# Пакет IP Tables

В большинстве систем UNIX широко применяют пакет IP Filter – в основном для целей фильтрации и NAT. В Linux эту роль выполняет пакет IP Tables (пришел на смену Ipfwadm и IP Chains).

Для нормальной работы IP Tables должны быть включены некоторые опции ядра.

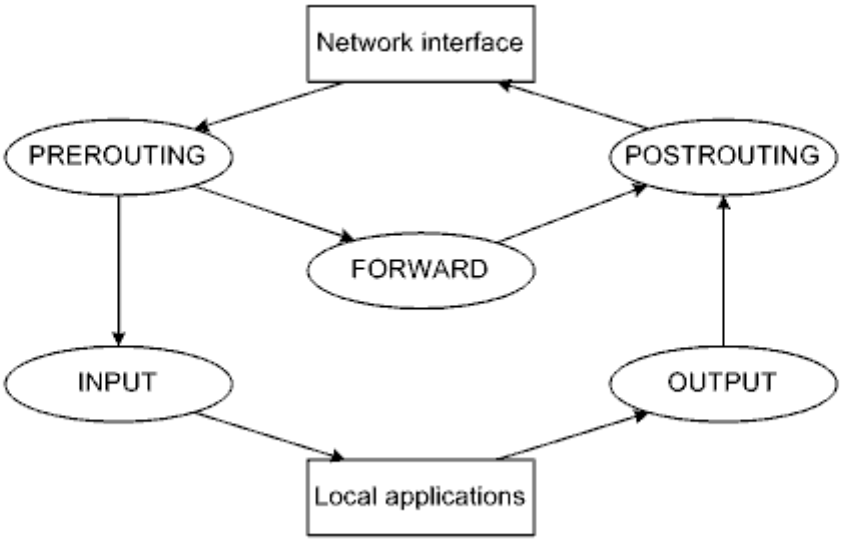
Для обеспечения возможности управления введен одноименный сервис iptables.

Фильтры строятся на основе правил (rules).

Каждое правило -- это строка, содержащая в себе условия, определяющие подпадает ли пакет под правило, и действие, которое необходимо осуществить в случае выполнения условий.

Правила могут объединяться в цепочки (chains) и образовывать сложную иерархию.

Следовательно, при работе с IP Tables необходимо внимательно проверять содержимое и последовательность правил.




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

Примеры таблиц (tables):
filter -- нужна для фильтрации пакетов;
mangle -- нужна для внесения изменений в заголовки пакетов (например, в поле TTL);
nat -- нужна для преобразования адресов.

Примеры команд (commands):
-A (--append) -- добавить новое правило в конец цепочки;

-D (--delete) -- удалить правило из цепочки;
-F (--flush) -- удалить все правила из цепочки;
-I (--insert) -- вставить новое правило в цепочку;
-L (--list) -- вывести на экран список правил в цепочке;
-N (--new-chain) -- создать новую цепочку с названием в таблице;
-P (--policy) -- определить политику по умолчанию для цепочки;
-R (--replace) -- заменить одно правило другим в цепочке;
-X (--delete-chain) -- удалить цепочку из таблицы.

Примеры критериев (matches):
-d (--destination) -- нужен для указания адреса назначения;
-f (--fragment) -- нужен для включения поддержки фрагментации;
-i (--in-interface) -- нужен для указания сетевого интерфейса, принимающего пакеты;
-o (--out-interface) -- нужен для указания сетевого интерфейса, передающего пакеты;
-p (--protocol) -- нужен для указания протокола;
-s (--source) -- нужен для указания адреса источника.

Примеры действий (targets) :
ACCEPT -- пакет прекращает движение по цепочке (и всем цепочкам, приведшим к текущей) и считается пропущенным, но он может быть отброшен следующими цепочками;
DNAT -- подмена адреса назначения;
DROP -- пакет отбрасывается (окончательно);
LOG -- протоколирование пакета или связанных с его прохождением событий;
MASQUERADE -- подмена адреса источника без явного указания заменяющего адреса;
REJECT -- равно DROP плюс посылка ответного ICMP-сообщения о недостижимости;
SNAT -- подмена адреса источника.
Переходы (jumps) позволяют передавать пакет другим цепочкам.