Контрол на трафика. IPtables

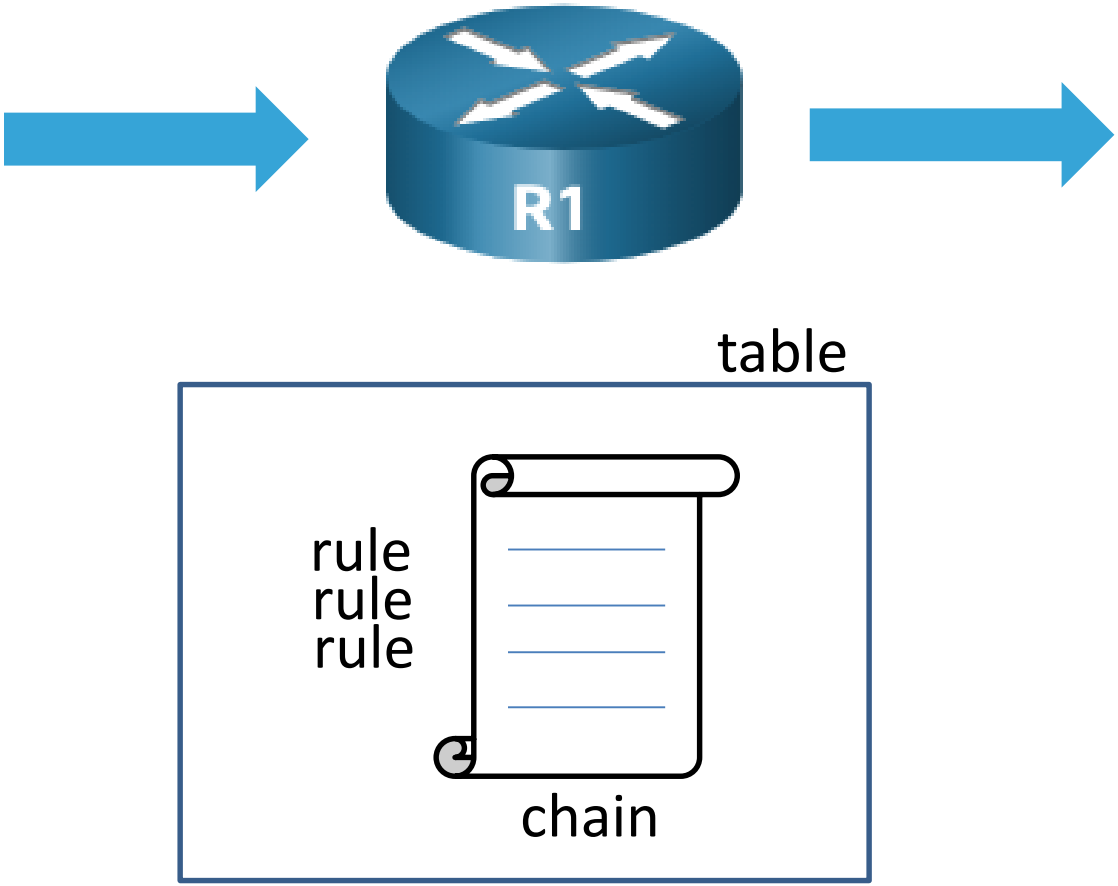
Филтриране на пакети под Linux

- Базирано е на модела Netfilter - общ програмен модел на филтриране на пакети, позволяващ улеснен и ефективен контрол на трафика.
- Софтуерната реализация е базирана на пакета iptables.
- Модулният принцип на изграждане на iptables дава възможност за постигане на гъвкавост при реализирането на различни стратегии за изграждане на firewall архитектури.

Таблици и правила

- Конфигурирането на Netfilter се базира на използването на таблици, всяка от които се състои от последователност от правила. Основен модул е *ip_tables*.
- Правилата дефинират критериите, които трябва да удовлетворят преминаващите през машината пакети и действията (целите - targets), които ще се предприемат при тяхното удовлетворяване.
- За всяка таблица са дефинирани последователности от правила (вериги - chains), по които преминават пакетите.
- Потребителят може да използва стандартните вериги, както и да дефинира собствени такива.

