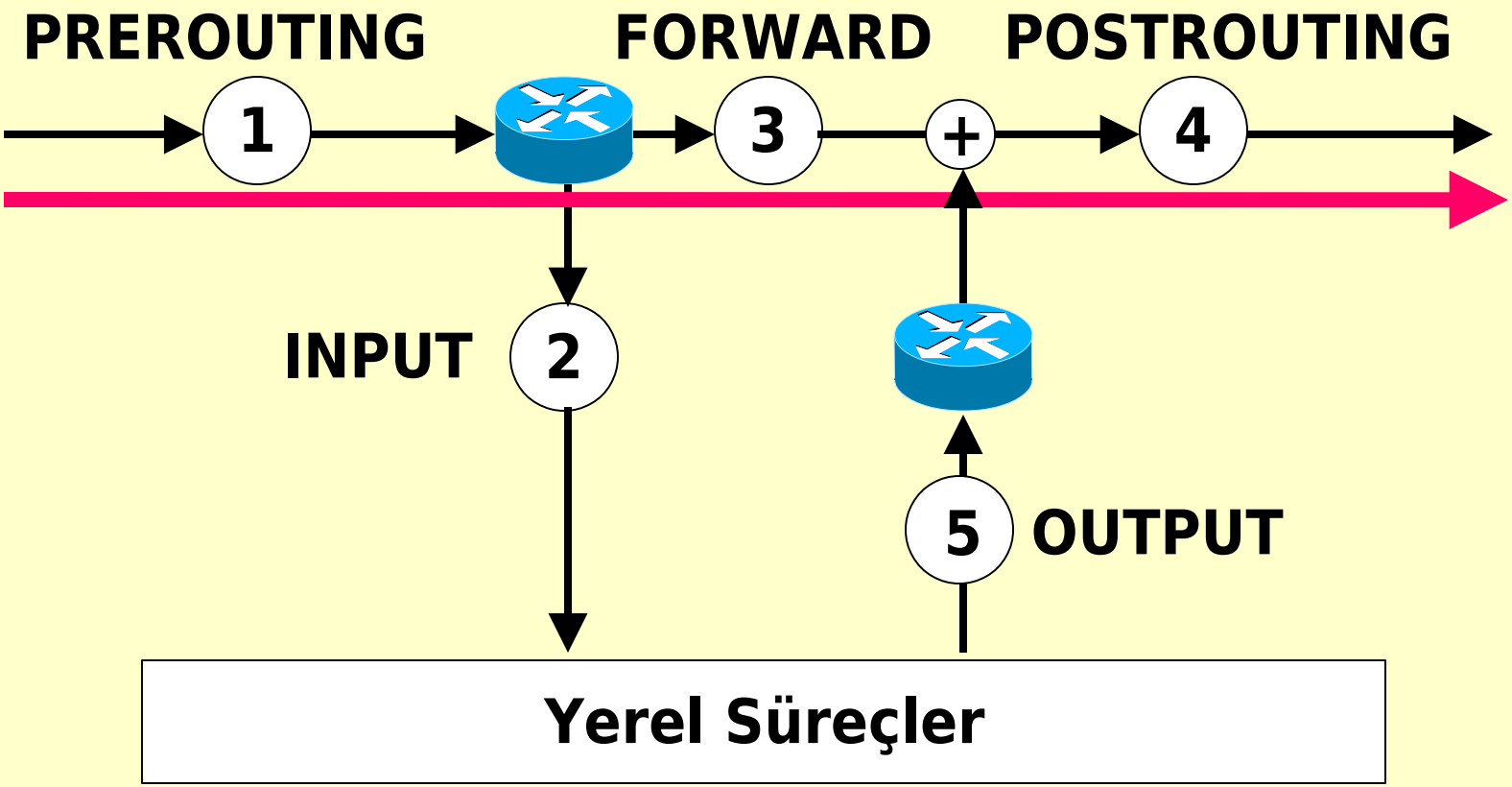
MASQUERADING



 # iptables -t nat -? POSTROUTING -j MASQUERADE

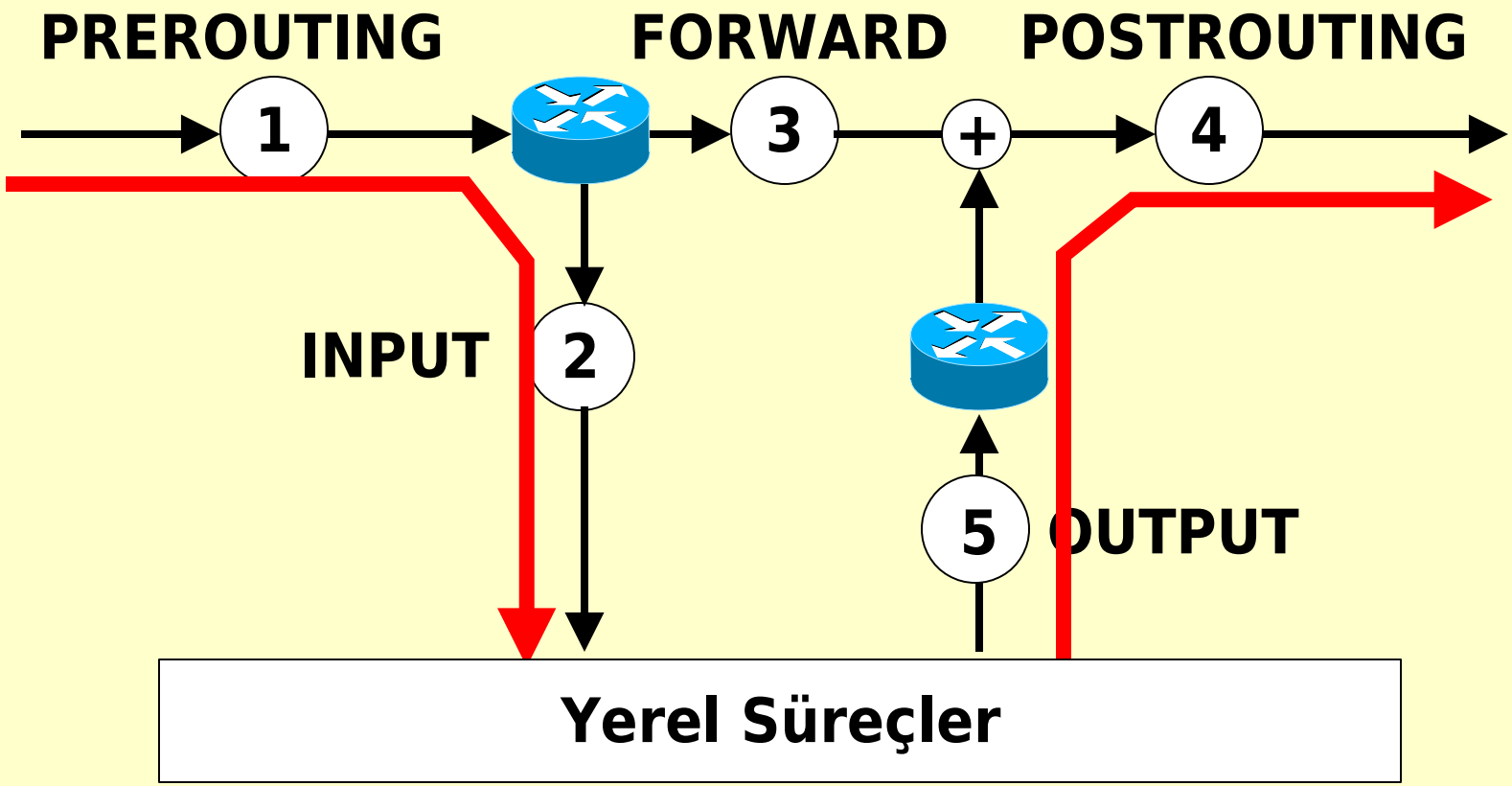
Örnekler..

* **Firewall Router olarak çalışan makineler..**



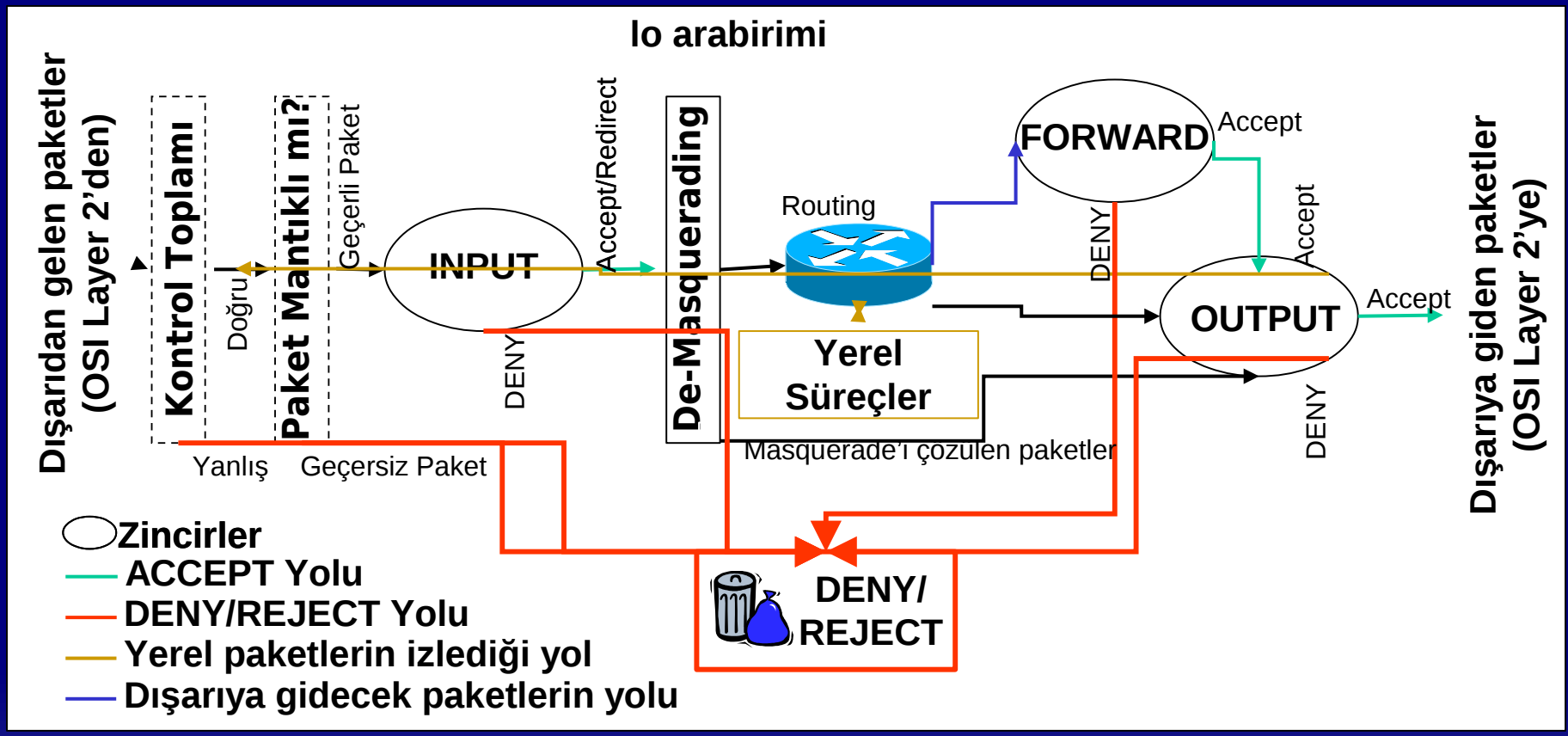
Örnekler..

