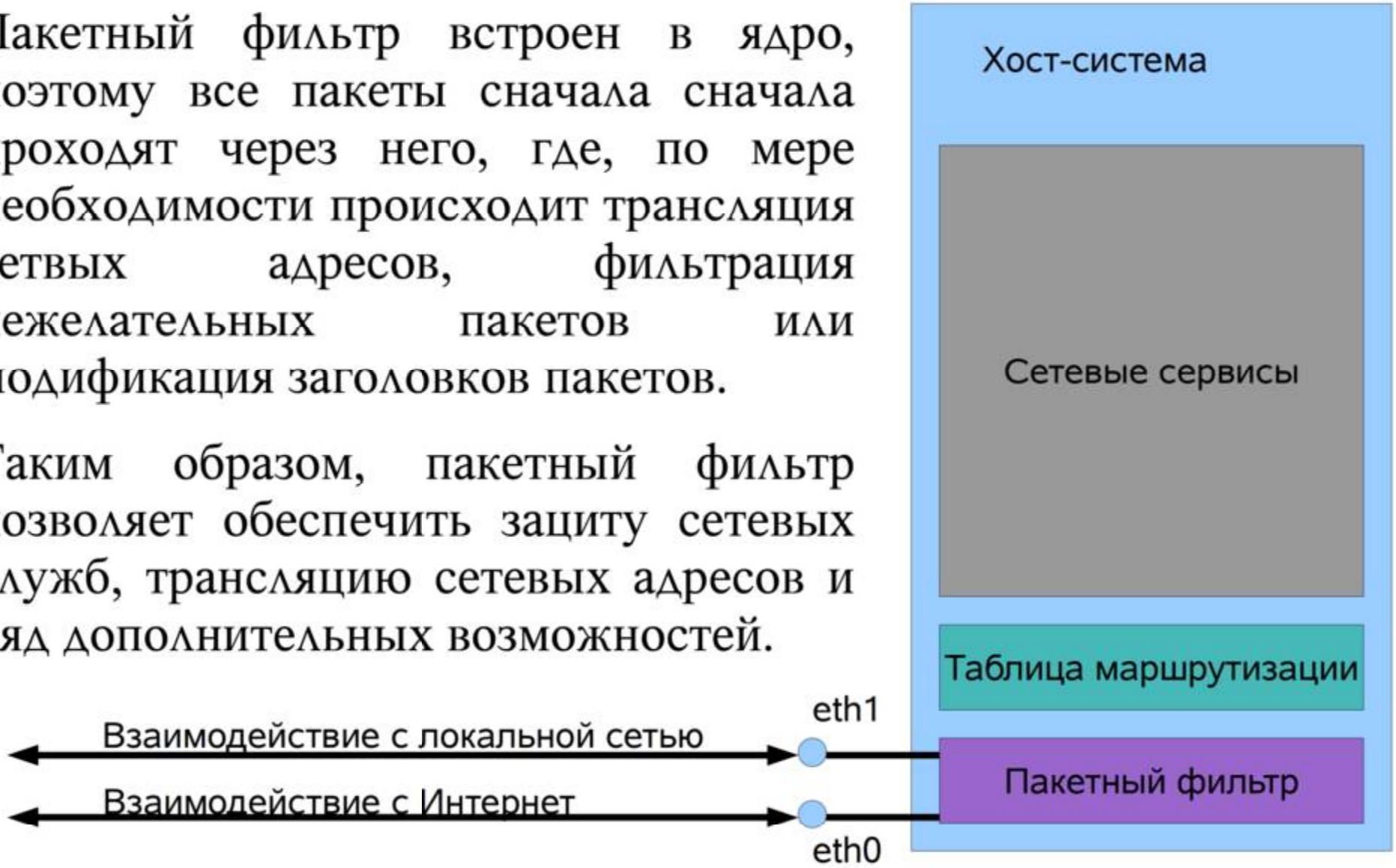
Пакетный фильтр

Пакетный фильтр встроен в ядро, поэтому все пакеты сначала сначала проходят через него, где, по мере необходимости происходит трансляция сетвых адресов, фильтрация нежелательных пакетов или модификация заголовков пакетов.

Таким образом, пакетный фильтр позволяет обеспечить зациту сетевых служб, трансляцию сетевых адресов и ряд дополнительных возможностей.



