Iptables

Linuxadministration I 1DV417

netfilter/iptables

iptables forts.

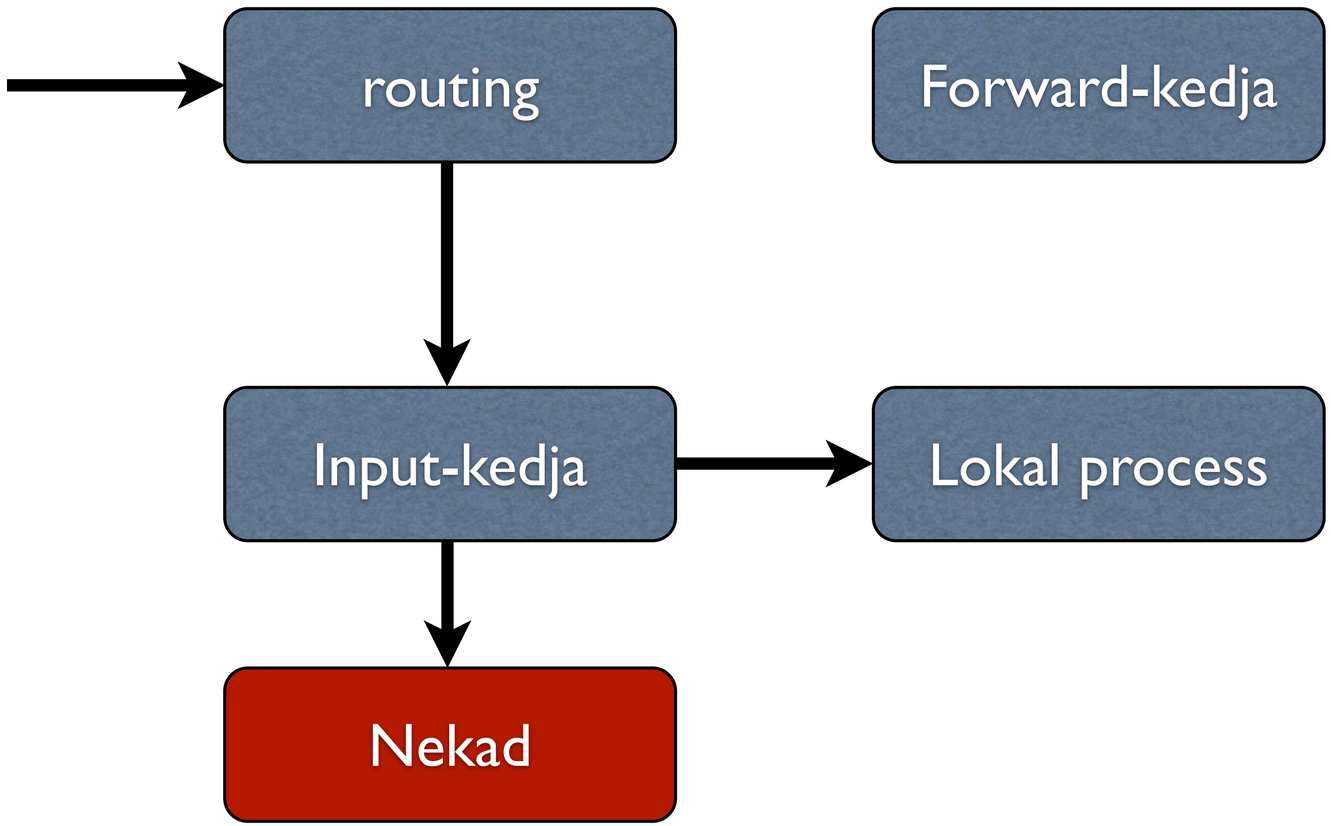
```
iptables –t nat –A PREROUTING –p tcp –i eth0 –o eth1 –j DNAT --to-destination 10.0.0.2
```