* **Server ve/veya Client olarak çalışan makineler..**



Örnekler..

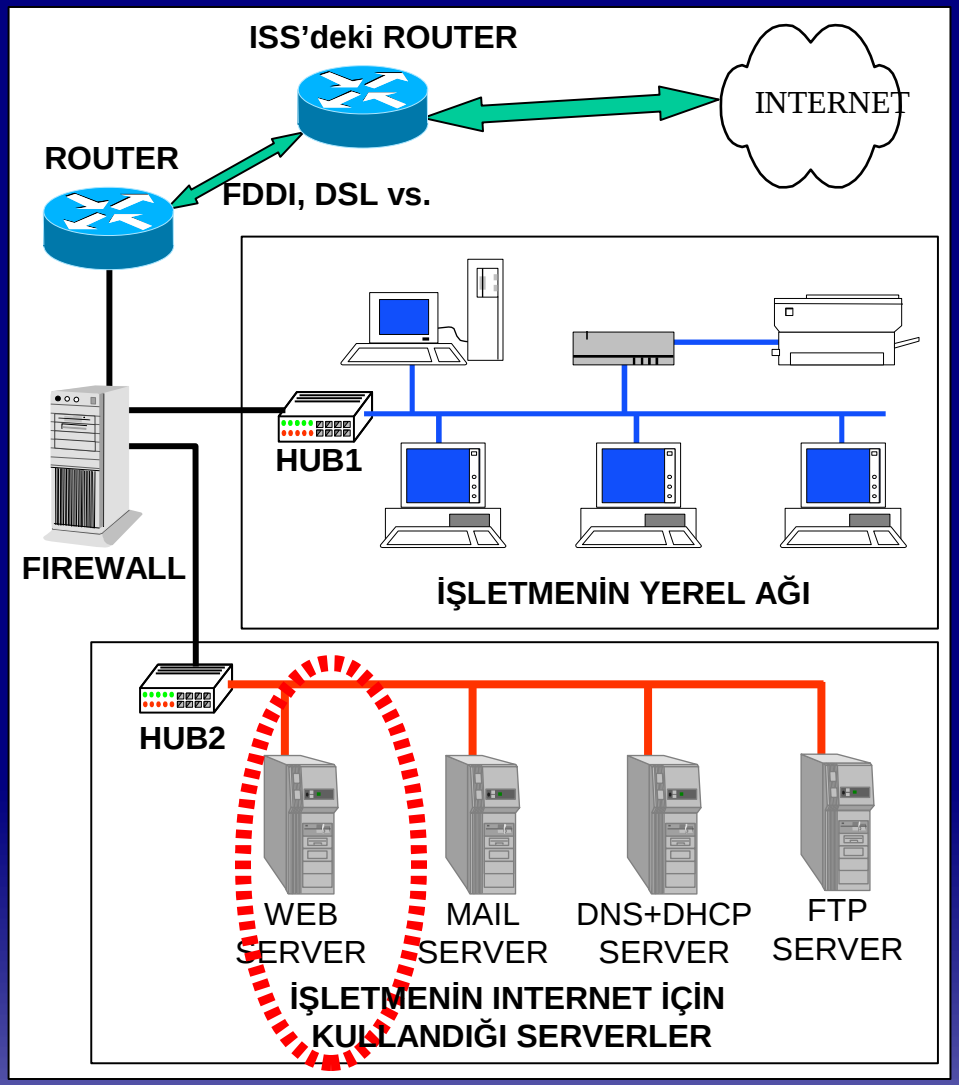
* **IPTables ile IPChains arasındaki farklar..**



IPTables, INPUT ve OUTPUT zincirlerinde sadece yerel paketler işlenebilir.

Örnekler..

* **Yerelde tek bir servise gelen paketleri kabul et.**

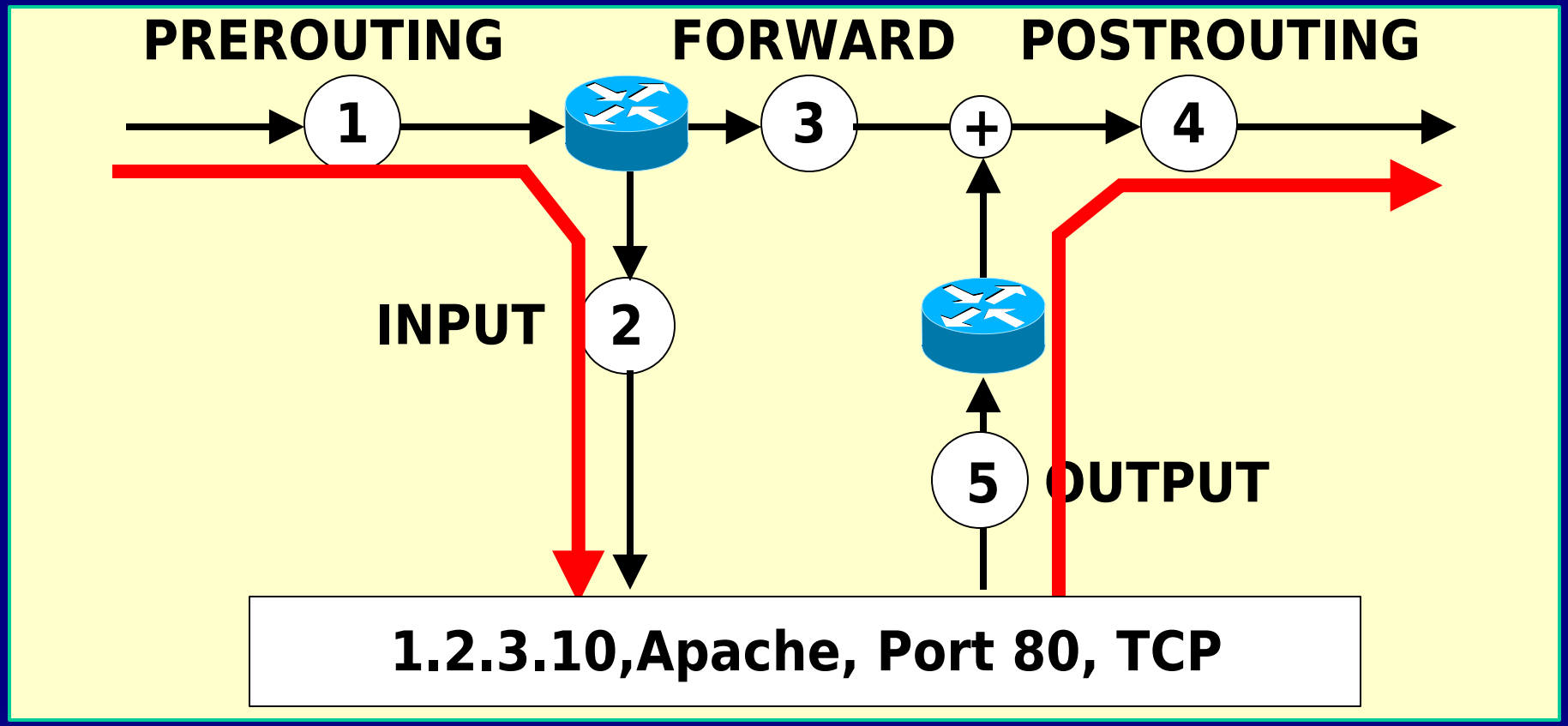


HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
LOCAL: 10.1.0.0/16

Örnekler..

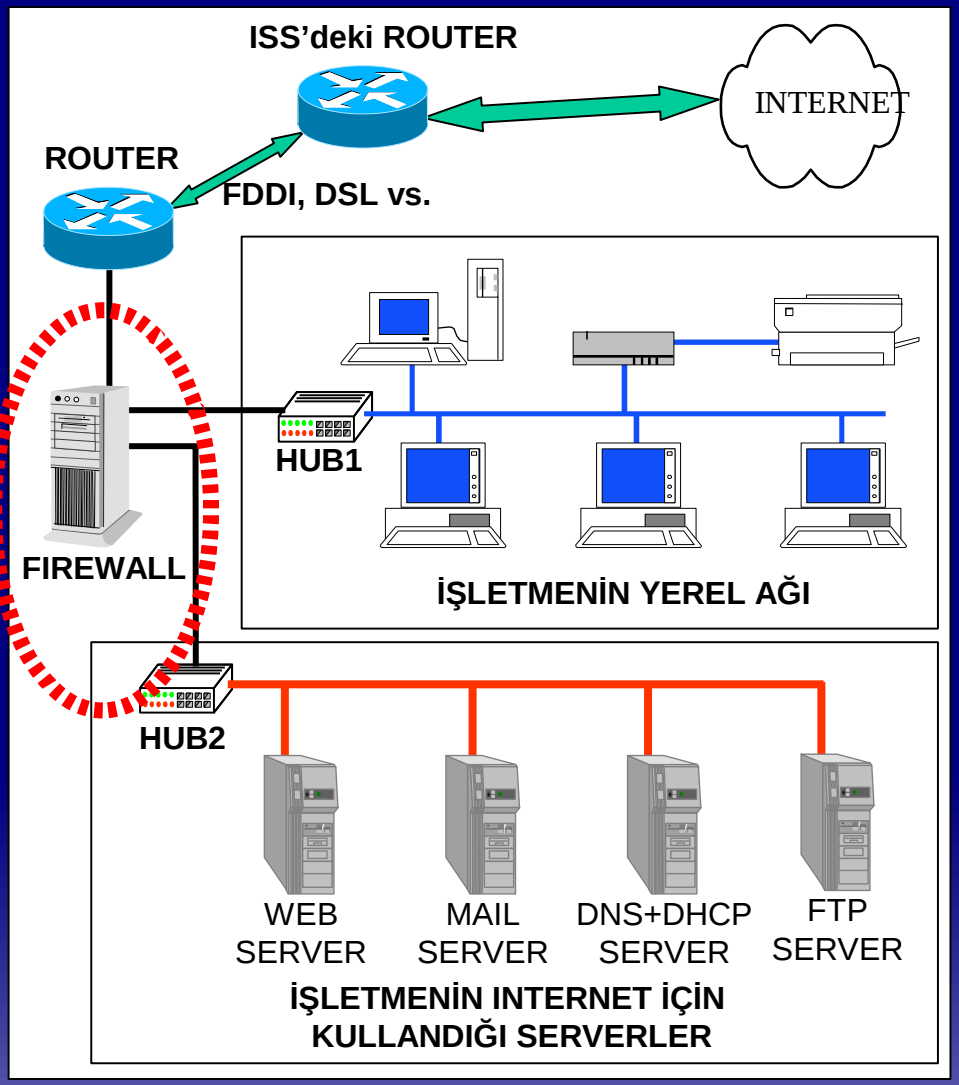
* **Yerelde tek bir servise gelen paketleri kabul et.**




```
# iptables -t filter -P PREROUTING DROP
# iptables -A PREROUTING -d 1.2.3.10 \
    -p tcp --dport 80 -j ACCEPT
```

Örnekler..