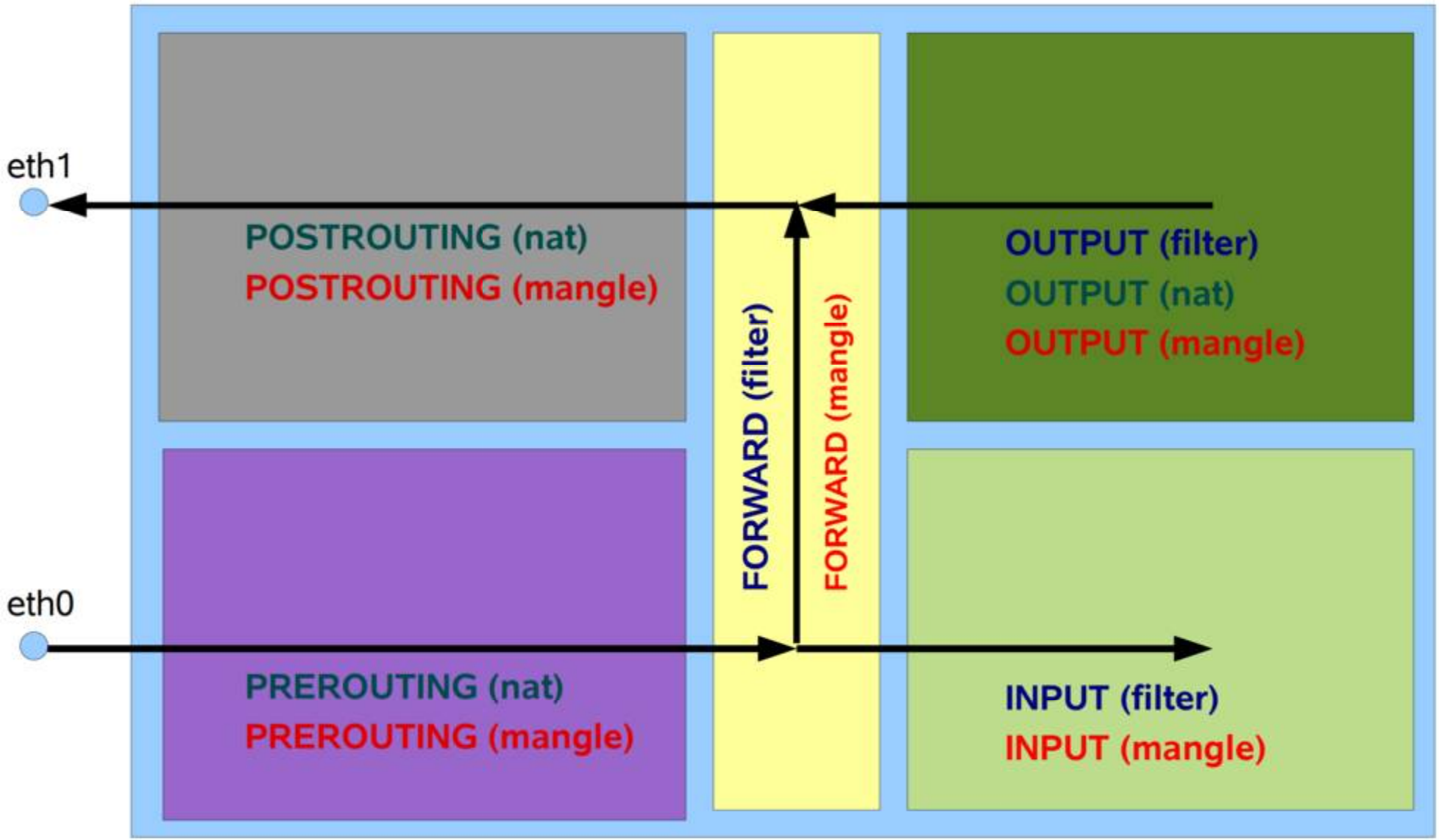
netfilter - пакетный фильтр Linux

Для управления пакетным фильтром используется программа iptables. Данная программа предназначена для определения правила фильтрации пакетов, выстраивая эти правила в цепочки, что позволяет задавать довольно сложную логику их обработки.