Filtermodulen

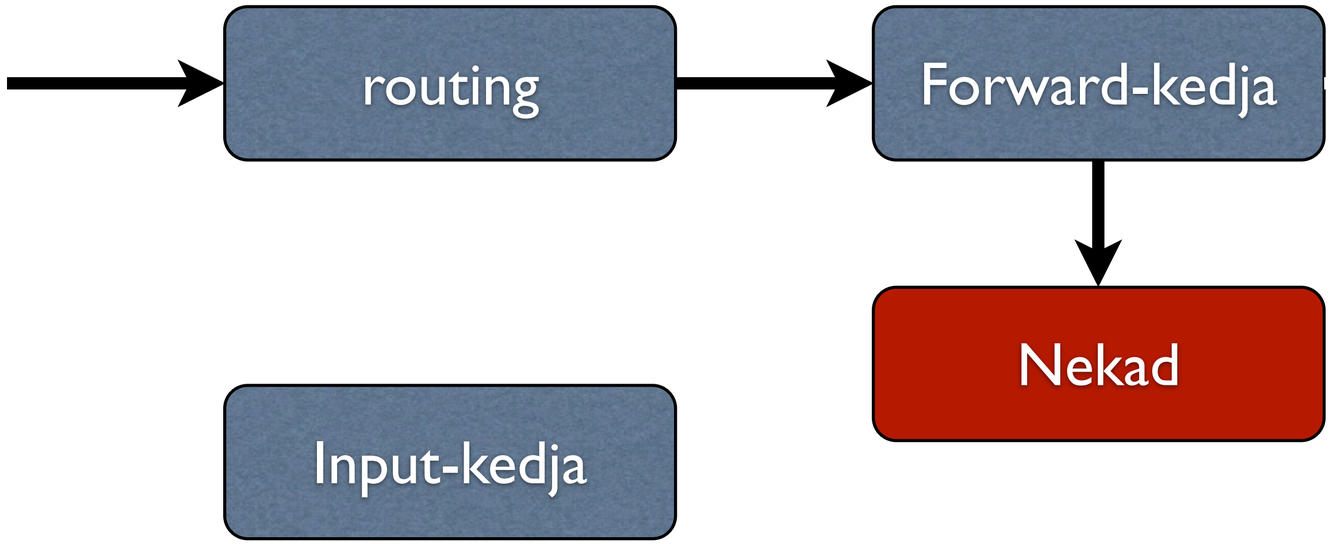
Filtermodulen forts.