* **Firewall'de tek bir servise giden paketleri kabul et.**

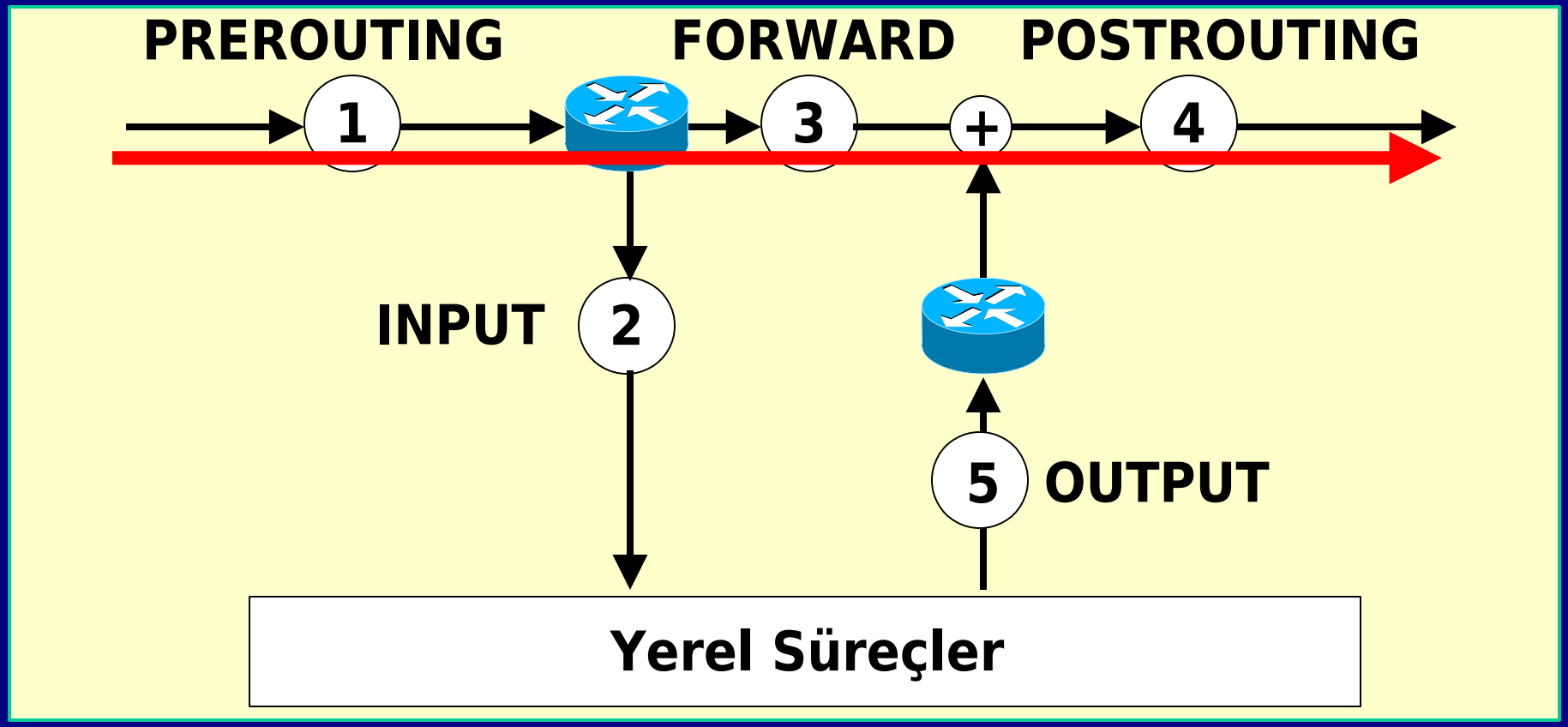


HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
LOCAL: 10.1.0.0/16

Örnekler..

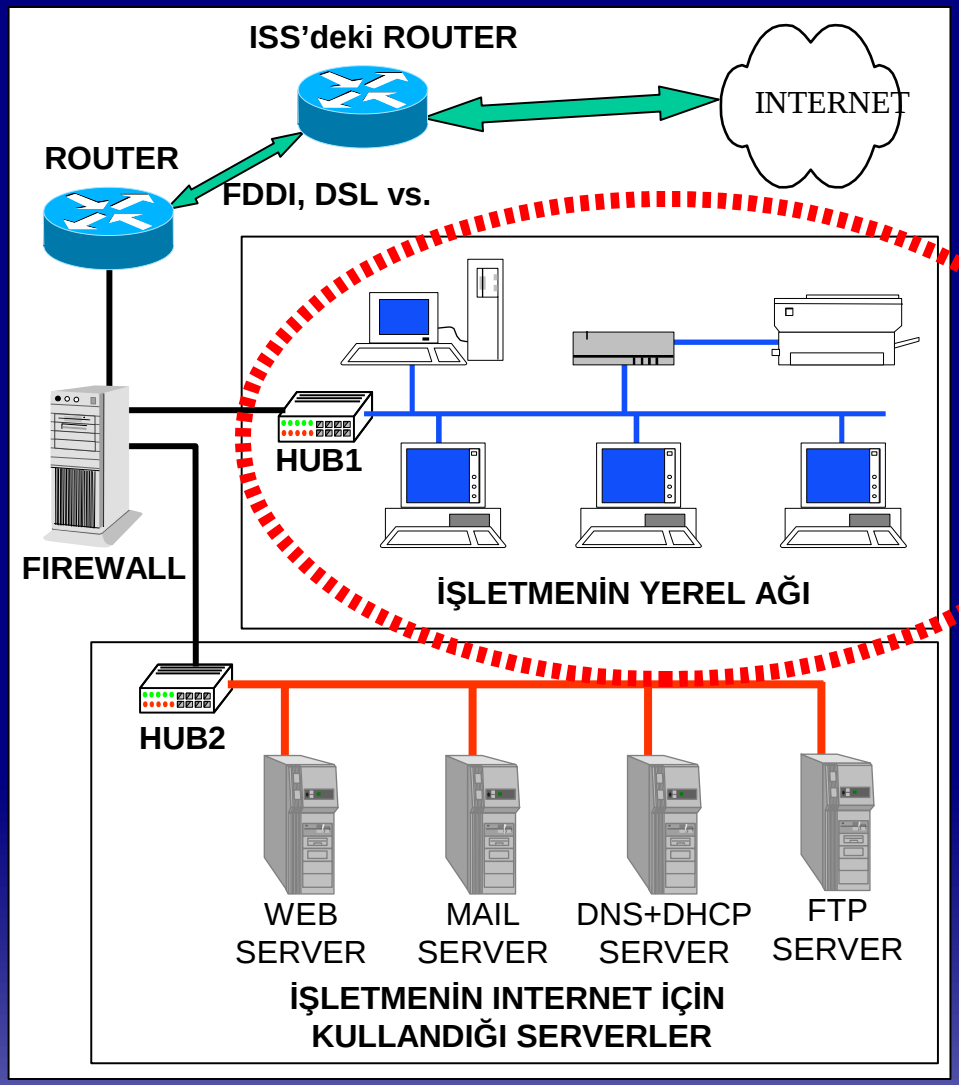
* **Firewall'de tek bir servise gelen paketleri kabul et.**




```
# iptables -A PREROUTING -d 1.2.3.10 \
    -p tcp --dport ! 80 -j DROP
```

Örnekler..

* **Yerel Ağdaki kullanıcıları internete çıkar..**

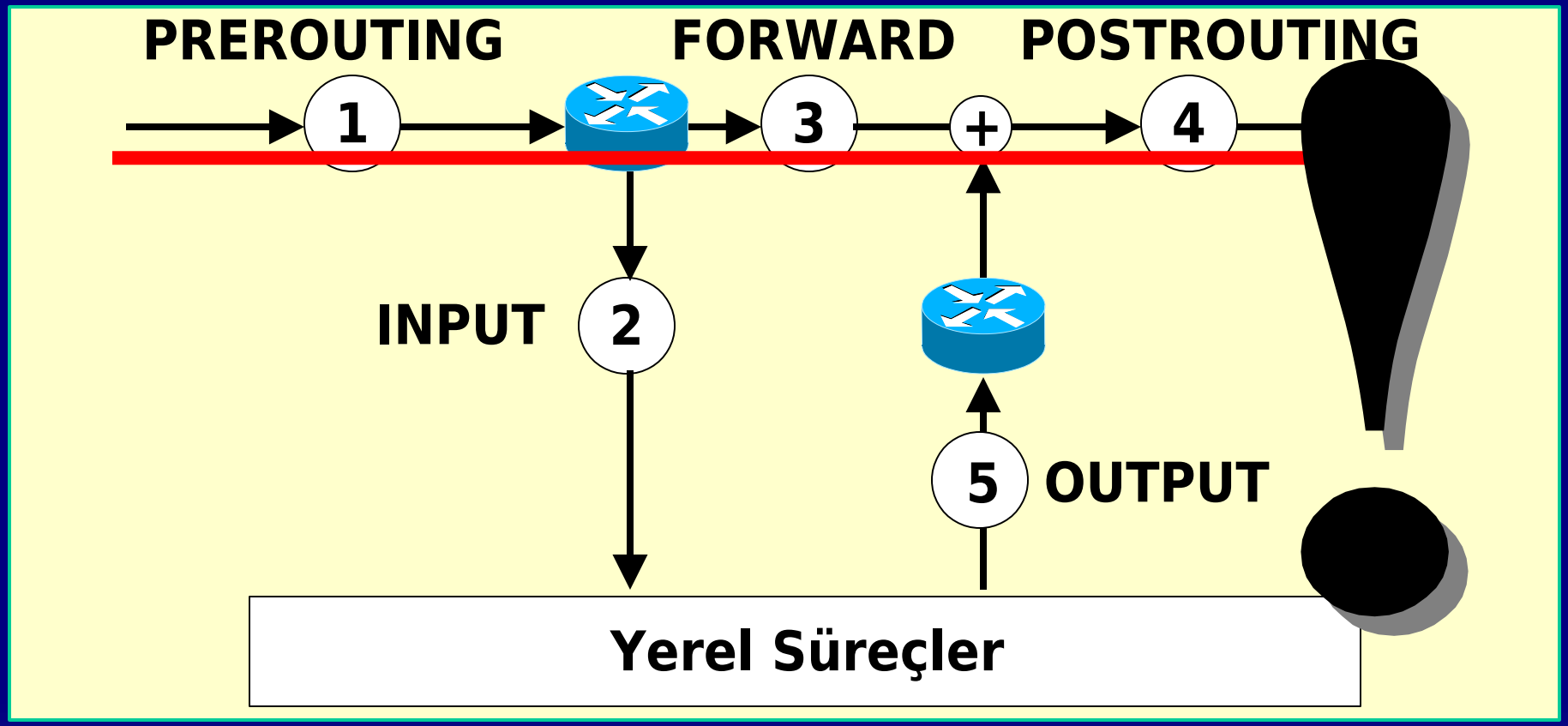


HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
LOCAL: 10.1.0.0/16

Örnekler..

