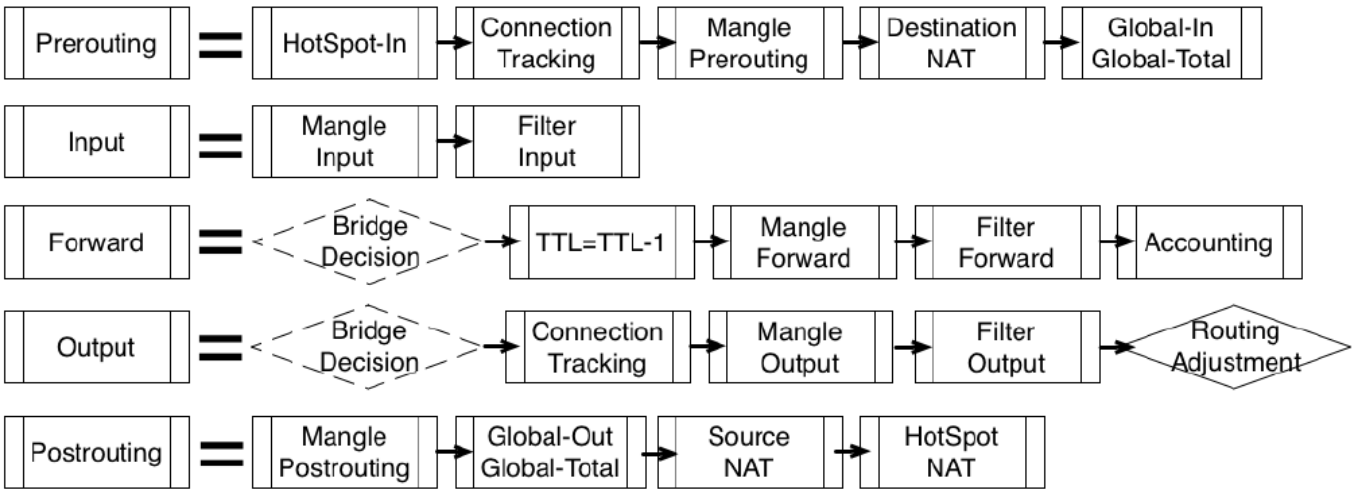
Mikrotik: базовая настройка firewall

RouterOS является разновидностью Linux, в качестве пакетного фильтра применяется netfilter со всеми вытекающими плюсами и минусами. Документация по netfilter: http://www.netfilter.org/documentation/ и http://www.opennet.ru/docs/RUS/iptables/

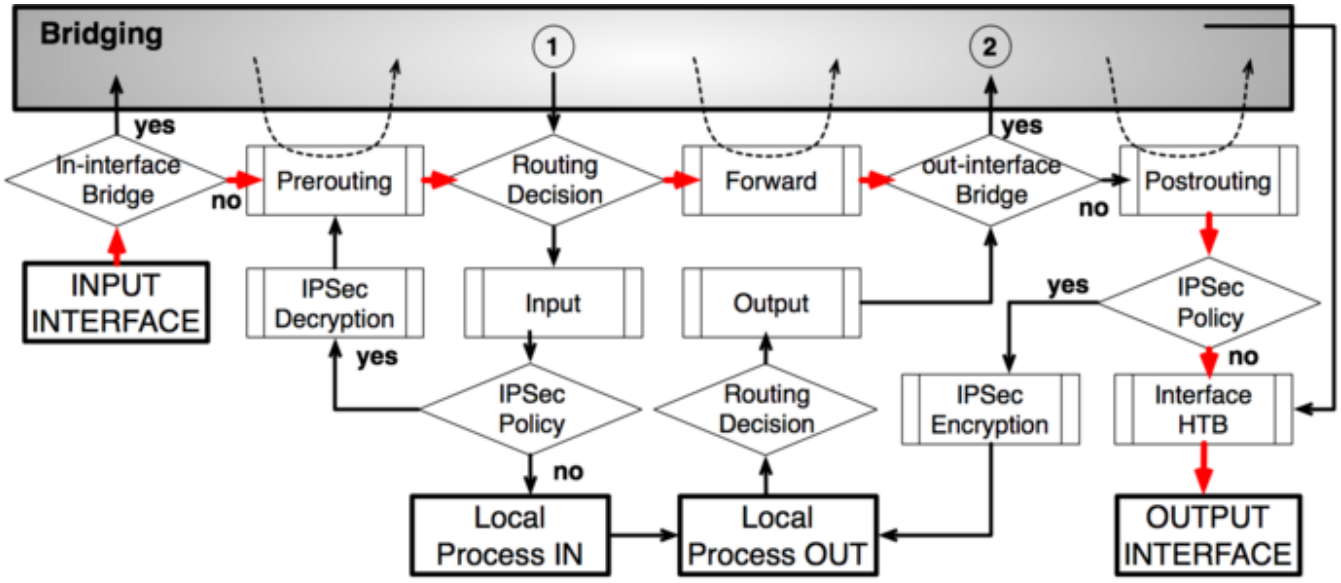
Существует 3 основных таблицы:

- filter
- nat
- mangle

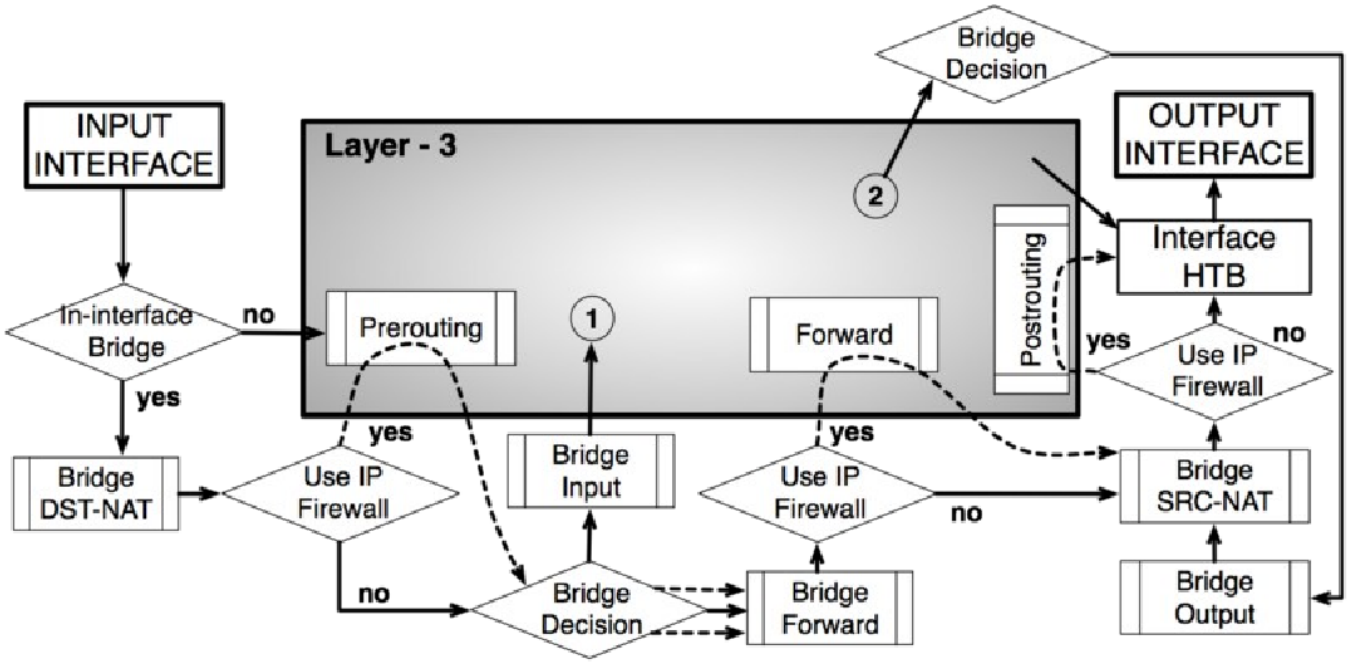
Общий порядок:



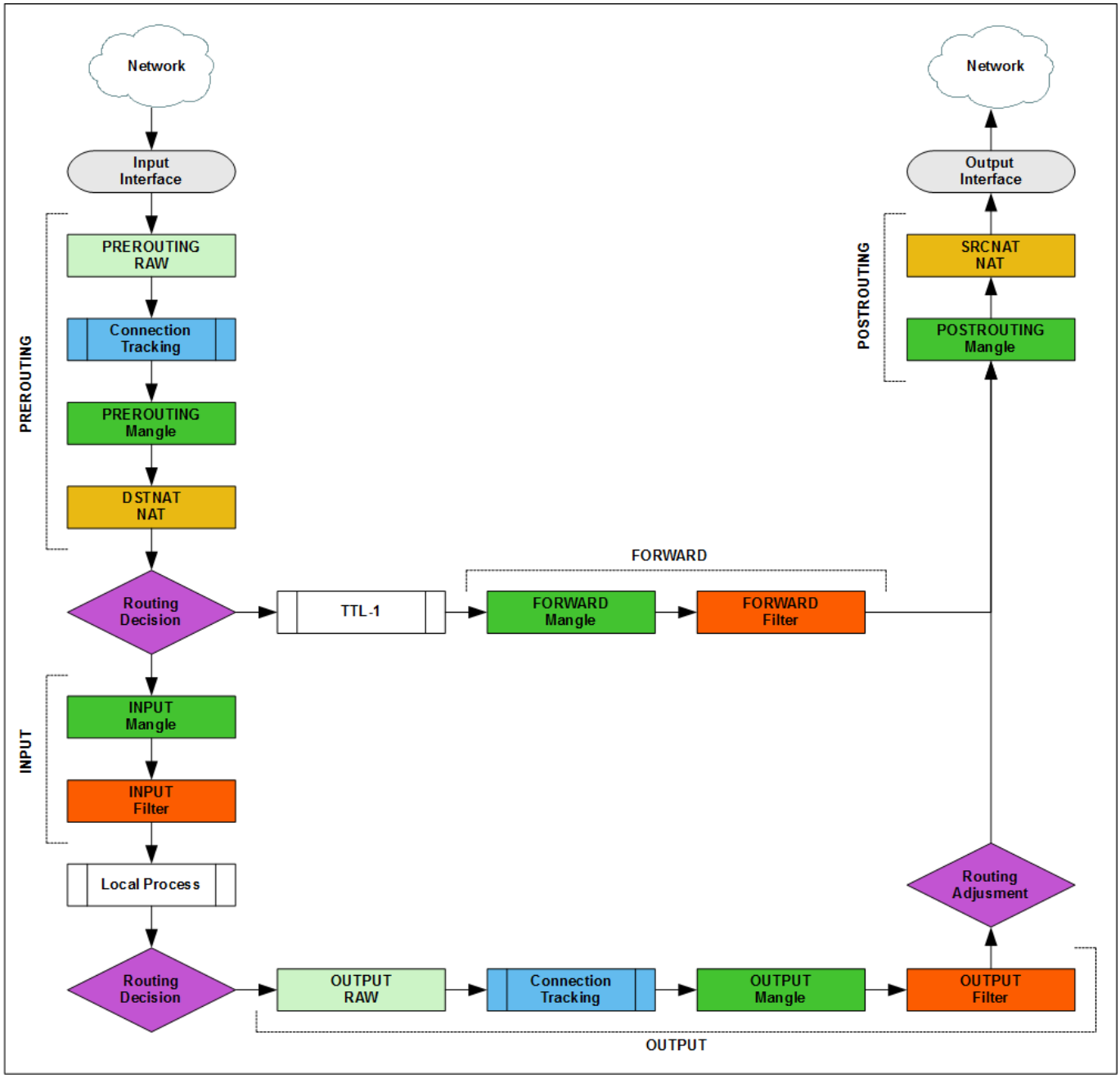
Роутинг трафика Layer 3 (IP):