Кроме того, сами цепочки входят в состав следущих таблиц, каждая из которых предназначена для решения определенного класса задач:

- **filter** — фильтрация пакетов (таблица по умолчанию)
  - INPUT — цепочка для входящих пакетов
  - FORWARD — цепочка для транзитных пакетов
  - OUTPUT — цепочка для исходящих пакетов
- **nat** — Трансляция сетевых адресов
  - PREROUTING — цепочка DNAT-преобразований
  - POSTROUTING — цепочка SNAT-преобразований
  - OUTPUT — цепочка для исходящих пакетов
- **mangle** — модификация заголовков пакетов
  - PREROUTING — цепочка предварительных преобразований заловков пакетов
  - POSTROUTING — финальных преобразований заловков пакетов
  - INPUT — цепочка для входящих пакетов
  - FORWARD — цепочка для транзитных пакетов
  - OUTPUT — цепочка для исходящих пакетов

netfilter - пакетный фильтр Linux



iptables — управление пакетным фильтром

В общем виде правила записываются примерно так:

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

Если в правило не включается спецификатор [-t table], то по умолчанию предполагается использование таблицы filter, если же предполагается использование другой таблицы, то это требуется указать явно.

Далее, непосредственно за именем таблицы, должна стоять команда. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables, например: вставить правило, или добавить правило в конец цепочки, или удалить правило и т.п.

Раздел matches задает критерии проверки, по которым определяется подпадает ли пакет под действие этого правила или нет. Здесь мы можем указать самые разные критерии -- и IP-адрес источника пакета или сети, и сетевой интерфейс и т.д.

И наконец target указывает, какое действие должно быть выполнено при условии выполнения критериев в правиле. Здесь можно заставить ядро передать пакет в другую цепочку правил, "сбросить" пакет и забыть про него, выдать на источник сообщение об ошибке и т.п.

Таблица filter

Используется главным образом для фильтрации пакетов. Для примера, здесь мы можем выполнить **DROP**, **LOG**, **ACCEPT** или **REJECT** без каких либо сложностей, как в других таблицах. Имеется три встроенных цепочки:

- **FORWARD**, используемая для фильтрации пакетов, идущих транзитом через брандмауэр.
- **INPUT**, через эту цепочку проходят пакеты, которые предназначены локальным приложениям (брандмауэру).
- **OUTPUT** – используется для фильтрации исходящих пакетов, сгенерированных приложениями на самом брандмауэре.

Таблица nat

Используется главным образом для преобразования сетевых адресов (Network Address Translation). Через эту таблицу проходит только первый пакет из потока. Преобразования адресов автоматически применяется ко всем последующим пакетам. Это один из факторов, исходя из которых мы не должны осуществлять какую-либо фильтрацию в этой таблице. Она содержит следующие цепочки:

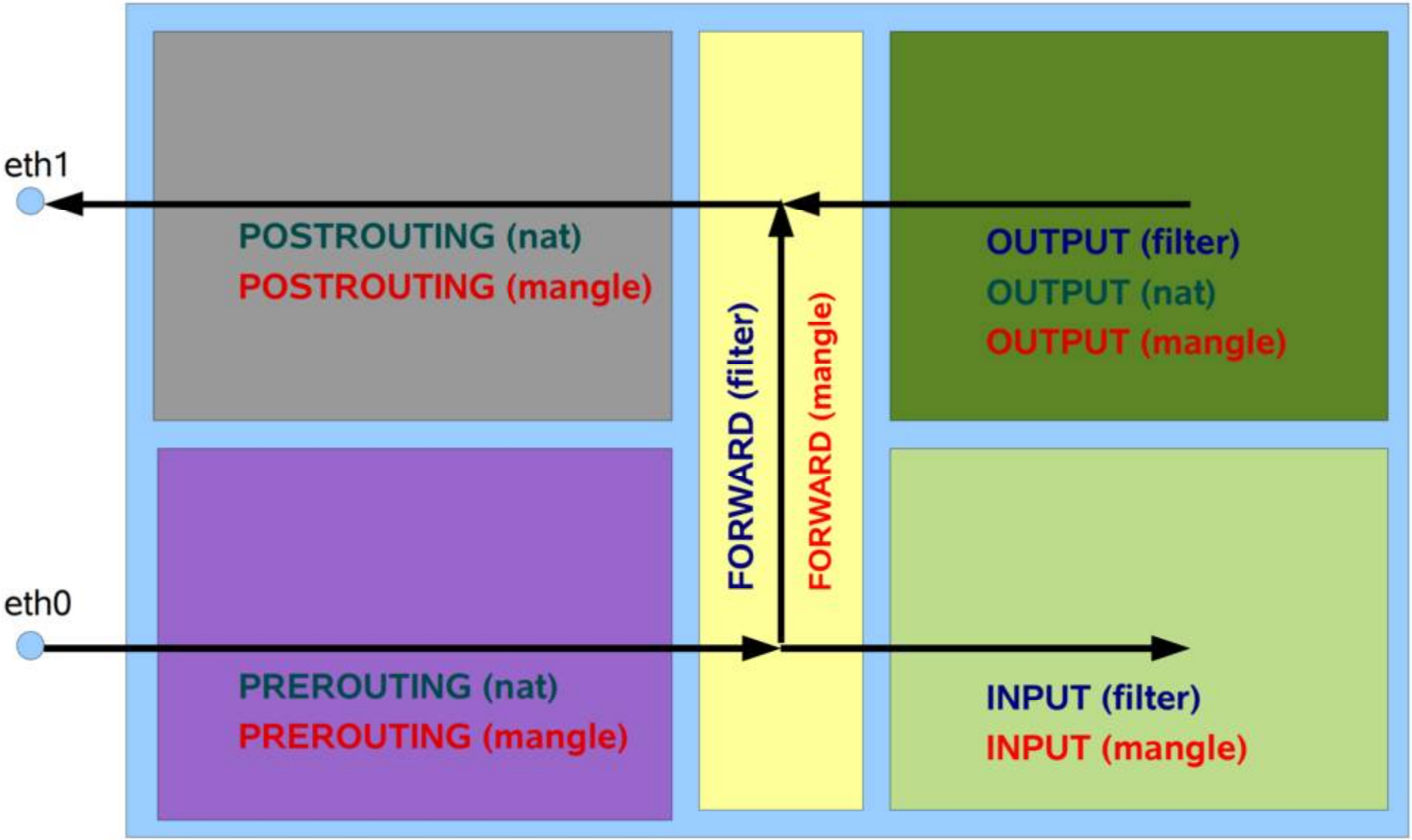
- **PREROUTING** – используется для внесения изменений в пакеты на входе в брандмауэр.
- **OUTPUT** – предназначена для преобразования пакетов, созданных приложениями внутри брандмауэра, перед принятием решения о маршрутизации.
- **POSTROUTING** – применяется для преобразования пакетов перед выдачей их во вне.

Таблица mangle

Эта таблица используется для внесения изменений в заголовки пакетов. Примером может служить изменение поля **TTL**, **TOS** или **MARK**. Важно: в действительности поле **MARK** не изменяется, но в памяти ядра заводится структура, которая сопровождает данный пакет все время его прохождения через машину, так что другие правила и приложения на данной машине (и только на данной машине) могут использовать это поле в своих целях. Заметьте, что таблица mangle ни в коем случае не должна использоваться для преобразования сетевых адресов или маскарадинга (Network Address Translation, Masquerading), поскольку для этих целей имеется таблица nat. Она содержит следующие цепочки:

- **PREROUTING** – используется для внесения изменений в пакеты на входе в брандмауэр.
- **POSTROUTING** – применяется для изменения заголовков пакетов перед выдачей их во вне.
- **INPUT**, через эту цепочку проходят пакеты, которые предназначены локальным приложениям (брандмауэру).
- **FORWARD**, используемая для модификации заголовков пакетов, идущих транзитом через брандмауэр.
- **OUTPUT** – для внесения изменений в заголовки пакетов, поступающих от приложений внутри брандмауэра.

Порядок прохождения пакетов



Команды iptables

-A – добавить правило в конец цепочки

-D – удалить правило из цепочки

-R – заменить одно правило другим

-I – вставить правило в указанное место в цепочке

-L – показать список правил

-F – очистить цепочку или таблицу

-Z – обнулить счетчики

-N – создать цепочку пользователя

-X – удалить цепочку пользователя

-P – установить политику по умолчанию

Команды iptables

-A – добавить правило в конец цепочки

При выполнении команды необходимо обязательно указать цепочку.