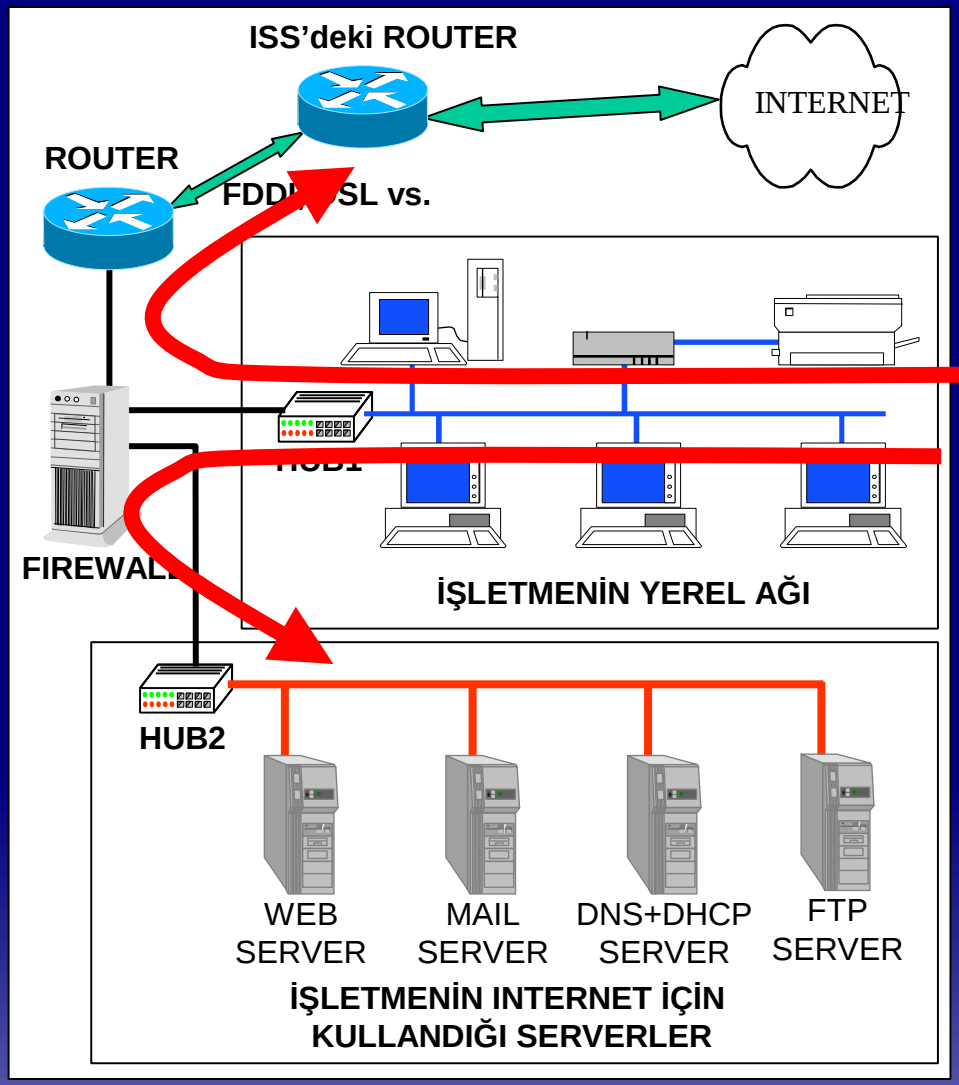
* **Yerel Ağdaki kullanıcıları internete çıkar..**




```
# iptables -t nat -A POSTROUTING -s 10.1.0.0/16    \
    -j MASQUERADE
```

Örnekler..

* **Server logları yerel ağ yerine Firewall'ı gösterir..**



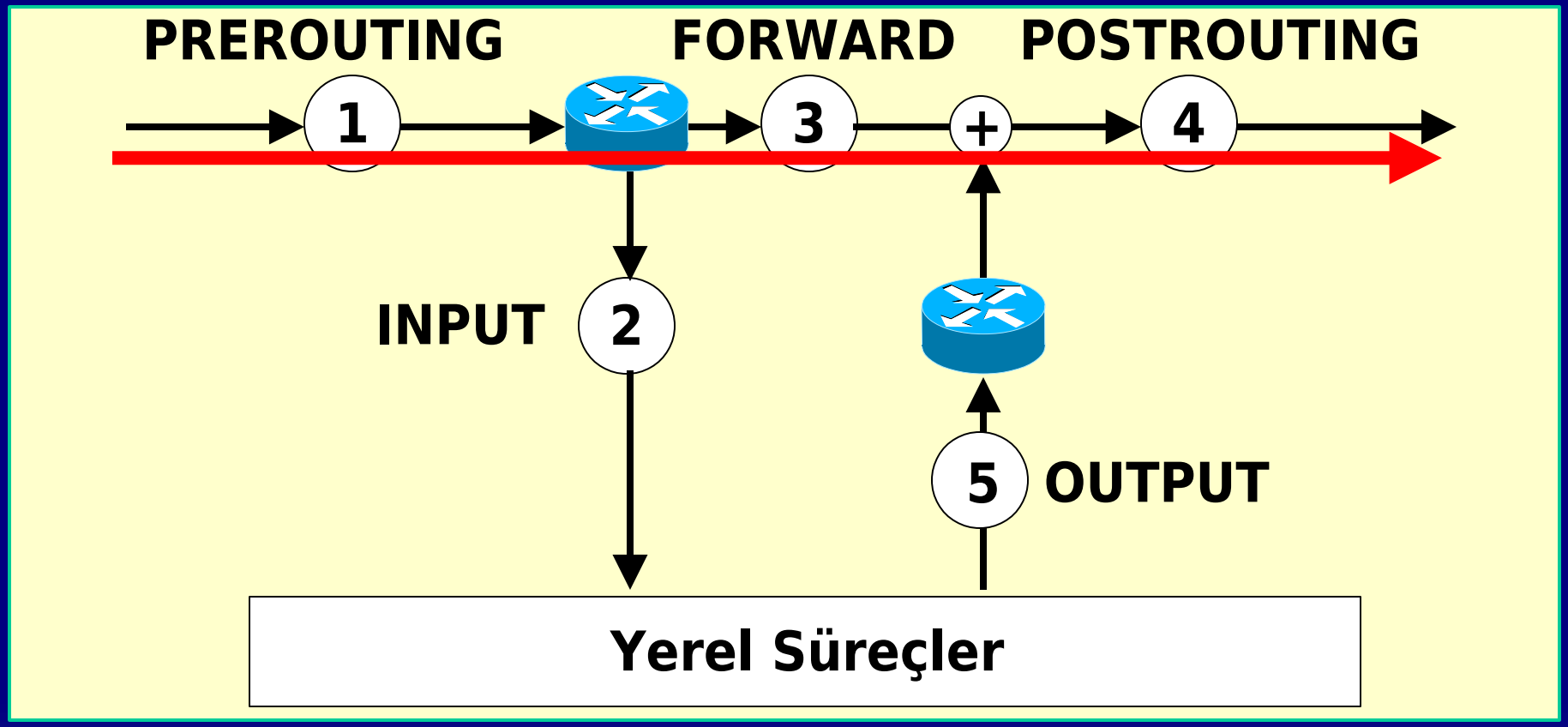
HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
DMZ: 10.1.0.0/16

eth0 <--> BAD(int.)
eth1 <--> GOOD(Local)
eth2 <--> DMZ(Srv.)

Örnekler..

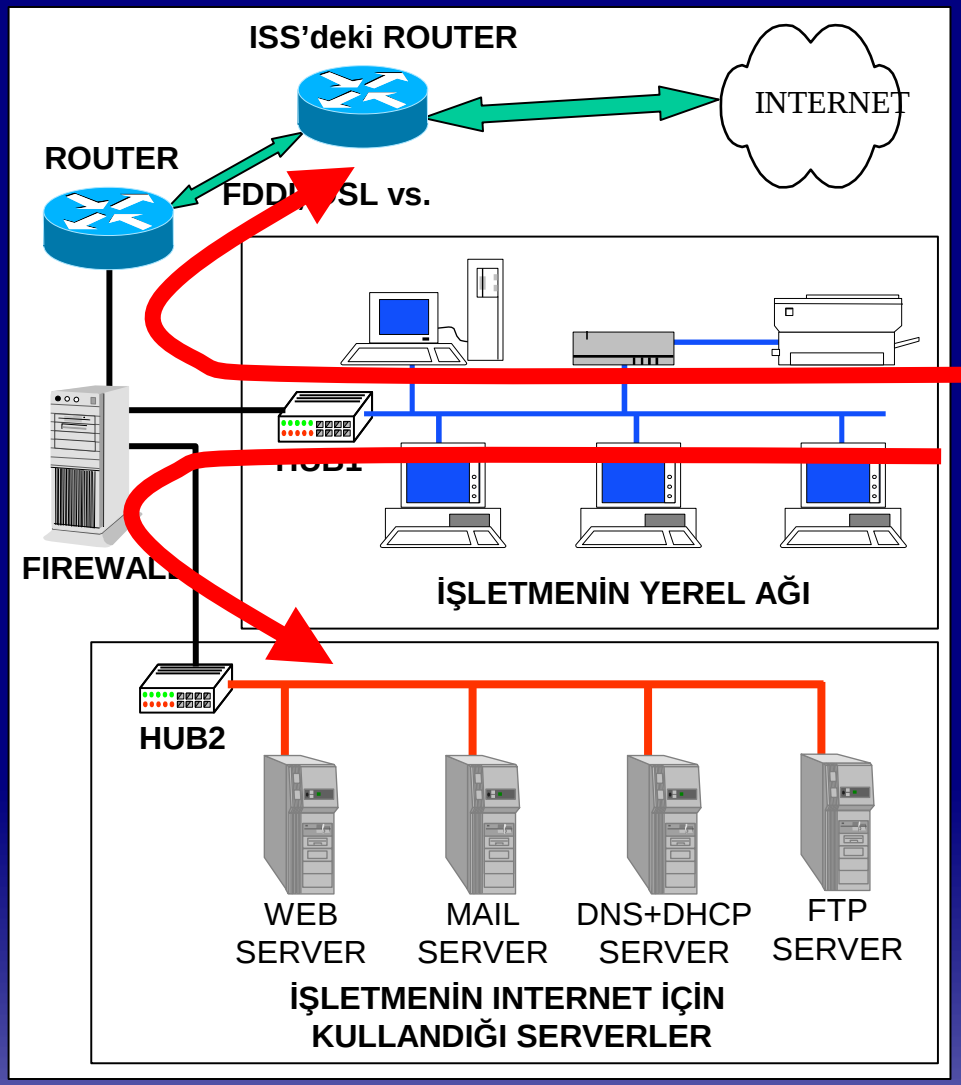
* **Yerel Ağdaki (GOOD) kullanıcıları internete çıkar..**




```
# iptables -t nat -A POSTROUTING -s 10.1.0.0/16    \
    -o eth0 -j MASQUERADE
```

Örnekler..