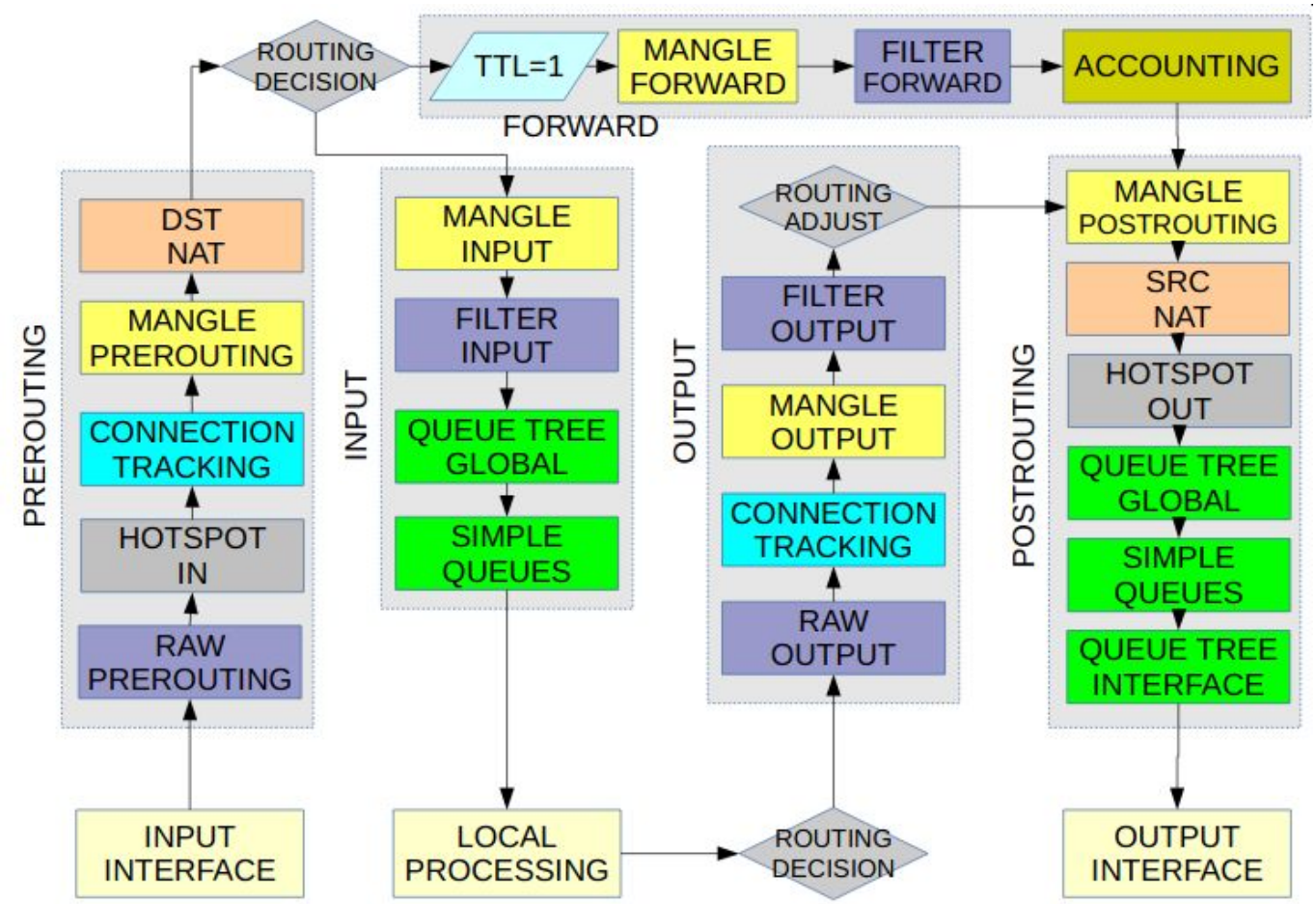
Бриджинга трафика Layer 2 (MAC):