Пример:

iptables -A INPUT -s 10.10.103.100 -j ACCEPT

Команды iptables

-D – удалить правило из цепочки

Существуют два способа удаления правила: по его номеру или с указанием всех критериев отбора

Примеры:

iptables -D INPUT 1

iptables -D INPUT -p tcp --dport 80 -j DROP

Команды iptables

-R – заменить одно правило другим

Так как команда заменяет одно правило другим необходмо указать порядковый номер этого правила в цепочке.

Пример:

iptables -R INPUT 1 -s 192.168.0.1 -j ACCEPT

Команды iptables

-I – вставить правило в указанное место в цепочке

Команда вставляет правило под указанным номером и увеличивает на единицу номера всех последующих правил в этой цепочке

Пример:

iptables -I INPUT 1 -p tcp --sport 80 -j ACCEPT

Команды iptables

-L – показать список правил

Если не указывать имя цепочки, команда показывает все правила текущей таблицы. А если указать имя цепочки – показывет все правила текущей цепочки.

Пример:

iptables -L INPUT

Команды iptables

-F – очистить цепочку или таблицу

Если не указывать имя цепочки, команда удаляет все правила из текущей таблицы. А если указать имя цепочки – удаляет все правила из текущей цепочки.

Пример:

iptables -F INPUT

Команды iptables

-Z – обнулить счетчики

Каждому правилу в каждой из таблиц соответствуют два счетчика: количество пакетов и количество байт сработавших на данном правиле. Команда обнуляет счетчики в текущей таблице, или, если указано имя цепочки, в заданной цепочке.

Пример:

iptables -Z INPUT

Команды iptables

-N – создать цепочку пользователя

Команда создает цепочку с заданным именем в указанной таблице. Если таблица не указана, то подразумевается таблица filter. Имя создаваемой цепочки должно быть уникальным в пределах таблицы и не должно совпадать с зарезервированными именами цепочек и действий.

Примеры:

iptables -N tcp_filter

iptables -N udp_filter

iptables -N icmp_filter

Команды iptables

-X – удалить цепочку пользователя

Удаляет цепочку пользователя из указанной таблицы. Если таблица не указана, то подразумевается таблица filter. Удалять можно только цепочки не содержащие правил, кроме того в других цепочках не должно быть правил ссылающихся на данную цепочку.

Примеры:

iptables -X tcp_filter

iptables -X udp_filter

iptables -X icmp_filter

Команды iptables

-P – установить политику по умолчанию

Команда задает политику по умолчанию для указанной цепочки. Если таблица не указана, то подразумевается таблица filter. Политика определяет, что нужно сделать с пакетом, на котором не сработало ни одно правило данной цепочки. Разрешенные значения политики ACCEPT и DROP.

Примеры:

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

Команды iptables

-A – добавить правило в конец цепочки

-D – удалить правило из цепочки

-R – заменить одно правило другим

-I – вставить правило в указанное место в цепочке

-L – показать список правил

-F – очистить цепочку или таблицу

-Z – обнулить счетчики

-N – создать цепочку пользователя

-X – удалить цепочку пользователя

-P – установить политику по умолчанию

Опции iptables

-v – показывать дополнительную информацию

-x – выводить точные значения счетчиков (без округления)

-n – не преобразовывать IP-адреса в DNS-имена

--line-numbers – включает вывод номеров правил в цепочке

-c – устанавливает значения счетчиков

Критерии отбора пакетов

Общие – не зависят от типа протокола и не требуют загрузки специальных модулей ядра

Неявные – зависят от типа протокола и не требуют загрузки специальных модулей ядра

Явные – требуют загрузки специальных модулей ядра

Общие критерии

-p – определяет протокол

-s – определяет IP-адрес источника

-d – определяет IP-адрес назначения

-i – определяет входящий интерфейс

-o – определяет исходящий интерфейс

-f – определяет фрагменты, фрагментированного пакета

Примеры:

-p tcp

-s 10.10.103.0/24

-o eth0

! -f

Внимание! Символ «!» инвертирует значение параметра.