Таблици и правила



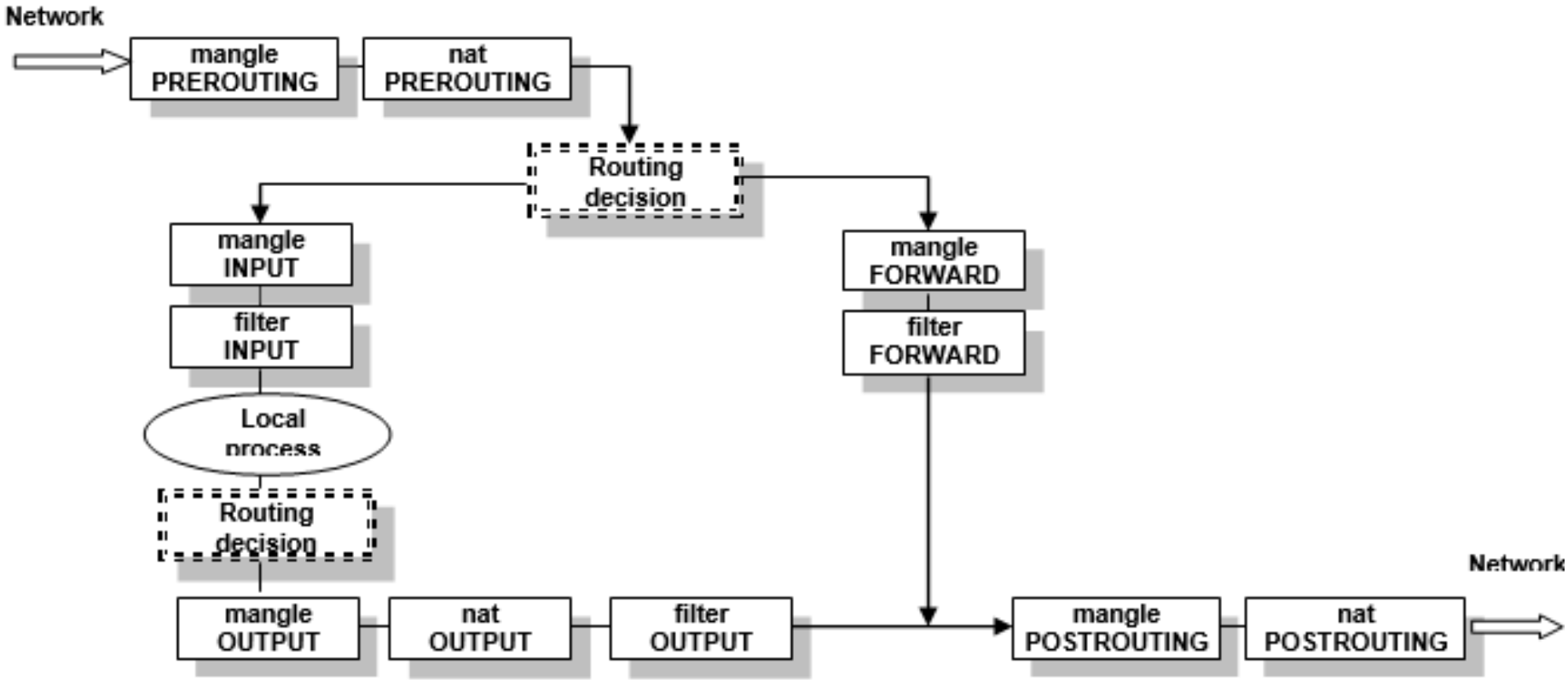
Стандартни таблици

- **mangle** – използва се за модифициране на пакетите. Основно това се отнася за промяна на полето Type of Service на пакета. За използването на таблицата е необходимо е първоначално зареждане на модула *iptable_mangle*;
- **nat** – тази таблица се използва основно за транслиране на адресите (Network Address Translation – NAT). За използването на таблицата е необходимо е първоначално зареждане на модула *iptable_nat*;
- **filter** – използва се основно за филтриране на пакетите. Принципно, всичките стандартни цели са приложими за тази таблица. За използването на таблицата е необходимо е първоначално зареждане на модула *iptable_filter*.

Стандартни вериги

- **INPUT** – входна верига за предназначените за локалната машина пакети;
- **OUTPUT** – изходна верига за пакетите, генерирани от локалната верига;
- **FORWARD** – верига за пакетите, предназначени за рутиране към други машини;
- **PREROUTING** – верига, по която преминават пакетите преди определяне на получателя им (локално или за друг хост);
- **POSTROUTING** – верига, по която преминават пакетите след определяне на техния получателя.