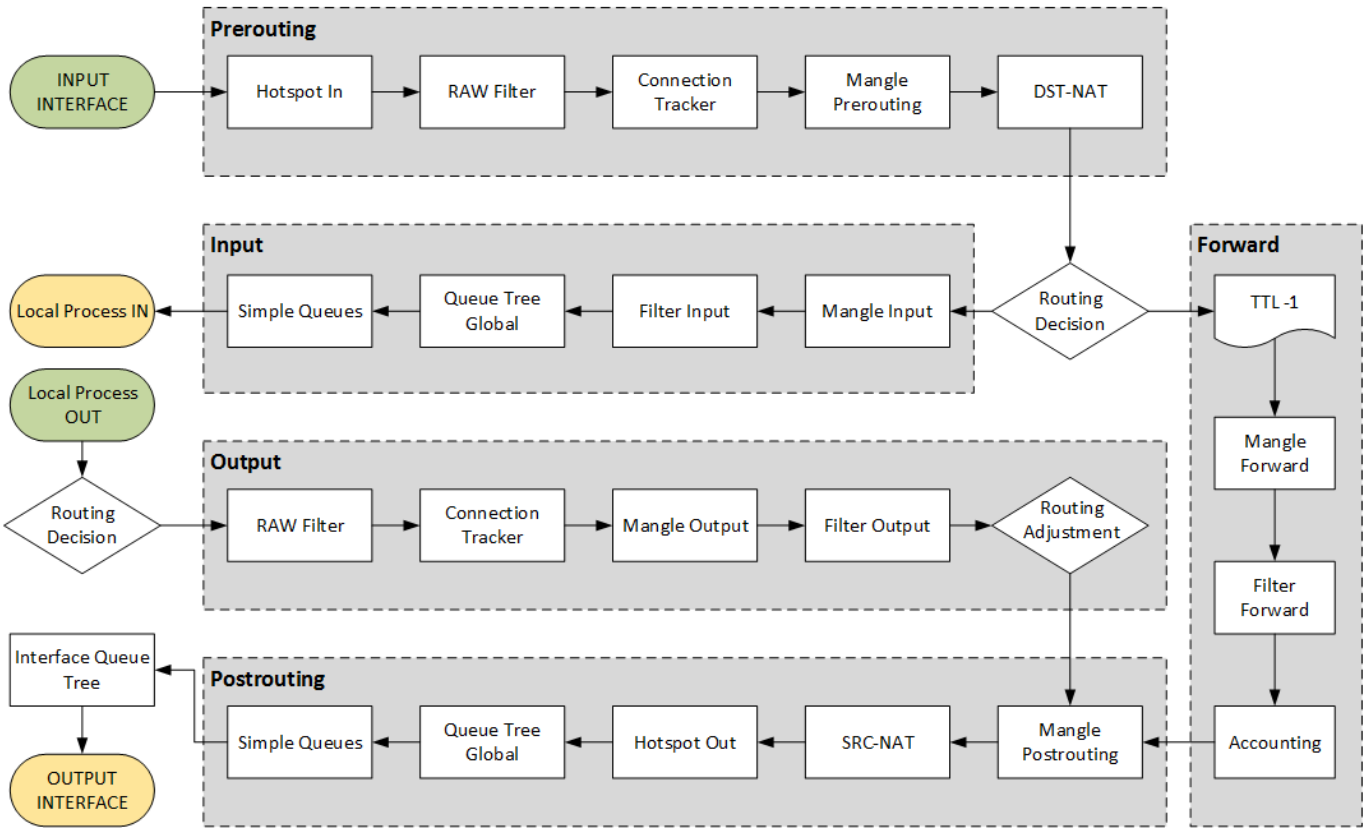


Packet Flow Diagram (упрощенная):



Более новые диаграммы:





Несколько принципов:

- Каждое правило принадлежит одной из этих таблиц и состоит из условий, находящихся в

четырех вкладках: General, Advanced, Extra и Action
- Правило может содержать множество условий, главное не делать их противоречивыми
- Если проходя по правилам пакет подходит под все условия, он обрабатывается соответствующим правилом (действие в закладке Action) и дальше не идет (на самом деле некоторые действия пропускают пакет дальше, просто запомните этот факт если планируете в будущем глубже разобраться с netfilter)
- Пакет проходит по списку правил сверху-вниз, поэтому порядок правил крайне важен
- Крайне желательно руководствоваться принципом «Запрещено все, кроме явно разрешенного»
- Чем больше правил - тем сильнее нагрузка на процессор, что может приводить к падению пропускной способности

При изменении правил вполне возможно заблокировать самому себе доступ к устройству! Во избежание таких выстрелов себе в ногу следует явно прописывать самым первым правилом разрешение себе на доступ к устройству и использовать кнопку Winbox'a обозначенную как «Safe Mode»