Input Output Forward

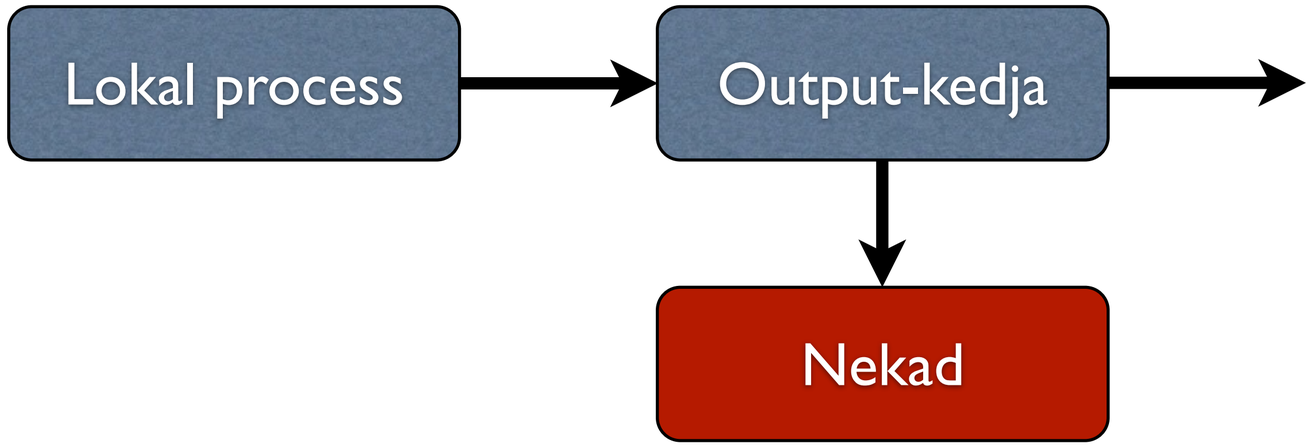
Scenario 1- Input-kedjan



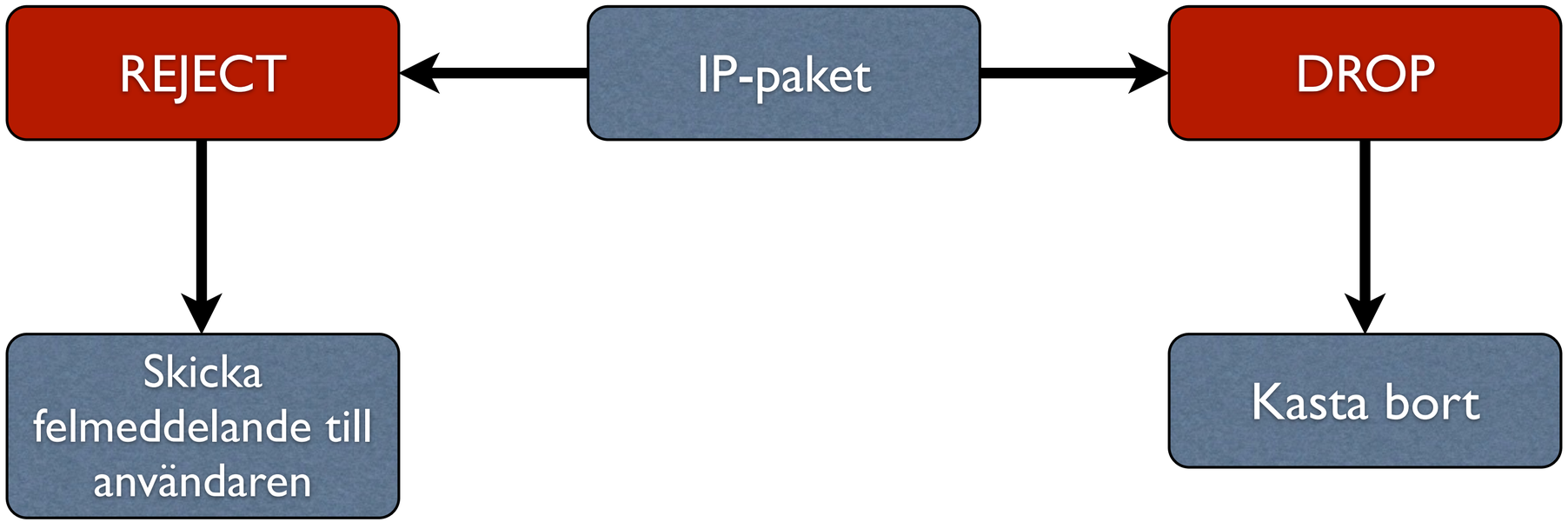
Scenario 2- Forward-kedjan



Scenario 3 - Output-kedjan



DROP och REJECT



Filter-modulens åtgärder

ACCEPT
LOG
RETURN
DROP
REJECT
Skicka vidare till annan kedja

```
iptables –A INPUT –p icmp -j ACCEPT
```

REJECT

```
iptables –A INPUT –p icmp -j REJECT --reject-with icmp-port-unreachable
```