Преминаване на пакетите



Състояние на конекциите

- **NEW** – указва първия наблюдаван пакет за специфична конекция. За TCP конекции това е пакетът с вдигнат единствено флаг SYN. При UDP и ICMP обмен това са първите пакети, предадени между източника и получателя;
- **ESTABLISHED** – всеки трафик в двете посоки удовлетворява това състояние. При TCP конекции това са пакетите с установен флаг ACK. При UDP обмен всички пакети между източника и получателя след първия предаден се третират в това състояние. ICMP съобщенията за грешки също се разглеждат в това състояние, ако преди това е бил изпратен пакет, който предизвиква генерирането на съответното съобщение за грешка;
- **RELATED** – една конекция е в това състояние, ако тя се явява относителна спрямо друга вече създадена (ESTABLISHED). Типичен пример на относителни конекции са FTP данновите конекции, които се създават допълнително спрямо създадените вече FTP контролни конекции;
- **INVALID** – в това състояние попадат пакетите, които не могат да се идентифицират или не са в нито едно от описаните състояния.

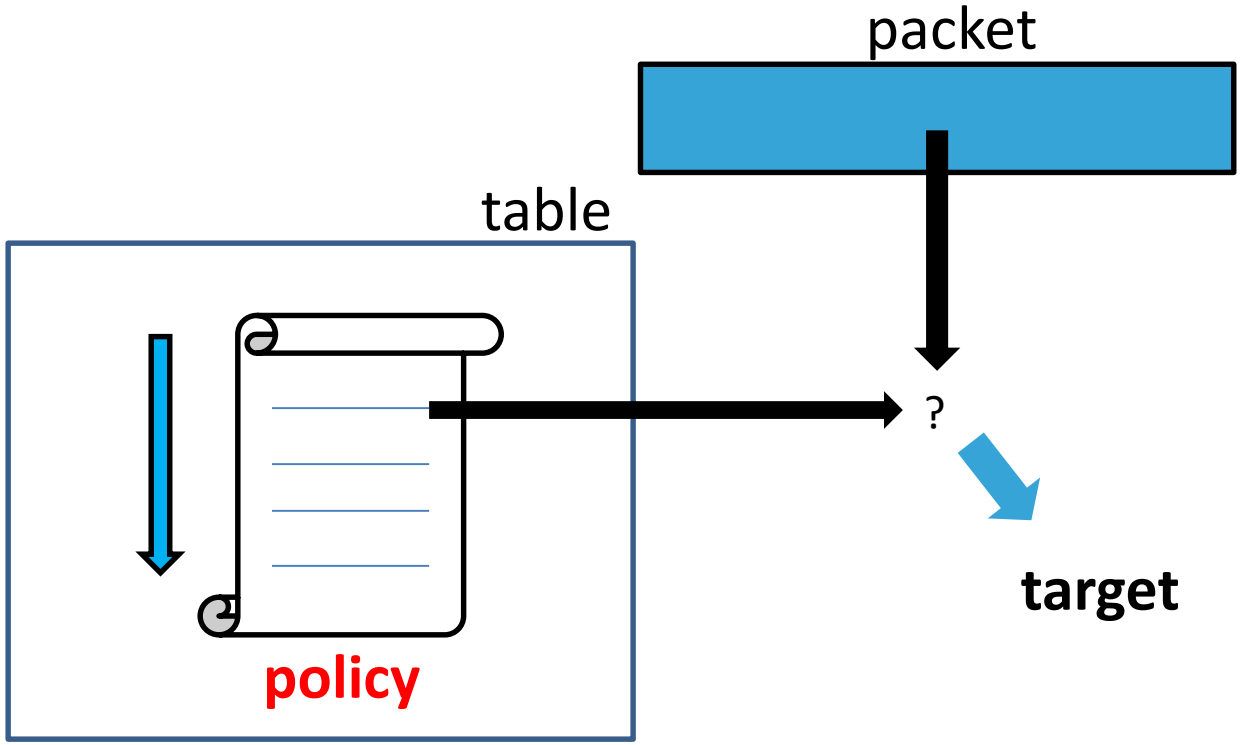
Създаване на правила

Правилата представляват указания на базата на които се блокират или разрешават различни конекции или пакети в специфична верига.