Неявные критерии

TCP критерии:

--sport – порт источника

--dport – порт назначения

--tcp-flags – определение TCP-флагов

--syn – запрос на соединение

UDP критерии:

--sport – порт источника

--dport – порт назначения

ICMP критерии:

--icmp-type – определяет тип ICMP пакета

Примеры:

-dport 1024:65535

--icmp-type echo-request

Явные критерии

limit – ограничивает количество срабатываний правила

mac – позволяет использовать MAC-адреса в качестве критерия отбора пакетов

multiport – позволяет указать список портов

state – определяет состояния пакетов

Явные критерии. Критерий limit.

--limit-burst – определяет количество пакетов, по умолчанию значение критерия равно 5.

--limit – задает единицу времени в формате N/t

где

N – кол-во срабатываний в единицу времени

t – единица времени (s,m,h или d)

Данные критерии используются совместно для того, чтобы ограничить прохождение пакетов в единицу времени

Пример:

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s \ --limit-burst 1 -j ACCEPT

Явные критерии. Критерий MAC.

--mac-source – Критерий определяет MAC-адрес сетевого узла, передавшего пакет. MAC-адрес должен указываться в формате XX:XX:XX:XX:XX:XX. Этот критерий имеет смысл только в цепочках PREROUTING, FORWARD и INPUT.

Символ «!» инвертирует значение параметра.

Пример:

iptables -A INPUT -m mac --mac-source 34:26:A6:1D:F7:04 -j ACCEPT

Явные критерии. Критерий multiport.

--source-port – Критерий используется для указания списка исходящих портов.

--destignation-port – Критерий используется для указания списка портов назначения.

Можно указать до 15 различных портов. Используется только с критериями -p tcp и -p udp.

Символ «!» инвертирует значение параметра.

Пример:

iptables -A INPUT -p tcp -m multiport --source-port 21,53 -j ACCEPT

Явные критерии. Критерий state.

--state – определяет состояние пакета.

Пакетный фильтр позволяет отслеживать не только TCP соединения, но и соединений по протоколам UDP и ICMP . Соединение может иметь одно из следующих состояний:

- **NEW** – пакет является первым для данного соединения
- **ESTABLISHED** – пакет принадлежит установленному соединению
- **RELATED** – пакет принадлежит к соединению связанному с уже установленным соединением
- **INVALID** – состояние пакета определить не удалось

Пример:

iptables -A INPUT -m state --state INVALID -j DROP

Действия и переходы

ACCEPT – принять пакет

DROP – сбросить пакет

REJECT – сбросить пакет с сообщением об ошибке

RETURN – возврат из цепочки

LOG – помещает информацию в системный журнал

Пример:

iptables -A INPUT -m state --state INVALID -j LOG \ --log-prefix «Strange:»

NAT преобразования

SNAT – замена IP-адреса или порта источника

MASQUERADE – является частным случаем SNAT-преобразования, который применяется в тех случаях когда IP-адрес получается динамически от DHCP-сервера.

DNAT – замена IP-адреса или порта назначения

REDIRECT – Выполняет перенаправление пакетов и потоков на другой порт той же самой машины.

SNAT

--to-source – определяет IP-адрес и порт на которые будут заменены соответствующие поля пакета.

Используется в тех случаях когда требуется организовать выход в интернет с компьютеров в локальной сети. Данное преобразование заменяет указанные в пакете IP-адрес и порт компьютера в локальной сети на IP-адрес и порт шлюза.

До SNAT		После SNAT	
IPs	Ports	IPs	Ports
192.168.1.2	6000	10.10.103.1	20001
192.168.1.3	6000	10.10.103.1	20002
192.168.1.4	6000	10.10.103.1	20003

Пример:

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 10.10.103.X

MASQUERADE

--to-ports – определяет порт или диапазон портов

Используется в тех случаях когда требуется организовать выход в интернет с компьютеров в локальной сети. Данное преобразование заменяет указанные в пакете IP-адрес и порт компьютера в локальной сети на IP-адрес и порт шлюза.

Пример:

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

DNAT

--to-destination – определяет IP-адрес и порт на которые будут заменены соответствующие поля пакета.

Используется в тех случаях когда требуется организовать доступ из интернета к компьютерам в DMZ. Данное преобразование заменяет указанные в пакете IP-адрес и порт компьютера в Интернет на IP-адрес и порт компьютера в локальной сети.

Пример:

iptables -t nat -A PREROUTING -i eth1 -j DNAT --to-destination 192.168.1.Y