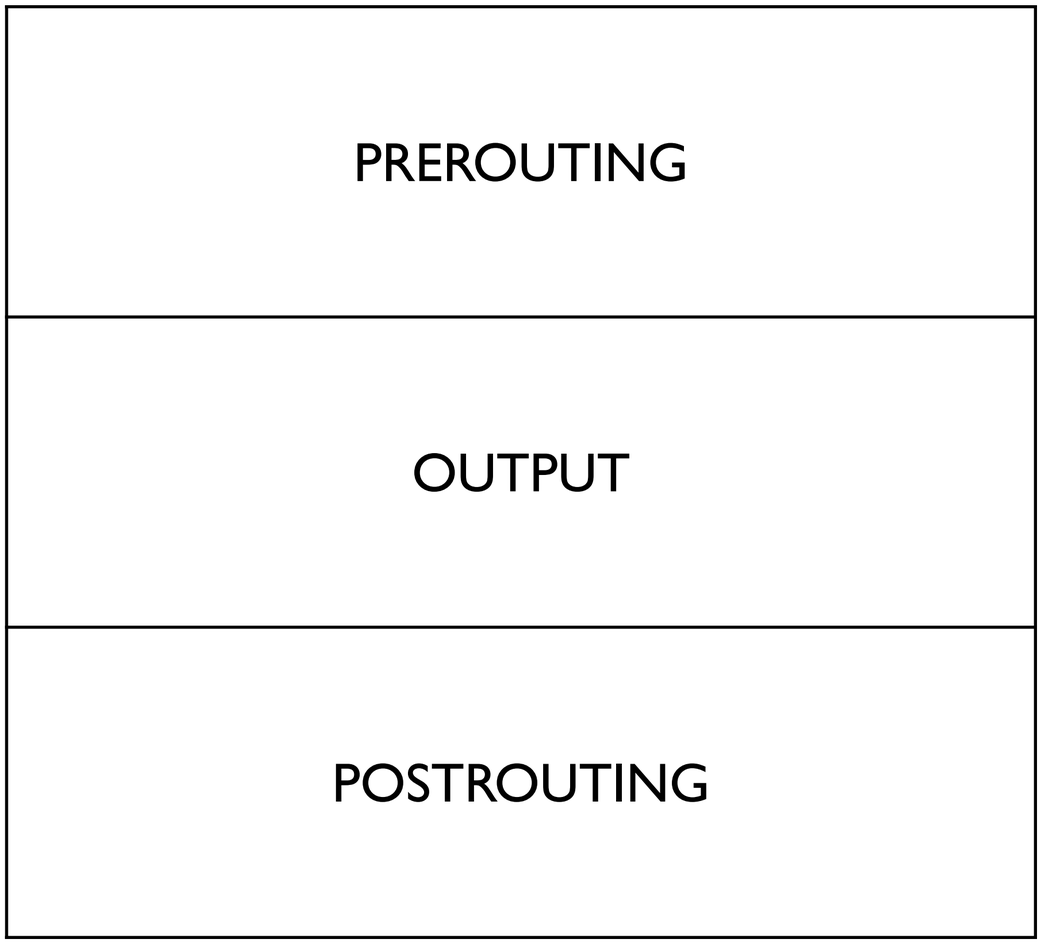
```
iptables –A INPUT –p tcp -j REJECT --reject-with tcp-reset
```

```
iptables –A INPUT –p udp -j REJECT --reject-with echo-reply
```