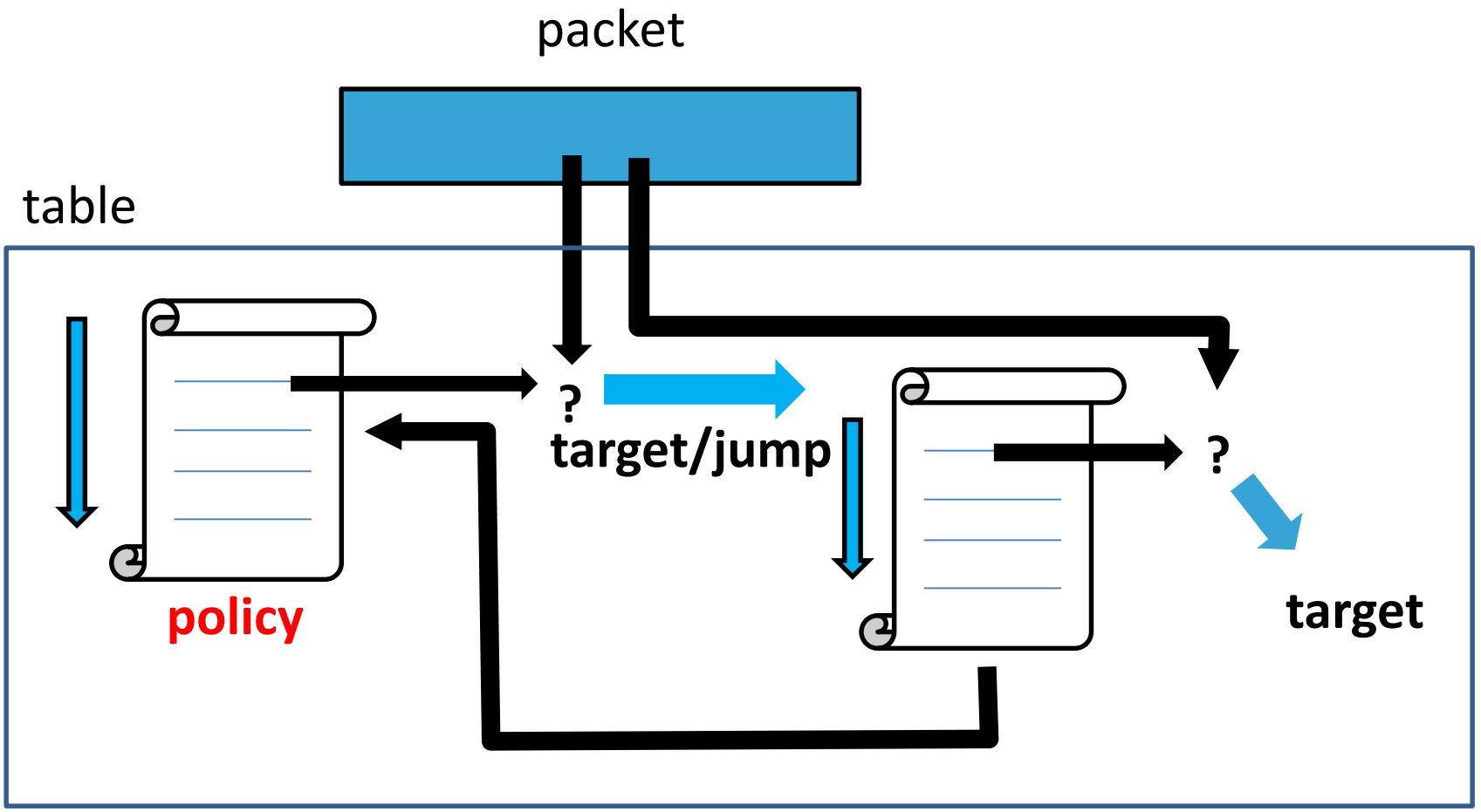
```
iptables [-t table] command [match] [target/jump]
```

- Критерии (match)
- Съответните действия (target) – отхвърляне / пропускане.
- Преход (jump) към друга верига при удовлетворяването на критериите
- Таблица (table) – по подразбиране е таблица filter
- Команда (command) – указва действието

Изпълнение на правила



Изпълнение на правила



Изпълнение на правила

- Правилата за дадена верига се изпълняват последователно от началото на списъка.
- При удовлетворяване на критериите за дадено правило се изпълняват съответните действия и се преустановява по-нататъшната обработка на списъка. Ако е указан преход към нова верига, то обработката продължава аналогично със списъка от правила в новата верига.
- В случай, че нито едно правило от новата верига не бъде удовлетворено, обработката продължава със следващото по ред правило от старата верига, следващо позицията от която е бил направен преди това преходът.
- Ако няма удовлетворяване на критериите на нито едно правило, то върху пакета се прилага политиката по подразбиране за дадената верига.