* **Yerel Ağdaki kullanıcıları internete çıkar..**



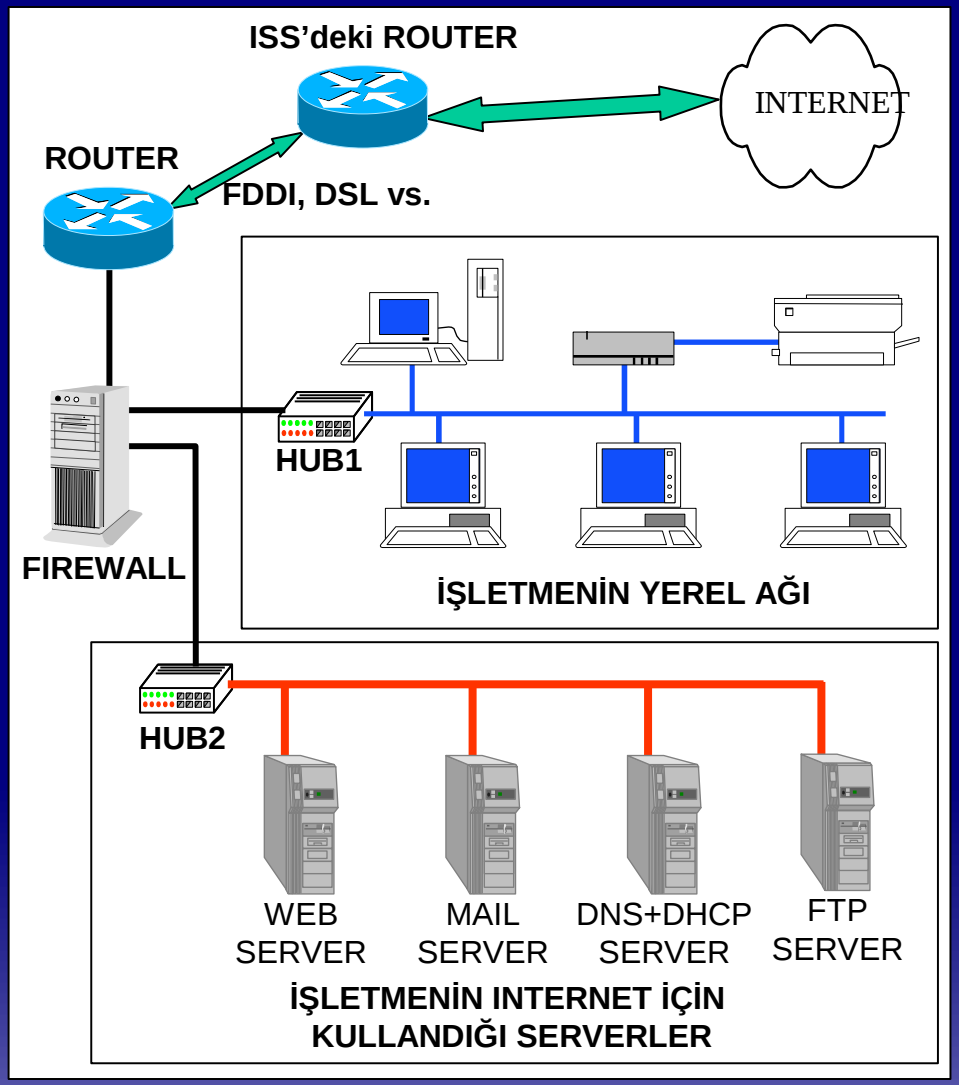
HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
DMZ: 10.1.0.0/16

eth0 <--> BAD(int.)
eth1 <--> GOOD(Local)
eth2 <--> DMZ(Srv.)

Örnekler..

* **BAD ağından erişilebilecek servisleri ayarla..**



HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
DMZ: 10.1.0.0/16

eth0 <--> BAD
eth1 <--> GOOD
eth2 <--> DMZ

Örnekler..

* **BAD ağından erişilebilecek servisleri ayarla..**

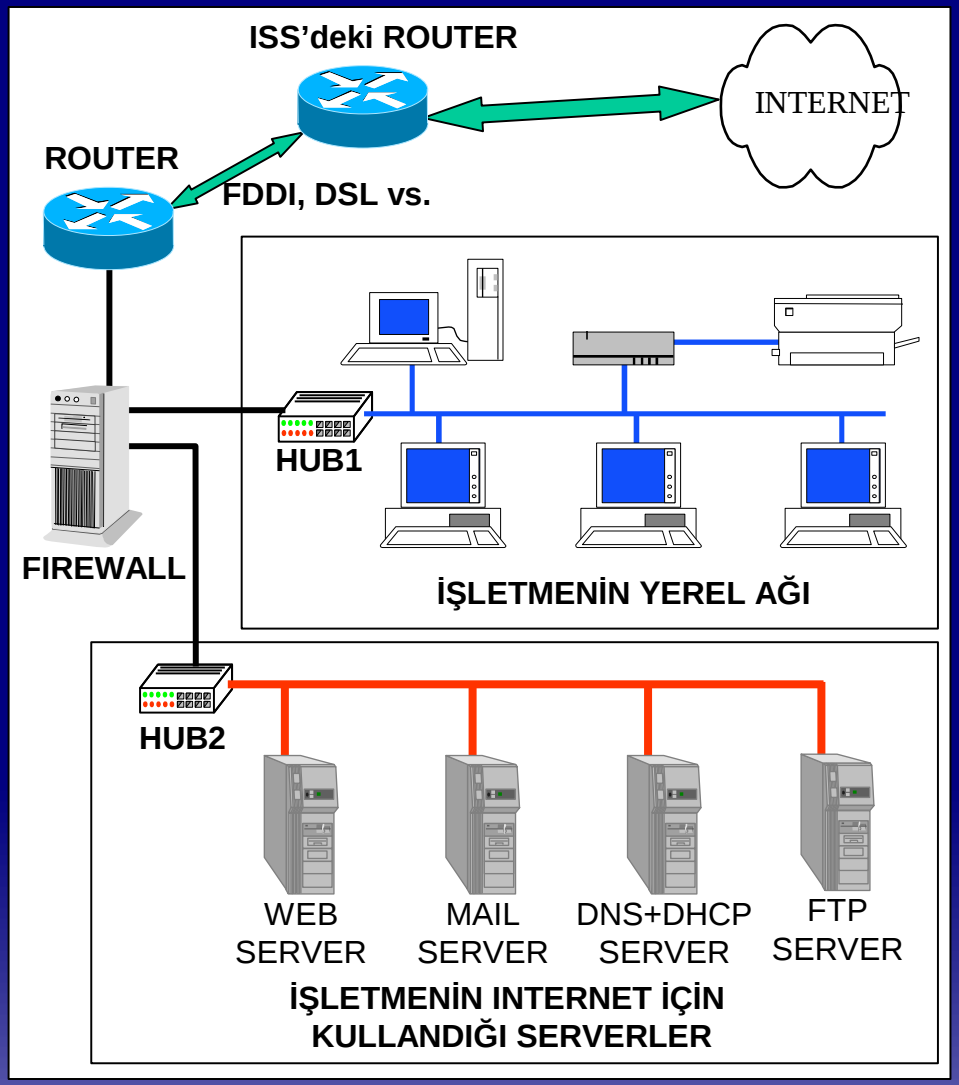
```
# iptables -P PREROUTING DROP

# iptables -A PREROUTING -d 1.2.3.10 -p tcp --dport 80 -j ACCEPT
# iptables -A PREROUTING -d 1.2.3.11 -p tcp --dport 25 -j ACCEPT
# iptables -A PREROUTING -d 1.2.3.11 -p tcp --dport 110 -j ACCEPT
# iptables -A PREROUTING -d 1.2.3.12 -p udp --dport 53  -j ACCEPT
# iptables -A PREROUTING -d 1.2.3.13 -p ftp --dport 21  -j ACCEPT

# iptables -A PREROUTING -s 10.1.0.0/16 -j ACCEPT
```

Örnekler..

* LOCAL AĞ için HTTP Transparent proxy



HTTP: 1.2.3.10
SMTP: 1.2.3.11
POP3: 1.2.3.11
DNS: 1.2.3.12
FTP: 1.2.3.13
SQUID: 1.2.3.14

SQL: 10.1.1.1
SMB: 10.1.1.2
DMZ: 10.1.0.0/16

eth0 <--> BAD
eth1 <--> GOOD
eth2 <--> DMZ

Örnekler..

* **LOCAL AĞ için HTTP Transparent proxy**

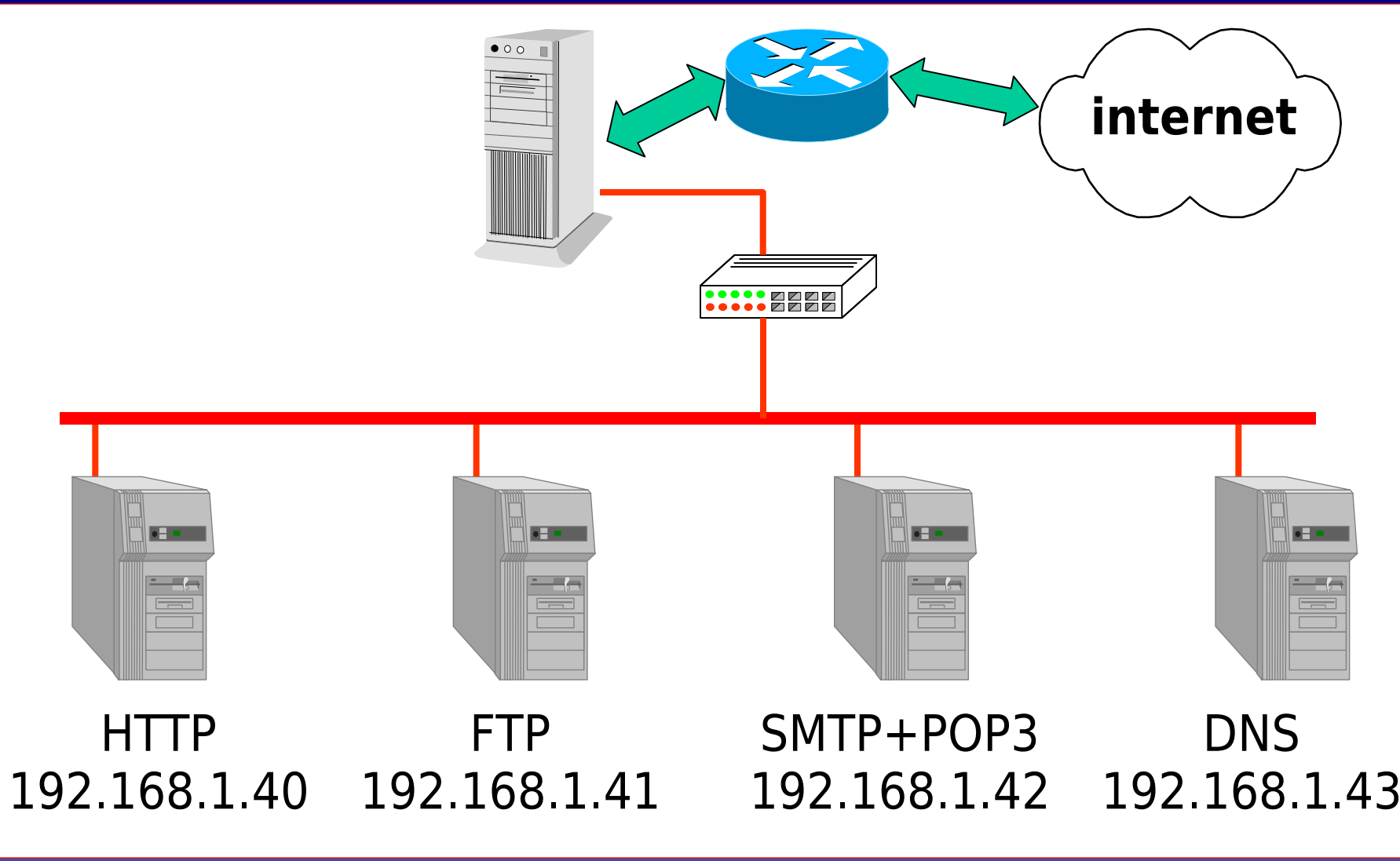
```
# iptables -t nat -A PREROUTING  \
   -s 10.1.0.0/16 -p tcp --dport 80 \
   -j DNAT --to 1.2.3.14:3128
```

Firewall üzerinde squid kuruluysa..

```
# iptables -t nat -A PREROUTING  \
   -s 10.1.0.0/16 -p tcp --dport 80  \
   -j REDIRECT --to 3128
```

Örnekler..