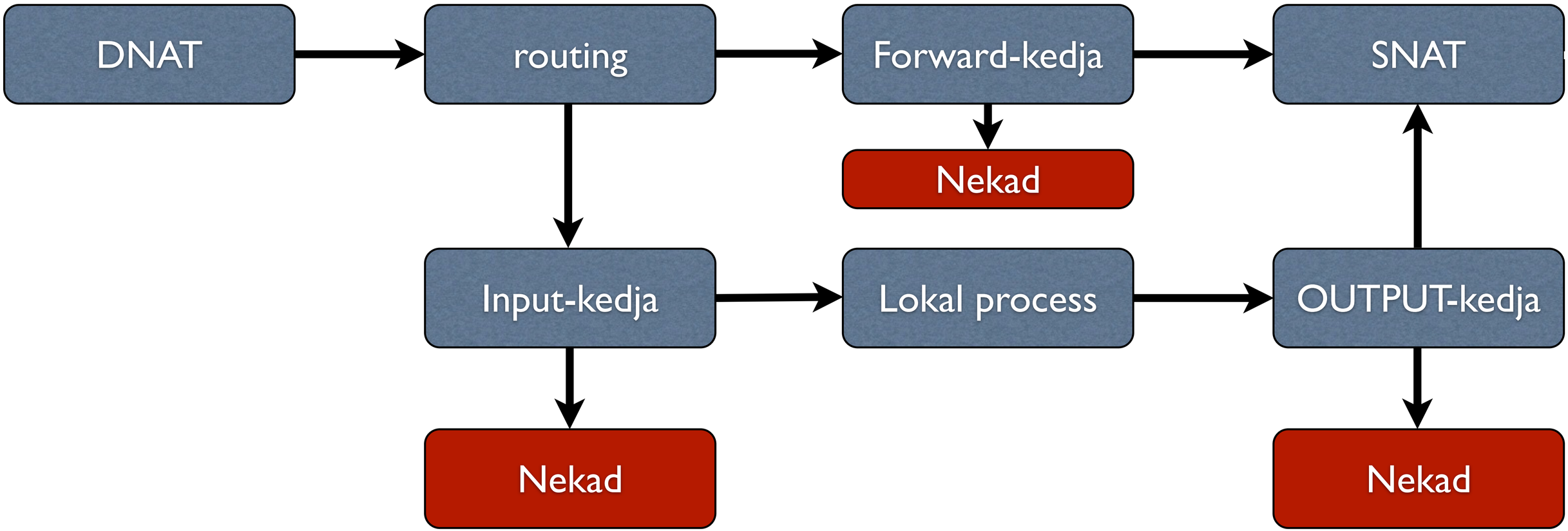
NAT-modulen

SNAT (Source NAT)
DNAT (Destination NAT)
MASQUERADE
REDIRECT

NATs inbyggda kedjor



Paketets väg genom NAT



Mangle

MARK

TTL

ToS

Kommandon

iptables
iptables-save
iptables-restore

```
iptables -N ftpchain
```

```
iptables -A ftpchain -p icmp -j ACCEPT
```

```
iptables -F ftpchain
```

```
iptables -X ftpchain
```

```
iptables -P INPUT DROP
```

```
iptables -L
iptables -L INPUT
```

Regler

Generell syntax

```
iptables -A OUTPUT –p tcp –j ACCEPT
```

-A alt. --append	`iptables -A INPUT –p icmp –j ACCEPT`
-I alt. --insert	`iptables -I INPUT 2 –p icmp –j ACCEPT`
-D alt. --delete	`iptables -D INPUT 2`
-R alt. --replace	`iptables -R INPUT 2 –p icmp –j ACCEPT`

Grundläggande villkor

```
iptables –A INPUT -i eth0 –p tcp –j DROP
iptables –A OUTPUT -o eth0 –p tcp –j DROP
iptables –A INPUT -p tcp –j DROP
iptables –A INPUT -s 10.0.0.0/8 –j DROP
iptables –A OUTPUT -d 10.0.0.0/8 –j DROP
```

Specificera en åtgärd för en regel

```
iptables –A INPUT –p tcp -j DROP
```

TCP-filter

--sport alt. --source-port	Avsändarens port
--dport alt. --destination-port	Mottagarens port
--tcp-flags	TCP-flaggor
--syn	Kontrollera att SYN-flaggan är satt
--tcp-option	Max-storleken på paket som mottagaren kan ta emot

UDP-filter

--sport alt. --source-port	Avsändarens port
--dport alt. --destination-port	Mottagarens port

ICMP-filter

--icmp-type

- echo-reply (0)
- destination-unreachable (3)
- source-quench (4)
- redirect (5)
- echo-request (8)
- time-exceeded (10)
- parameter-problem (11)