Команди

Добавяне на правило -A

```
iptables –A INPUT ...
```

Командата добавя ново правило в края на указаната верига.

Команди

Изчистване на верига -F

```
iptables –F INPUT
```

Изчиства всички правила от указаната верига.

Команди

Създаване на нова верига -N

```
iptables –N tcp_allowed
```

Създава се нова верига със зададеното име в съответната таблица.

Команди

Изтриване на нова верига -X

```
iptables -X tcp_allowed
```

Изтрива указаната верига от съответната таблица.
Необходимо е изтриваната верига да не съдържа правила.

Команди

Задаване политика по подразбиране -P

```
iptables -P INPUT DROP
```

Установява зададената цел (политика) към указаната верига. Всички пакети, които не удовлетворят нито едно правило ще попаднат под тази политика за веригата. Валидни цели са ACCEPT и DROP. При изчистването на правилата от дадена верига трябва да се има в предвид, че зададената преди това политика по подразбиране остава валидна. Това налага задължителна промяна на политиката при изчистване, особено ако тя е била зададена като DROP.

Общи критерии за удовлетворяване

Общите критерии са налични винаги, независимо от особеностите на целевия протокол или разширенията на критериите, които могат да бъдат допълнително зареждани към ядрото.

Критерии

Протокол -p

```
iptables –A INPUT –p tcp –j DROP

iptables –A OUTPUT –p ALL –j ACCEPT
```

Указва проверка за специфичен протокол като стандартно дефинираните TCP, UDP и ICMP или стойност, описана във файла /etc/protocols. Могат да се изброят няколко имена на протоколи, разделени със запетая. За указване на всичките тези три протокола се използва ключовата дума ALL.

Критерии

Източник на пакета -s

```
iptables –A INPUT –s 192.168.0.1

iptables –A INPUT –s 192.168.0.0/24
```

Указва съвпадение с пакети, имащи зададения IP адрес на източника. Може да се указва както конкретен IP адрес, така и адрес на мрежа с добавяне на мрежова маска.

Критерии

Получател на пакета -d

```
iptables –A INPUT –d 192.168.0.1

iptables –A INPUT –d 192.168.0.0/24
```

Указва съвпадение с пакети, имащи зададения IP адрес на получателя. Функционирането е аналогично както при указване на източник.

Критерии

Входен интерфейс -i

```
iptables –A INPUT –i eth0
```

Указва съвпадение с интерфейса, по който пакетът се е получил. Тази опция е валидна единствено за веригите INPUT, FORWARD и PREROUTING. Указване на произволна последователност от букви и цифри се задава със символа +.

Критерии

Изходен интерфейс -o

```
iptables –A FORWARD –o eth1
```

Аналогично за пакети, които напускат по указания интерфейс. Опцията е валидна единствено за веригите OUTPUT, FORWARD и POSTROUTING.

Неявни критерии за удовлетворяване

Неявните критерии се прилагат автоматично. Съществуват три типа неявни критерии, прилагащи се диференцирано по отношение на TCP, UDP и ICMP пакети.

Критерии

TCP порт на източника --sport

```
iptables –A FORWARD –p tcp --sport 80
```

Аналогично за пакети, които напускат по указания интерфейс. Указва съвпадение по зададен порт на източника. Без зададен порт се подразбират всички портове. Ако се използва име на услуга, то трябва да бъде дефинирано във файла */etc/services*. Могат да се задават диапазон от портове във вида <начален_порт>:<краен_порт>. Ако не се зададе начален_порт, се подразбира порт 0. Ако не се зададе краен_порт се подразбира порт 65535.

Критерии

TCP порт на получателя --dport

```
iptables –A FORWARD –p tcp --dport 22
```

Аналогично, по отношение на порт на получателя.

Критерии

TCP флагове --tcp-flags

```
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN SYN
```

Указва съвпадение с TCP флагове в пакета. Задава се списък от флагове за проверка (маска) и втори списък от флагове, които трябва да бъдат установени в 1. Двата списъка се разделят със запетаи. Съвпадението е по отношение на флаговете SYN, ACK, FIN, RST, URG и PSH, като всичките могат да се укажат с ALL, а нито един – с NONE ключовите думи.

Критерии

UDP порт на източника --sport

```
iptables -A FORWARD -p udp --sport 53
```

Функционира аналогично както при TCP протокола.

Критерии

UDP порт на получателя --dport

```
iptables -A FORWARD -p udp --dport 53
```

Функционира аналогично както при TCP протокола.