* **IP Bazında yük dengeleme / IP tasarrufu**



Örnekler..

* **IP Bazında yük dengeleme / IP tasarrufu**

```
# iptables -t nat -A PREROUTING  \
   -d 1.2.3.4 -p tcp --dport 80 \
   -j DNAT --to 192.168.1.40
```

```
# iptables -t nat -A PREROUTING  \
   -d 1.2.3.4 -p tcp --dport  21 \
   -j DNAT --to 192.168.1.41
```

```
# iptables -t nat -A PREROUTING  \
   -d 1.2.3.4 -p tcp -m multiport --dport  25,110 \
   -j DNAT --to 192.168.1.42
```

```
# iptables -t nat -A PREROUTING  \
   -d 1.2.3.4 -p udp --dport  53  \
   -j DNAT --to 192.168.1.43
```

Örnekler..

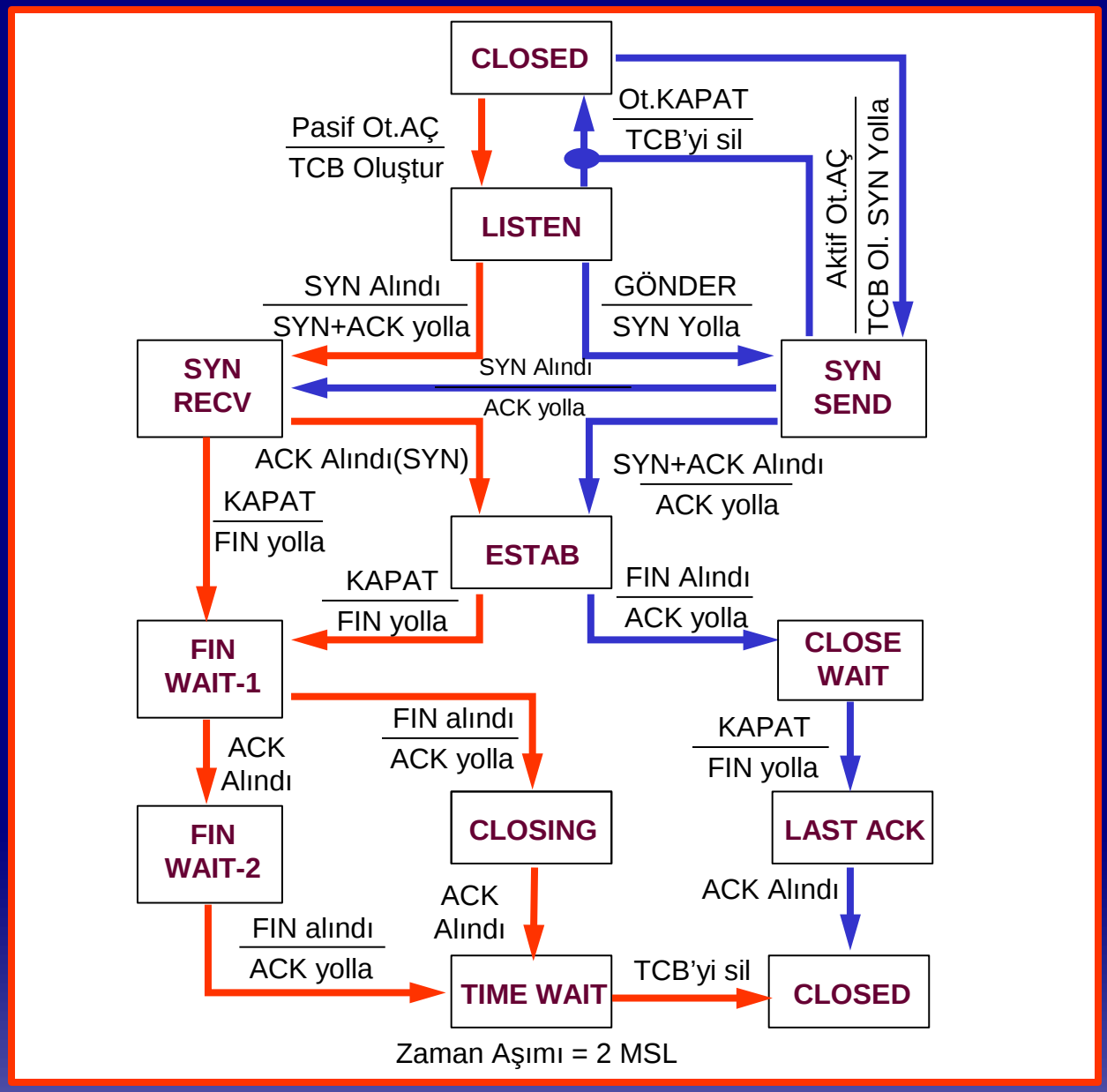
* **Yük dengeleme / Adi Kümeleme**


```
# iptables -t nat -A PREROUTING  \
   -s 0.0.0.1/0.0.0.1 -p tcp --dport 80 \
   -j DNAT --to-destination 192.168.1.40
```

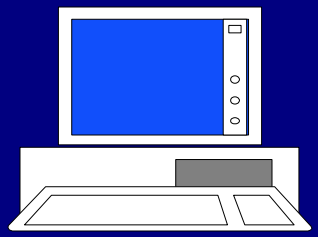
TCP Flags..

URG: Urgent Pointer field significant
ACK: Acknowledgment field significant
PSH: Push Function
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: No more data from sender

TCP Flags.. TCP States..

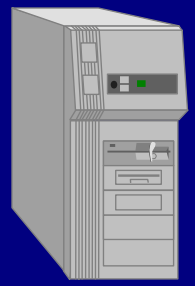


TCP Flags..



CLIENT

SERVER



CLOSED

LISTEN

SYN-SENT <CTL=SYN> --> ...

SYN-RECEIVED <CTL=SYN>

<CTL=SYN> --> SYN-RECE

SYN-RECEIVED <CTL=SYN,ACK>

ESTABLISHED <CTL=SYN,ACK>

... <CTL=ACK> ESTABLISHED

Örnekler..

* **DMZ Ağından Dışarıya Bağlantıları Engelleme**

```
# iptables -A FORWARD  \
   -s 1.2.3.0/24 -p tcp --syn \
   -j DROP
```

Peki Bizim serverin geri yollayacağı SYN DROP edilmez mi ?

CONNTRACK, Bağlantıyı takip ederek bu sorunu giderir..

Limit - Kullanışlı bir modül..

--limit ***n***

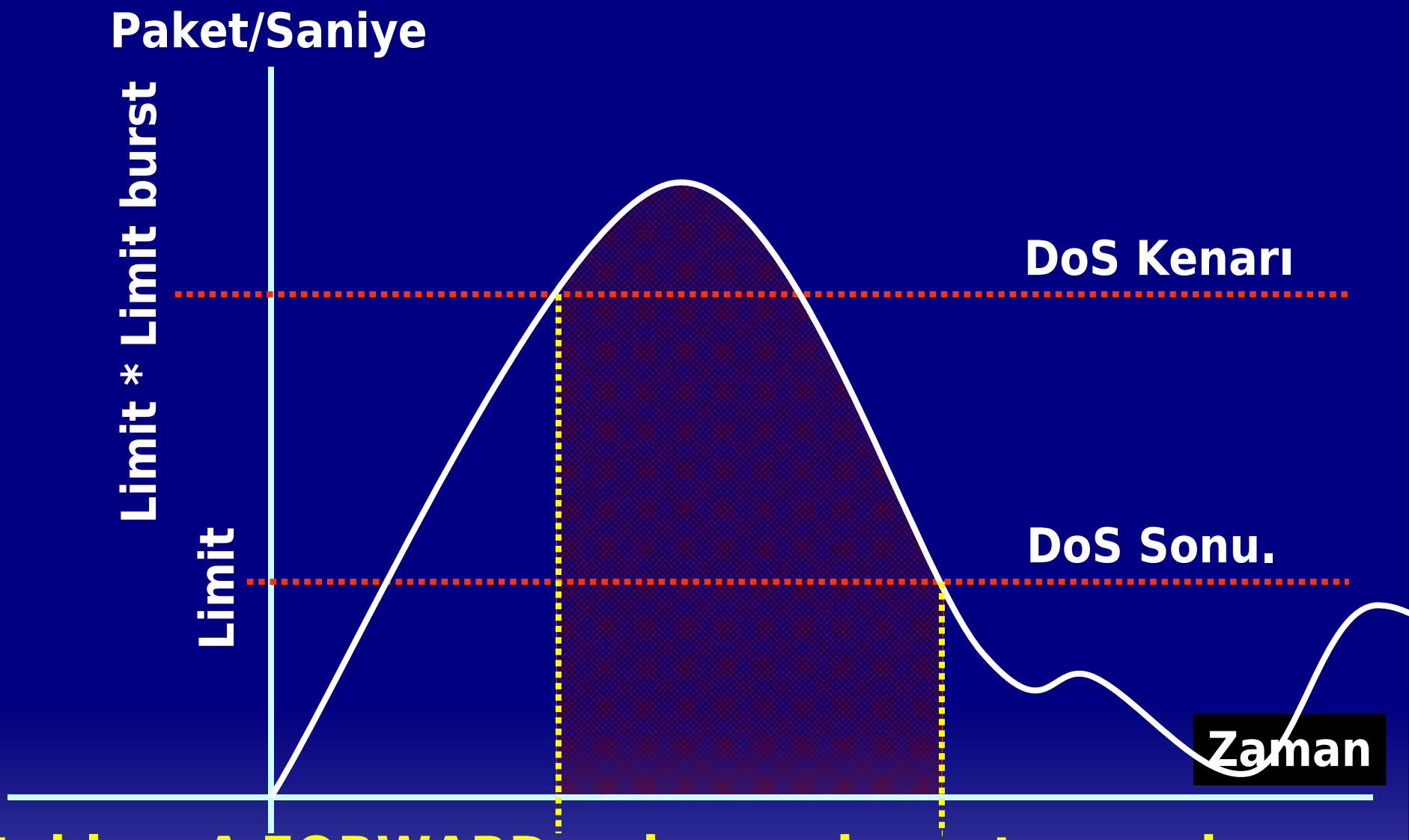
***n*, saniyedeki paket sayısı.**
n/second - Saniyede Paket..
n/minute - Dakikada Paket..
n/hour - Saatlik Paket..
n/day - Günlük Paket..