LOG-filter

```
iptables –A INPUT –i eth0 –j LOG --log-prefix “eth0-log: ”
```

match

-m alt. --match

```
iptables –A FORWARD –p tcp –i eth0 –o eth1 –m state --state NEW,ESTABLISHED,RELATED –j ACCEPT
```

SNAT och MASQUERADE

```
iptables –t nat –A POSTROUTING -o eth0 –j SNAT --to-source 194.46.13.5
```

```
iptables –t nat –A POSTROUTING -o eth0 –j MASQUERADE
```

```
iptables –t nat –A POSTROUTING -o eth0 –j MASQUERADE --to-ports 1-1024
```

DNAT

```
iptables –t nat –A PREROUTING –i eth0 --dport 80 -j DNAT --to-destination 10.0.0.2:80
```

```
iptables –t nat –A PREROUTING –i eth0 --dport 80 -j DNAT --to-destination 10.0.0.2-10.0.0.10:80
```

```
iptables –t nat –A PREROUTING –i eth0 -j DNAT --to-destination 10.0.0.2:1-1024
```

Scenario 1 - Enkel brandvägg

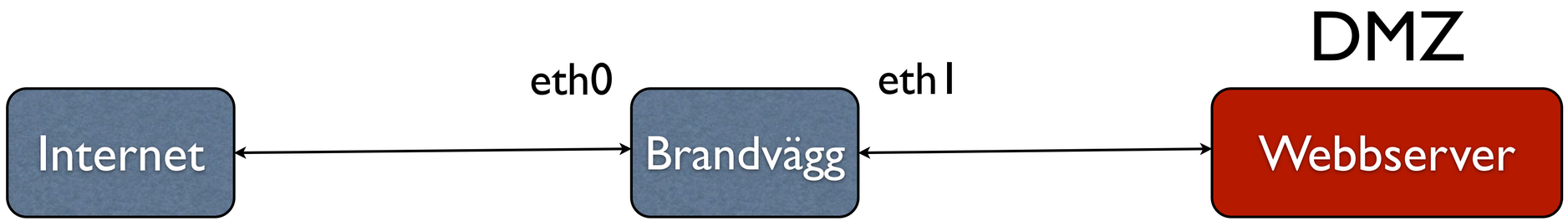
Brandväggen ska
- Släppa igenom TCP-kommunikation från det interna nätverket
- Släppa igenom TCP-kommunikation från internet om statusen på paketen är ESTABLISHED eller RELATED
- Blockera övrig trafik in och ut genom brandväggen

```
iptables –A FORWARD –i eth1 –o eth0 –p tcp –j ACCEPT
```

```
iptables –A FORWARD –p tcp –i eth0 –o eth1 –m state --state ESTABLISHED,RELATED –j ACCEPT
```

```
iptables –P FORWARD DROP
```

Scenario 2 - DNAT



Brandväggen ska

- Genomföra en DNAT för paket som ska till webbservern i DMZ (10.0.0.2)
- Skicka paket vidare från det publika nätverkskortet (eth0) till DMZ-nätverkskortet (eth1) om paketens status är NEW, ESTABLISHED eller RELATED
- Skicka paket vidare från DMZ-nätverkskortet (eth1) till det publika nätverkskortet (eth0) om statusen på paketet är ESTABLISHED eller RELATED

```
iptables –t nat –A PREROUTING –p tcp -i eth0 –j DNAT --to-destination 10.0.0.2
```

```
iptables –A FORWARD –i eth0 –o eth1 –p tcp –d 10.0.0.2 --dport 80 -m state --state NEW –j ACCEPT
```

```
iptables –A FORWARD –i eth0 –o eth1 –m state --state ESTABLISHED,RELATED –j ACCEPT
```

```
iptables –A FORWARD –i eth1 –o eth0 –m state --state ESTABLISHED,RELATED –j ACCEPT
```

Kommandon

iptables –L

iptables –F

iptables –t nat –F

iptables-save

iptables-restore (iptables-restore < filnamn)