Критерии

ICMP тип --icmp-type

```
iptables –A FORWARD –p icmp --icmp-type 8
```

Указва съвпадение по ICMP тип съгласно RFC792. За получаване на пълния списък от типовете ICMP съобщения, може да се изпълни командата **iptables –p icmp --help**.

Явни критерии за удовлетворяване

Явните критерии трябва да се заредят изрично с опцията **–m, --match module**. Някои от тях са специфични за даден протокол, други са въведени с цел тестване и експерименти с iptables.

Критерии

Съвпадение по MAC адрес --mac-source

```
iptables -A INPUT -m mac --mac-source 2b:00:01:1a:2a:05
```

Използва се за установяване на пакети по Ethernet MAC адреса на източника. Опцията е валидна единствено за веригите PREROUTING, FORWARD и INPUT.

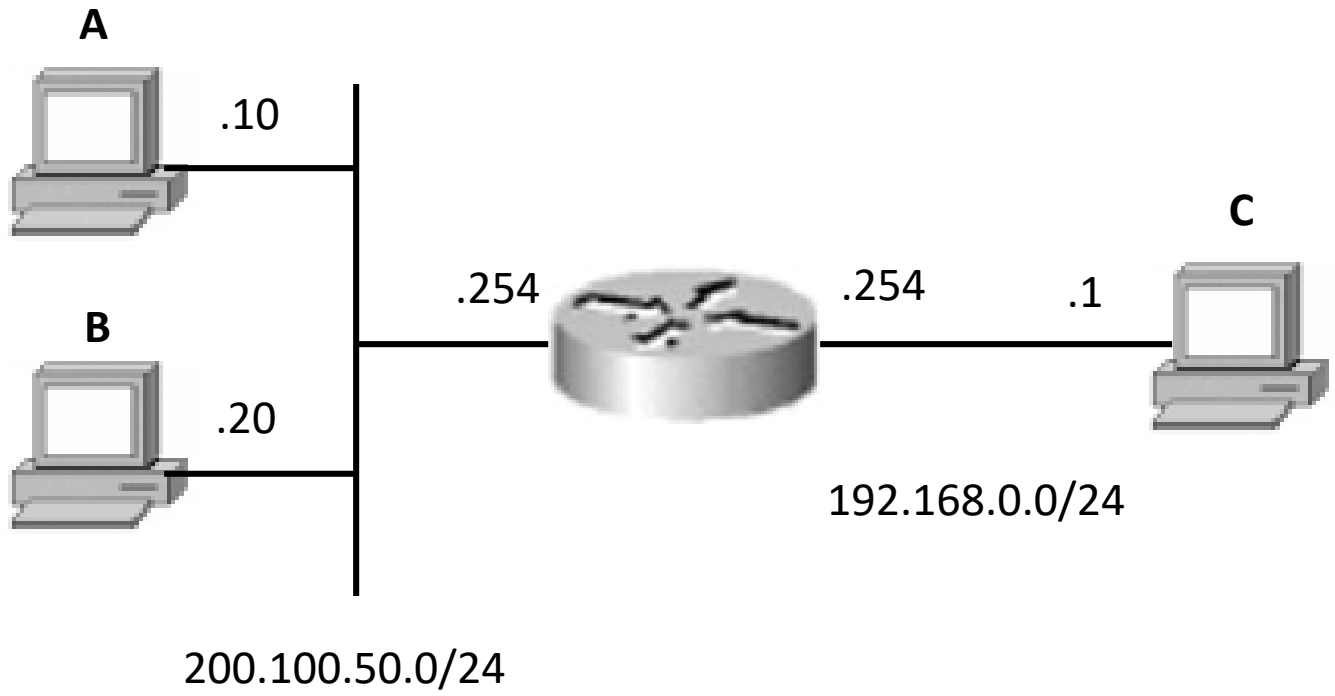
Критерии

Съвпадение по състояние на конекциите --state

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED
```

Позволява откриване на конекция в определено състояние. Тази възможност изисква изрично зареждане с опцията **–m state**. За използването на състояния е необходимо предварително зареждане на модула *ipt_state*.

Да се разреши достъп по HTTP до C само от A.



HTTP – порт 80

Всичко е разрешено, ограничен е само определен трафик между определени машини.

```
iptables -F FORWARD
iptables -P FORWARD ACCEPT

iptables -A FORWARD -p tcp -s 200.100.50.10 -d 192.168.0.1
                                --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s ALL -d 192.168.0.1 --dport 80
                                -j DROP
```

Въпроси ?