--limit-burst ***n***

***n*, ardı ardına maksimum paket sayısı.**
Varsayılanı 5 paket/saniye

```
# iptables -m limit --limit n/süre
# iptables -m limit --limit-burst n
```

Tipik bir DoS Saldırısı - Ping-of-Death..



ptables -A FORWARD -p icmp --icmp-type echo-requ
-m limit --limit 1/s -j ACCEPT

Script Kiddie Oyuncakları için...

* **Syn-flood..**

```
# iptables -A FORWARD -p tcp --syn
    -m limit --limit 1/s -j ACCEPT
```

* **Port Scanners..**

```
# iptables -A FORWARD -p tcp
    --tcp-flags SYN,ACK,FIN,RST RST
    -m limit --limit 1/s -j ACCEPT
```

LOG - Paketleri zapta almak..

-j LOG --log-prefix ‘tanım’ --log-level ‘seviye’

7	Debug
6	info
5	notice
4	warning
3	err
2	critical
1	alert
0	emergency

--log-ip-options

--log-tcp-sequence

--log-tcp-options

İlgili Dosyalar..

/var/log/messages

/etc/syslogd.conf

LOG - Log Format..

Apr 16 00:30:45 proxy kernel: NF: D(I,Priv)
IN=eth1 OUT=
MAC=00:80:8c:1e:12:60:00:10:76:00:2f:c2:08:00

Syslogd mesajı
--log-prefix
Hangi arabirimden geldiği/gittiği
MAC Adresi=
Gideceği Arabimin Mac Adresi
Geldiği Arabirimin MAC adresi
Taşıyıcı Tipi (08:00 - Ethernet Frame)

LOG - Log Format..

SRC=211.251.142.65 DST=203.164.4.223 LEN=60
TOS=0x00 PREC=0x00 TTL=44 ID=31526
CE DF MF FRAG=179
OPT (072728CBA404DFCBA40253CBA4032
ECBA403A2CBA4033ECBA40
2C1180746EA18074C52892734A200)

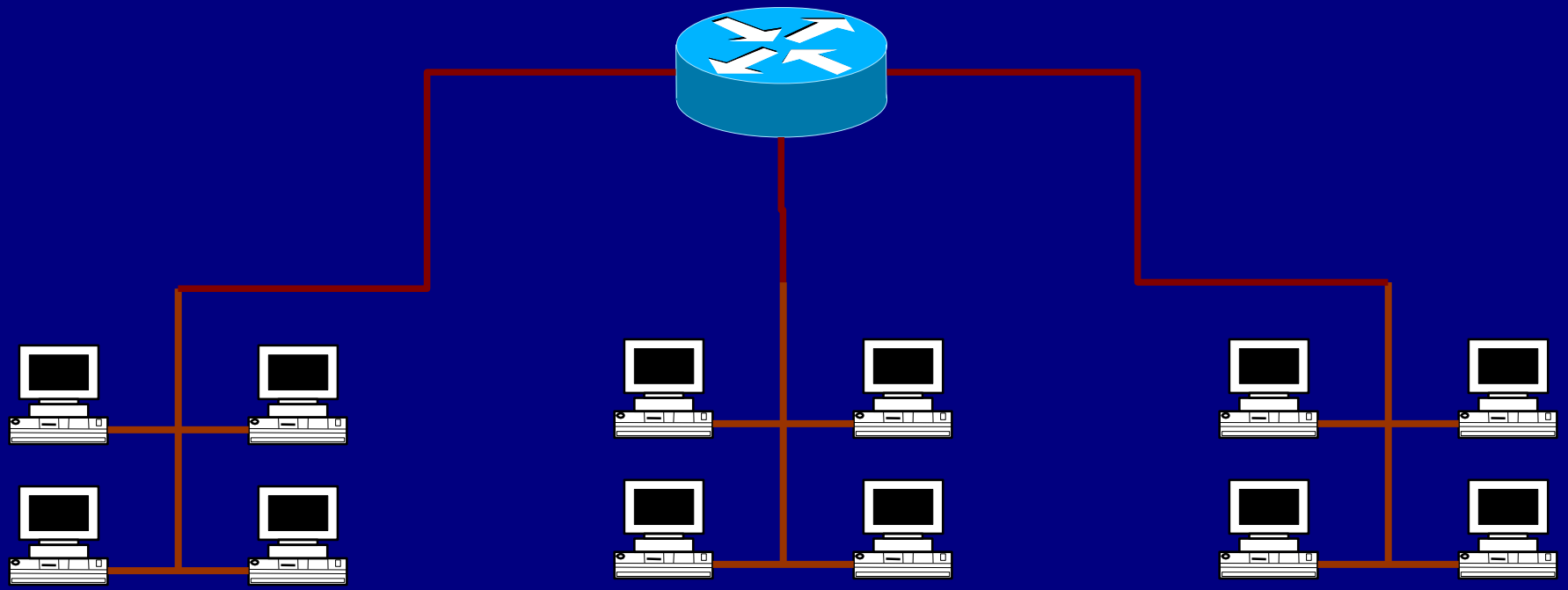
Paket Başlık bilgileri
TOS Precedense
Unique ID for IP Datagram. Fragmented paketler için..
CE=ECN CE, Congestion Experienced (RFC 2481)
DF=Don’t fragment..
MF=More Fragments Following
FRAG=Fragment Offset / 8. 179x8=1432. Byte...
OPT TCP Options, (--log-ip-options)

LOG - Log Format..

PROTO=TCP SPT=4515 DPT=111
SEQ=1168094040 ACK=0 WINDOW=32120
RES=0x03 URG ACK PSH RST SYN FIN
URGP=0
OPT (020405B40402080A05E3
F3C4000000001030300)

Protokol, Kaynak/Hedef Port
TCP Sequence Numarası (--log-tcp-sequence)
Acknowledge Numarası (--log-tcp-sequence)
TCP Window Size..
RES=Reserved Bits ve Flags..
URGP=Urgent Pointer
TCP options (--log-tcp-options)

iproute2 + IPTABLES = Advanced Router

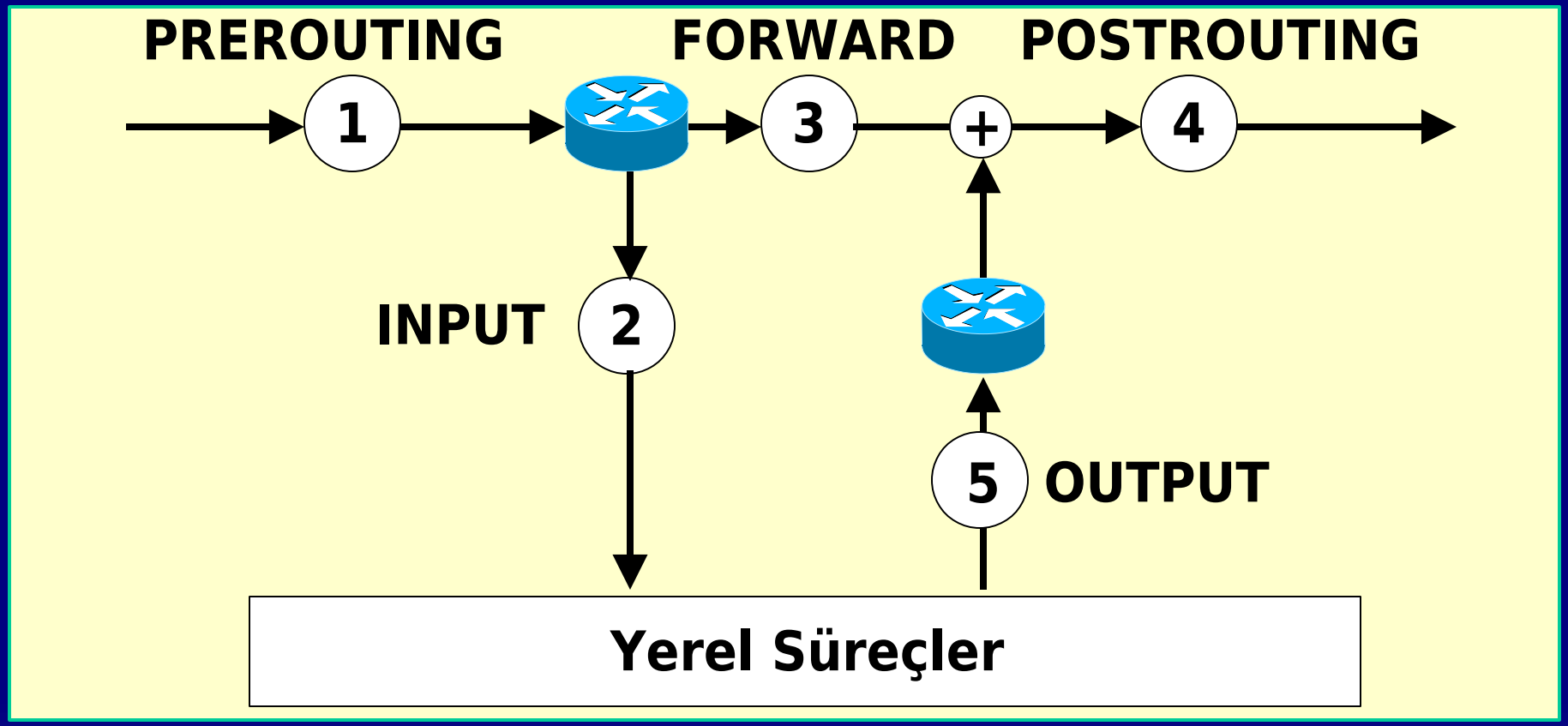


Routing, gelen paket hangi ağa gidecekse o ağa bağlı olan arabirime paketi iletmekten ibarettir.