Самый минимальный набор правил

Таблица filter

Описание строк:

- 0,1 - отбрасывать все неверные пакеты
- 2,3,4,5 - пропускать все уже установленные соединения
- 6,7 - пропускать все icmp-пакеты (ping и т.д.). Небезопасно, но для дома сойдет
- 8 - разрешить DNS-запросы из локальной сети
- 9-14 - Защита SSH от атаки bruteforce, подробнее тут: Mikrotik: защищаем SSH от брутфорса
- 15 - Доступ к роутеру по SSH
- 16 - Доступ к роутеру по HTTPS
- 17 - Доступ к роутеру по Winbox
- 18 - разрешить сервер времени из локальной сети
- 19 - разрешить выход в интернет для локальной сети
- 20,21 - запретить все остальное

```
> /ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Drop all INVALID
      chain=input action=drop connection-state=invalid log=no log-prefix=""
 1    chain=forward action=drop connection-state=invalid log=no log-
prefix=""
 2    ;;; Allow all ESTABLISHED
      chain=input action=accept connection-state=established log=no log-
prefix=""
 3    chain=forward action=accept connection-state=established log=no log-
prefix=""
```

```
 4    ;;; Allow all RELATED
      chain=input action=accept connection-state=related log=no log-
prefix=""
 5    chain=forward action=accept connection-state=related log=no log-
prefix=""
 6    ;;; Allow ICMP from all
      chain=input action=accept protocol=icmp log=no log-prefix=""
 7    chain=forward action=accept protocol=icmp log=no log-prefix=""
 8    ;;; Allow DNS from LAN
      chain=input action=accept protocol=udp src-address=192.168.88.0/24 in-
interface=bridge-local dst-port=53 log=no log-prefix=""
 9    ;;; SSH anti-bruteforce
      chain=input action=drop protocol=tcp src-address-list=ssh_blacklist
dst-port=22 log=no log-prefix=""
10    chain=input action=add-src-to-address-list connection-state=new
protocol=tcp src-address-list=ssh_stage3 address-list=ssh_blacklist address-
list-timeout=30m dst-port=22 log=no log-prefix=""
11    chain=input action=add-src-to-address-list connection-state=new
protocol=tcp src-address-list=ssh_stage2 address-list=ssh_stage3 address-
list-timeout=1m dst-port=22 log=no log-prefix=""
12    chain=input action=add-src-to-address-list connection-state=new
protocol=tcp src-address-list=ssh_stage1 address-list=ssh_stage2 address-
list-timeout=1m dst-port=22 log=no log-prefix=""
13    chain=input action=add-src-to-address-list connection-state=new
protocol=tcp address-list=ssh_stage1 address-list-timeout=1m dst-port=22
log=no log-prefix=""
14    chain=input action=accept connection-state=new protocol=tcp dst-
port=22 log=no log-prefix=""
15    ;;; Allow SSH from all
      chain=input action=accept protocol=tcp dst-port=22 log=no log-
prefix=""
16    ;;; Allow HTTPS from all
      chain=input action=accept protocol=tcp dst-port=443 log=no log-
prefix=""
17    ;;; Allow WINBOX from Home
      chain=input action=accept protocol=tcp in-interface=bridge-local dst-
port=8291 log=no log-prefix=""
18    ;;; Allow NTP from LAN
      chain=input action=accept protocol=udp in-interface=bridge-local dst-
port=123 log=no log-prefix=""
19    ;;; Allow Internet from LAN
      chain=forward action=accept src-address=192.168.88.0/24 in-
interface=bridge-local log=no log-prefix=""
20    ;;; DROP ALL REQUEST
      chain=input action=drop log=no log-prefix=""
21    chain=forward action=drop log=no log-prefix=""
```

Таблица NAT

Разрешает выход компьютеров локальной сети в интернет через PPPoE-интерфейс с именем

MY_PROVIDER

```
 > /ip firewall nat  print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Masquerade for LAN to ISP
      chain=srcnat action=masquerade src-address=192.168.88.0/24 out-
interface=MY_PROVIDER log=no log-prefix=""
```

mikrotik, firewall, rules, basic settings