Advanced Router, bantgenişliği paylaşımı, protokol/servis bazında arabirim seçimi gibi güçlü özellikler ekler..

iproute2 + IPTABLES = Advanced Router

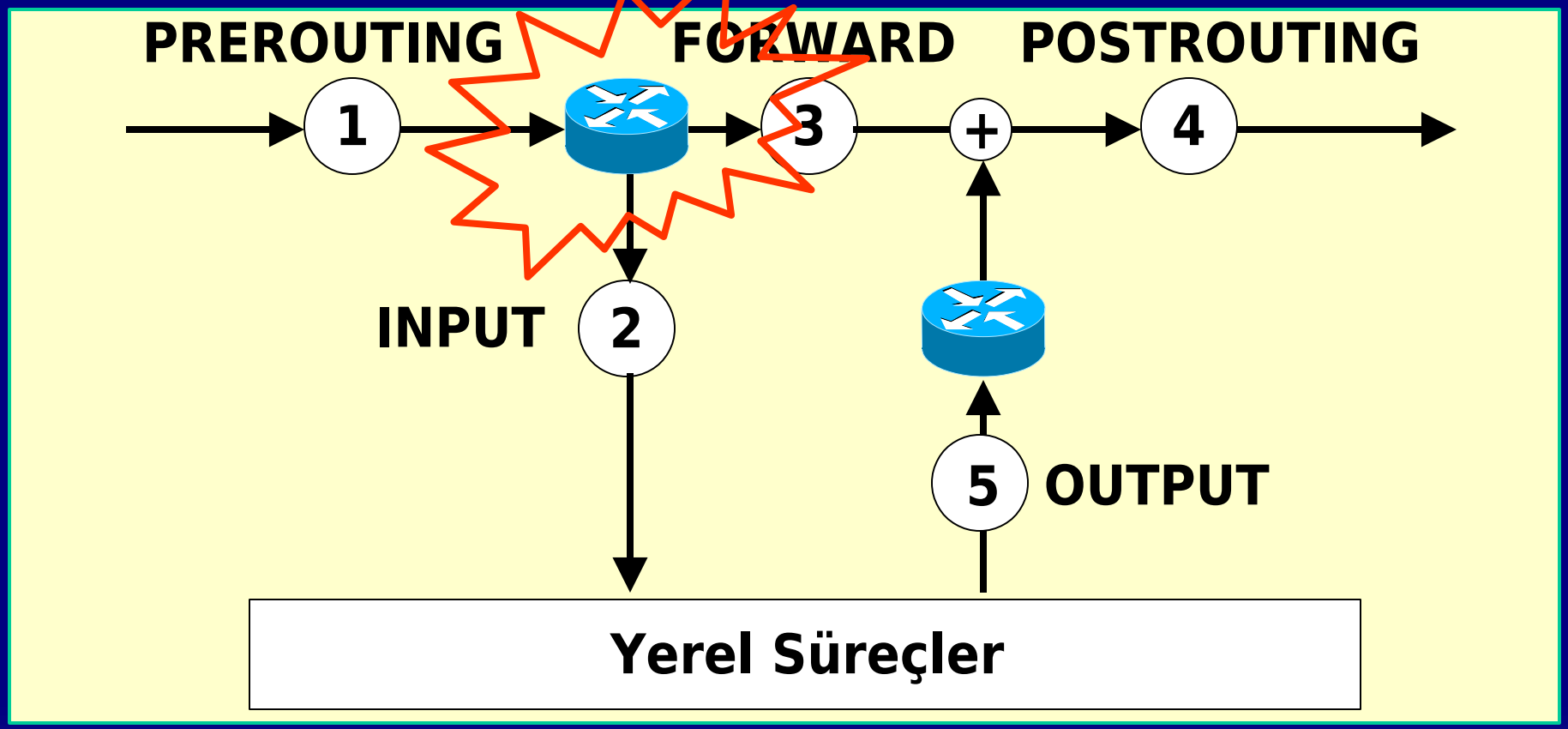
* **IPTABLES paketleri işaretler..**




```
# iptables -A PREROUTING -t mangle \
                -p tcp --dport 80 -j MARK --set-mark 1
```

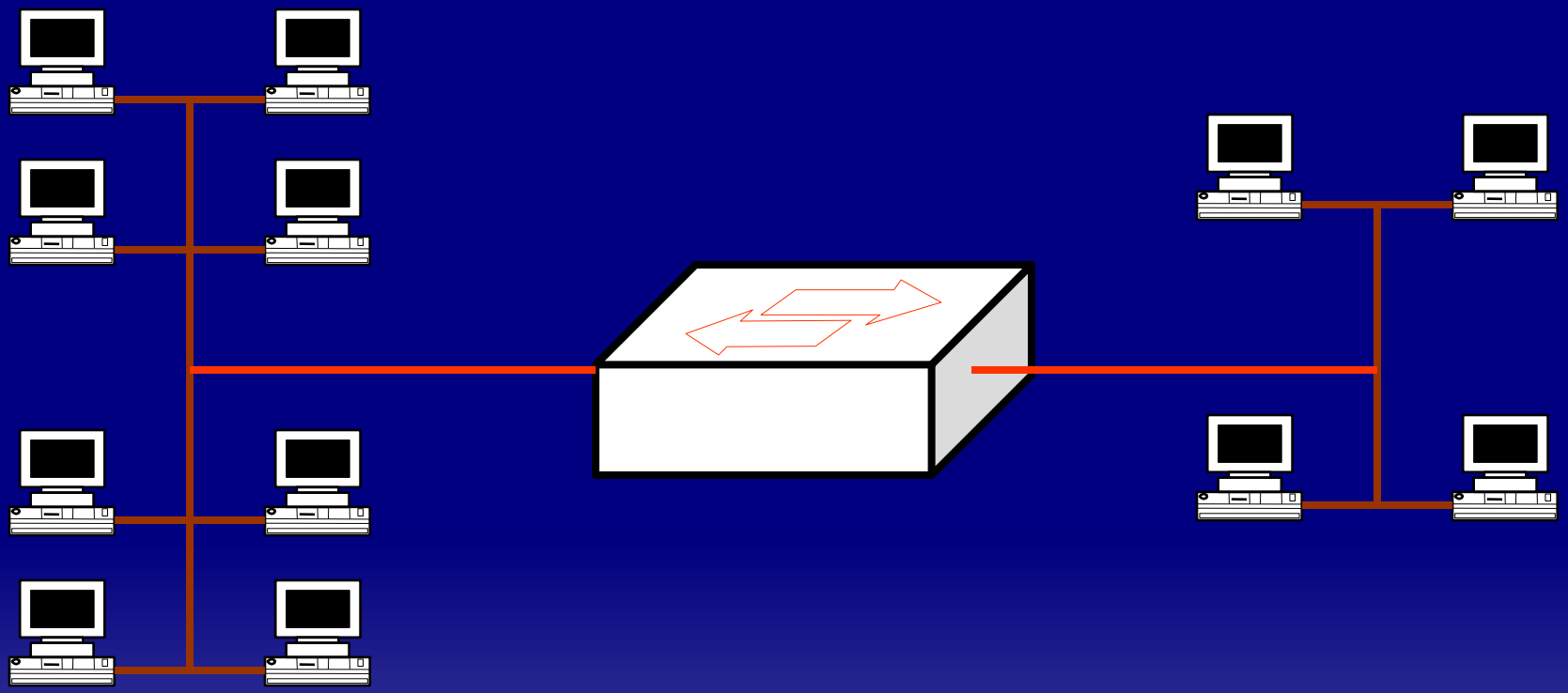
iproute2 + IPTABLES = Advanced Router

* **Kernel Advanced Router Paketi işler..**




```
# ip rule add fwmark 1 table webdata
# ip route add default via 195.255.51.3 \
    dev ppp1 table webdata
```

Hayalet Firewall - Bridge + Firewall



Hayalet Firewall - Bridge + Firewall

2.2.4 Kernel için

http://bridge.sourceforge.net/devel/bridge-nf/bridge-nf-0.0.7-against-2.4.18.diff

Hayalet Firewall - Bridge + Firewall

```
ifconfig eth0 0.0.0.0
ifconfig eth1 0.0.0.0

insmod bridge
brctl addbr br0
brctl addif br0 eth0
brctl addif br0 eth1

ifconfig br0 1.2.3.4 netmask 255.255.255.240 up

echo "0" > /proc/sys/net/ipv4/ip_forward

route add -net 0.0.0.0 gw 1.2.3.4 dev br0
```

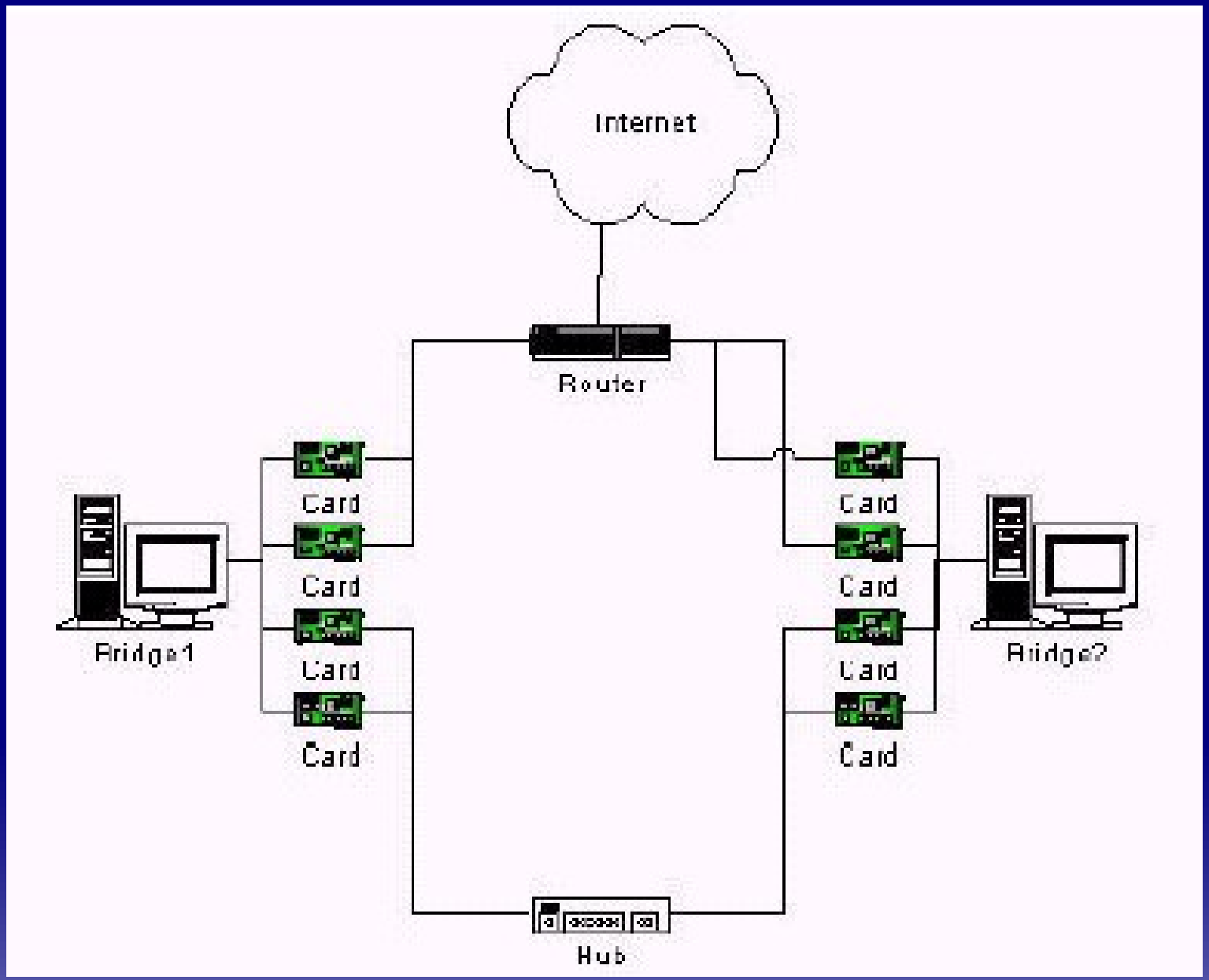
Hayalet Firewall - Bridge + Firewall

```
iptables -I FORWARD -p tcp -s 0.0.0.0/0 \
                -d 1.2.3.5 --dport 1433 -j DROP
```

-i ve -o kullanmayın..

rtl8139 sorunlar çıkarabilir..

Hayalet Firewall - Bridge + Firewall



Faydalı kaynaklar..

netfilter.samba.org

netfilter.samba.org/ipchains

Advanced routing - HOWTO

Bridge+Firewall+ADSL HOWTO

Bridge+Firewall+ADSL HOWTO

http://www.pom.gr/ilisepe1/firewall_help.html

www.linux.org.tr